

**NISTIR XXXX Draft**

**Ongoing Face Recognition  
Vendor Test (FRVT)  
Part 1: Verification**

Patrick Grother  
Mei Ngan  
Kayee Hanaoka  
*Information Access Division  
Information Technology Laboratory*

This publication is available free of charge from:  
<https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing>

2019/11/19

## ACKNOWLEDGMENTS

The authors are grateful to staff in the NIST Biometrics Research Laboratory for infrastructure supporting rapid evaluation of algorithms.

## DISCLAIMER

Specific hardware and software products identified in this report were used in order to perform the evaluations described in this document. In no case does identification of any commercial product, trade name, or vendor, imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products and equipment identified are necessarily the best available for the purpose.



## FRVT STATUS

**This report** is a draft NIST Interagency Report, and is open for comment. It is the sixteenth edition of the report since the first was published in June 2017. Prior editions of this report are maintained on the FRVT website, and may contain useful information about older algorithms and datasets no longer used in FRVT.

**FRVT remains open:** All [four tracks](#) of the FRVT remain open to new algorithm submissions indefinitely. This report will be updated as new algorithms are evaluated, as new datasets are added, and as new analyses are included. Comments and suggestions should be directed to [frvt@nist.gov](mailto:frvt@nist.gov).

### Changes since October 16, 2019:

- ▷ The report adds results for ten new developers: Ai-Union Technology, ASUSTek Computer, DiDi ChuXing Technology, Innovative Technology, Luxand, MVision, Pyramid Cyber Security + Forensic, Scanovate, Shenzhen AiMall Tech, and TUPU Technology.
- ▷ The report adds results for 12 retiring developers: CTBC Bank Glory Gorilla Technology Guangzhou Pixel Solutions Imagus Technology Incode Technologies Lomonosov Moscow State University Rank One Computing Samtech InfoNet Shanghai Ulucu Electronics Technology Synesis, and Winsense.
- ▷ We have dropped results from this edition of the report per policy to only list results for two algorithms per developer: glory-000, gorilla-002, incode-003, rankone-006, and synesis-004.
- ▷ Results for five recently submitted algorithms will appear in the next report.

### Changes since September 11, 2019:

- ▷ The report adds results for five new participants: Awidit Systems (Awiros), Momemtum Digital (Sertis), Trueface AI, Shanghai Jiao Tong University, and X-Laboratory.
- ▷ The reports adds results for five new algorithms from returning developers: Cyberlink, Hengrui AI Technology, Idemia, Panasonic R+D Singapore, and Tevian. This causes three algorithm, to be de-listed from the report per policy to list results for two algorithms per developer.

### Changes since July 31 2019:

- ▷ The HTML table on the [FRVT 1:1 homepage](#) has been updated to include a column for cross-domain Visa-Border verification. Results for this new dataset appeared in the July 29 report under the name "CrossEV" - these are now renamed "Visa-Border".
- ▷ The [FRVT 1:1 homepage](#) lists algorithms according to lowest mean rank accuracy:
  - Rank(FNMR<sub>VISA</sub> at FMR = 0.000001) +
  - Rank(FNMR<sub>VISA-BORDER</sub> at FMR = 0.000001) +
  - Rank(FNMR<sub>MUGSHOT</sub> at FMR = 0.00001 after 14 years) +
  - Rank(FNMR<sub>WILD</sub> at FMR = 0.00001)
 This ordering rewards high accuracy across all datasets.
- ▷ The main results in Table 8 is now in landscape format to accomodate extra columns for the Visa-Border set, and mugshot comparisons after at least 12 years.
- ▷ The report adds results for nine new participants: Alpha SSTG, Intel Research, ULSee, Chungwa Telecon, iSAP Solution, Rokid, Shenzhen EI Networks, CSA Intellicloud, Shenzhen Intellifusion Technologies.
- ▷ The reports adds results for six new algorithms from returning developers: Innovatrics, Dahua Technology, Tech5 SA, Intellivision, Nodeflux and Imperial College, London. One algorithm, from Imperial has been retired, per policy to list results for two algorithms per developer.

- ▷ The cross-country false match rate heatmaps starting from Figure 326 have been replotted to reveal more structure by listing countries by region instead of alphabetically.
- ▷ The next version of this report will be posted around October 18, 2019.

#### Changes since July 3 2019:

- ▷ The HTML table on the [FRVT 1:1 homepage](#) has been updated to list the 20 most accurate developers rather than algorithms, choosing the most accurate algorithm from each developer based on visa and mugshot results. Also, the algorithms are ordered in terms of lowest mean rank across mugshot, visa and wild datasets, rewarding broad accuracy over a good result on one particular dataset.
- ▷ This report includes results for a new dataset - see the column labelled "crossEV" in Table 5. It compares a new set of high quality visa portraits with a set webcam photos that exhibit moderately poor pose variations and background illumination. The two new sets are described in sections 2.3 and 2.5. The comparisons are "cross-domain" in that the algorithm must compare "visa" and "wild" images. Results for other algorithms will be added in future reports as they become available.
- ▷ This report adds results for algorithms from 9 developers submitted in early July 2019. These are from 3DiVi, Camvi, EverAI-Paravision, Facesoft, Farbar (F8), Institute of Information Technologies, Shanghai U. Film Academy, Via Technologies, and Ulucu Electronics Tech. Six of these are new participants.
- ▷ Several other algorithms have been submitted and are being evaluated. Results will be released in the next report, scheduled for September 5. That report will include results for new datasets.
- ▷ Older algorithms from Everai, Camvi and 3DiVi, have been retired, per the policy to list only two algorithms per developer.

#### Changes since June 20 2019:

- ▷ This report adds results for algorithms from 18 developers submitted in early June 2019. These are from CTBC Bank, Deep Glint, Thales Cogent, Ever AI Paravision, Gorilla Technology, Imagus, Incode, Kneron, N-Tech Lab, Neurotechnology, Notiontag Technologies, Star Hybrid, Videonetics, Vigilant Solutions, Winsense, Anke Investments, CEIEC, and DSK. Nine of these are new participants.
- ▷ Several other algorithms have been submitted and are being evaluated. Results will be released in the next report, scheduled for August 1.
- ▷ Older algorithms from Everai, Thales Cogent, Gorilla Technology, Incode, Neurotechnology, N-Tech Lab and Vigilant Solutions have been retired, per the policy to list only two algorithms per developer.

#### Changes since April 2019:

- ▷ This report adds results for nine algorithms from nine developers submitted in early June 2019. These are from Tencent Deepsea, Hengrui, Kedacom, Moontime, Guangzhou Pixel, Rank One Computing, Synesis, Sensetime and Vocord.
- ▷ Another 23 algorithms have been submitted and are being evaluated. Results will be released in the next report, scheduled for July 3.
- ▷ Older algorithms for Rank One, Synesis, and Vocord have been retired, per the policy to list only two algorithms per developer.

#### Changes since February 2019:

- ▷ This report adds results for 49 algorithms from 42 developers submitted in early March 2019.
- ▷ This report omits results for algorithms that we retired. We retired for three reasons: 1. The developer submitted a new algorithm, and we only list two. 2. The algorithm needs a GPU, and we no longer allow GPU-based algorithms. 3. Inoperable algorithms.
- ▷ Previous results for retired algorithms are available in older editions of this report linked [here](#).

- ▷ The mugshot database used from February 2017 to January 2019 has been replaced with an extract of the mugshot database documented in NIST Interagency Report 8238, November 2018. The new mugshot set is described in section 2.4 and is adopted because:
  - ▷▷ It has much better identity label integrity, so that false non-match rates are substantially lower than those reported in FRVT 1:1 reports to date - see Figure 38.
  - ▷▷ It includes images collected over a 17 year period such that ageing can be much better characterized - - see Figure 138.
- ▷ Using the new mugshot database, Figure 138 shows accuracy for four demographic groups identified in the biographic metadata that accompanies the data: black females, black males, white females and white males.
- ▷ The report adds Figure 11 with results for the twenty human-difficult pairs used in the May 2018 paper *Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms* by Phillips et al. [1].
- ▷ The report uses an update to the wild image database that corrects some ground truth labels.
- ▷ Some results for the child exploitation database are not complete. They are typically updated less frequently than for other image sets.

# Contents

<b>ACKNOWLEDGMENTS</b>	<b>1</b>
<b>DISCLAIMER</b>	<b>1</b>
<b>1 METRICS</b>	<b>28</b>
1.1 CORE ACCURACY	28
<b>2 DATASETS</b>	<b>29</b>
2.1 CHILD EXPLOITATION IMAGES	29
2.2 VISA IMAGES	29
2.3 VISA IMAGES II	29
2.4 MUGSHOT IMAGES	30
2.5 WEBCAM IMAGES	30
2.6 WILD IMAGES	31
<b>3 RESULTS</b>	<b>31</b>
3.1 TEST GOALS	31
3.2 TEST DESIGN	31
3.3 FAILURE TO ENROLL	34
3.4 RECOGNITION ACCURACY	38
3.5 GENUINE DISTRIBUTION STABILITY	149
3.5.1 EFFECT OF BIRTH PLACE ON THE GENUINE DISTRIBUTION	149
3.5.2 EFFECT OF AGEING	164
3.5.3 EFFECT OF AGE ON GENUINE SUBJECTS	176
3.6 IMPOSTOR DISTRIBUTION STABILITY	192
3.6.1 EFFECT OF BIRTH PLACE ON THE IMPOSTOR DISTRIBUTION	192
3.6.2 EFFECT OF AGE ON IMPOSTORS	528

## List of Tables

1	ALGORITHM SUMMARY	18
2	ALGORITHM SUMMARY	19
3	ALGORITHM SUMMARY	20
4	ALGORITHM SUMMARY	21
5	FALSE NON-MATCH RATE	22
6	FALSE NON-MATCH RATE	23
7	FALSE NON-MATCH RATE	24
8	FALSE NON-MATCH RATE	25
9	FAILURE TO ENROL RATES	35
10	FAILURE TO ENROL RATES	36
11	FAILURE TO ENROL RATES	37

## List of Figures

1	PERFORMANCE SUMMARY: FNMR VS. TEMPLATE SIZE TRADEOFF	26
2	PERFORMANCE SUMMARY: FNMR VS. TEMPLATE TIME TRADEOFF	27
3	EXAMPLE IMAGES	31
(A)	VISA	31
(B)	MUGSHOT	31
(C)	WILD	31

4	PERFORMANCE ON 20 HUMAN-DIFFICULT PAIRS . . . . .	39
5	PERFORMANCE ON 20 HUMAN-DIFFICULT PAIRS . . . . .	40
6	PERFORMANCE ON 20 HUMAN-DIFFICULT PAIRS . . . . .	41
7	PERFORMANCE ON 20 HUMAN-DIFFICULT PAIRS . . . . .	42
8	PERFORMANCE ON 20 HUMAN-DIFFICULT PAIRS . . . . .	43
9	PERFORMANCE ON 20 HUMAN-DIFFICULT PAIRS . . . . .	44
10	PERFORMANCE ON 20 HUMAN-DIFFICULT PAIRS . . . . .	45
11	PERFORMANCE ON 20 HUMAN-DIFFICULT PAIRS . . . . .	46
12	ERROR TRADEOFF CHARACTERISTIC: VISA IMAGES . . . . .	47
13	ERROR TRADEOFF CHARACTERISTIC: VISA IMAGES . . . . .	48
14	ERROR TRADEOFF CHARACTERISTIC: VISA IMAGES . . . . .	49
15	ERROR TRADEOFF CHARACTERISTIC: VISA IMAGES . . . . .	50
16	ERROR TRADEOFF CHARACTERISTIC: VISA IMAGES . . . . .	51
17	ERROR TRADEOFF CHARACTERISTIC: VISA IMAGES . . . . .	52
18	ERROR TRADEOFF CHARACTERISTIC: VISA IMAGES . . . . .	53
19	ERROR TRADEOFF CHARACTERISTIC: VISA IMAGES . . . . .	54
20	ERROR TRADEOFF CHARACTERISTIC: VISA IMAGES . . . . .	55
21	ERROR TRADEOFF CHARACTERISTIC: VISA IMAGES . . . . .	56
22	ERROR TRADEOFF CHARACTERISTIC: VISA IMAGES . . . . .	57
23	ERROR TRADEOFF CHARACTERISTIC: VISA IMAGES . . . . .	58
24	ERROR TRADEOFF CHARACTERISTIC: VISA IMAGES . . . . .	59
25	ERROR TRADEOFF CHARACTERISTIC: VISA IMAGES . . . . .	60
26	ERROR TRADEOFF CHARACTERISTIC: VISA IMAGES . . . . .	61
27	ERROR TRADEOFF CHARACTERISTIC: VISA IMAGES . . . . .	62
28	ERROR TRADEOFF CHARACTERISTIC: VISA IMAGES . . . . .	63
29	ERROR TRADEOFF CHARACTERISTIC: VISA IMAGES . . . . .	64
30	ERROR TRADEOFF CHARACTERISTIC: MUGSHOT IMAGES . . . . .	65
31	ERROR TRADEOFF CHARACTERISTIC: MUGSHOT IMAGES . . . . .	66
32	ERROR TRADEOFF CHARACTERISTIC: MUGSHOT IMAGES . . . . .	67
33	ERROR TRADEOFF CHARACTERISTIC: MUGSHOT IMAGES . . . . .	68
34	ERROR TRADEOFF CHARACTERISTIC: MUGSHOT IMAGES . . . . .	69
35	ERROR TRADEOFF CHARACTERISTIC: MUGSHOT IMAGES . . . . .	70
36	ERROR TRADEOFF CHARACTERISTIC: MUGSHOT IMAGES . . . . .	71
37	ERROR TRADEOFF CHARACTERISTIC: MUGSHOT IMAGES . . . . .	72
38	ERROR TRADEOFF CHARACTERISTIC: MUGSHOT IMAGES . . . . .	73
39	ERROR TRADEOFF CHARACTERISTIC: WILD IMAGES . . . . .	74
40	ERROR TRADEOFF CHARACTERISTIC: WILD IMAGES . . . . .	75
41	ERROR TRADEOFF CHARACTERISTIC: WILD IMAGES . . . . .	76
42	ERROR TRADEOFF CHARACTERISTIC: WILD IMAGES . . . . .	77
43	ERROR TRADEOFF CHARACTERISTIC: WILD IMAGES . . . . .	78
44	ERROR TRADEOFF CHARACTERISTIC: WILD IMAGES . . . . .	79
45	ERROR TRADEOFF CHARACTERISTIC: WILD IMAGES . . . . .	80
46	ERROR TRADEOFF CHARACTERISTICS: CHILD EXPLOITATION IMAGES . . . . .	81
47	ERROR TRADEOFF CHARACTERISTICS: CHILD EXPLOITATION IMAGES . . . . .	82
48	ERROR TRADEOFF CHARACTERISTICS: CHILD EXPLOITATION IMAGES . . . . .	83
49	ERROR TRADEOFF CHARACTERISTICS: CHILD EXPLOITATION IMAGES . . . . .	84
50	CMC CHARACTERISTICS: CHILD EXPLOITATION IMAGES . . . . .	85
51	CMC CHARACTERISTICS: CHILD EXPLOITATION IMAGES . . . . .	86
52	CMC CHARACTERISTICS: CHILD EXPLOITATION IMAGES . . . . .	87
53	CMC CHARACTERISTICS: CHILD EXPLOITATION IMAGES . . . . .	88
54	FALSE MATCH RATES WITHIN AND ACROSS DEMOGRAPHIC GROUPS . . . . .	89
55	FALSE MATCH RATES WITHIN AND ACROSS DEMOGRAPHIC GROUPS . . . . .	90
56	FALSE MATCH RATES WITHIN AND ACROSS DEMOGRAPHIC GROUPS . . . . .	91
57	FALSE MATCH RATES WITHIN AND ACROSS DEMOGRAPHIC GROUPS . . . . .	92
58	FALSE MATCH RATES WITHIN AND ACROSS DEMOGRAPHIC GROUPS . . . . .	93
59	FALSE MATCH RATES WITHIN AND ACROSS DEMOGRAPHIC GROUPS . . . . .	94
60	FALSE MATCH RATES WITHIN AND ACROSS DEMOGRAPHIC GROUPS . . . . .	95

61	FALSE MATCH RATES WITHIN AND ACROSS DEMOGRAPHIC GROUPS	96
62	FALSE MATCH RATES WITHIN AND ACROSS DEMOGRAPHIC GROUPS	97
63	SEX AND RACE EFFECTS: MUGSHOT IMAGES	98
64	SEX AND RACE EFFECTS: MUGSHOT IMAGES	99
65	SEX AND RACE EFFECTS: MUGSHOT IMAGES	100
66	SEX AND RACE EFFECTS: MUGSHOT IMAGES	101
67	SEX AND RACE EFFECTS: MUGSHOT IMAGES	102
68	SEX AND RACE EFFECTS: MUGSHOT IMAGES	103
69	SEX AND RACE EFFECTS: MUGSHOT IMAGES	104
70	SEX AND RACE EFFECTS: MUGSHOT IMAGES	105
71	SEX AND RACE EFFECTS: MUGSHOT IMAGES	106
72	SEX EFFECTS: VISA IMAGES	107
73	SEX EFFECTS: VISA IMAGES	108
74	SEX EFFECTS: VISA IMAGES	109
75	SEX EFFECTS: VISA IMAGES	110
76	SEX EFFECTS: VISA IMAGES	111
77	SEX EFFECTS: VISA IMAGES	112
78	SEX EFFECTS: VISA IMAGES	113
79	SEX EFFECTS: VISA IMAGES	114
80	SEX EFFECTS: VISA IMAGES	115
81	SEX EFFECTS: VISA IMAGES	116
82	SEX EFFECTS: VISA IMAGES	117
83	SEX EFFECTS: VISA IMAGES	118
84	SEX EFFECTS: VISA IMAGES	119
85	SEX EFFECTS: VISA IMAGES	120
86	FALSE MATCH RATE CALIBRATION: MUGSHOT IMAGES	121
87	FALSE MATCH RATE CALIBRATION: MUGSHOT IMAGES	122
88	FALSE MATCH RATE CALIBRATION: MUGSHOT IMAGES	123
89	FALSE MATCH RATE CALIBRATION: MUGSHOT IMAGES	124
90	FALSE MATCH RATE CALIBRATION: MUGSHOT IMAGES	125
91	FALSE MATCH RATE CALIBRATION: MUGSHOT IMAGES	126
92	FALSE MATCH RATE CALIBRATION: MUGSHOT IMAGES	127
93	FALSE MATCH RATE CALIBRATION: MUGSHOT IMAGES	128
94	FALSE MATCH RATE CALIBRATION: MUGSHOT IMAGES	129
95	FALSE MATCH RATE CALIBRATION: VISA IMAGES	130
96	FALSE MATCH RATE CALIBRATION: VISA IMAGES	131
97	FALSE MATCH RATE CALIBRATION: VISA IMAGES	132
98	FALSE MATCH RATE CALIBRATION: VISA IMAGES	133
99	FALSE MATCH RATE CALIBRATION: VISA IMAGES	134
100	FALSE MATCH RATE CALIBRATION: VISA IMAGES	135
101	FALSE MATCH RATE CALIBRATION: VISA IMAGES	136
102	FALSE MATCH RATE CALIBRATION: VISA IMAGES	137
103	FALSE MATCH RATE CALIBRATION: VISA IMAGES	138
104	FALSE MATCH RATE CALIBRATION: VISA IMAGES	139
105	FALSE MATCH RATE CALIBRATION: VISA IMAGES	140
106	FALSE MATCH RATE CALIBRATION: VISA IMAGES	141
107	FALSE MATCH RATE CALIBRATION: VISA IMAGES	142
108	FALSE MATCH RATE CALIBRATION: VISA IMAGES	143
109	FALSE MATCH RATE CALIBRATION: VISA IMAGES	144
110	FALSE MATCH RATE CALIBRATION: VISA IMAGES	145
111	FALSE MATCH RATE CALIBRATION: VISA IMAGES	146
112	FALSE MATCH RATE CALIBRATION: VISA IMAGES	147
113	FALSE MATCH RATE CONCENTRATION: VISA IMAGES	148
114	EFFECT OF COUNTRY OF BIRTH ON FNMR	150
115	EFFECT OF COUNTRY OF BIRTH ON FNMR	151
116	EFFECT OF COUNTRY OF BIRTH ON FNMR	152

117	EFFECT OF COUNTRY OF BIRTH ON FNMR	153
118	EFFECT OF COUNTRY OF BIRTH ON FNMR	154
119	EFFECT OF COUNTRY OF BIRTH ON FNMR	155
120	EFFECT OF COUNTRY OF BIRTH ON FNMR	156
121	EFFECT OF COUNTRY OF BIRTH ON FNMR	157
122	EFFECT OF COUNTRY OF BIRTH ON FNMR	158
123	EFFECT OF COUNTRY OF BIRTH ON FNMR	159
124	EFFECT OF COUNTRY OF BIRTH ON FNMR	160
125	EFFECT OF COUNTRY OF BIRTH ON FNMR	161
126	EFFECT OF COUNTRY OF BIRTH ON FNMR	162
127	EFFECT OF COUNTRY OF BIRTH ON FNMR	163
128	ERROR TRADEOFF CHARACTERISTIC: MUGSHOT IMAGES	165
129	ERROR TRADEOFF CHARACTERISTIC: MUGSHOT IMAGES	166
130	ERROR TRADEOFF CHARACTERISTIC: MUGSHOT IMAGES	167
131	ERROR TRADEOFF CHARACTERISTIC: MUGSHOT IMAGES	168
132	ERROR TRADEOFF CHARACTERISTIC: MUGSHOT IMAGES	169
133	ERROR TRADEOFF CHARACTERISTIC: MUGSHOT IMAGES	170
134	ERROR TRADEOFF CHARACTERISTIC: MUGSHOT IMAGES	171
135	ERROR TRADEOFF CHARACTERISTIC: MUGSHOT IMAGES	172
136	ERROR TRADEOFF CHARACTERISTIC: MUGSHOT IMAGES	173
137	ERROR TRADEOFF CHARACTERISTIC: MUGSHOT IMAGES	174
138	ERROR TRADEOFF CHARACTERISTIC: MUGSHOT IMAGES	175
139	EFFECT OF SUBJECT AGE ON FNMR	177
140	EFFECT OF SUBJECT AGE ON FNMR	178
141	EFFECT OF SUBJECT AGE ON FNMR	179
142	EFFECT OF SUBJECT AGE ON FNMR	180
143	EFFECT OF SUBJECT AGE ON FNMR	181
144	EFFECT OF SUBJECT AGE ON FNMR	182
145	EFFECT OF SUBJECT AGE ON FNMR	183
146	EFFECT OF SUBJECT AGE ON FNMR	184
147	EFFECT OF SUBJECT AGE ON FNMR	185
148	EFFECT OF SUBJECT AGE ON FNMR	186
149	EFFECT OF SUBJECT AGE ON FNMR	187
150	EFFECT OF SUBJECT AGE ON FNMR	188
151	EFFECT OF SUBJECT AGE ON FNMR	189
152	EFFECT OF SUBJECT AGE ON FNMR	190
153	WORST CASE REGIONAL EFFECT FNMR	193
154	IMPOSTOR DISTRIBUTION SHIFTS FOR SELECT COUNTRY PAIRS	195
155	ALGORITHM 3DIVI-003 CROSS REGION FMR	196
156	ALGORITHM 3DIVI-004 CROSS REGION FMR	197
157	ALGORITHM ADERA-001 CROSS REGION FMR	198
158	ALGORITHM AIMALL-001 CROSS REGION FMR	199
159	ALGORITHM AIUNIONFACE-000 CROSS REGION FMR	200
160	ALGORITHM ALCHERA-000 CROSS REGION FMR	201
161	ALGORITHM ALCHERA-001 CROSS REGION FMR	202
162	ALGORITHM ALLGOVISION-000 CROSS REGION FMR	203
163	ALGORITHM ALPHAFACE-001 CROSS REGION FMR	204
164	ALGORITHM AMPLIFIEDGROUP-001 CROSS REGION FMR	205
165	ALGORITHM ANKE-003 CROSS REGION FMR	206
166	ALGORITHM ANKE-004 CROSS REGION FMR	207
167	ALGORITHM ANYVISION-002 CROSS REGION FMR	208
168	ALGORITHM ANYVISION-004 CROSS REGION FMR	209
169	ALGORITHM ASUSAICS-000 CROSS REGION FMR	210
170	ALGORITHM AWARE-003 CROSS REGION FMR	211
171	ALGORITHM AWARE-004 CROSS REGION FMR	212

172	ALGORITHM AWIROS-001 CROSS REGION FMR	213
173	ALGORITHM AYONIX-000 CROSS REGION FMR	214
174	ALGORITHM BM-001 CROSS REGION FMR	215
175	ALGORITHM CAMVI-002 CROSS REGION FMR	216
176	ALGORITHM CAMVI-004 CROSS REGION FMR	217
177	ALGORITHM CEIEC-001 CROSS REGION FMR	218
178	ALGORITHM CEIEC-002 CROSS REGION FMR	219
179	ALGORITHM CHTFACE-001 CROSS REGION FMR	220
180	ALGORITHM COGENT-003 CROSS REGION FMR	221
181	ALGORITHM COGENT-004 CROSS REGION FMR	222
182	ALGORITHM COGNITEC-000 CROSS REGION FMR	223
183	ALGORITHM COGNITEC-001 CROSS REGION FMR	224
184	ALGORITHM CTBCBANK-000 CROSS REGION FMR	225
185	ALGORITHM CTBCBANK-001 CROSS REGION FMR	226
186	ALGORITHM CYBEREXTRUDER-001 CROSS REGION FMR	227
187	ALGORITHM CYBEREXTRUDER-002 CROSS REGION FMR	228
188	ALGORITHM CYBERLINK-002 CROSS REGION FMR	229
189	ALGORITHM CYBERLINK-003 CROSS REGION FMR	230
190	ALGORITHM DAHUA-002 CROSS REGION FMR	231
191	ALGORITHM DAHUA-003 CROSS REGION FMR	232
192	ALGORITHM DEEPGLINT-001 CROSS REGION FMR	233
193	ALGORITHM DEEPSEA-001 CROSS REGION FMR	234
194	ALGORITHM DERMALOG-005 CROSS REGION FMR	235
195	ALGORITHM DERMALOG-006 CROSS REGION FMR	236
196	ALGORITHM DIDIGLOBALFACE-001 CROSS REGION FMR	237
197	ALGORITHM DIGITALBARRIERS-002 CROSS REGION FMR	238
198	ALGORITHM DSK-000 CROSS REGION FMR	239
199	ALGORITHM EINETWORKS-000 CROSS REGION FMR	240
200	ALGORITHM EVERAI-002 CROSS REGION FMR	241
201	ALGORITHM F8-001 CROSS REGION FMR	242
202	ALGORITHM FACESOFT-000 CROSS REGION FMR	243
203	ALGORITHM GLORY-001 CROSS REGION FMR	244
204	ALGORITHM GLORY-002 CROSS REGION FMR	245
205	ALGORITHM GORILLA-003 CROSS REGION FMR	246
206	ALGORITHM GORILLA-004 CROSS REGION FMR	247
207	ALGORITHM HIK-001 CROSS REGION FMR	248
208	ALGORITHM HR-001 CROSS REGION FMR	249
209	ALGORITHM HR-002 CROSS REGION FMR	250
210	ALGORITHM ID3-003 CROSS REGION FMR	251
211	ALGORITHM ID3-004 CROSS REGION FMR	252
212	ALGORITHM IDEMIA-004 CROSS REGION FMR	253
213	ALGORITHM IDEMIA-005 CROSS REGION FMR	254
214	ALGORITHM IIT-000 CROSS REGION FMR	255
215	ALGORITHM IIT-001 CROSS REGION FMR	256
216	ALGORITHM IMAGUS-000 CROSS REGION FMR	257
217	ALGORITHM IMAGUS-001 CROSS REGION FMR	258
218	ALGORITHM IMPERIAL-000 CROSS REGION FMR	259
219	ALGORITHM IMPERIAL-002 CROSS REGION FMR	260
220	ALGORITHM INCODE-004 CROSS REGION FMR	261
221	ALGORITHM INCODE-005 CROSS REGION FMR	262
222	ALGORITHM INNOVATIVETECHNOLOGYLTD-001 CROSS REGION FMR	263
223	ALGORITHM INNOVATRICES-004 CROSS REGION FMR	264
224	ALGORITHM INNOVATRICES-006 CROSS REGION FMR	265
225	ALGORITHM INTELICLOUDAI-001 CROSS REGION FMR	266
226	ALGORITHM INTELLIFUSION-001 CROSS REGION FMR	267
227	ALGORITHM INTELLIVISION-001 CROSS REGION FMR	268
228	ALGORITHM INTELLIVISION-002 CROSS REGION FMR	269



229	ALGORITHM INTELRESEARCH-000 CROSS REGION FMR	270
230	ALGORITHM INTSYSMSU-000 CROSS REGION FMR	271
231	ALGORITHM INTSYSMSU-001 CROSS REGION FMR	272
232	ALGORITHM IQFACE-000 CROSS REGION FMR	273
233	ALGORITHM ISAP-001 CROSS REGION FMR	274
234	ALGORITHM ISITYOU-000 CROSS REGION FMR	275
235	ALGORITHM ISYSTEMS-001 CROSS REGION FMR	276
236	ALGORITHM ISYSTEMS-002 CROSS REGION FMR	277
237	ALGORITHM ITMO-005 CROSS REGION FMR	278
238	ALGORITHM ITMO-006 CROSS REGION FMR	279
239	ALGORITHM KAKAO-001 CROSS REGION FMR	280
240	ALGORITHM KAKAO-002 CROSS REGION FMR	281
241	ALGORITHM KEDACOM-000 CROSS REGION FMR	282
242	ALGORITHM KNERON-003 CROSS REGION FMR	283
243	ALGORITHM LOOKMAN-002 CROSS REGION FMR	284
244	ALGORITHM LOOKMAN-004 CROSS REGION FMR	285
245	ALGORITHM LUXAND-000 CROSS REGION FMR	286
246	ALGORITHM MEGVII-001 CROSS REGION FMR	287
247	ALGORITHM MEGVII-002 CROSS REGION FMR	288
248	ALGORITHM MEIYA-001 CROSS REGION FMR	289
249	ALGORITHM MICROFOCUS-001 CROSS REGION FMR	290
250	ALGORITHM MICROFOCUS-002 CROSS REGION FMR	291
251	ALGORITHM MT-000 CROSS REGION FMR	292
252	ALGORITHM MVISION-001 CROSS REGION FMR	293
253	ALGORITHM NEUROTECHNOLOGY-005 CROSS REGION FMR	294
254	ALGORITHM NEUROTECHNOLOGY-006 CROSS REGION FMR	295
255	ALGORITHM NODEFLUX-001 CROSS REGION FMR	296
256	ALGORITHM NODEFLUX-002 CROSS REGION FMR	297
257	ALGORITHM NOTIONTAG-000 CROSS REGION FMR	298
258	ALGORITHM NTECHLAB-006 CROSS REGION FMR	299
259	ALGORITHM NTECHLAB-007 CROSS REGION FMR	300
260	ALGORITHM PIXELALL-002 CROSS REGION FMR	301
261	ALGORITHM PIXELALL-003 CROSS REGION FMR	302
262	ALGORITHM PSL-002 CROSS REGION FMR	303
263	ALGORITHM PSL-003 CROSS REGION FMR	304
264	ALGORITHM PYRAMID-000 CROSS REGION FMR	305
265	ALGORITHM RANKONE-007 CROSS REGION FMR	306
266	ALGORITHM RANKONE-008 CROSS REGION FMR	307
267	ALGORITHM REALNETWORKS-002 CROSS REGION FMR	308
268	ALGORITHM REALNETWORKS-003 CROSS REGION FMR	309
269	ALGORITHM REMARKAI-000 CROSS REGION FMR	310
270	ALGORITHM REMARKAI-001 CROSS REGION FMR	311
271	ALGORITHM ROKID-000 CROSS REGION FMR	312
272	ALGORITHM SAFFE-001 CROSS REGION FMR	313
273	ALGORITHM SAFFE-002 CROSS REGION FMR	314
274	ALGORITHM SAMTECH-001 CROSS REGION FMR	315
275	ALGORITHM SCANOVATE-001 CROSS REGION FMR	316
276	ALGORITHM SENSETIME-001 CROSS REGION FMR	317
277	ALGORITHM SENSETIME-002 CROSS REGION FMR	318
278	ALGORITHM SERTIS-000 CROSS REGION FMR	319
279	ALGORITHM SHAMAN-000 CROSS REGION FMR	320
280	ALGORITHM SHAMAN-001 CROSS REGION FMR	321
281	ALGORITHM SHU-001 CROSS REGION FMR	322
282	ALGORITHM SIAT-002 CROSS REGION FMR	323
283	ALGORITHM SIAT-004 CROSS REGION FMR	324
284	ALGORITHM SJTU-001 CROSS REGION FMR	325
285	ALGORITHM SMILART-002 CROSS REGION FMR	326

286	ALGORITHM SMILART-003 CROSS REGION FMR	327
287	ALGORITHM STARHYBRID-001 CROSS REGION FMR	328
288	ALGORITHM SYNESIS-005 CROSS REGION FMR	329
289	ALGORITHM SYNESIS-006 CROSS REGION FMR	330
290	ALGORITHM SYNOLOGY-000 CROSS REGION FMR	331
291	ALGORITHM TECH5-002 CROSS REGION FMR	332
292	ALGORITHM TECH5-003 CROSS REGION FMR	333
293	ALGORITHM TEVIAN-004 CROSS REGION FMR	334
294	ALGORITHM TEVIAN-005 CROSS REGION FMR	335
295	ALGORITHM TIGER-002 CROSS REGION FMR	336
296	ALGORITHM TIGER-003 CROSS REGION FMR	337
297	ALGORITHM TONGYI-005 CROSS REGION FMR	338
298	ALGORITHM TOSHIBA-002 CROSS REGION FMR	339
299	ALGORITHM TOSHIBA-003 CROSS REGION FMR	340
300	ALGORITHM TRUEFACE-000 CROSS REGION FMR	341
301	ALGORITHM TUPUTECH-000 CROSS REGION FMR	342
302	ALGORITHM ULSEE-001 CROSS REGION FMR	343
303	ALGORITHM ULUFACE-002 CROSS REGION FMR	344
304	ALGORITHM ULUFACE-003 CROSS REGION FMR	345
305	ALGORITHM UPC-001 CROSS REGION FMR	346
306	ALGORITHM VCOG-002 CROSS REGION FMR	347
307	ALGORITHM VD-001 CROSS REGION FMR	348
308	ALGORITHM VERIDAS-001 CROSS REGION FMR	349
309	ALGORITHM VERIDAS-002 CROSS REGION FMR	350
310	ALGORITHM VIA-000 CROSS REGION FMR	351
311	ALGORITHM VIDEONETICS-001 CROSS REGION FMR	352
312	ALGORITHM VIGILANTSOLUTIONS-006 CROSS REGION FMR	353
313	ALGORITHM VIGILANTSOLUTIONS-007 CROSS REGION FMR	354
314	ALGORITHM VION-000 CROSS REGION FMR	355
315	ALGORITHM VISIONBOX-000 CROSS REGION FMR	356
316	ALGORITHM VISIONBOX-001 CROSS REGION FMR	357
317	ALGORITHM VISIONLABS-006 CROSS REGION FMR	358
318	ALGORITHM VISIONLABS-007 CROSS REGION FMR	359
319	ALGORITHM VOCORD-006 CROSS REGION FMR	360
320	ALGORITHM VOCORD-007 CROSS REGION FMR	361
321	ALGORITHM WINSENSE-000 CROSS REGION FMR	362
322	ALGORITHM WINSENSE-001 CROSS REGION FMR	363
323	ALGORITHM X-LABORATORY-000 CROSS REGION FMR	364
324	ALGORITHM YISHENG-004 CROSS REGION FMR	365
325	ALGORITHM YITU-003 CROSS REGION FMR	366
326	ALGORITHM 3DIVI-003 CROSS COUNTRY FMR	367
327	ALGORITHM 3DIVI-004 CROSS COUNTRY FMR	368
328	ALGORITHM ADERA-001 CROSS COUNTRY FMR	369
329	ALGORITHM AIMALL-001 CROSS COUNTRY FMR	370
330	ALGORITHM AIUNIONFACE-000 CROSS COUNTRY FMR	371
331	ALGORITHM ALCHERA-000 CROSS COUNTRY FMR	372
332	ALGORITHM ALCHERA-001 CROSS COUNTRY FMR	373
333	ALGORITHM ALLGOVISION-000 CROSS COUNTRY FMR	374
334	ALGORITHM ALPHAFACE-001 CROSS COUNTRY FMR	375
335	ALGORITHM AMPLIFIEDGROUP-001 CROSS COUNTRY FMR	376
336	ALGORITHM ANKE-003 CROSS COUNTRY FMR	377
337	ALGORITHM ANKE-004 CROSS COUNTRY FMR	378
338	ALGORITHM ANYVISION-002 CROSS COUNTRY FMR	379
339	ALGORITHM ANYVISION-004 CROSS COUNTRY FMR	380
340	ALGORITHM ASUSAICS-000 CROSS COUNTRY FMR	381
341	ALGORITHM AWARE-003 CROSS COUNTRY FMR	382
342	ALGORITHM AWARE-004 CROSS COUNTRY FMR	383

343	ALGORITHM AWIROS-001 CROSS COUNTRY FMR	384
344	ALGORITHM AYONIX-000 CROSS COUNTRY FMR	385
345	ALGORITHM BM-001 CROSS COUNTRY FMR	386
346	ALGORITHM CAMVI-002 CROSS COUNTRY FMR	387
347	ALGORITHM CAMVI-004 CROSS COUNTRY FMR	388
348	ALGORITHM CEIEC-001 CROSS COUNTRY FMR	389
349	ALGORITHM CEIEC-002 CROSS COUNTRY FMR	390
350	ALGORITHM CHTFACE-001 CROSS COUNTRY FMR	391
351	ALGORITHM COGENT-003 CROSS COUNTRY FMR	392
352	ALGORITHM COGENT-004 CROSS COUNTRY FMR	393
353	ALGORITHM COGNITEC-000 CROSS COUNTRY FMR	394
354	ALGORITHM COGNITEC-001 CROSS COUNTRY FMR	395
355	ALGORITHM CTBCBANK-000 CROSS COUNTRY FMR	396
356	ALGORITHM CTBCBANK-001 CROSS COUNTRY FMR	397
357	ALGORITHM CYBEREXTRUDER-001 CROSS COUNTRY FMR	398
358	ALGORITHM CYBEREXTRUDER-002 CROSS COUNTRY FMR	399
359	ALGORITHM CYBERLINK-002 CROSS COUNTRY FMR	400
360	ALGORITHM DAHUA-002 CROSS COUNTRY FMR	401
361	ALGORITHM DAHUA-003 CROSS COUNTRY FMR	402
362	ALGORITHM DEEPGLINT-001 CROSS COUNTRY FMR	403
363	ALGORITHM DEEPSEA-001 CROSS COUNTRY FMR	404
364	ALGORITHM DERMALOG-005 CROSS COUNTRY FMR	405
365	ALGORITHM DERMALOG-006 CROSS COUNTRY FMR	406
366	ALGORITHM DIDIGLOBALFACE-001 CROSS COUNTRY FMR	407
367	ALGORITHM DIGITALBARRIERS-002 CROSS COUNTRY FMR	408
368	ALGORITHM DSK-000 CROSS COUNTRY FMR	409
369	ALGORITHM EINETWORKS-000 CROSS COUNTRY FMR	410
370	ALGORITHM EVERAI-002 CROSS COUNTRY FMR	411
371	ALGORITHM F8-001 CROSS COUNTRY FMR	412
372	ALGORITHM FACESOFT-000 CROSS COUNTRY FMR	413
373	ALGORITHM GLORY-001 CROSS COUNTRY FMR	414
374	ALGORITHM GLORY-002 CROSS COUNTRY FMR	415
375	ALGORITHM GORILLA-003 CROSS COUNTRY FMR	416
376	ALGORITHM GORILLA-004 CROSS COUNTRY FMR	417
377	ALGORITHM HIK-001 CROSS COUNTRY FMR	418
378	ALGORITHM HR-001 CROSS COUNTRY FMR	419
379	ALGORITHM HR-002 CROSS COUNTRY FMR	420
380	ALGORITHM ID3-003 CROSS COUNTRY FMR	421
381	ALGORITHM ID3-004 CROSS COUNTRY FMR	422
382	ALGORITHM IDEMIA-004 CROSS COUNTRY FMR	423
383	ALGORITHM IDEMIA-005 CROSS COUNTRY FMR	424
384	ALGORITHM IIT-000 CROSS COUNTRY FMR	425
385	ALGORITHM IIT-001 CROSS COUNTRY FMR	426
386	ALGORITHM IMAGUS-000 CROSS COUNTRY FMR	427
387	ALGORITHM IMAGUS-001 CROSS COUNTRY FMR	428
388	ALGORITHM IMPERIAL-000 CROSS COUNTRY FMR	429
389	ALGORITHM IMPERIAL-002 CROSS COUNTRY FMR	430
390	ALGORITHM INCODE-004 CROSS COUNTRY FMR	431
391	ALGORITHM INNOVATIVETECHNOLOGYLTD-001 CROSS COUNTRY FMR	432
392	ALGORITHM INNOVATRICES-004 CROSS COUNTRY FMR	433
393	ALGORITHM INNOVATRICES-006 CROSS COUNTRY FMR	434
394	ALGORITHM INTELICLOUDAI-001 CROSS COUNTRY FMR	435
395	ALGORITHM INTELLIFUSION-001 CROSS COUNTRY FMR	436
396	ALGORITHM INTELLIVISION-001 CROSS COUNTRY FMR	437
397	ALGORITHM INTELLIVISION-002 CROSS COUNTRY FMR	438
398	ALGORITHM INTELRESEARCH-000 CROSS COUNTRY FMR	439
399	ALGORITHM INTSYSMSU-000 CROSS COUNTRY FMR	440

400	ALGORITHM INTSYSMSU-001 CROSS COUNTRY FMR	441
401	ALGORITHM IQFACE-000 CROSS COUNTRY FMR	442
402	ALGORITHM ISAP-001 CROSS COUNTRY FMR	443
403	ALGORITHM ISITYOU-000 CROSS COUNTRY FMR	444
404	ALGORITHM ISYSTEMS-001 CROSS COUNTRY FMR	445
405	ALGORITHM ISYSTEMS-002 CROSS COUNTRY FMR	446
406	ALGORITHM ITMO-005 CROSS COUNTRY FMR	447
407	ALGORITHM ITMO-006 CROSS COUNTRY FMR	448
408	ALGORITHM KAKAO-001 CROSS COUNTRY FMR	449
409	ALGORITHM KAKAO-002 CROSS COUNTRY FMR	450
410	ALGORITHM KEDACOM-000 CROSS COUNTRY FMR	451
411	ALGORITHM KNERON-003 CROSS COUNTRY FMR	452
412	ALGORITHM LOOKMAN-002 CROSS COUNTRY FMR	453
413	ALGORITHM LOOKMAN-004 CROSS COUNTRY FMR	454
414	ALGORITHM MEGVII-001 CROSS COUNTRY FMR	455
415	ALGORITHM MEGVII-002 CROSS COUNTRY FMR	456
416	ALGORITHM MEIYA-001 CROSS COUNTRY FMR	457
417	ALGORITHM MICROFOCUS-001 CROSS COUNTRY FMR	458
418	ALGORITHM MICROFOCUS-002 CROSS COUNTRY FMR	459
419	ALGORITHM MT-000 CROSS COUNTRY FMR	460
420	ALGORITHM MVISION-001 CROSS COUNTRY FMR	461
421	ALGORITHM NEUROTECHNOLOGY-005 CROSS COUNTRY FMR	462
422	ALGORITHM NEUROTECHNOLOGY-006 CROSS COUNTRY FMR	463
423	ALGORITHM NODEFLUX-001 CROSS COUNTRY FMR	464
424	ALGORITHM NODEFLUX-002 CROSS COUNTRY FMR	465
425	ALGORITHM NOTIONTAG-000 CROSS COUNTRY FMR	466
426	ALGORITHM NTECHLAB-006 CROSS COUNTRY FMR	467
427	ALGORITHM NTECHLAB-007 CROSS COUNTRY FMR	468
428	ALGORITHM PIXELALL-002 CROSS COUNTRY FMR	469
429	ALGORITHM PIXELALL-003 CROSS COUNTRY FMR	470
430	ALGORITHM PSL-002 CROSS COUNTRY FMR	471
431	ALGORITHM PYRAMID-000 CROSS COUNTRY FMR	472
432	ALGORITHM RANKONE-007 CROSS COUNTRY FMR	473
433	ALGORITHM REALNETWORKS-002 CROSS COUNTRY FMR	474
434	ALGORITHM REALNETWORKS-003 CROSS COUNTRY FMR	475
435	ALGORITHM REMARKAI-000 CROSS COUNTRY FMR	476
436	ALGORITHM REMARKAI-001 CROSS COUNTRY FMR	477
437	ALGORITHM ROKID-000 CROSS COUNTRY FMR	478
438	ALGORITHM SAFFE-001 CROSS COUNTRY FMR	479
439	ALGORITHM SAFFE-002 CROSS COUNTRY FMR	480
440	ALGORITHM SAMTECH-001 CROSS COUNTRY FMR	481
441	ALGORITHM SENSETIME-001 CROSS COUNTRY FMR	482
442	ALGORITHM SENSETIME-002 CROSS COUNTRY FMR	483
443	ALGORITHM SHAMAN-000 CROSS COUNTRY FMR	484
444	ALGORITHM SHAMAN-001 CROSS COUNTRY FMR	485
445	ALGORITHM SHU-001 CROSS COUNTRY FMR	486
446	ALGORITHM SIAT-002 CROSS COUNTRY FMR	487
447	ALGORITHM SIAT-004 CROSS COUNTRY FMR	488
448	ALGORITHM SJTU-001 CROSS COUNTRY FMR	489
449	ALGORITHM SMILART-002 CROSS COUNTRY FMR	490
450	ALGORITHM SMILART-003 CROSS COUNTRY FMR	491
451	ALGORITHM STARHYBRID-001 CROSS COUNTRY FMR	492
452	ALGORITHM SYNESIS-005 CROSS COUNTRY FMR	493
453	ALGORITHM SYNESIS-006 CROSS COUNTRY FMR	494
454	ALGORITHM SYNOLOGY-000 CROSS COUNTRY FMR	495
455	ALGORITHM TECH5-002 CROSS COUNTRY FMR	496

456	ALGORITHM TECH5-003 CROSS COUNTRY FMR	497
457	ALGORITHM TEVIAN-004 CROSS COUNTRY FMR	498
458	ALGORITHM TIGER-002 CROSS COUNTRY FMR	499
459	ALGORITHM TIGER-003 CROSS COUNTRY FMR	500
460	ALGORITHM TONGYI-005 CROSS COUNTRY FMR	501
461	ALGORITHM TOSHIBA-002 CROSS COUNTRY FMR	502
462	ALGORITHM TOSHIBA-003 CROSS COUNTRY FMR	503
463	ALGORITHM TRUEFACE-000 CROSS COUNTRY FMR	504
464	ALGORITHM ULSEE-001 CROSS COUNTRY FMR	505
465	ALGORITHM ULUFACE-002 CROSS COUNTRY FMR	506
466	ALGORITHM UPC-001 CROSS COUNTRY FMR	507
467	ALGORITHM VCOG-002 CROSS COUNTRY FMR	508
468	ALGORITHM VD-001 CROSS COUNTRY FMR	509
469	ALGORITHM VERIDAS-001 CROSS COUNTRY FMR	510
470	ALGORITHM VERIDAS-002 CROSS COUNTRY FMR	511
471	ALGORITHM VIA-000 CROSS COUNTRY FMR	512
472	ALGORITHM VIDEONETICS-001 CROSS COUNTRY FMR	513
473	ALGORITHM VIGILANTSOLUTIONS-006 CROSS COUNTRY FMR	514
474	ALGORITHM VIGILANTSOLUTIONS-007 CROSS COUNTRY FMR	515
475	ALGORITHM VION-000 CROSS COUNTRY FMR	516
476	ALGORITHM VISIONBOX-000 CROSS COUNTRY FMR	517
477	ALGORITHM VISIONBOX-001 CROSS COUNTRY FMR	518
478	ALGORITHM VISIONLABS-006 CROSS COUNTRY FMR	519
479	ALGORITHM VISIONLABS-007 CROSS COUNTRY FMR	520
480	ALGORITHM VOCORD-006 CROSS COUNTRY FMR	521
481	ALGORITHM VOCORD-007 CROSS COUNTRY FMR	522
482	ALGORITHM WINSENSE-000 CROSS COUNTRY FMR	523
483	ALGORITHM X-LABORATORY-000 CROSS COUNTRY FMR	524
484	ALGORITHM YISHENG-004 CROSS COUNTRY FMR	525
485	ALGORITHM YITU-003 CROSS COUNTRY FMR	526
486	IMPOSTOR COUNTS FOR CROSS COUNTRY FMR CALCULATIONS	527
487	ALGORITHM 3DIVI-003 CROSS AGE FMR	529
488	ALGORITHM 3DIVI-004 CROSS AGE FMR	530
489	ALGORITHM ADERA-001 CROSS AGE FMR	531
490	ALGORITHM AIUNIONFACE-000 CROSS AGE FMR	532
491	ALGORITHM ALCHERA-000 CROSS AGE FMR	533
492	ALGORITHM ALCHERA-001 CROSS AGE FMR	534
493	ALGORITHM ALLGOVISION-000 CROSS AGE FMR	535
494	ALGORITHM ALPHAFACE-001 CROSS AGE FMR	536
495	ALGORITHM AMPLIFIEDGROUP-001 CROSS AGE FMR	537
496	ALGORITHM ANKE-003 CROSS AGE FMR	538
497	ALGORITHM ANKE-004 CROSS AGE FMR	539
498	ALGORITHM ANYVISION-002 CROSS AGE FMR	540
499	ALGORITHM ANYVISION-004 CROSS AGE FMR	541
500	ALGORITHM ASUSAICS-000 CROSS AGE FMR	542
501	ALGORITHM AWARE-003 CROSS AGE FMR	543
502	ALGORITHM AWARE-004 CROSS AGE FMR	544
503	ALGORITHM AWIROS-001 CROSS AGE FMR	545
504	ALGORITHM AYONIX-000 CROSS AGE FMR	546
505	ALGORITHM BM-001 CROSS AGE FMR	547
506	ALGORITHM CAMVI-002 CROSS AGE FMR	548
507	ALGORITHM CAMVI-004 CROSS AGE FMR	549
508	ALGORITHM CEIEC-001 CROSS AGE FMR	550
509	ALGORITHM CEIEC-002 CROSS AGE FMR	551
510	ALGORITHM CHTFACE-001 CROSS AGE FMR	552
511	ALGORITHM COGENT-003 CROSS AGE FMR	553
512	ALGORITHM COGENT-004 CROSS AGE FMR	554

513	ALGORITHM COGNITEC-000 CROSS AGE FMR	555
514	ALGORITHM COGNITEC-001 CROSS AGE FMR	556
515	ALGORITHM CTBCBANK-000 CROSS AGE FMR	557
516	ALGORITHM CTBCBANK-001 CROSS AGE FMR	558
517	ALGORITHM CYBEREXTRUDER-001 CROSS AGE FMR	559
518	ALGORITHM CYBEREXTRUDER-002 CROSS AGE FMR	560
519	ALGORITHM CYBERLINK-002 CROSS AGE FMR	561
520	ALGORITHM CYBERLINK-003 CROSS AGE FMR	562
521	ALGORITHM DAHUA-002 CROSS AGE FMR	563
522	ALGORITHM DAHUA-003 CROSS AGE FMR	564
523	ALGORITHM DEEPLINT-001 CROSS AGE FMR	565
524	ALGORITHM DEEPSEA-001 CROSS AGE FMR	566
525	ALGORITHM DERMALOG-005 CROSS AGE FMR	567
526	ALGORITHM DERMALOG-006 CROSS AGE FMR	568
527	ALGORITHM DIDIGLOBALFACE-001 CROSS AGE FMR	569
528	ALGORITHM DIGITALBARRIERS-002 CROSS AGE FMR	570
529	ALGORITHM DSK-000 CROSS AGE FMR	571
530	ALGORITHM EINETWORKS-000 CROSS AGE FMR	572
531	ALGORITHM EVERAI-002 CROSS AGE FMR	573
532	ALGORITHM F8-001 CROSS AGE FMR	574
533	ALGORITHM FACESOFT-000 CROSS AGE FMR	575
534	ALGORITHM GLORY-001 CROSS AGE FMR	576
535	ALGORITHM GORILLA-003 CROSS AGE FMR	577
536	ALGORITHM HIK-001 CROSS AGE FMR	578
537	ALGORITHM HR-001 CROSS AGE FMR	579
538	ALGORITHM HR-002 CROSS AGE FMR	580
539	ALGORITHM ID3-003 CROSS AGE FMR	581
540	ALGORITHM ID3-004 CROSS AGE FMR	582
541	ALGORITHM IDEMIA-004 CROSS AGE FMR	583
542	ALGORITHM IDEMIA-005 CROSS AGE FMR	584
543	ALGORITHM IIT-000 CROSS AGE FMR	585
544	ALGORITHM IIT-001 CROSS AGE FMR	586
545	ALGORITHM IMAGUS-000 CROSS AGE FMR	587
546	ALGORITHM IMPERIAL-000 CROSS AGE FMR	588
547	ALGORITHM IMPERIAL-002 CROSS AGE FMR	589
548	ALGORITHM INCODE-004 CROSS AGE FMR	590
549	ALGORITHM INCODE-005 CROSS AGE FMR	591
550	ALGORITHM INNOVATIVETECHNOLOGYLTD-001 CROSS AGE FMR	592
551	ALGORITHM INNOVATRICES-004 CROSS AGE FMR	593
552	ALGORITHM INNOVATRICES-006 CROSS AGE FMR	594
553	ALGORITHM INTELICLOUDAI-001 CROSS AGE FMR	595
554	ALGORITHM INTELLIFUSION-001 CROSS AGE FMR	596
555	ALGORITHM INTELLIVISION-001 CROSS AGE FMR	597
556	ALGORITHM INTELLIVISION-002 CROSS AGE FMR	598
557	ALGORITHM INTELRESEARCH-000 CROSS AGE FMR	599
558	ALGORITHM INTSYSMSU-000 CROSS AGE FMR	600
559	ALGORITHM INTSYSMSU-001 CROSS AGE FMR	601
560	ALGORITHM IQFACE-000 CROSS AGE FMR	602
561	ALGORITHM ISAP-001 CROSS AGE FMR	603
562	ALGORITHM ISITYOU-000 CROSS AGE FMR	604
563	ALGORITHM ISYSTEMS-001 CROSS AGE FMR	605
564	ALGORITHM ISYSTEMS-002 CROSS AGE FMR	606
565	ALGORITHM ITMO-005 CROSS AGE FMR	607
566	ALGORITHM ITMO-006 CROSS AGE FMR	608
567	ALGORITHM KAKAO-001 CROSS AGE FMR	609
568	ALGORITHM KAKAO-002 CROSS AGE FMR	610
569	ALGORITHM KEDACOM-000 CROSS AGE FMR	611



570	ALGORITHM KNERON-003 CROSS AGE FMR	612
571	ALGORITHM LOOKMAN-002 CROSS AGE FMR	613
572	ALGORITHM LOOKMAN-004 CROSS AGE FMR	614
573	ALGORITHM MEGVII-001 CROSS AGE FMR	615
574	ALGORITHM MEGVII-002 CROSS AGE FMR	616
575	ALGORITHM MEIYA-001 CROSS AGE FMR	617
576	ALGORITHM MICROFOCUS-001 CROSS AGE FMR	618
577	ALGORITHM MICROFOCUS-002 CROSS AGE FMR	619
578	ALGORITHM MT-000 CROSS AGE FMR	620
579	ALGORITHM NEUROTECHNOLOGY-005 CROSS AGE FMR	621
580	ALGORITHM NEUROTECHNOLOGY-006 CROSS AGE FMR	622
581	ALGORITHM NODEFLUX-001 CROSS AGE FMR	623
582	ALGORITHM NODEFLUX-002 CROSS AGE FMR	624
583	ALGORITHM NOTIONTAG-000 CROSS AGE FMR	625
584	ALGORITHM NTECHLAB-006 CROSS AGE FMR	626
585	ALGORITHM NTECHLAB-007 CROSS AGE FMR	627
586	ALGORITHM PIXELALL-002 CROSS AGE FMR	628
587	ALGORITHM PIXELALL-003 CROSS AGE FMR	629
588	ALGORITHM PSL-002 CROSS AGE FMR	630
589	ALGORITHM PSL-003 CROSS AGE FMR	631
590	ALGORITHM RANKONE-007 CROSS AGE FMR	632
591	ALGORITHM REALNETWORKS-002 CROSS AGE FMR	633
592	ALGORITHM REALNETWORKS-003 CROSS AGE FMR	634
593	ALGORITHM REMARKAI-000 CROSS AGE FMR	635
594	ALGORITHM REMARKAI-001 CROSS AGE FMR	636
595	ALGORITHM ROKID-000 CROSS AGE FMR	637
596	ALGORITHM SAFFE-001 CROSS AGE FMR	638
597	ALGORITHM SAFFE-002 CROSS AGE FMR	639
598	ALGORITHM SAMTECH-001 CROSS AGE FMR	640
599	ALGORITHM SENSETIME-001 CROSS AGE FMR	641
600	ALGORITHM SENSETIME-002 CROSS AGE FMR	642
601	ALGORITHM SERTIS-000 CROSS AGE FMR	643
602	ALGORITHM SHAMAN-000 CROSS AGE FMR	644
603	ALGORITHM SHAMAN-001 CROSS AGE FMR	645
604	ALGORITHM SHU-001 CROSS AGE FMR	646
605	ALGORITHM SIAT-002 CROSS AGE FMR	647
606	ALGORITHM SIAT-004 CROSS AGE FMR	648
607	ALGORITHM SJTU-001 CROSS AGE FMR	649
608	ALGORITHM SMILART-002 CROSS AGE FMR	650
609	ALGORITHM SMILART-003 CROSS AGE FMR	651
610	ALGORITHM STARHYBRID-001 CROSS AGE FMR	652
611	ALGORITHM SYNESIS-005 CROSS AGE FMR	653
612	ALGORITHM SYNESIS-006 CROSS AGE FMR	654
613	ALGORITHM SYNOLOGY-000 CROSS AGE FMR	655
614	ALGORITHM TECH5-002 CROSS AGE FMR	656
615	ALGORITHM TECH5-003 CROSS AGE FMR	657
616	ALGORITHM TEVIAN-004 CROSS AGE FMR	658
617	ALGORITHM TEVIAN-005 CROSS AGE FMR	659
618	ALGORITHM TIGER-002 CROSS AGE FMR	660
619	ALGORITHM TIGER-003 CROSS AGE FMR	661
620	ALGORITHM TONGYI-005 CROSS AGE FMR	662
621	ALGORITHM TOSHIBA-002 CROSS AGE FMR	663
622	ALGORITHM TOSHIBA-003 CROSS AGE FMR	664
623	ALGORITHM TRUEFACE-000 CROSS AGE FMR	665
624	ALGORITHM TUPUTECH-000 CROSS AGE FMR	666
625	ALGORITHM ULSEE-001 CROSS AGE FMR	667
626	ALGORITHM ULUFACE-002 CROSS AGE FMR	668

---

627	ALGORITHM UPC-001 CROSS AGE FMR . . . . .	669
628	ALGORITHM VCOG-002 CROSS AGE FMR . . . . .	670
629	ALGORITHM VD-001 CROSS AGE FMR . . . . .	671
630	ALGORITHM VERIDAS-001 CROSS AGE FMR . . . . .	672
631	ALGORITHM VERIDAS-002 CROSS AGE FMR . . . . .	673
632	ALGORITHM VIA-000 CROSS AGE FMR . . . . .	674
633	ALGORITHM VIDEONETICS-001 CROSS AGE FMR . . . . .	675
634	ALGORITHM VIGILANTSOLUTIONS-006 CROSS AGE FMR . . . . .	676
635	ALGORITHM VIGILANTSOLUTIONS-007 CROSS AGE FMR . . . . .	677
636	ALGORITHM VION-000 CROSS AGE FMR . . . . .	678
637	ALGORITHM VISIONBOX-000 CROSS AGE FMR . . . . .	679
638	ALGORITHM VISIONBOX-001 CROSS AGE FMR . . . . .	680
639	ALGORITHM VISIONLABS-006 CROSS AGE FMR . . . . .	681
640	ALGORITHM VISIONLABS-007 CROSS AGE FMR . . . . .	682
641	ALGORITHM VOCORD-006 CROSS AGE FMR . . . . .	683
642	ALGORITHM VOCORD-007 CROSS AGE FMR . . . . .	684
643	ALGORITHM WINSENSE-000 CROSS AGE FMR . . . . .	685
644	ALGORITHM WINSENSE-001 CROSS AGE FMR . . . . .	686
645	ALGORITHM X-LABORATORY-000 CROSS AGE FMR . . . . .	687
646	ALGORITHM YISHENG-004 CROSS AGE FMR . . . . .	688
647	ALGORITHM YITU-003 CROSS AGE FMR . . . . .	689



	Developer	Short	Seq.	Validation	Config <sup>1</sup>	Template			GPU	Comparison Time (ns) <sup>3</sup>	
	Name	Name	Num.	Date	Data (KB)	Size (B)	Time (ms) <sup>2</sup>		Genuine	Impostor	
1	3DiVi	3divi	003	2018-10-09	191636	<sup>163</sup> 4096 ± 0	<sup>109</sup> 650 ± 90	No	<sup>18</sup> 627 ± 11	<sup>22</sup> 623 ± 32	
2	3DiVi	3divi	004	2019-07-22	263670	<sup>89</sup> 2048 ± 0	<sup>172</sup> 984 ± 131	No	<sup>31</sup> 794 ± 35	<sup>33</sup> 801 ± 40	
3	Adera Global PTE Ltd	adera	001	2019-06-17	0	<sup>151</sup> 2560 ± 0	<sup>497</sup> ± 0	No	<sup>67</sup> 1604 ± 71	<sup>68</sup> 1649 ± 56	
4	Shenzhen AiMall Tech Ltd	aimall	001	2019-11-12	128820	<sup>35</sup> 1024 ± 0	<sup>44</sup> 328 ± 0	No	<sup>124</sup> 5038 ± 40	<sup>132</sup> 6849 ± 401	
5	AiUnion Technology Co. Ltd	aiunionface	000	2019-10-22	0	<sup>91</sup> 2048 ± 0	<sup>112</sup> 653 ± 32	No	<sup>103</sup> 3439 ± 47	<sup>106</sup> 3657 ± 167	
6	Alchera	alchera	000	2019-03-01	258450	<sup>77</sup> 2048 ± 0	<sup>94</sup> 587 ± 13	No	<sup>99</sup> 3189 ± 32	<sup>95</sup> 3031 ± 142	
7	Alchera	alchera	000	2019-03-01	174013	<sup>74</sup> 2048 ± 0	<sup>102</sup> 627 ± 11	No	<sup>101</sup> 3342 ± 81	<sup>98</sup> 3243 ± 47	
8	AllGoVision	allgovision	000	2019-03-01	172509	<sup>104</sup> 2048 ± 0	<sup>54</sup> 384 ± 8	No	<sup>163</sup> 29903 ± 406	<sup>164</sup> 29735 ± 194	
9	AlphaSSTG	alphaface	001	2019-09-03	259849	<sup>83</sup> 2048 ± 0	<sup>98</sup> 613 ± 3	No	<sup>104</sup> 3482 ± 41	<sup>100</sup> 3279 ± 91	
10	Amplified Group	amplifiedgroup	001	2019-03-01	0	<sup>29</sup> 866 ± 2	<sup>393</sup> ± 0	No	<sup>167</sup> 57803 ± 4210	<sup>167</sup> 56365 ± 1196	
11	Anke Investments	anke	003	2019-02-27	340160	<sup>135</sup> 2056 ± 0	<sup>147</sup> 811 ± 23	No	<sup>5</sup> 425 ± 28	<sup>6</sup> 437 ± 32	
12	Anke Investments	anke	004	2019-06-27	349388	<sup>132</sup> 2056 ± 0	<sup>101</sup> 625 ± 1	No	<sup>19</sup> 633 ± 22	<sup>24</sup> 632 ± 34	
13	AnyVision	anyvision	002	2018-01-31	662659	<sup>39</sup> 1024 ± 0	<sup>23</sup> 248 ± 0	No	<sup>168</sup> 74069 ± 188	<sup>168</sup> 74019 ± 198	
14	AnyVision	anyvision	004	2018-06-15	401001	<sup>34</sup> 1024 ± 0	<sup>48</sup> 355 ± 1	No	<sup>76</sup> 1891 ± 51	<sup>73</sup> 1829 ± 85	
15	ASUSTek Computer Inc	asusaics	000	2019-10-24	257418	<sup>80</sup> 2048 ± 0	<sup>69</sup> 488 ± 18	No	<sup>139</sup> 8118 ± 128	<sup>139</sup> 8053 ± 456	
16	Aware	aware	003	2018-10-19	377729	<sup>156</sup> 3108 ± 0	<sup>144</sup> 783 ± 10	No	<sup>59</sup> 1392 ± 42	<sup>61</sup> 1334 ± 80	
17	Aware	aware	004	2019-03-01	427829	<sup>145</sup> 2084 ± 0	<sup>164</sup> 900 ± 10	No	<sup>55</sup> 1279 ± 50	<sup>60</sup> 1287 ± 100	
18	Awidit Systems	awiros	001	2019-09-23	15499	<sup>15</sup> 512 ± 0	<sup>599</sup> ± 8	No	<sup>74</sup> 1868 ± 100	<sup>89</sup> 2467 ± 78	
19	Ayonix	ayonix	000	2017-06-22	58505	<sup>40</sup> 1036 ± 0	<sup>1</sup> 18 ± 2	No	<sup>17</sup> 621 ± 23	<sup>21</sup> 620 ± 26	
20	Bitmain	bitmain	001	2018-10-17	287734	<sup>1</sup> 64 ± 0	<sup>65</sup> 444 ± 88	No	<sup>75</sup> 1887 ± 31	<sup>74</sup> 1877 ± 26	
21	Camvi Technologies	camvitech	002	2018-10-19	236278	<sup>37</sup> 1024 ± 0	<sup>124</sup> 677 ± 7	No	<sup>16</sup> 612 ± 26	<sup>17</sup> 603 ± 20	
22	Camvi Technologies	camvitech	004	2019-07-12	280733	<sup>98</sup> 2048 ± 0	<sup>139</sup> 759 ± 10	No	<sup>38</sup> 948 ± 40	<sup>40</sup> 963 ± 31	
23	China Electronics Import-Export Corp	ceiec	001	2019-03-01	159618	<sup>38</sup> 1024 ± 0	<sup>41</sup> 314 ± 3	No	<sup>157</sup> 22831 ± 108	<sup>157</sup> 22813 ± 120	
24	China Electronics Import-Export Corp	ceiec	002	2019-06-12	269063	<sup>73</sup> 2048 ± 0	<sup>97</sup> 612 ± 17	No	<sup>83</sup> 2188 ± 57	<sup>83</sup> 2301 ± 56	
25	Chunghwa Telecom Co. Ltd	chtface	001	2019-08-06	94088	<sup>100</sup> 2048 ± 0	<sup>19</sup> 218 ± 12	No	<sup>80</sup> 2089 ± 45	<sup>79</sup> 2087 ± 23	
26	Gemalto Cogent	cogent	003	2019-03-01	698290	<sup>30</sup> 973 ± 0	<sup>169</sup> 952 ± 0	No	<sup>145</sup> 12496 ± 75	<sup>144</sup> 11822 ± 163	
27	Gemalto Cogent	cogent	004	2019-06-14	722919	<sup>59</sup> 1983 ± 0	<sup>168</sup> 941 ± 28	No	<sup>149</sup> 14448 ± 56	<sup>150</sup> 15882 ± 81	
28	Cognitec Systems GmbH	cognitec	000	2018-10-19	474759	<sup>121</sup> 2052 ± 0	<sup>20</sup> 224 ± 1	No	<sup>112</sup> 3835 ± 108	<sup>109</sup> 3782 ± 83	
29	Cognitec Systems GmbH	cognitec	001	2019-03-01	476809	<sup>127</sup> 2052 ± 0	<sup>37</sup> 297 ± 17	No	<sup>117</sup> 4253 ± 59	<sup>114</sup> 4102 ± 167	
30	CTBC Bank Co. Ltd	ctcbank	000	2019-06-28	257208	<sup>78</sup> 2048 ± 0	<sup>89</sup> 568 ± 43	No	<sup>106</sup> 3551 ± 87	<sup>121</sup> 4805 ± 209	
31	CTBC Bank Co. Ltd	ctcbank	001	2019-10-28	275511	<sup>107</sup> 2048 ± 0	<sup>114</sup> 654 ± 33	No	<sup>134</sup> 6321 ± 283	<sup>130</sup> 6218 ± 286	
32	Cyberextruder	cyberex	001	2017-08-02	121211	<sup>9</sup> 256 ± 0	<sup>163</sup> 893 ± 25	No	<sup>45</sup> 1083 ± 16	<sup>48</sup> 1079 ± 19	
33	Cyberextruder	cyberex	002	2018-01-30	168909	<sup>62</sup> 2048 ± 0	<sup>76</sup> 532 ± 6	No	<sup>73</sup> 1803 ± 14	<sup>71</sup> 1779 ± 22	
34	Cyberlink Corp	cyberlink	002	2019-06-12	222311	<sup>123</sup> 2052 ± 0	<sup>116</sup> 656 ± 22	No	<sup>86</sup> 2264 ± 71	<sup>92</sup> 2649 ± 195	
35	Cyberlink Corp	cyberlink	003	2019-10-07	470949	<sup>120</sup> 2052 ± 0	<sup>61</sup> 424 ± 1	No	<sup>122</sup> 4857 ± 53	<sup>123</sup> 5168 ± 69	
36	Dahua Technology Co. Ltd	dahua	002	2019-03-01	526452	<sup>75</sup> 2048 ± 0	<sup>103</sup> 628 ± 7	No	<sup>6</sup> 461 ± 23	<sup>8</sup> 454 ± 20	
37	Dahua Technology Co. Ltd	dahua	003	2019-08-14	605337	<sup>99</sup> 2048 ± 0	<sup>78</sup> 537 ± 4	No	<sup>22</sup> 653 ± 28	<sup>18</sup> 606 ± 38	
38	Deepglint	deepglint	001	2019-06-21	569802	<sup>161</sup> 4096 ± 0	<sup>131</sup> 721 ± 4	No	<sup>108</sup> 3680 ± 35	<sup>103</sup> 3517 ± 182	
39	Tencent Deepsea Lab	deepsea	001	2019-06-03	147497	<sup>31</sup> 1024 ± 0	<sup>104</sup> 630 ± 7	No	<sup>61</sup> 1401 ± 37	<sup>64</sup> 1467 ± 50	
40	Dermalog	dermalog	005	2018-02-02	0	<sup>2</sup> 128 ± 0	<sup>8</sup> 130 ± 11	No	<sup>9</sup> 499 ± 22	<sup>11</sup> 500 ± 22	
41	Dermalog	dermalog	006	2018-10-18	0	<sup>3</sup> 128 ± 0	<sup>75</sup> 532 ± 12	No	<sup>10</sup> 506 ± 23	<sup>9</sup> 459 ± 23	
42	DiDi ChuXing Technology Co	didiglobalface	001	2019-10-23	259849	<sup>82</sup> 2048 ± 0	<sup>108</sup> 650 ± 13	No	<sup>107</sup> 3592 ± 32	<sup>109</sup> 3588 ± 83	
43	Digital Barriers	barriers	002	2019-03-01	83002	<sup>136</sup> 2056 ± 0	<sup>17</sup> 209 ± 11	No	<sup>147</sup> 13409 ± 228	<sup>147</sup> 13267 ± 206	
44	DSK	dsk	000	2019-06-28	11967	<sup>17</sup> 512 ± 0	<sup>39</sup> 304 ± 47	No	<sup>136</sup> 7152 ± 115	<sup>134</sup> 7134 ± 111	

Notes	
1	The configuration size does not capture static data included in libraries. We do not count these because some algorithms include common ancillary libraries for image processing (e.g. openCV) or numerical computation (e.g. blas).
2	The median template creation times are measured on Intel®Xeon®CPU E5-2630 v4 @ 2.20GHz processors or, for GPU-enabled implementations, NVidia Tesla K40.
3	The comparison durations, in nanoseconds, are estimated using std::chrono::high_resolution_clock which on the machine in (2) counts 1ns clock ticks. Precision is somewhat worse than that however. The ± value is the median absolute deviation times 1.48 for Normal consistency.

Table 1: Summary of algorithms and properties included in this report. The red superscripts give ranking for the quantity in that column.

	Developer	Short	Seq.	Validation	Config <sup>1</sup>	Template		GPU	Comparison Time (ns) <sup>3</sup>	
	Name	Name	Num.	Date	Data (KB)	Size (B)	Time (ms) <sup>2</sup>		Genuine	Impostor
45	Shenzhen EI Networks Limited	einetworks	000	2019-08-13	372608	<sup>140</sup> 2056 ± 0	<sup>107</sup> 645 ± 3	No	<sup>123</sup> 4876 ± 66	<sup>122</sup> 5156 ± 77
46	Ever AI	everai	002	2019-03-01	561727	<sup>165</sup> 4096 ± 0	<sup>137</sup> 758 ± 0	No	<sup>21</sup> 644 ± 14	<sup>23</sup> 624 ± 35
47	Ever AI Paravision	everai paravision	003	2019-07-01	539802	<sup>160</sup> 4096 ± 0	<sup>122</sup> 674 ± 4	No	<sup>27</sup> 699 ± 20	<sup>28</sup> 713 ± 47
48	FarBar Inc.	f8	001	2019-07-11	272977	<sup>72</sup> 2048 ± 0	<sup>152</sup> 822 ± 39	No	<sup>150</sup> 15262 ± 139	<sup>149</sup> 15277 ± 212
49	FaceSoft Ltd.	facesoft	000	2019-07-10	370120	<sup>115</sup> 2048 ± 0	<sup>123</sup> 675 ± 18	No	<sup>84</sup> 2239 ± 28	<sup>82</sup> 2277 ± 96
50	Glory Ltd	glory	001	2018-06-08	0	<sup>56</sup> 1726 ± 0	<sup>56</sup> 393 ± 2	No	<sup>143</sup> 9607 ± 128	<sup>142</sup> 9539 ± 182
51	Glory Ltd	glory	002	2019-11-12	0	<sup>147</sup> 2106 ± 0	<sup>95</sup> 594 ± 5	No	<sup>142</sup> 8815 ± 105	<sup>141</sup> 8782 ± 78
52	Gorilla Technology	gorilla	003	2019-06-19	94409	<sup>44</sup> 1132 ± 0	<sup>46</sup> 334 ± 25	No	<sup>93</sup> 2840 ± 42	<sup>93</sup> 2865 ± 87
53	Gorilla Technology	gorilla	004	2019-11-04	186952	<sup>150</sup> 2192 ± 0	<sup>58</sup> 397 ± 3	No	<sup>127</sup> 5269 ± 84	<sup>125</sup> 5259 ± 105
54	Hikvision	hik	001	2019-03-01	667866	<sup>49</sup> 1408 ± 0	<sup>110</sup> 651 ± 0	No	<sup>8</sup> 488 ± 19	<sup>10</sup> 477 ± 22
55	Hengrui AI Technology Ltd	hr	001	2019-06-04	346156	<sup>142</sup> 2057 ± 0	<sup>117</sup> 665 ± 3	No	<sup>152</sup> 17816 ± 260	<sup>152</sup> 17878 ± 464
56	Hengrui AI Technology Ltd	hr	001	2019-10-08	390059	<sup>143</sup> 2057 ± 0	<sup>166</sup> 904 ± 4	No	<sup>159</sup> 24112 ± 766	<sup>158</sup> 23859 ± 739
57	ID3 Technology	id3	003	2018-10-05	265951	<sup>11</sup> 264 ± 0	<sup>42</sup> 316 ± 19	No	<sup>58</sup> 1330 ± 25	<sup>62</sup> 1354 ± 28
58	ID3 Technology	id3	004	2019-03-01	171526	<sup>10</sup> 264 ± 0	<sup>82</sup> 541 ± 11	No	<sup>46</sup> 1135 ± 23	<sup>53</sup> 1156 ± 32
59	Idemia	Idemia	004	2019-03-01	406924	<sup>13</sup> 352 ± 0	<sup>40</sup> 306 ± 5	No	<sup>128</sup> 5592 ± 518	<sup>127</sup> 5533 ± 426
60	Idemia	Idemia	005	2019-10-11	509824	<sup>27</sup> 588 ± 0	<sup>74</sup> 524 ± 20	No	<sup>137</sup> 7543 ± 370	<sup>143</sup> 10415 ± 174
61	Institute of Information Technologies	iitvision	000	2019-03-01	237317	<sup>36</sup> 1024 ± 0	<sup>16</sup> 197 ± 8	No	<sup>64</sup> 1537 ± 81	<sup>59</sup> 1282 ± 20
62	Institute of Information Technologies	iitvision	001	2019-07-05	269176	<sup>93</sup> 2048 ± 0	<sup>127</sup> 699 ± 4	No	<sup>43</sup> 1060 ± 48	<sup>46</sup> 1074 ± 54
63	Imagus Technology Pty Ltd	imagus	000	2019-06-19	183453	<sup>109</sup> 2048 ± 0	<sup>63</sup> 425 ± 24	No	<sup>47</sup> 1145 ± 25	<sup>70</sup> 1718 ± 63
64	Imagus Technology Pty Ltd	imagus	001	2019-10-22	282680	<sup>90</sup> 2048 ± 0	<sup>150</sup> 820 ± 45	No	<sup>109</sup> 3700 ± 34	<sup>104</sup> 3585 ± 238
65	Imperial College London	imperial	000	2019-03-01	370120	<sup>88</sup> 2048 ± 0	<sup>119</sup> 669 ± 1	No	<sup>81</sup> 2130 ± 32	<sup>78</sup> 2052 ± 100
66	Imperial College London	imperial	002	2019-08-28	472327	<sup>64</sup> 2048 ± 0	<sup>90</sup> 570 ± 2	No	<sup>121</sup> 4827 ± 69	<sup>118</sup> 4557 ± 160
67	Incode Technologies Inc	incode	004	2019-06-12	260224	<sup>69</sup> 2048 ± 0	<sup>67</sup> 479 ± 23	No	<sup>77</sup> 1913 ± 60	<sup>87</sup> 2443 ± 114
68	Incode Technologies Inc	incode	004	2019-10-17	256242	<sup>87</sup> 2048 ± 0	<sup>88</sup> 567 ± 4	No	<sup>118</sup> 4443 ± 91	<sup>120</sup> 4685 ± 72
69	Innovative Technology Ltd	innovativetechnologyltd	001	2019-10-22	177232	<sup>94</sup> 2048 ± 0	<sup>64</sup> 432 ± 7	No	<sup>119</sup> 4676 ± 34	<sup>116</sup> 4468 ± 169
70	Innovatrics	innovatrics	004	2018-10-19	0	<sup>43</sup> 1076 ± 0	<sup>55</sup> 391 ± 0	No	<sup>141</sup> 8573 ± 274	<sup>138</sup> 7929 ± 244
71	Innovatrics	innovatrics	006	2019-08-13	0	<sup>23</sup> 538 ± 0	<sup>153</sup> 824 ± 10	No	<sup>131</sup> 5763 ± 217	<sup>59</sup> 5631 ± 824
72	CSA IntelliCloud Technology	intellcloudai	001	2019-08-13	220831	<sup>113</sup> 2048 ± 0	<sup>68</sup> 479 ± 18	No	<sup>41</sup> 1010 ± 16	<sup>43</sup> 1024 ± 31
73	Shenzhen Intellifusion Technologies Co. Ltd	intellifusion	001	2019-08-22	271872	<sup>68</sup> 2048 ± 0	<sup>141</sup> 778 ± 61	No	<sup>111</sup> 3756 ± 59	<sup>113</sup> 3953 ± 126
74	Intellivision	intellivision	001	2017-10-10	43692	<sup>138</sup> 2056 ± 0	<sup>2</sup> 62 ± 2	No	<sup>89</sup> 2573 ± 91	<sup>91</sup> 2544 ± 38
75	Intellivision	intellivision	002	2019-08-23	43692	<sup>133</sup> 2056 ± 0	<sup>47</sup> 342 ± 30	No	<sup>151</sup> 16049 ± 195	<sup>148</sup> 15136 ± 389
76	Intel Research Group	intelresearch	000	2019-07-08	388229	<sup>65</sup> 2048 ± 0	<sup>165</sup> 902 ± 6	No	<sup>120</sup> 4800 ± 152	<sup>119</sup> 4561 ± 97
77	Lomonosov Moscow State University	intsysmsu	000	2019-06-18	650193	<sup>67</sup> 2048 ± 0	<sup>77</sup> 535 ± 20	No	<sup>14</sup> 610 ± 22	<sup>20</sup> 613 ± 31
78	Lomonosov Moscow State University	intsysmsu	001	2019-10-22	384409	<sup>86</sup> 2048 ± 0	<sup>99</sup> 617 ± 5	No	<sup>97</sup> 3135 ± 26	<sup>102</sup> 3440 ± 235
79	iQIYI Inc	iqface	000	2019-06-04	268819	<sup>170</sup> 4750 ± 32	<sup>79</sup> 538 ± 26	No	<sup>171</sup> 636433 ± 38446	<sup>171</sup> 632654 ± 85615
80	iSAP Solution Corporation	isap	001	2019-08-07	99049	<sup>164</sup> 4096 ± 0	<sup>10</sup> 171 ± 12	No	<sup>144</sup> 12413 ± 154	<sup>145</sup> 12251 ± 382
81	Is It You	isityou	000	2017-06-26	48010	<sup>171</sup> 19200 ± 0	<sup>6</sup> 113 ± 5	No	<sup>169</sup> 237517 ± 1318	<sup>169</sup> 237374 ± 1279
82	Innovation Systems	isystems	001	2018-06-12	274621	<sup>60</sup> 2048 ± 0	<sup>34</sup> 291 ± 9	No	<sup>12</sup> 557 ± 16	<sup>14</sup> 564 ± 22
83	Innovation Systems	isystems	002	2018-10-18	358984	<sup>97</sup> 2048 ± 0	<sup>151</sup> 822 ± 8	No	<sup>29</sup> 749 ± 31	<sup>25</sup> 632 ± 28
84	ITMO University	itmo	005	2018-10-19	482155	<sup>169</sup> 4173 ± 0	<sup>138</sup> 759 ± 1	No	<sup>146</sup> 13214 ± 164	<sup>146</sup> 12576 ± 257
85	ITMO University	itmo	006	2019-03-01	599187	<sup>149</sup> 2121 ± 0	<sup>148</sup> 814 ± 1	No	<sup>160</sup> 26154 ± 148	<sup>159</sup> 26217 ± 260
86	Kakao Corp	kakao	001	2019-03-01	107616	<sup>33</sup> 1024 ± 0	<sup>53</sup> 379 ± 1	No	<sup>35</sup> 930 ± 22	<sup>39</sup> 948 ± 38
87	Kakao Corp	kakao	002	2019-06-19	479406	<sup>116</sup> 2048 ± 0	<sup>134</sup> 747 ± 6	No	<sup>70</sup> 1720 ± 62	<sup>69</sup> 1715 ± 83
88	Kedacom International Pte	kedacom	000	2019-06-03	245292	<sup>12</sup> 292 ± 0	<sup>72</sup> 506 ± 3	No	<sup>23</sup> 684 ± 14	<sup>26</sup> 682 ± 16

Notes	
1	The configuration size does not capture static data included in libraries. We do not count these because some algorithms include common ancilliary libraries for image processing (e.g. openCV) or numerical computation (e.g. blas).
2	The median template creation times are measured on Intel®Xeon®CPU E5-2630 v4 @ 2.20GHz processors or, for GPU-enabled implementations, NVidia Tesla K40.
3	The comparison durations, in nanoseconds, are estimated using std::chrono::high_resolution_clock which on the machine in (2) counts 1ns clock ticks. Precision is somewhat worse than that however. The ± value is the median absolute deviation times 1.48 for Normal consistency.

Table 2: Summary of algorithms and properties included in this report. The red superscripts give ranking for the quantity in that column.

	Developer	Short	Seq.	Validation	Config <sup>1</sup>	Template		GPU	Comparison Time (ns) <sup>3</sup>	
	Name	Name	Num.	Date	Data (KB)	Size (B)	Time (ms) <sup>2</sup>		Genuine	Impostor
89	Kneron Inc	kenron	003	2019-07-01	58366	<sup>84</sup> 2048 ± 0	<sup>32</sup> 281 ± 3	No	<sup>126</sup> 5237 ± 63	<sup>126</sup> 5274 ± 99
90	Lookman Electroplast Industries	lookman	002	2018-06-13	138200	<sup>25</sup> 548 ± 0	<sup>11</sup> 173 ± 1	No	<sup>15</sup> 610 ± 19	<sup>19</sup> 612 ± 22
91	Lookman Electroplast Industries	lookman	004	2019-06-03	244775	<sup>24</sup> 548 ± 0	<sup>73</sup> 507 ± 5	No	<sup>33</sup> 871 ± 29	<sup>38</sup> 878 ± 29
92	Luxand Inc	luxand	000	2019-11-07	0	<sup>41</sup> 1040 ± 0	<sup>60</sup> 406 ± 22	No	<sup>85</sup> 2240 ± 32	<sup>81</sup> 2234 ± 25
93	Megvii/Face++	megvii	001	2018-06-15	1361523	<sup>112</sup> 2048 ± 0	<sup>83</sup> 543 ± 0	No	<sup>125</sup> 5228 ± 32	<sup>124</sup> 5252 ± 60
94	Megvii/Face++	megvii	002	2018-10-19	1809564	<sup>167</sup> 4100 ± 0	<sup>106</sup> 644 ± 0	No	<sup>166</sup> 50630 ± 183	<sup>166</sup> 47591 ± 716
95	Xiamen Meiya Pico Information Co. Ltd	meiya	001	2019-03-01	280055	<sup>118</sup> 2049 ± 0	<sup>100</sup> 622 ± 12	No	<sup>140</sup> 8356 ± 615	<sup>140</sup> 8134 ± 97
96	MicroFocus	microfocus	001	2018-06-13	104524	<sup>8</sup> 256 ± 0	<sup>27</sup> 264 ± 18	No	<sup>1</sup> 215 ± 8	<sup>1</sup> 217 ± 10
97	MicroFocus	microfocus	002	2018-10-17	96288	<sup>6</sup> 256 ± 0	<sup>25</sup> 259 ± 18	No	<sup>3</sup> 337 ± 34	<sup>2</sup> 230 ± 25
98	Moontime Smart Technology	mt	000	2019-06-03	372169	<sup>117</sup> 2049 ± 0	<sup>132</sup> 724 ± 12	No	<sup>69</sup> 1678 ± 47	<sup>67</sup> 1614 ± 85
99	MVision	mvision	001	2019-11-12	227502	<sup>20</sup> 512 ± 0	<sup>126</sup> 690 ± 21	No	<sup>72</sup> 1797 ± 38	<sup>72</sup> 1788 ± 32
100	Neurotechnology	neurotech	005	2019-03-01	270450	<sup>7</sup> 256 ± 0	<sup>59</sup> 399 ± 0	No	<sup>2</sup> 238 ± 10	<sup>3</sup> 237 ± 7
101	Neurotechnology	neurotech	006	2019-06-26	525541	<sup>18</sup> 512 ± 0	<sup>125</sup> 678 ± 56	No	<sup>11</sup> 513 ± 14	<sup>13</sup> 535 ± 26
102	Nodeflux	nodeflux	001	2019-03-01	262553	<sup>96</sup> 2048 ± 0	<sup>22</sup> 247 ± 1	No	<sup>100</sup> 3242 ± 81	<sup>99</sup> 3255 ± 93
103	Nodeflux	nodeflux	002	2019-08-13	774668	<sup>114</sup> 2048 ± 0	<sup>130</sup> 717 ± 16	No	<sup>132</sup> 5922 ± 170	<sup>137</sup> 7911 ± 367
104	NotionTag Technologies Private Limited	notiontag	000	2019-06-12	92753	<sup>28</sup> 584 ± 0	<sup>86</sup> 548 ± 64	No	<sup>165</sup> 44672 ± 269	<sup>165</sup> 44593 ± 358
105	N-Tech Lab	ntech	006	2019-03-01	7901590	<sup>154</sup> 2600 ± 0	<sup>135</sup> 749 ± 1	No	<sup>42</sup> 1055 ± 93	<sup>36</sup> 844 ± 48
106	N-Tech Lab	ntech	007	2019-06-25	2509686	<sup>157</sup> 3348 ± 0	<sup>145</sup> 792 ± 3	No	<sup>50</sup> 1209 ± 59	<sup>57</sup> 1267 ± 65
107	Guangzhou Pixel Solutions Co. Ltd	pixelall	002	2019-06-06	0	<sup>152</sup> 2560 ± 0	<sup>15</sup> 191 ± 1	No	<sup>51</sup> 1223 ± 56	<sup>55</sup> 1230 ± 47
108	Guangzhou Pixel Solutions Co. Ltd	pixelall	003	2019-10-15	0	<sup>153</sup> 2560 ± 0	<sup>129</sup> 708 ± 21	No	<sup>116</sup> 4216 ± 257	<sup>117</sup> 4488 ± 56
109	Panasonic R+D Center Singapore	psl	002	2019-02-28	804934	<sup>124</sup> 2052 ± 0	<sup>162</sup> 888 ± 9	No	<sup>66</sup> 1590 ± 48	<sup>49</sup> 1133 ± 78
110	Panasonic R+D Center Singapore	psl	003	2019-10-01	1159643	<sup>148</sup> 2120 ± 0	<sup>159</sup> 867 ± 7	No	<sup>114</sup> 3915 ± 50	<sup>114</sup> 3899 ± 226
111	Pyramid Cyber Security + Forensic (P) Ltd	pyramid	000	2019-11-04	372608	<sup>130</sup> 2056 ± 0	<sup>93</sup> 583 ± 2	No	<sup>135</sup> 7147 ± 59	<sup>135</sup> 7586 ± 425
112	Rank One Computing	rankone	007	2019-06-03	0	<sup>5</sup> 165 ± 0	<sup>21</sup> 245 ± 5	No	<sup>24</sup> 688 ± 20	<sup>16</sup> 601 ± 16
113	Rank One Computing	rankone	008	2019-11-12	0	<sup>4</sup> 165 ± 0	<sup>30</sup> 272 ± 4	No	<sup>37</sup> 944 ± 29	<sup>37</sup> 864 ± 26
114	Realnetworks Inc	realnetworks	002	2019-02-28	95328	<sup>58</sup> 1848 ± 0	<sup>24</sup> 250 ± 2	No	<sup>56</sup> 1285 ± 17	<sup>56</sup> 1247 ± 42
115	Realnetworks Inc	realnetworks	003	2019-06-12	95334	<sup>57</sup> 1848 ± 0	<sup>13</sup> 177 ± 10	No	<sup>63</sup> 1516 ± 29	<sup>65</sup> 1522 ± 60
116	KanKan Ai	remarkai	000	2019-03-01	240152	<sup>61</sup> 2048 ± 0	<sup>154</sup> 829 ± 7	No	<sup>34</sup> 873 ± 4	<sup>35</sup> 835 ± 35
117	KanKan Ai	remarkai	001	2019-03-01	241857	<sup>126</sup> 2052 ± 0	<sup>155</sup> 831 ± 6	No	<sup>52</sup> 1229 ± 20	<sup>34</sup> 805 ± 56
118	Rokid Corporation Ltd	rokid	000	2019-08-01	258612	<sup>139</sup> 2056 ± 0	<sup>84</sup> 547 ± 2	No	<sup>110</sup> 3711 ± 88	<sup>108</sup> 3746 ± 209
119	Saffe Ltd	saffe	001	2018-10-19	85973	<sup>47</sup> 1280 ± 0	<sup>31</sup> 281 ± 1	No	<sup>54</sup> 1274 ± 19	<sup>58</sup> 1277 ± 26
120	Saffe Ltd	saffe	002	2019-03-01	260622	<sup>106</sup> 2048 ± 0	<sup>149</sup> 817 ± 11	No	<sup>28</sup> 717 ± 7	<sup>29</sup> 714 ± 29
121	Samtech InfoNet Limited	samtech	001	2019-10-15	288082	<sup>134</sup> 2056 ± 0	<sup>35</sup> 294 ± 3	No	<sup>138</sup> 7694 ± 59	<sup>136</sup> 7678 ± 91
122	Scanovate Ltd.	scanovate	001	2019-11-12	257083	<sup>70</sup> 2048 ± 0	<sup>92</sup> 579 ± 24	No	<sup>148</sup> 14306 ± 352	<sup>151</sup> 16031 ± 538
123	Sensetime Group Ltd	sensetime	002	2018-10-19	531783	<sup>119</sup> 2052 ± 0	<sup>133</sup> 725 ± 3	No	<sup>88</sup> 2546 ± 102	<sup>85</sup> 2371 ± 45
124	Sensetime Group Ltd	sensetime	002	2018-10-19	531783	<sup>128</sup> 2052 ± 0	<sup>146</sup> 797 ± 3	No	<sup>92</sup> 2713 ± 90	<sup>84</sup> 2301 ± 25
125	Momentum Digital Co. Ltd	sertis	000	2019-10-07	265572	<sup>66</sup> 2048 ± 0	<sup>136</sup> 755 ± 0	No	<sup>113</sup> 3883 ± 44	<sup>111</sup> 3884 ± 66
126	Shaman Software	shaman	000	2017-12-05	0	<sup>162</sup> 4096 ± 0	<sup>113</sup> 653 ± 16	No	<sup>4</sup> 380 ± 25	<sup>5</sup> 379 ± 31
127	Shaman Software	shaman	001	2018-01-13	0	<sup>159</sup> 4096 ± 0	<sup>36</sup> 294 ± 2	No	<sup>20</sup> 635 ± 19	<sup>7</sup> 441 ± 25
128	Shanghai University - Shanghai Film Academy	shu	001	2019-06-17	329513	<sup>111</sup> 2048 ± 0	<sup>96</sup> 612 ± 5	No	<sup>91</sup> 2619 ± 19	<sup>94</sup> 2987 ± 143
129	Shenzhen Inst. Adv. Integrated Tech. CAS	SIAT	002	2018-06-13	486842	<sup>129</sup> 2052 ± 0	<sup>91</sup> 579 ± 0	No	<sup>30</sup> 769 ± 13	<sup>31</sup> 750 ± 13
130	Shenzhen Inst. Adv. Integrated Tech. CAS	SIAT	004	2019-03-01	940063	<sup>166</sup> 4100 ± 0	<sup>120</sup> 670 ± 0	No	<sup>115</sup> 4013 ± 45	<sup>110</sup> 3782 ± 173
131	Shanghai Jiao Tong University	sytu	001	2019-09-27	347115	<sup>63</sup> 2048 ± 0	<sup>111</sup> 651 ± 4	No	<sup>172</sup> 2674654 ± 64798	<sup>172</sup> 2376946 ± 202419
132	Smilart	smilart	002	2018-02-06	111826	<sup>32</sup> 1024 ± 0	<sup>12</sup> 176 ± 16	No	<sup>154</sup> 18784 ± 136	<sup>155</sup> 18795 ± 151

Notes	
1	The configuration size does not capture static data included in libraries. We do not count these because some algorithms include common ancilliary libraries for image processing (e.g. openCV) or numerical computation (e.g. blas).
2	The median template creation times are measured on Intel®Xeon®CPU E5-2630 v4 @ 2.20GHz processors or, for GPU-enabled implementations, NVidia Tesla K40.
3	The comparison durations, in nanoseconds, are estimated using std::chrono::high_resolution_clock which on the machine in (2) counts 1ns clock ticks. Precision is somewhat worse than that however. The ± value is the median absolute deviation times 1.48 for Normal consistency.

Table 3: Summary of algorithms and properties included in this report. The red superscripts give ranking for the quantity in that column.

	Developer	Short	Seq.	Validation	Config <sup>1</sup>	Template		GPU	Comparison Time (ns) <sup>3</sup>	
	Name	Name	Num.	Date	Data (KB)	Size (B)	Time (ms) <sup>2</sup>		Genuine	Impostor
133	Smilart	smilart	003	2018-06-18	67339	<sup>16</sup> 512 ± 0	<sup>14</sup> 180 ± 12	No	<sup>60</sup> 1395 ± 74	<sup>44</sup> 1027 ± 66
134	Star Hybrid Limited	starhybrid	001	2019-06-19	100509	<sup>79</sup> 2048 ± 0	<sup>50</sup> 358 ± 82	No	<sup>44</sup> 1075 ± 51	<sup>47</sup> 1078 ± 53
135	Synesis	synesis	005	2019-06-06	146509	<sup>95</sup> 2048 ± 0	<sup>18</sup> 211 ± 9	No	<sup>13</sup> 599 ± 23	<sup>15</sup> 581 ± 32
136	Synesis	synesis	006	2019-10-10	731941	<sup>168</sup> 4104 ± 0	<sup>89</sup> 547 ± 1	No	<sup>129</sup> 5658 ± 17	<sup>128</sup> 5603 ± 148
137	Synology Inc	synology	000	2019-10-23	221021	<sup>71</sup> 2048 ± 0	<sup>62</sup> 425 ± 25	No	<sup>158</sup> 23628 ± 206	<sup>162</sup> 29262 ± 4987
138	Tech5 SA	tech5	002	2019-03-01	1150887	<sup>48</sup> 1280 ± 0	<sup>142</sup> 780 ± 10	No	<sup>62</sup> 1406 ± 120	<sup>45</sup> 1048 ± 57
139	Tech5 SA	tech5	003	2019-08-19	1427464	<sup>50</sup> 1536 ± 0	<sup>167</sup> 937 ± 39	No	<sup>57</sup> 1313 ± 35	<sup>63</sup> 1360 ± 41
140	Tevian	tevia	004	2019-03-01	863474	<sup>81</sup> 2048 ± 0	<sup>71</sup> 506 ± 30	No	<sup>7</sup> 474 ± 31	<sup>4</sup> 326 ± 20
141	Tevian	tevia	005	2019-09-21	921043	<sup>103</sup> 2048 ± 0	<sup>105</sup> 642 ± 32	No	<sup>95</sup> 3097 ± 31	<sup>107</sup> 3700 ± 278
142	TigerIT Americas LLC	tiger	002	2018-06-13	341638	<sup>137</sup> 2056 ± 0	<sup>57</sup> 393 ± 20	No	<sup>82</sup> 2135 ± 29	<sup>80</sup> 2137 ± 38
143	TigerIT Americas LLC	tiger	003	2018-10-16	426164	<sup>131</sup> 2056 ± 0	<sup>66</sup> 458 ± 21	No	<sup>79</sup> 2031 ± 35	<sup>77</sup> 2029 ± 38
144	TongYi Transportation Technology	tongyi	005	2019-06-12	1140701	<sup>146</sup> 2089 ± 0	<sup>9</sup> 165 ± 1	No	<sup>155</sup> 18924 ± 65	<sup>156</sup> 20158 ± 103
145	Toshiba	toshiba	002	2018-10-19	813606	<sup>53</sup> 1560 ± 0	<sup>81</sup> 541 ± 0	No	<sup>105</sup> 3521 ± 369	<sup>88</sup> 2449 ± 124
146	Toshiba	toshiba	003	2019-03-01	984125	<sup>54</sup> 1560 ± 0	<sup>80</sup> 540 ± 0	No	<sup>87</sup> 2390 ± 41	<sup>86</sup> 2407 ± 81
147	Trueface.ai	trueface	000	2019-10-08	255123	<sup>108</sup> 2048 ± 0	<sup>51</sup> 368 ± 11	No	<sup>94</sup> 3040 ± 26	<sup>96</sup> 3144 ± 51
148	TUPU Technology Co. Ltd	tuputech	000	2019-10-11	11476	<sup>76</sup> 2048 ± 0	<sup>7</sup> 124 ± 7	No	<sup>161</sup> 26308 ± 269	<sup>161</sup> 28022 ± 2594
149	ULSee Inc	ulsee	001	2019-07-31	370519	<sup>105</sup> 2048 ± 0	<sup>115</sup> 654 ± 2	No	<sup>133</sup> 6065 ± 94	<sup>131</sup> 6228 ± 77
150	Shanghai Ulucu Electronics Technology Co. Ltd	uluface	002	2019-07-10	0	<sup>92</sup> 2048 ± 0	<sup>160</sup> 873 ± 42	No	<sup>156</sup> 19207 ± 1114	<sup>154</sup> 18501 ± 274
151	Shanghai Ulucu Electronics Technology Co. Ltd	uluface	003	2019-11-12	97357	<sup>155</sup> 3072 ± 0	<sup>170</sup> 970 ± 15	No	<sup>162</sup> 27666 ± 198	<sup>163</sup> 29560 ± 244
152	China University of Petroleum	upc	001	2019-06-05	0	<sup>42</sup> 1052 ± 0	<sup>87</sup> 551 ± 15	No	<sup>90</sup> 3114 ± 44	<sup>97</sup> 3165 ± 97
153	VCognition	vcog	002	2017-06-12	3229434	<sup>172</sup> 61504 ± 5	<sup>49</sup> 357 ± 25	No	<sup>170</sup> 296154 ± 3077	<sup>170</sup> 296436 ± 4183
154	Visidon	visidon	001	2019-02-26	170262	<sup>122</sup> 2052 ± 0	<sup>43</sup> 316 ± 6	No	<sup>53</sup> 1258 ± 38	<sup>51</sup> 1148 ± 109
155	Veridas Digital Authentication Solutions S.L.	veridas	001	2019-03-01	196540	<sup>85</sup> 2048 ± 0	<sup>121</sup> 671 ± 21	No	<sup>130</sup> 5748 ± 20	<sup>133</sup> 7111 ± 148
156	Veridas Digital Authentication Solutions S.L.	veridas	000	2019-03-01	193466	<sup>22</sup> 512 ± 0	<sup>118</sup> 669 ± 20	No	<sup>71</sup> 1733 ± 81	<sup>75</sup> 1934 ± 44
157	Via Technologies Inc.	via	000	2019-07-08	124422	<sup>101</sup> 2048 ± 0	<sup>128</sup> 707 ± 8	No	<sup>40</sup> 966 ± 28	<sup>42</sup> 1021 ± 44
158	Videonetics Technology Pvt Ltd	videonetics	001	2019-06-19	30875	<sup>14</sup> 512 ± 0	<sup>26</sup> 262 ± 3	No	<sup>48</sup> 1153 ± 38	<sup>50</sup> 1142 ± 65
159	Vigilant Solutions	vigilant	006	2019-03-01	343048	<sup>52</sup> 1548 ± 0	<sup>157</sup> 841 ± 8	No	<sup>36</sup> 939 ± 32	<sup>27</sup> 711 ± 37
160	Vigilant Solutions	vigilant	007	2019-06-27	255600	<sup>51</sup> 1548 ± 0	<sup>70</sup> 493 ± 6	No	<sup>32</sup> 803 ± 35	<sup>32</sup> 800 ± 40
161	Beijing Vion Technology Inc	vion	000	2018-10-19	228219	<sup>125</sup> 2052 ± 0	<sup>45</sup> 333 ± 1	No	<sup>164</sup> 39839 ± 3561	<sup>160</sup> 26830 ± 2241
162	Vision-Box	visionbox	000	2019-02-26	176501	<sup>110</sup> 2048 ± 0	<sup>38</sup> 304 ± 7	No	<sup>68</sup> 1648 ± 57	<sup>54</sup> 1192 ± 42
163	Vision-Box	visionbox	001	2019-03-01	256869	<sup>102</sup> 2048 ± 0	<sup>171</sup> 983 ± 7	No	<sup>49</sup> 1161 ± 22	<sup>52</sup> 1154 ± 20
164	VisionLabs	visionlabs	006	2019-03-01	353044	<sup>21</sup> 512 ± 0	<sup>28</sup> 270 ± 0	No	<sup>26</sup> 698 ± 19	<sup>30</sup> 734 ± 28
165	VisionLabs	visionlabs	007	2019-06-12	357204	<sup>19</sup> 512 ± 0	<sup>29</sup> 272 ± 0	No	<sup>39</sup> 965 ± 41	<sup>41</sup> 972 ± 31
166	Vocord	vocord	006	2019-03-01	559457	<sup>28</sup> 768 ± 0	<sup>161</sup> 886 ± 1	No	<sup>78</sup> 2020 ± 72	<sup>76</sup> 1969 ± 62
167	Vocord	vocord	007	2019-06-06	587489	<sup>55</sup> 1664 ± 0	<sup>143</sup> 780 ± 2	No	<sup>90</sup> 2593 ± 83	<sup>90</sup> 2526 ± 59
168	Winsense Co. Ltd	winsense	000	2019-06-17	270819	<sup>45</sup> 1280 ± 0	<sup>33</sup> 283 ± 1	No	<sup>65</sup> 1551 ± 31	<sup>66</sup> 1532 ± 42
169	Winsense Co. Ltd	winsense	001	2019-10-16	264428	<sup>46</sup> 1280 ± 0	<sup>140</sup> 768 ± 9	No	<sup>98</sup> 3143 ± 32	<sup>118</sup> 4230 ± 226
170	X-Laboratory	x-laboratory	000	2019-09-03	520020	<sup>141</sup> 2056 ± 0	<sup>156</sup> 832 ± 38	No	<sup>102</sup> 3380 ± 91	<sup>101</sup> 3314 ± 253
171	Zhuhai Yisheng Electronics Technology	yisheng	004	2018-06-12	486351	<sup>158</sup> 3704 ± 0	<sup>52</sup> 378 ± 12	No	<sup>25</sup> 693 ± 137	<sup>12</sup> 526 ± 34
172	Shanghai Yitu Technology	yitu	003	2019-03-01	1525719	<sup>144</sup> 2082 ± 0	<sup>158</sup> 860 ± 0	No	<sup>153</sup> 18305 ± 71	<sup>153</sup> 18286 ± 62

Notes	
1	The configuration size does not capture static data included in libraries. We do not count these because some algorithms include common ancillary libraries for image processing (e.g. openCV) or numerical computation (e.g. blas).
2	The median template creation times are measured on Intel®Xeon®CPU E5-2630 v4 @ 2.20GHz processors or, for GPU-enabled implementations, NVidia Tesla K40.
3	The comparison durations, in nanoseconds, are estimated using std::chrono::high_resolution_clock which on the machine in (2) counts 1ns clock ticks. Precision is somewhat worse than that however. The ± value is the median absolute deviation times 1.48 for Normal consistency.

Table 4: Summary of algorithms and properties included in this report. The red superscripts give ranking for the quantity in that column.

		FALSE NON-MATCH RATE (FNMR)															
Algorithm		CONSTRAINED, COOPERATIVE										LESS CONSTRAINED, NON-COOP.					
Name		VISAMC		VISA		VISA		MUGSHOT		MUGSHOT12+YRS		VISABORDER		WILD		CHILDEXP	
FMR		0.0001		1E-06		0.0001		1E-05		1E-05		1E-06		0.0001		0.01	
1	3divi-003	0.0318	124	0.0588	124	0.0097	115	0.0389	126	0.0639	122	0.0619	108	0.0867	117	0.5365	25
2	3divi-004	0.0095	43	0.0153	47	0.0049	66	0.0097	45	0.0145	42	0.0175	51	0.0665	110	-	-
3	adera-001	0.1021	140	0.1757	137	0.0368	139	0.1823	146	0.2967	143	0.1714	121	0.1965	133	0.7202	52
4	aimall-001	0.0176	97	0.0324	102	0.0074	103	0.0225	109	0.0407	105	-	-	0.0344	67	-	-
5	aiunionface-000	0.0104	50	0.0154	49	0.0051	70	0.0082	33	0.0122	30	0.0141	33	0.0306	45	-	-
6	alchera-000	0.0165	92	0.0243	84	0.0086	108	0.0125	77	0.0186	71	0.0204	59	0.0370	74	-	-
7	alchera-001	0.0183	99	0.0299	96	0.0078	104	0.0142	83	0.0234	86	0.0239	70	0.0372	75	-	-
8	allgovision-000	0.0346	126	0.0527	120	0.0210	129	0.0232	111	0.0339	98	-	-	0.0607	106	-	-
9	alphaface-001	0.0065	23	0.0097	22	0.0025	24	0.0039	4	0.0063	7	0.0083	8	0.0280	9	-	-
10	amplifiedgroup-001	0.5034	160	0.5848	160	0.2999	162	0.6973	160	0.8316	157	0.7807	135	0.4250	150	-	-
11	anke-003	0.0131	70	0.0213	68	0.0056	74	0.0094	42	0.0175	64	0.0134	32	0.0302	37	-	-
12	anke-004	0.0080	36	0.0154	48	0.0031	32	0.0073	21	0.0112	24	0.0102	18	0.0288	23	0.3577	4
13	anyvision-002	0.0660	134	0.0898	130	0.0387	140	0.0928	139	0.1512	135	-	-	0.2227	135	0.6960	45
14	anyvision-004	0.0267	119	0.0385	115	0.0081	106	0.0258	115	0.0487	116	-	-	0.0470	94	0.4633	12
15	asusaics-000	0.0125	66	0.0209	67	0.0043	50	0.0085	34	0.0134	36	0.0143	35	0.0295	30	-	-
16	aware-003	0.0793	136	0.1161	135	0.0288	137	0.1028	140	0.1708	138	0.1698	120	0.3180	146	0.8512	65
17	aware-004	0.0690	135	0.0949	133	0.0257	132	0.0837	137	0.1436	133	0.1171	118	0.0516	100	-	-
18	awiros-001	0.4044	155	0.4622	154	0.2880	161	0.5530	155	0.6518	152	0.2008	122	0.5584	152	-	-
19	ayonix-000	0.4351	157	0.4872	155	0.2299	156	0.6150	157	0.7510	154	0.6557	133	0.3635	147	0.8434	63
20	bm-001	0.7431	166	0.9494	167	0.6188	167	0.9586	164	0.9843	161	0.9049	139	0.9935	156	0.8845	70
21	camvi-002	0.0125	67	0.0221	73	0.0049	68	0.0089	38	0.0145	44	0.0142	34	0.0288	22	0.5760	31
22	camvi-004	0.0171	95	0.0316	101	0.0049	65	0.0042	6	0.0049	3	0.0097	17	0.0284	15	-	-
23	ceiec-001	0.0328	125	0.0475	118	0.0163	124	0.0295	121	0.0478	115	0.0621	109	0.0847	113	-	-
24	ceiec-002	0.0161	90	0.0193	62	0.0124	121	0.0122	74	0.0164	59	0.0270	75	0.0465	93	0.5156	22
25	chtface-001	0.9993	170	0.9994	170	0.9993	170	0.9999	167	-	-	1.0000	142	0.9980	157	-	-
26	cogent-003	0.0091	39	0.0188	59	0.0032	33	0.0098	47	0.0132	35	0.0187	54	0.0406	81	-	-
27	cogent-004	0.0064	22	0.0116	33	0.0024	23	0.0096	43	0.0134	37	0.0157	39	0.0379	76	0.7177	51
28	cognitec-000	0.0116	58	0.0177	53	0.0036	39	0.0118	70	0.0167	61	0.0285	80	0.0953	120	0.8365	62
29	cognitec-001	0.0126	68	0.0185	58	0.0047	61	0.0120	72	0.0168	62	0.0270	74	0.0598	105	-	-
30	ctcbank-000	0.0168	93	0.0250	89	0.0064	83	0.0146	86	0.0224	81	0.0211	61	1.0000	165	0.8803	68
31	ctcbank-001	0.0155	86	0.0235	81	0.0060	79	0.0148	89	0.0243	88	0.0207	60	1.0000	167	-	-
32	cyberextruder-001	0.1972	147	0.2547	145	0.0755	148	0.4686	154	0.6387	151	-	-	0.1747	130	0.7804	60
33	cyberextruder-002	0.0811	137	0.1336	136	0.0265	134	0.1465	144	0.2266	142	-	-	0.1000	123	0.6105	35
34	cyberlink-002	0.0114	57	0.0195	63	0.0044	51	0.0101	51	0.0163	56	0.0160	40	0.0298	34	0.5003	18
35	cyberlink-003	0.0118	60	0.0192	61	0.0042	47	0.0098	48	0.0161	54	0.0153	38	0.0303	39	-	-
36	dahua-002	0.0129	69	0.0157	50	0.0090	111	0.0116	67	0.0153	48	0.0134	31	0.0323	55	-	-
37	dahua-003	0.0052	12	0.0068	10	0.0023	22	0.0056	11	0.0062	6	0.0113	24	0.0285	16	-	-
38	deepglint-001	0.0040	6	0.0062	7	0.0014	8	0.0047	7	0.0067	8	0.0069	4	0.0278	6	0.4006	7
39	deepsea-001	0.0136	75	0.0215	70	0.0071	100	0.0142	84	0.0214	77	0.0163	44	0.0347	68	0.5606	29
40	dermalog-005	0.1526	145	0.1823	140	0.0658	146	0.2580	148	0.4018	145	-	-	0.0855	115	0.6842	42
41	dermalog-006	0.0253	117	0.0369	113	0.0172	126	0.0171	97	0.0283	94	-	-	0.0623	108	0.5852	32
42	didiglobalface-001	0.0055	15	0.0092	18	0.0016	9	0.0030	1	0.0045	1	0.0088	11	0.0282	14	-	-
43	digitalbarriers-002	0.3360	153	0.3690	150	0.0968	151	0.0877	138	0.1557	136	0.0971	117	0.0436	87	-	-
44	dsk-000	0.1526	144	0.2169	142	0.0765	149	0.3787	152	0.5426	150	0.3115	127	0.2201	134	0.7313	54

Table 5: FNMR is the proportion of mated comparisons below a threshold set to achieve the FMR given in the header on the fourth row. FMR is the proportion of impostor comparisons at or above that threshold. The light grey values give rank over all algorithms in that column. The pink column uses only same-sex impostors; others are selected regardless of demographics. The exception, in the green column, uses "matched-covariates" i.e. impostors of the same sex, age group, and country of birth. The pink column includes effects of extended ageing. Missing entries for border, visa, mugshot and wild images generally mean the algorithm did not run to completion. For child exploitation, missing entries arise because NIST executes those runs only infrequently.



		FALSE NON-MATCH RATE (FNMR)														
Algorithm		CONSTRAINED, COOPERATIVE						LESS CONSTRAINED, NON-COOP.								
Name	VisAMC	VisA		VisA	MUGSHOT	MUGSHOT12+YRS	VisABORDER	WILD	CHILDEXP							
FMR	0.0001	1E-06		0.0001	1E-05	1E-05	1E-06	0.0001	0.01							
45	einetworks-000	0.0099	46	0.0180	55	0.0047	60	0.0088	36	0.0140	40	0.0130	29	0.0293	29	-
46	everai-002	0.0104	53	0.0159	51	0.0041	46	0.0063	17	0.0112	25	0.0182	52	0.0294	27	-
47	everai-paravision-003	0.0034	2	0.0050	3	0.0011	3	0.0036	3	0.0052	4	0.0092	13	0.0278	7	0.2669
48	f8-001	0.0249	116	0.0336	104	0.0182	127	0.0178	99	0.0232	85	0.0303	87	0.0475	95	0.5272
49	facesoft-000	0.0085	38	0.0112	32	0.0032	35	0.0064	18	0.0107	21	0.0091	12	0.0275	3	0.4992
50	glory-001	0.0902	138	0.1082	134	0.0410	141	0.1642	145	0.2065	141	-	-	0.4261	151	0.8831
51	glory-002	0.0241	111	0.0311	100	0.0188	128	0.0116	68	0.0151	47	-	-	0.1265	126	-
52	gorilla-003	0.0165	91	0.0291	94	0.0053	71	0.0205	106	0.0437	108	0.0297	85	0.0359	72	0.9756
53	gorilla-004	0.0138	76	0.0239	83	0.0049	67	0.0243	113	0.0444	109	0.0275	77	0.0287	21	-
54	hik-001	0.0096	44	0.0125	36	0.0036	41	0.0093	41	0.0164	58	0.0108	21	0.0271	1	-
55	hr-001	0.0044	9	0.0072	12	0.0019	14	0.0073	23	0.0108	22	0.0125	26	0.0303	38	0.5499
56	hr-002	0.0043	7	0.0059	5	0.0017	11	0.0054	8	0.0076	10	0.0076	6	0.0338	65	-
57	id3-003	0.0361	127	0.0757	127	0.0104	119	0.0292	119	0.0476	112	0.0447	99	0.0848	114	0.5865
58	id3-004	0.0198	106	0.0344	107	0.0084	107	0.0238	112	0.0423	107	0.0289	82	-	-	-
59	idemia-004	0.0160	89	0.0244	86	0.0065	85	0.0199	104	0.0354	101	0.0268	73	0.0309	48	-
60	idemia-005	0.0132	71	0.0216	71	0.0057	76	0.0121	73	0.0218	80	0.0215	63	0.0294	28	-
61	iit-000	0.1516	143	0.1981	141	0.0620	145	0.0828	136	0.1442	134	0.2214	125	-	-	-
62	iit-001	0.0104	51	0.0179	54	0.0048	64	0.0099	50	0.0142	41	0.1222	119	0.3092	145	0.4836
63	imagus-000	0.0642	132	0.0882	128	0.0330	138	0.0497	129	0.0905	126	0.0848	113	0.1158	124	0.6936
64	imagus-001	0.0245	113	0.0407	116	0.0091	112	0.0257	114	0.0497	118	0.0514	102	0.0971	121	-
65	imperial-000	0.0067	26	0.0108	30	0.0022	20	0.0080	29	0.0134	38	0.0087	10	0.0281	11	-
66	imperial-002	0.0058	17	0.0081	15	0.0027	25	0.0055	10	0.0085	13	0.0083	9	0.0273	2	-
67	incode-004	0.0077	34	0.0132	38	0.0034	37	0.0096	44	0.0160	52	0.0171	48	0.0313	50	0.5102
68	incode-005	0.0111	56	0.0189	60	0.0042	48	0.0156	94	0.0304	96	0.0195	57	0.0562	104	-
69	innovativetechnologyltd-001	0.0578	130	0.0938	132	0.0258	133	0.0501	130	0.0981	127	-	-	0.0449	89	-
70	innovatrics-004	0.0194	103	0.0292	95	0.0068	93	0.0344	123	0.0617	121	0.0562	105	0.0454	92	0.4650
71	innovatrics-006	0.0058	18	0.0089	17	0.0021	17	0.0061	16	0.0096	18	0.0096	16	0.0281	10	-
72	intellicloudai-001	0.0142	79	0.0234	80	0.0064	84	0.0092	40	0.0145	43	0.0162	42	0.0409	82	-
73	intellifusion-001	0.0072	30	0.0094	20	0.0028	29	0.0056	12	0.0085	14	0.0111	23	0.0289	24	-
74	intellivision-001	0.1335	142	0.2205	143	0.0417	142	0.1090	142	0.1670	137	-	-	0.2445	137	0.7766
75	intellivision-002	0.1000	139	0.1775	138	0.0265	135	0.0610	133	0.1009	128	0.0805	112	0.0768	112	-
76	intelresearch-000	0.0307	122	0.0578	123	0.0093	113	0.0385	125	0.0751	125	0.0409	94	0.0324	56	-
77	intsymsu-000	0.0135	73	0.0204	64	0.0069	95	0.0112	62	0.0161	53	0.0148	36	0.2330	136	-
78	intsymsu-001	0.9543	169	0.9888	169	0.9165	169	0.9923	165	-	-	0.9977	140	0.7871	153	-
79	iqface-000	0.0091	40	0.0143	42	0.0043	49	0.0075	26	0.0110	23	0.0171	49	0.0381	77	0.6490
80	isap-001	0.5092	161	0.6588	162	0.2338	158	0.6899	159	0.7978	155	0.7200	134	0.1931	132	-
81	isityou-000	0.5682	163	0.7033	163	0.4145	165	1.0000	168	-	-	-	-	1.0000	161	1.0000
82	isystems-001	0.0149	84	0.0245	87	0.0067	90	0.0138	82	0.0210	76	-	-	0.0524	103	0.5152
83	isystems-002	0.0118	59	0.0182	57	0.0066	86	0.0111	59	0.0162	55	-	-	0.0516	101	0.4876
84	itmo-005	0.0182	98	0.0345	108	0.0067	91	0.0181	100	0.0348	100	-	-	0.0433	85	0.4808
85	itmo-006	0.0125	65	0.0220	72	0.0046	56	0.0149	90	0.0266	93	0.0233	66	0.0329	59	-
86	kakao-001	0.4553	159	0.5532	159	0.2034	155	0.6580	158	0.8150	156	0.4831	131	1.0000	171	-
87	kakao-002	0.0625	131	0.1779	139	0.0168	125	0.0791	135	0.1381	132	0.0636	110	1.0000	163	1.0000
88	kedacom-000	0.0055	14	0.0081	16	0.0027	26	0.0111	61	0.0120	28	0.0415	95	0.2511	139	0.7650

Table 6: FNMR is the proportion of mated comparisons below a threshold set to achieve the FMR given in the header on the fourth row. FMR is the proportion of impostor comparisons at or above that threshold. The light grey values give rank over all algorithms in that column. The pink column uses only same-sex impostors; others are selected regardless of demographics. The exception, in the green column, uses “matched-covariates” i.e. impostors of the same sex, age group, and country of birth. The pink column includes effects of extended ageing. Missing entries for border, visa, mugshot and wild images generally mean the algorithm did not run to completion. For child exploitation, missing entries arise because NIST executes those runs only infrequently.

		FALSE NON-MATCH RATE (FNMR)															
Algorithm		CONSTRAINED, COOPERATIVE										LESS CONSTRAINED, NON-COOP.					
Name		VISAMC		VISA		VISA		MUGSHOT		MUGSHOT12+YRS		VISABORDER		WILD		CHILDEXP	
FMR		0.0001		1E-06		0.0001		1E-05		1E-05		1E-06		0.0001		0.01	
89	kneron-003	0.0542	129	0.0902	131	0.0218	130	0.0346	124	0.0562	120	0.0919	115	0.3053	144	0.6962	46
90	lookman-002	0.0297	121	0.0547	122	0.0102	118	0.0339	122	0.0562	119	0.0614	107	0.2640	142	-	-
91	lookman-004	0.0074	32	0.0099	24	0.0037	42	0.0124	76	0.0149	45	0.0430	98	0.2516	140	0.7664	58
92	luxand-000	-	-	-	-	-	-	0.4053	153	0.5365	149	-	-	-	-	-	-
93	megvii-001	0.0157	87	0.0244	85	0.0045	55	0.0392	127	0.0671	123	-	-	0.0916	119	0.4418	10
94	megvii-002	0.0104	52	0.0145	44	0.0036	40	0.0225	108	0.0345	99	-	-	0.0692	111	0.3013	2
95	meiya-001	0.0171	94	0.0275	93	0.0066	88	0.0159	95	0.0261	92	0.0311	88	0.0363	73	-	-
96	microfocus-001	0.4482	158	0.5524	158	0.2309	157	0.7256	161	0.8416	158	-	-	0.2567	141	0.6890	43
97	microfocus-002	0.3605	154	0.5057	156	0.1566	154	0.5783	156	0.7223	153	-	-	0.1582	129	0.6517	39
98	mt-000	0.0100	47	0.0170	52	0.0047	59	0.0074	25	0.0118	27	0.0127	27	0.0326	58	0.3773	6
99	mvision-001	0.0191	101	0.0233	78	0.0131	122	0.0204	105	0.0356	102	-	-	0.0431	84	-	-
100	neurotechnology-005	0.0141	78	0.0300	97	0.0051	69	0.0108	57	0.0163	57	0.0204	58	0.0332	60	-	-
101	neurotechnology-006	0.0098	45	0.0136	39	0.0040	45	0.0105	54	0.0182	68	0.0164	46	0.0303	40	0.5911	34
102	nodeflux-001	1.0000	171	1.0000	171	1.0000	171	1.0000	172	-	-	0.5169	132	1.0000	168	-	-
103	nodeflux-002	0.0186	100	0.0340	105	0.0070	97	0.0261	116	0.0451	111	0.0548	104	0.0299	35	-	-
104	notiontag-000	0.6669	164	0.7885	164	0.3222	164	0.3715	151	0.4978	148	0.8571	137	0.1807	131	0.6479	37
105	ntechlab-006	0.0078	35	0.0111	31	0.0021	18	0.0112	63	0.0227	84	0.0108	20	0.0275	4	-	-
106	ntechlab-007	0.0056	16	0.0076	13	0.0018	12	0.0073	24	0.0128	33	0.0079	7	0.0276	5	0.3316	3
107	pixelall-002	0.0193	102	0.0340	106	0.0066	87	0.0127	79	0.0209	74	0.0234	68	0.0342	66	0.8963	71
108	pixelall-003	0.0074	33	0.0118	34	0.0032	34	0.0057	13	0.0079	11	0.0121	25	0.0285	18	-	-
109	psl-002	0.0107	54	0.0180	56	0.0048	63	0.0089	37	0.0120	29	0.0790	111	0.0295	31	-	-
110	psl-003	0.0065	24	0.0099	25	0.0028	27	0.0055	9	0.0075	9	1.0000	143	0.0296	33	-	-
111	pyramid-000	0.0136	74	0.0233	79	0.0056	73	0.0117	69	0.0192	73	0.0185	53	0.0304	42	-	-
112	rankone-007	0.0197	105	0.0366	112	0.0057	77	0.0113	65	0.0177	66	0.0286	81	0.0450	90	0.6686	40
113	rankone-008	0.0124	63	0.0232	77	0.0045	54	0.0082	32	0.0107	20	-	-	0.0420	83	-	-
114	realnetworks-002	0.0248	114	0.0358	109	0.0099	116	0.0513	131	0.1127	129	0.0371	92	0.0334	61	-	-
115	realnetworks-003	0.0259	118	0.0372	114	0.0100	117	0.0541	132	0.1208	131	0.0378	93	0.0335	63	0.5152	20
116	remarkai-000	0.0147	82	0.0257	91	0.0062	82	0.0102	52	0.0158	50	0.0163	45	0.0304	41	-	-
117	remarkai-001	0.0144	80	0.0256	90	0.0061	80	0.0102	53	0.0159	51	0.0162	43	0.0308	47	-	-
118	rokid-000	0.0093	42	0.0145	43	0.0038	43	0.0073	22	0.0102	19	0.0164	47	0.0857	116	-	-
119	saffe-001	0.4339	156	0.5261	157	0.2340	159	0.7539	163	0.8736	160	0.7977	136	0.3887	148	0.8973	72
120	saffe-002	0.0119	62	0.0206	65	0.0054	72	0.0107	56	0.0177	65	0.0244	71	0.0308	46	-	-
121	samtech-001	0.0197	104	0.0365	110	0.0066	89	0.0146	87	0.0241	87	0.0238	69	0.0337	64	-	-
122	scanovate-001	0.0175	96	0.0331	103	0.0061	81	0.0163	96	0.0248	89	-	-	0.4060	149	-	-
123	sensetime-001	0.0063	21	0.0092	19	0.0030	30	0.0130	80	-	-	0.0252	72	1.0000	160	0.6997	47
124	sensetime-002	0.0068	27	0.0098	23	0.0035	38	0.0143	85	-	-	0.0278	79	0.9999	158	0.5309	24
125	sertis-000	0.0118	61	0.0208	66	0.0047	57	0.0080	28	0.0127	31	0.0110	22	0.0285	17	-	-
126	shaman-000	0.9297	168	0.9774	168	0.9128	168	0.9990	166	-	-	0.9999	141	0.9575	155	0.9618	74
127	shaman-001	0.3346	152	0.4616	153	0.1360	153	0.2368	147	0.3723	144	0.3574	129	0.1498	128	0.8990	73
128	shu-001	0.0103	49	0.0140	41	0.0044	52	0.0293	120	0.0688	124	0.0172	50	0.0986	122	0.4590	11
129	siat-002	0.0091	41	0.0126	37	0.0039	44	0.0109	58	0.0190	72	0.0276	78	0.0520	102	0.4277	9
130	siat-004	0.0067	25	0.0099	26	0.0028	28	0.0152	92	-	-	0.0275	76	1.0000	159	-	-
131	situ-001	0.0051	11	0.0080	14	0.0019	13	0.0211	107	0.0446	110	0.0131	30	0.0289	25	-	-
132	smilart-002	0.2440	150	0.3532	149	0.0821	150	-	-	-	-	0.3785	130	-	-	0.6999	48

Table 7: FNMR is the proportion of mated comparisons below a threshold set to achieve the FMR given in the header on the fourth row. FMR is the proportion of impostor comparisons at or above that threshold. The light grey values give rank over all algorithms in that column. The pink column uses only same-sex impostors; others are selected regardless of demographics. The exception, in the green column, uses "matched-covariates" i.e. impostors of the same sex, age group, and country of birth. The pink column includes effects of extended ageing. Missing entries for border, visa, mugshot and wild images generally mean the algorithm did not run to completion. For child exploitation, missing entries arise because NIST executes those runs only infrequently.

		FALSE NON-MATCH RATE (FNMR)															
Algorithm		CONSTRAINED, COOPERATIVE										LESS CONSTRAINED, NON-COOP.					
Name		VISAMC		VISA		VISA		MUGSHOT		MUGSHOT12+YRS		VISABORDER		WILD		CHILDEXP	
FMR		0.0001		1E-06		0.0001		1E-05		1E-05		1E-06		0.0001		0.01	
133	smilart-003	0.6944	165	0.8836	165	0.1088	152	0.0695	134	0.1193	130	0.0894	114	0.1190	125	-	-
134	starhybrid-001	0.0108	55	0.0138	40	0.0058	78	0.0081	30	0.0113	26	0.0152	37	0.0350	70	0.5584	27
135	synesis-005	0.0147	81	0.0226	75	0.0073	102	0.0153	93	0.0226	82	0.0213	62	0.0334	62	0.5601	28
136	synesis-006	0.0070	28	0.0096	21	0.0023	21	0.0107	55	0.0166	60	-	-	0.0292	26	-	-
137	synology-000	0.0149	83	0.0238	82	0.0067	92	0.0148	88	0.0261	91	0.0221	64	-	-	-	-
138	tech5-002	0.0046	10	0.0063	8	0.0009	2	0.0113	66	0.0216	79	0.0233	67	0.0310	49	-	-
139	tech5-003	0.0053	13	0.0070	11	0.0014	7	0.0099	49	0.0185	69	0.0095	15	0.0306	43	-	-
140	tevia-004	0.0228	109	0.0304	98	0.0069	94	0.0226	110	0.0478	113	0.0128	28	0.0394	79	-	-
141	tevia-005	0.0043	8	0.0062	6	0.0020	16	0.0057	14	0.0085	15	0.0070	5	0.0300	36	-	-
142	tiger-002	0.0658	133	0.0889	129	0.0227	131	0.1083	141	0.1766	139	0.0952	116	0.0512	99	0.7862	61
143	tiger-003	0.0313	123	0.0602	126	0.0087	109	0.0188	102	0.0359	103	0.0344	89	0.0482	97	0.5610	30
144	tongyi-005	0.0073	31	0.0146	45	0.0019	15	0.0187	101	0.0421	106	0.0161	41	0.0399	80	0.6195	36
145	toshiba-002	0.0134	72	0.0222	74	0.0048	62	0.0097	46	0.0154	49	-	-	0.0434	86	0.7103	49
146	toshiba-003	0.0125	64	0.0214	69	0.0047	58	0.0085	35	0.0131	34	-	-	0.0282	12	-	-
147	trueface-000	0.0249	115	0.4321	152	0.0069	96	0.0119	71	0.0180	67	0.0297	86	0.0614	107	-	-
148	tuputech-000	0.3218	151	0.3696	151	0.2779	160	-	-	-	-	0.3237	128	0.9415	154	-	-
149	ulsee-001	0.0151	85	0.0246	88	0.0080	105	0.0113	64	0.0185	70	0.0187	55	0.0316	52	-	-
150	ulface-002	0.0081	37	0.0123	35	0.0033	36	0.0071	20	0.0095	17	0.0107	19	0.0444	88	0.6729	41
151	ulface-003	0.0100	48	0.0150	46	0.0044	53	0.0079	27	0.0128	32	-	-	0.0635	109	-	-
152	upc-001	0.0234	110	0.0519	119	0.0071	99	0.0291	118	0.0490	117	0.0294	83	0.0314	51	0.4224	8
153	vcog-002	0.7522	167	0.9033	166	0.5040	166	-	-	-	-	-	-	-	-	0.7523	55
154	vd-001	0.0243	112	0.0452	117	0.0093	114	0.0271	117	0.0402	104	0.0424	97	0.1389	127	-	-
155	veridas-001	0.1998	149	0.2724	146	0.0742	147	0.2987	150	0.4587	147	0.2599	126	0.0501	98	-	-
156	veridas-002	0.1733	146	0.2257	144	0.0528	144	0.2617	149	0.4147	146	0.2073	124	0.0450	91	-	-
157	via-000	0.0216	108	0.0365	111	0.0088	110	0.0177	98	0.0287	95	0.0296	84	0.0349	69	0.7638	56
158	videonetics-001	0.5483	162	0.6446	161	0.3063	163	0.7517	162	0.8607	159	0.8664	138	0.2986	143	0.7297	53
159	vigilantsolutions-006	0.1264	141	0.3221	147	0.0136	123	0.0150	91	0.0254	90	0.0493	101	0.0321	54	-	-
160	vigilantsolutions-007	0.0202	107	0.0307	99	0.0070	98	0.0136	81	0.0227	83	0.0356	91	0.0306	44	1.0000	160
161	vion-000	0.0419	128	0.0590	125	0.0288	136	0.0422	128	0.0478	114	0.0581	106	0.2479	138	0.8765	67
162	visionbox-000	0.0293	120	0.0541	121	0.0110	120	0.0197	103	0.0339	97	0.0349	90	0.0476	96	-	-
163	visionbox-001	0.0159	88	0.0270	92	0.0072	101	0.0111	60	0.0173	63	0.0190	56	0.0389	78	-	-
164	visionlabs-006	0.0037	3	0.0066	9	0.0012	4	0.0041	5	0.0060	5	0.0061	2	0.0285	19	-	-
165	visionlabs-007	0.0038	4	0.0048	2	0.0012	6	0.0036	2	0.0048	2	0.0057	1	0.0286	20	0.3708	5
166	vocord-006	0.0062	19	0.0102	28	0.0016	10	0.0082	31	0.0151	46	0.0475	100	0.0282	13	-	-
167	vocord-007	0.0039	5	0.0053	4	0.0012	5	0.0061	15	0.0094	16	0.0520	103	0.0280	8	0.8468	64
168	winsense-000	0.0140	77	0.0228	76	0.0056	75	0.0125	78	0.0215	78	0.0226	65	0.0352	71	0.8600	66
169	winsense-001	0.0062	20	0.0099	27	0.0022	19	0.0092	39	0.0210	75	0.0093	14	0.0320	53	-	-
170	x-laboratory-000	0.0071	29	0.0106	29	0.0030	31	0.0123	75	0.0138	39	0.0419	96	0.0295	32	-	-
171	yisheng-004	0.1988	148	0.3329	148	0.0475	143	0.1147	143	0.1849	140	0.2044	123	0.0908	118	0.7152	50
172	yitu-003	0.0015	1	0.0026	1	0.0003	1	0.0066	19	0.0085	12	0.0064	3	0.0325	57	-	-

Table 8: FNMR is the proportion of mated comparisons below a threshold set to achieve the FMR given in the header on the fourth row. FMR is the proportion of impostor comparisons at or above that threshold. The light grey values give rank over all algorithms in that column. The pink column uses only same-sex impostors; others are selected regardless of demographics. The exception, in the green column, uses “matched-covariates” i.e. impostors of the same sex, age group, and country of birth. The pink column includes effects of extended ageing. Missing entries for border, visa, mugshot and wild images generally mean the algorithm did not run to completion. For child exploitation, missing entries arise because NIST executes those runs only infrequently.



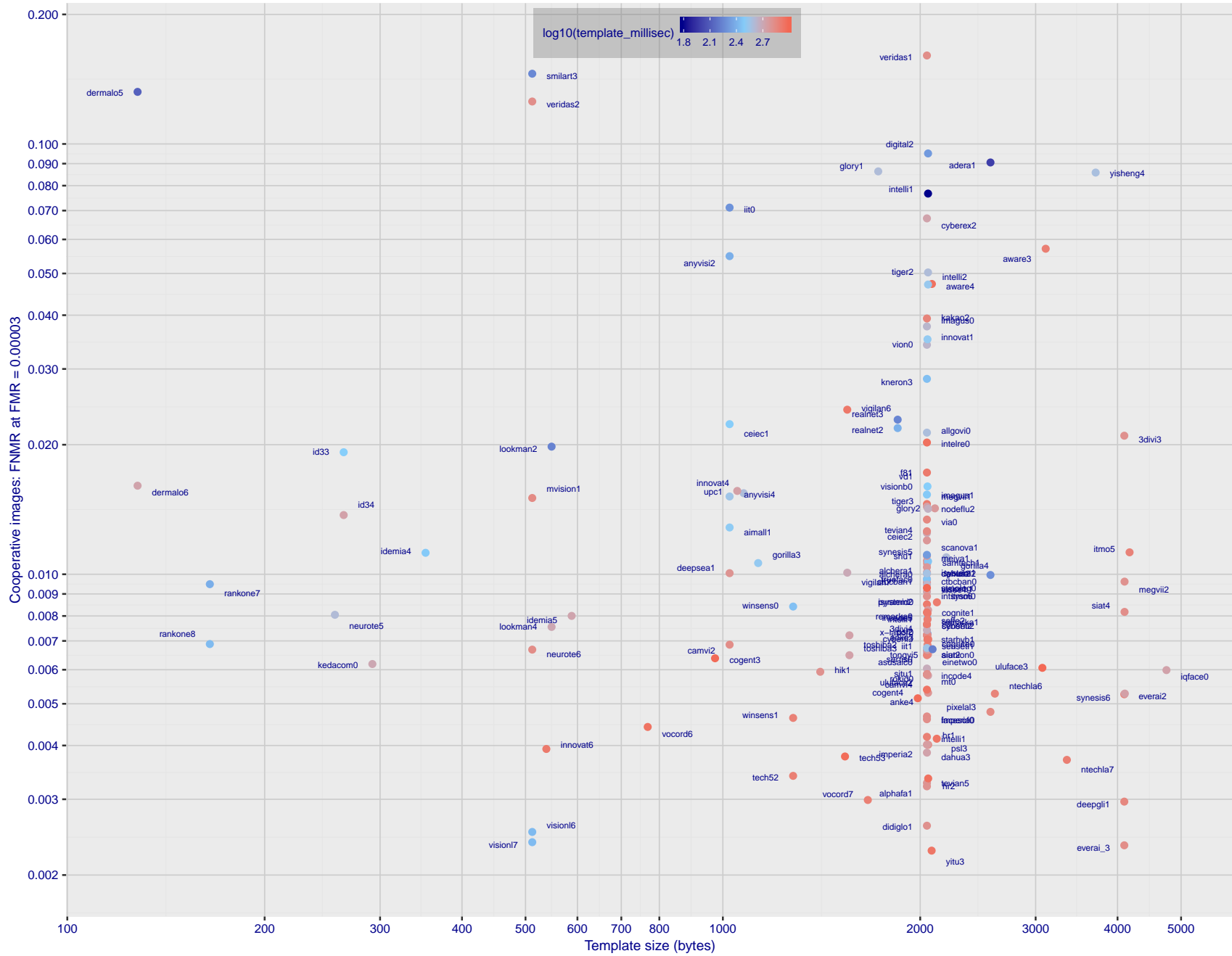


Figure 1: The points show false non-match rates (FNMR) versus the size of the encoded template. FNMR is the geometric mean of FNMR values for visa and mugshot images (from Figs. 29 and 38) at a false match rate (FMR) of 0.0001. The color of the points encodes template generation time - which spans at least one order of magnitude. Durations are measured on a single core of a c. 2016 Intel Xeon CPU E5-2630 v4 running at 2.20GHz. Algorithms with poor FNMR are omitted.

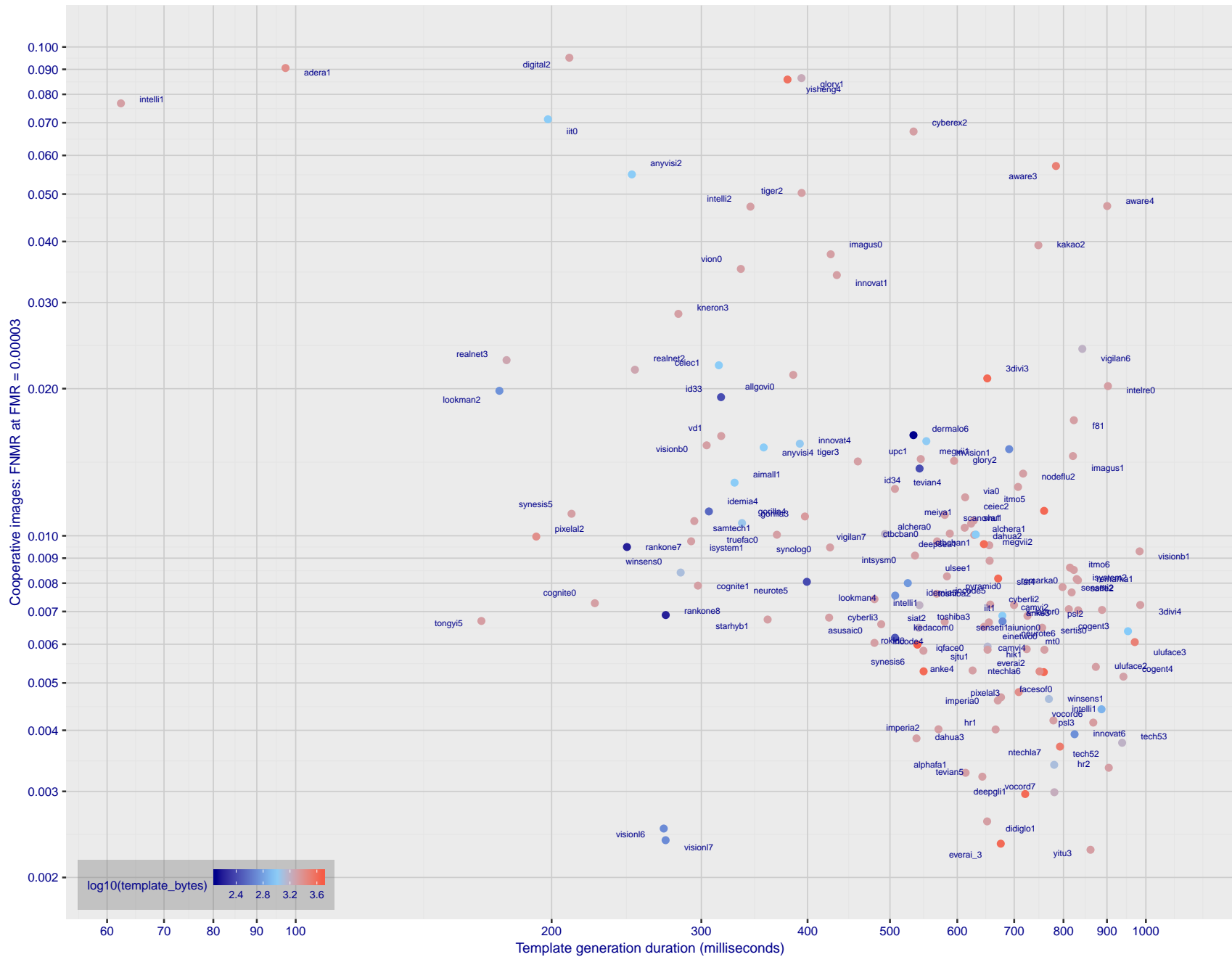


Figure 2: The points show false non-match rates (FNMR) versus the duration of the template generation operation. FNMR is the geometric mean of FNMR values for visa and mugshot images (from Figs. 29 and 38) at a false match rate (FMR) of 0.0001. Template generation time is a median estimated over 640 x 480 pixel portraits. It is measured on a single core of a c. 2016 Intel Xeon CPU E5-2630 v4 running at 2.20GHz. The color of the points encodes template size - which span two orders of magnitude. Algorithms with poor FNMR are omitted.

# 1 Metrics

## 1.1 Core accuracy

Given a vector of  $N$  genuine scores,  $u$ , the false non-match rate (FNMR) is computed as the proportion below some threshold,  $T$ :

$$\text{FNMR}(T) = 1 - \frac{1}{N} \sum_{i=1}^N H(u_i - T) \quad (1)$$

where  $H(x)$  is the unit step function, and  $H(0)$  taken to be 1.

Similarly, given a vector of  $N$  impostor scores,  $v$ , the false match rate (FMR) is computed as the proportion above  $T$ :

$$\text{FMR}(T) = \frac{1}{N} \sum_{i=1}^N H(v_i - T) \quad (2)$$

The threshold,  $T$ , can take on any value. We typically generate a set of thresholds from quantiles of the observed impostor scores,  $v$ , as follows. Given some interesting false match rate range,  $[\text{FMR}_L, \text{FMR}_U]$ , we form a vector of  $K$  thresholds corresponding to FMR measurements evenly spaced on a logarithmic scale

$$T_k = Q_v(1 - \text{FMR}_k) \quad (3)$$

where  $Q$  is the quantile function, and  $\text{FMR}_k$  comes from

$$\log_{10} \text{FMR}_k = \log_{10} \text{FMR}_L + \frac{k}{K} [\log_{10} \text{FMR}_U - \log_{10} \text{FMR}_L] \quad (4)$$

Error tradeoff characteristics are plots of  $\text{FNMR}(T)$  vs.  $\text{FMR}(T)$ . These are plotted with  $\text{FMR}_U \rightarrow 1$  and  $\text{FMR}_L$  as low as is sustained by the number of impostor comparisons,  $N$ . This is somewhat higher than the “rule of three” limit  $3/N$  because samples are not independent, due to re-use of images.

## 2 Datasets

### 2.1 Child exploitation images

- ▷ The number of images is on the order of  $10^4$ .
- ▷ The number of subjects is on the order of  $10^3$ .
- ▷ The number of subjects with two images on the order of  $10^3$ .
- ▷ The images are operational. They are taken from ongoing investigations of child exploitation crimes. The images are arbitrarily unconstrained. Pose varies considerably around all three axes, including subject lying down. Resolution varies very widely. Faces can be occluded by other objects, including hair and hands. Lighting varies, although the images are intended for human viewing. Mis-focus is rare. Images are given to the algorithm without any cropping; faces may occupy widely varying areas.
- ▷ The images are usually large from contemporary cameras. The mean interocular distance (IOD) is 70 pixels.
- ▷ The images are of subjects from several countries, due to the global production of this imagery.
- ▷ The images are of children, from infancy to late adolescence.
- ▷ All of the images are live capture, none are scanned. Many have been cropped.
- ▷ When these images are input to the algorithm, they are labelled as being of type "EXPLOITATION" - see Table 4 of the FRVT API.

### 2.2 Visa images

- ▷ The number of images is on the order of  $10^5$ .
- ▷ The number of subjects is on the order of  $10^5$ .
- ▷ The number of subjects with two images on the order of  $10^4$ .
- ▷ The images have geometry in reasonable conformance with the ISO/IEC 19794-5 Full Frontal image type. Pose is generally excellent.
- ▷ The images are of size 252x300 pixels. The mean interocular distance (IOD) is 69 pixels.
- ▷ The images are of subjects from greater than 100 countries, with significant imbalance due to visa issuance patterns.
- ▷ The images are of subjects of all ages, including children, again with imbalance due to visa issuance demand.
- ▷ Many of the images are live capture. A substantial number of the images are photographs of paper photographs.
- ▷ When these images are input to the algorithm, they are labelled as being of type "ISO" - see Table 4 of the FRVT API.

### 2.3 Visa images II

- ▷ The number of images is on the order of  $10^6$ .
- ▷ The number of subjects is on the order of  $10^6$ .
- ▷ The number of subjects with two images on the order of  $10^6$ .

- ▷ The images have geometry in good conformance with the ISO/IEC 19794-5 Full Frontal image type. Pose is generally excellent.
- ▷ The images are of size 300x300 pixels. The mean interocular distance (IOD) is 61 pixels.
- ▷ The images are of subjects from greater than 100 countries, with significant imbalance due to population and immigration patterns.
- ▷ The images are of subjects of all ages, including children, again with imbalance due to population and immigration patterns and demand.
- ▷ All of the images are live capture.
- ▷ When these images are input to the algorithm, they are labelled as being of type "ISO" - see Table 4 of the FRVT API.

## 2.4 Mugshot images

- ▷ The number of images is on the order of  $10^6$ .
- ▷ The number of subjects is on the order of  $10^6$ .
- ▷ The number of subjects with two images on the order of  $10^6$ .
- ▷ The images have geometry in reasonable conformance with the ISO/IEC 19794-5 Full Frontal image type.
- ▷ The images are of variable sizes. The median IOD is 105 pixels. The mean IOD is 113 pixels. The 1-st, 5-th, 10-th, 25-th, 75-th, 90-th and 99-th percentiles are 34, 58, 70, 87, 121, 161 and 297 pixels.
- ▷ The images are of subjects from the United States.
- ▷ The images are of adults.
- ▷ The images are all live capture.
- ▷ When these images are input to the algorithm, they are labelled as being of type "mugshot" - see Table 4 of the FRVT API.

## 2.5 Webcam images

- ▷ The number of images is on the order of  $10^6$ .
- ▷ The number of subjects is on the order of  $10^6$ .
- ▷ All subjects have a webcam image, and a portrait image.
- ▷ The portrait images are in poor conformance with the ISO/IEC 19794-5 Full Frontal image type.
- ▷ The webcam images are taken with at camera oriented by an attendant toward a cooperating subject. This is done under time constraints so there are role, pitch and yaw angle variation. Also background illumination is sometimes strong, so the face is under exposed. There is sometimes perspective distortion due to close range images.
- ▷ The images have mean IOD of 38 pixels.
- ▷ The images are all live capture.
- ▷ When these images are input to the algorithm, they are labelled as being of type "WILD" - see Table 4 of the FRVT API.

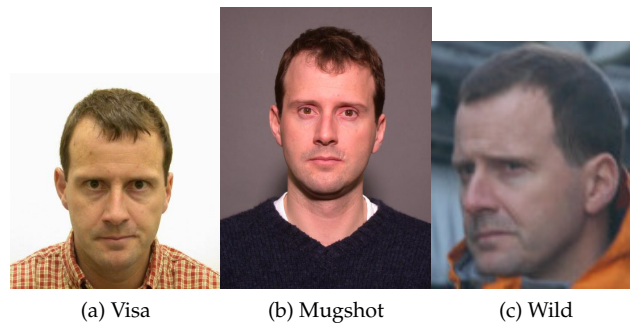


Figure 3: The figure gives simulated samples of image types used in this report.

## 2.6 Wild images

- ▷ The number of images is on the order of  $10^5$ .
- ▷ The number of subjects is on the order of  $10^3$ .
- ▷ The number of subjects with two images on the order of  $10^3$ .
- ▷ The images include many photojournalism-style images. Images are given to the algorithm using a variable but generally tight crop of the head. Resolution varies very widely. The images are very unconstrained, with wide yaw and pitch pose variation. Faces can be occluded, including hair and hands.
- ▷ The images are of adults.
- ▷ All of the images are live capture, none are scanned.
- ▷ When these images are input to the algorithm, they are labelled as being of type "WILD" - see Table 4 of the FRVT API.

## 3 Results

### 3.1 Test goals

- ▷ To state overall accuracy.
- ▷ To compare algorithms.

### 3.2 Test design

**Method:** For visa images:

- ▷ The comparisons are of visa photos against visa photos.
- ▷ The number of genuine comparisons is on the order of  $10^4$ .
- ▷ The number of impostor comparisons is on the order of  $10^{10}$ .
- ▷ The comparisons are fully zero-effort, meaning impostors are paired without attention to sex, age or other covariates. However, later analysis is conducted on subsets.

- ▷ The number of persons is on the order of  $10^5$ .
- ▷ The number of images used to make 1 template is 1.
- ▷ The number of templates used to make each comparison score is two corresponding to simple one-to-one verification.

For mugshot images:

- ▷ The comparisons are of mugshot photos against mugshot photos.
- ▷ The number of genuine comparisons is on the order of  $10^6$ .
- ▷ The number of impostor comparisons is on the order of  $10^8$ .
- ▷ The impostors are paired by sex, but not by age or other covariates.
- ▷ The number of persons is on the order of  $10^6$ .
- ▷ The number of images used to make 1 template is 1.
- ▷ The number of templates used to make each comparison score is two corresponding to simple one-to-one verification.

**Method:** For wild images:

- ▷ The comparisons are of wild photos against wild photos.
- ▷ The number of genuine comparisons is on the order of  $10^6$ .
- ▷ The number of impostor comparisons is on the order of  $10^7$ .
- ▷ The comparisons are fully zero-effort, meaning impostors are paired without attention to sex, age or other covariates.
- ▷ The number of persons is on the order of  $10^4$ .
- ▷ The number of images used to make 1 template is 1.
- ▷ The number of templates used to make each comparison score is two corresponding to simple one-to-one verification.

For child exploitation images:

- ▷ The comparisons are of unconstrained child exploitation photos against others of the same type.
- ▷ The number of genuine comparisons is on the order of  $10^4$ .
- ▷ The number of impostor comparisons is on the order of  $10^7$ .
- ▷ The comparisons are fully zero-effort, meaning impostors are paired without attention to sex, age or other covariates.
- ▷ The number of persons is on the order of  $10^3$ .
- ▷ The number of images used to make 1 template is 1.
- ▷ The number of templates used to make each comparison score is two corresponding to simple one-to-one verification.

- ▷ We produce two performance statements. First, is a DET as used for visa and mugshot images. The second is a cumulative match characteristic (CMC) summarizing a simulated one-to-many search process. This is done as follows.
- We regard  $M$  enrollment templates as items in a gallery.
  - These  $M$  templates come from  $M > N$  individuals, because multiple images of a subject are present in the gallery under separate identifiers.
  - We regard the verification templates as search templates.
  - For each search we compute the rank of the highest scoring mate.
  - This process should properly be conducted with a 1:N algorithm, such as those tested in NIST IR 8009. We use the 1:1 algorithms in a simulated 1:N mode here to a) better reflect what a child exploitation analyst does, and b) to show algorithm efficacy is better than that revealed in the verification DETs.



### 3.3 Failure to enroll

	Algorithm Name	Failure to Enrol Rate <sup>1</sup>							
		CHILD-EXPLOIT		MUGSHOT		VISA		WILD	
1	3divi-003	0.1806	56	0.0007	127	0.0006	118	0.0294	139
2	3divi-004	-	172	0.0008	130	0.0006	120	0.0222	137
3	adara-001	0.1928	59	0.0003	98	0.0005	114	0.0505	150
4	aimall-001	-	172	0.0000	15	0.0000	14	0.0001	43
5	aiunionface-000	-	172	0.0000	22	0.0000	22	0.0000	38
6	alchera-000	-	172	0.0004	112	0.0014	149	0.0038	106
7	alchera-001	-	172	0.0004	111	0.0014	148	0.0038	105
8	allgovision-000	-	172	0.0026	158	0.0052	167	0.0131	128
9	alphaface-001	-	172	0.0000	58	0.0004	94	0.0004	61
10	amplifiedgroup-001	-	172	0.0189	171	0.0279	173	0.1390	164
11	anke-003	-	172	0.0001	73	0.0004	81	0.0006	74
12	anke-004	0.0944	42	0.0001	74	0.0004	95	0.0006	78
13	anyvision-002	0.4866	79	0.0070	168	0.0090	170	0.1146	160
14	anyvision-004	0.1660	53	0.0001	82	0.0004	87	0.0080	118
15	asusaics-000	-	172	0.0000	17	0.0000	16	0.0000	12
16	aware-003	0.3314	73	0.0016	151	0.0013	145	0.0745	156
17	aware-004	-	172	0.0002	87	0.0005	102	0.0014	95
18	awiros-001	-	172	0.0386	172	0.0872	174	0.3415	168
19	ayonix-000	0.0000	3	0.0113	169	0.0137	172	0.1194	161
20	bm-001	0.0000	17	0.0000	43	0.0000	17	0.0000	13
21	camvi-002	0.0000	4	0.0000	28	0.0000	28	0.0000	22
22	camvi-004	-	172	0.0000	32	0.0000	32	0.0000	26
23	ceiec-001	-	172	0.0029	161	0.0023	156	0.0068	115
24	ceiec-002	0.2482	67	0.0036	163	0.0031	163	0.0081	119
25	chtface-001	-	172	0.0000	35	0.0000	35	0.0000	29
26	cogent-003	-	172	0.0001	68	0.0004	84	0.0009	90
27	cogent-004	0.0000	6	0.0000	4	0.0000	4	0.0000	2
28	cognitec-000	0.6342	83	0.0007	128	0.0007	126	0.0388	147
29	cognitec-001	-	172	0.0008	134	0.0010	129	0.0185	133
30	ctcbank-000	0.3285	72	0.0011	141	0.0019	153	0.0868	159
31	ctcbank-001	-	172	0.0005	121	0.0010	130	0.0844	158
32	cyberextruder-001	0.5338	81	0.0024	155	0.0029	161	0.0597	154
33	cyberextruder-002	0.2672	70	0.0027	159	0.0028	160	0.0335	144
34	cyberlink-002	0.1463	52	0.0004	105	0.0004	101	0.0007	79
35	cyberlink-003	-	172	0.0001	61	0.0004	72	0.0008	81
36	dahua-002	-	172	0.0024	156	0.0022	155	0.0009	87
37	dahua-003	-	172	0.0002	92	0.0003	51	0.0002	47
38	deepglint-001	0.0000	18	0.0000	18	0.0000	18	0.0000	14
39	deepsea-001	0.0000	8	0.0000	7	0.0000	7	0.0000	5
40	dermalog-005	0.1796	54	0.0013	146	0.0041	164	0.0163	131
41	dermalog-006	0.1797	55	0.0013	145	0.0041	165	0.0163	132
42	didiglobalface-001	-	172	0.0000	57	0.0004	93	0.0004	60
43	digitalbarriers-002	-	172	0.0028	160	0.0027	159	0.0071	116
44	dsk-000	0.0000	14	0.0000	13	0.0000	12	0.0000	9
45	einetworks-000	-	172	0.0002	90	0.0005	112	0.0008	82
46	everai-002	-	172	0.0002	93	0.0004	66	0.0004	69
47	everai-paravision-003	0.0705	38	0.0002	86	0.0004	73	0.0004	67
48	f8-001	0.2026	61	0.0035	162	0.0030	162	0.0087	122
49	facesoft-000	0.0000	22	0.0000	42	0.0000	42	0.0000	34
50	glory-001	0.0000	11	0.0051	166	0.0010	131	0.1651	165
51	glory-002	-	172	0.0015	148	0.0011	142	0.0557	152
52	gorilla-003	0.1347	48	0.0003	104	0.0004	100	0.0043	109
53	gorilla-004	-	172	0.0000	46	0.0003	55	0.0004	64
54	hik-001	-	172	0.0000	34	0.0000	34	0.0000	28
55	hr-001	0.1198	47	0.0001	60	0.0004	75	0.0003	56
56	hr-002	-	172	0.0002	89	0.0004	96	0.0004	59
57	id3-003	0.3032	71	0.0016	152	0.0011	141	0.0317	142
58	id3-004	-	172	0.0015	150	0.0011	140	-	172
59	idemia-004	-	172	0.0000	49	0.0004	69	0.0003	57
60	idemia-005	-	172	0.0000	45	0.0003	57	0.0003	52

Table 9: FTE is the proportion of failed template generation attempts. Failures can occur because the software throws an exception, or because the software electively refuses to process the input image. This would typically occur if a face is not detected. FTE is measured as the number of function calls that give EITHER a non-zero error code OR that give a “small” template. This is defined as one whose size is less than 0.3 times the median template size for that algorithm. This second rule is needed because some algorithms incorrectly fail to return a non-zero error code when template generation fails.

<sup>1</sup>The effects of FTE are included in the accuracy results of this report by regarding any template comparison involving a failed template to produce a low similarity score. Thus higher FTE results in higher FNMR and lower FMR.

	Algorithm Name	Failure to Enrol Rate <sup>1</sup>							
		CHILD-EXPLOIT		MUGSHOT		VISA		WILD	
61	iit-000	-	172	0.0007	126	0.0011	135	0.0836	157
62	iit-001	0.0843	41	0.0001	84	0.0004	90	0.0104	123
63	imagus-000	0.1107	45	0.0010	140	0.0012	144	0.0347	145
64	imagus-001	-	172	0.0001	75	0.0004	91	0.0396	148
65	imperial-000	-	172	0.0000	21	0.0000	21	0.0000	17
66	imperial-002	-	172	0.0000	6	0.0000	6	0.0000	4
67	incode-004	0.2202	62	0.0004	116	0.0007	122	0.0014	94
68	incode-005	-	172	0.0001	69	0.0004	89	0.0007	80
69	innovativetechnologyltd-001	-	172	0.0024	157	0.0025	158	0.0055	113
70	innovatrics-004	0.1170	46	0.0000	56	0.0004	92	0.0041	108
71	innovatrics-006	-	172	0.0000	51	0.0004	65	0.0003	58
72	intellcloudai-001	-	172	0.0000	41	0.0000	41	0.0001	44
73	intellifusion-001	-	172	0.0001	65	0.0003	60	0.0005	73
74	intellivision-001	0.5495	82	0.0048	165	0.0042	166	0.1358	162
75	intellivision-002	-	172	0.0012	143	0.0005	116	0.0146	129
76	intelresearch-000	-	172	0.0000	53	0.0003	59	0.0001	45
77	intsymsu-000	-	172	0.0004	110	0.0012	143	0.0031	104
78	intsymsu-001	-	172	0.0001	72	0.0004	88	0.0004	65
79	iqface-000	0.0000	9	0.0000	33	0.0000	33	0.0000	27
80	isap-001	-	172	0.0000	31	0.0000	31	0.0000	25
81	isityou-000	0.4714	77	0.0023	153	0.0010	133	0.0663	155
82	isystems-001	0.1421	50	0.0010	138	0.0007	123	0.0128	126
83	isystems-002	0.1421	51	0.0010	139	0.0007	124	0.0128	127
84	itmo-005	0.1353	49	0.0005	118	0.0002	44	0.0075	117
85	itmo-006	-	172	0.0004	115	0.0004	86	0.0006	77
86	kakao-001	-	172	0.0002	94	0.0005	105	0.0310	140
87	kakao-002	0.2494	68	0.0002	95	0.0005	109	0.0310	141
88	kedacom-000	0.0000	16	0.0000	16	0.0000	15	0.0000	11
89	kneron-003	0.4883	80	0.0044	164	0.0016	152	0.1823	166
90	lookman-002	-	172	0.0000	30	0.0000	30	0.0000	24
91	lookman-004	0.0000	1	0.0000	26	0.0000	26	0.0000	20
92	luxand-000	-	172	0.0000	8	-	172	-	172
93	megvii-001	0.0274	27	0.0007	129	0.0004	71	0.0152	130
94	megvii-002	0.0274	26	0.0054	167	0.0004	70	0.0126	125
95	meiya-001	-	172	0.0004	117	0.0010	134	0.0025	101
96	microfocus-001	0.0791	40	0.0008	133	0.0016	151	0.0220	136
97	microfocus-002	0.0791	39	0.0008	132	0.0016	150	0.0220	135
98	mt-000	0.1043	43	0.0002	91	0.0004	97	0.0004	62
99	mvision-001	-	172	0.0000	27	0.0000	27	0.0000	21
100	neurotechnology-005	-	172	0.0004	108	0.0004	77	0.0018	97
101	neurotechnology-006	0.1068	44	0.0004	109	0.0004	78	0.0018	98
102	nodeflux-001	-	172	0.0001	76	0.0002	47	0.0003	51
103	nodeflux-002	-	172	0.0008	131	0.0005	111	0.0008	86
104	notiontag-000	0.0000	20	0.0000	23	0.0000	23	0.0000	18
105	ntechlab-006	-	172	0.0000	44	0.0004	63	0.0003	50
106	ntechlab-007	0.0682	37	0.0001	62	0.0004	67	0.0005	72
107	pixelall-002	0.0001	23	0.0000	12	0.0000	11	0.0001	40
108	pixelall-003	-	172	0.0000	37	0.0000	37	0.0000	30
109	psl-002	-	172	0.0000	14	0.0000	13	0.0000	10
110	psl-003	-	172	0.0000	54	0.0004	85	0.0003	55
111	pyramid-000	-	172	0.0005	120	0.0007	125	0.0015	96
112	rankone-007	0.3518	75	0.0003	100	0.0004	98	0.0043	110
113	rankone-008	-	172	0.0003	96	0.0004	61	0.0040	107
114	realnetworks-002	-	172	0.0004	107	0.0003	53	0.0004	66
115	realnetworks-003	0.0076	24	0.0004	106	0.0003	52	0.0004	68
116	remarkai-000	-	172	0.0000	2	0.0000	2	0.0000	37
117	remarkai-001	-	172	0.0000	25	0.0000	25	0.0000	39
118	rokid-000	-	172	0.0001	71	0.0005	110	0.0354	146
119	saffe-001	0.0000	19	0.0000	20	0.0000	20	0.0000	16
120	saffe-002	-	172	0.0000	39	0.0000	39	0.0000	31

Table 10: FTE is the proportion of failed template generation attempts. Failures can occur because the software throws an exception, or because the software electively refuses to process the input image. This would typically occur if a face is not detected. FTE is measured as the number of function calls that give EITHER a non-zero error code OR that give a “small” template. This is defined as one whose size is less than 0.3 times the median template size for that algorithm. This second rule is needed because some algorithms incorrectly fail to return a non-zero error code when template generation fails.

<sup>1</sup>The effects of FTE are included in the accuracy results of this report by regarding any template comparison involving a failed template to produce a low similarity score. Thus higher FTE results in higher FNMR and lower FMR.

	Algorithm Name	Failure to Enrol Rate <sup>1</sup>							
		CHILD-EXPLOIT		MUGSHOT		VISA		WILD	
121	samtech-001	-	172	0.0004	114	0.0008	127	0.0013	93
122	scanovate-001	-	172	0.0024	154	0.0014	147	0.2751	167
123	sensetime-001	0.0631	36	0.0000	48	0.0004	80	0.0003	53
124	sensetime-002	0.3345	74	0.0011	142	0.0005	115	0.0218	134
125	sertis-000	-	172	0.0000	59	0.0004	74	0.0004	63
126	shaman-000	0.0000	5	0.0000	29	0.0000	29	0.0000	23
127	shaman-001	0.0000	2	0.0000	1	0.0000	1	0.0000	35
128	shu-001	0.1822	57	0.0010	137	0.0006	117	0.0499	149
129	siat-002	0.0616	33	0.0000	52	0.0004	83	0.0048	112
130	siat-004	-	172	0.0000	50	0.0004	82	0.0003	54
131	sjtu-001	-	172	0.0005	119	0.0004	99	0.0008	84
132	smilart-002	0.2422	65	0.0003	103	0.0011	137	0.0575	153
133	smilart-003	-	172	0.0014	147	0.0013	146	0.0555	151
134	starhybrid-001	0.2340	64	0.0009	136	0.0023	157	0.0044	111
135	synesis-005	0.1862	58	0.0001	70	0.0005	103	0.0021	99
136	synesis-006	-	172	0.0000	55	0.0003	49	0.0002	49
137	synology-000	-	172	0.0000	10	0.0000	9	0.0000	7
138	tech5-002	-	172	0.0001	67	0.0003	48	0.0000	36
139	tech5-003	-	172	0.0001	66	0.0003	50	0.0002	46
140	tevian-004	-	172	0.0002	88	0.0005	113	0.0057	114
141	tevian-005	-	172	0.0006	125	0.0006	121	0.0012	92
142	tiger-002	0.0619	34	0.0001	79	0.0004	79	0.0082	121
143	tiger-003	0.0619	35	0.0001	77	0.0004	76	0.0082	120
144	tongyi-005	0.0000	7	0.0000	5	0.0000	5	0.0000	3
145	toshiba-002	0.0000	13	0.0000	11	0.0000	10	0.0000	8
146	toshiba-003	-	172	0.0001	80	0.0001	43	0.0002	48
147	trueface-000	-	172	0.0000	40	0.0000	40	0.0000	32
148	tuputech-000	-	172	0.0414	173	0.0081	169	0.6383	169
149	ulsee-001	-	172	0.0000	38	0.0000	38	0.0001	41
150	uluface-002	0.0000	21	0.0000	24	0.0000	24	0.0000	19
151	uluface-003	-	172	0.0002	85	0.0002	45	0.0244	138
152	upc-001	0.0450	28	0.0003	97	0.0003	58	0.0011	91
153	vd-001	-	172	0.0004	113	0.0009	128	0.0024	100
154	veridas-001	-	172	0.0001	78	0.0005	106	0.0006	75
155	veridas-002	-	172	0.0001	81	0.0005	108	0.0006	76
156	via-000	0.0000	10	0.0000	36	0.0000	36	0.0001	42
157	videonetics-001	0.4799	78	0.0015	149	0.0010	132	0.0112	124
158	vigilantsolutions-006	-	172	0.0001	64	0.0004	68	0.0005	71
159	vigilantsolutions-007	0.2538	69	0.0001	63	0.0004	64	0.0005	70
160	vion-000	0.6388	84	0.0130	170	0.0078	168	0.1389	163
161	visionbox-000	-	172	0.0005	124	0.0011	139	0.0028	103
162	visionbox-001	-	172	0.0005	123	0.0011	138	0.0028	102
163	visionlabs-006	-	172	0.0003	102	0.0005	107	0.0009	89
164	visionlabs-007	0.1939	60	0.0003	101	0.0005	104	0.0008	85
165	vocord-006	-	172	0.0003	99	0.0003	56	0.0008	83
166	vocord-007	0.0000	15	0.0001	83	0.0004	62	0.0009	88
167	winsense-000	0.0000	12	0.0000	9	0.0000	8	0.0000	6
168	winsense-001	-	172	0.0000	19	0.0000	19	0.0000	15
169	x-laboratory-000	-	172	0.0005	122	0.0002	46	0.0000	33
170	yisheng-004	0.4279	76	0.0013	144	0.0006	119	0.0321	143
171	yitu-003	-	172	0.0009	135	0.0000	3	0.0000	1

Table 11: FTE is the proportion of failed template generation attempts. Failures can occur because the software throws an exception, or because the software electively refuses to process the input image. This would typically occur if a face is not detected. FTE is measured as the number of function calls that give EITHER a non-zero error code OR that give a “small” template. This is defined as one whose size is less than 0.3 times the median template size for that algorithm. This second rule is needed because some algorithms incorrectly fail to return a non-zero error code when template generation fails.

<sup>1</sup>The effects of FTE are included in the accuracy results of this report by regarding any template comparison involving a failed template to produce a low similarity score. Thus higher FTE results in higher FNMR and lower FMR.

### 3.4 Recognition accuracy

Core algorithm accuracy is stated via:

▷ **Cooperative subjects**

- The summary table of Figure 8;
- The visa image DETs of Figure 29;
- The mugshot DETs of Figure 38;
- The mugshot ageing profiles of Figure 138;
- The human-difficult pairs of Figure 11

▷ **Non-cooperative subjects**

- The photojournalism DET of Figure 45
- The child-exploitation DET of Figure 49;
- The child-exploitation CMC of Figure 52.

Figure 112 shows dependence of false match rate on algorithm score threshold. This allows a deployer to set a threshold to target a particular false match rate appropriate to the security objectives of the application.

Figure 94 likewise shows FMR(T) but for mugshots, and specially four subsets of the population.

Note that in both the mugshot and visa sets false match rates vary with the ethnicity, age, and sex, of the enrollee and impostor - see section 3.6. For example figure 62 summarizes FMR for impostors paired from four groups black females, black males, white females, white males.

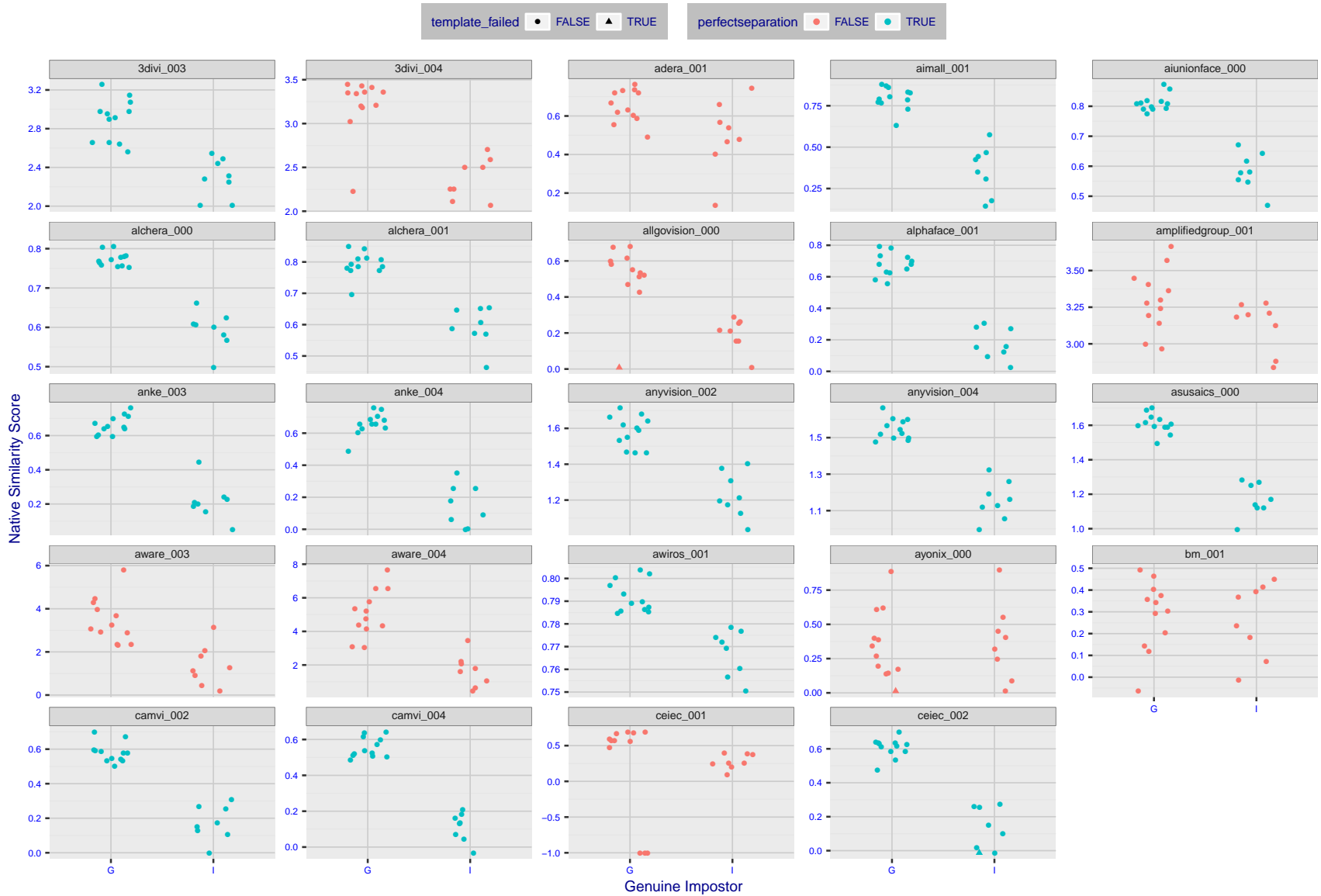


Figure 4: The Figure shows, in blue, algorithms that correctly separate the 12 genuine and 8 impostor pairs used in the May 2018 paper [Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms \(Phillips et al. \[1\]\)](#). In red are algorithms that are imperfect. Some algorithms fail only because they failed to make a template e.g. due to face detection failure (shown as a triangle). Others fail because the pairs were selected for that study because they had been difficult for three leading algorithms used in FRVT 2006. Caution: Given the small sample size (n=20) the figure may change substantially if larger or different sets were used. The images can be downloaded from the [Supplemental Information](#) page provided with that publication.

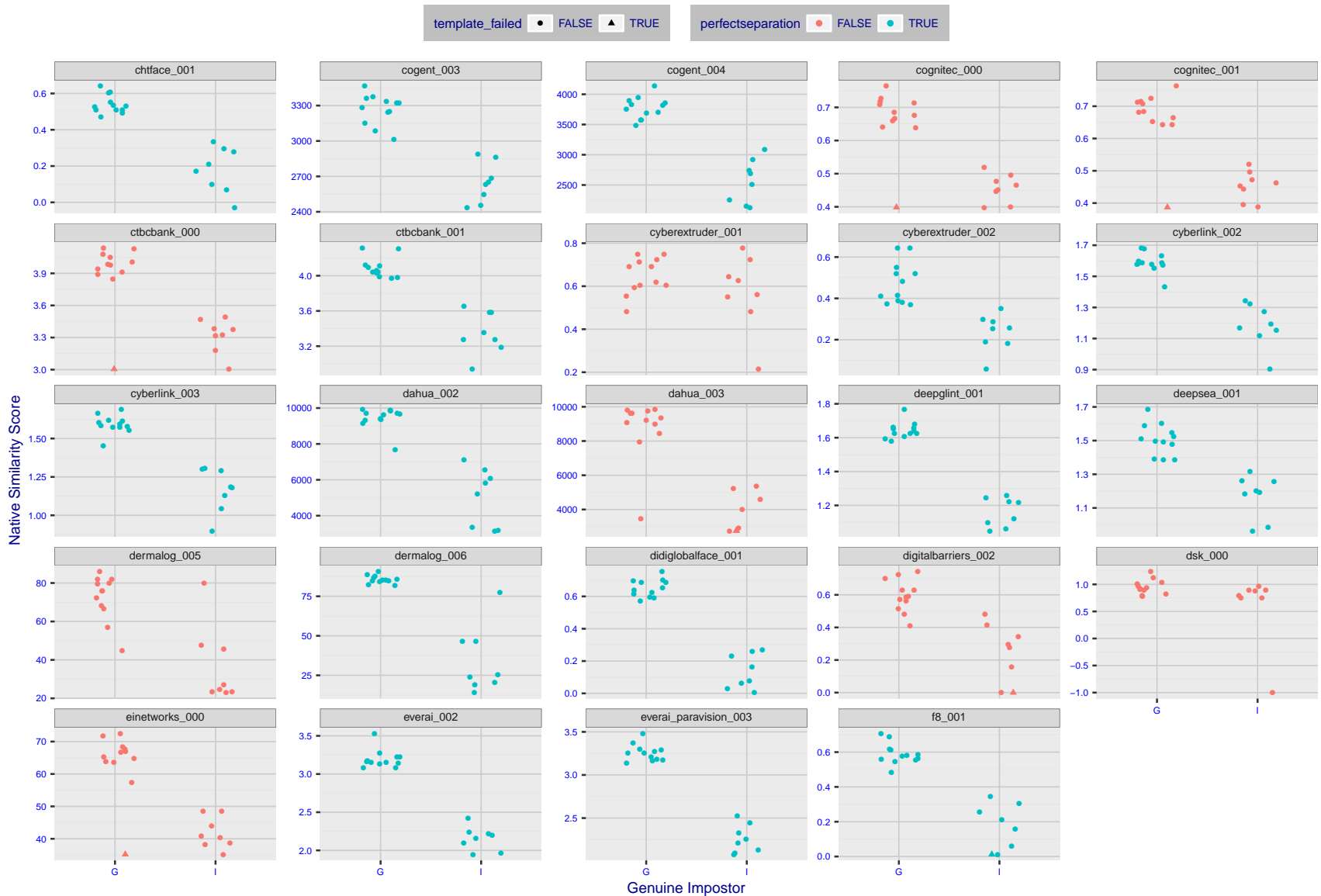


Figure 5: The Figure shows, in blue, algorithms that correctly separate the 12 genuine and 8 impostor pairs used in the May 2018 paper [Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms \(Phillips et al. \[1\]\)](#). In red are algorithms that are imperfect. Some algorithms fail only because they failed to make a template e.g. due to face detection failure (shown as a triangle). Others fail because the pairs were selected for that study because they had been difficult for three leading algorithms used in FRVT 2006. Caution: Given the small sample size (n=20) the figure may change substantially if larger or different sets were used. The images can be downloaded from the [Supplemental Information](#) page provided with that publication.



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 6: The Figure shows, in blue, algorithms that correctly separate the 12 genuine and 8 impostor pairs used in the May 2018 paper [Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms \(Phillips et al. \[1\]\)](#). In red are algorithms that are imperfect. Some algorithms fail only because they failed to make a template e.g. due to face detection failure (shown as a triangle). Others fail because the pairs were selected for that study because they had been difficult for three leading algorithms used in FRVT 2006. Caution: Given the small sample size (n=20) the figure may change substantially if larger or different sets were used. The images can be downloaded from the [Supplemental Information](#) page provided with that publication.





Figure 7: The Figure shows, in blue, algorithms that correctly separate the 12 genuine and 8 impostor pairs used in the May 2018 paper [Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms \(Phillips et al. \[1\]\)](#). In red are algorithms that are imperfect. Some algorithms fail only because they failed to make a template e.g. due to face detection failure (shown as a triangle). Others fail because the pairs were selected for that study because they had been difficult for three leading algorithms used in FRVT 2006. Caution: Given the small sample size (n=20) the figure may change substantially if larger or different sets were used. The images can be downloaded from the [Supplemental Information](#) page provided with that publication.

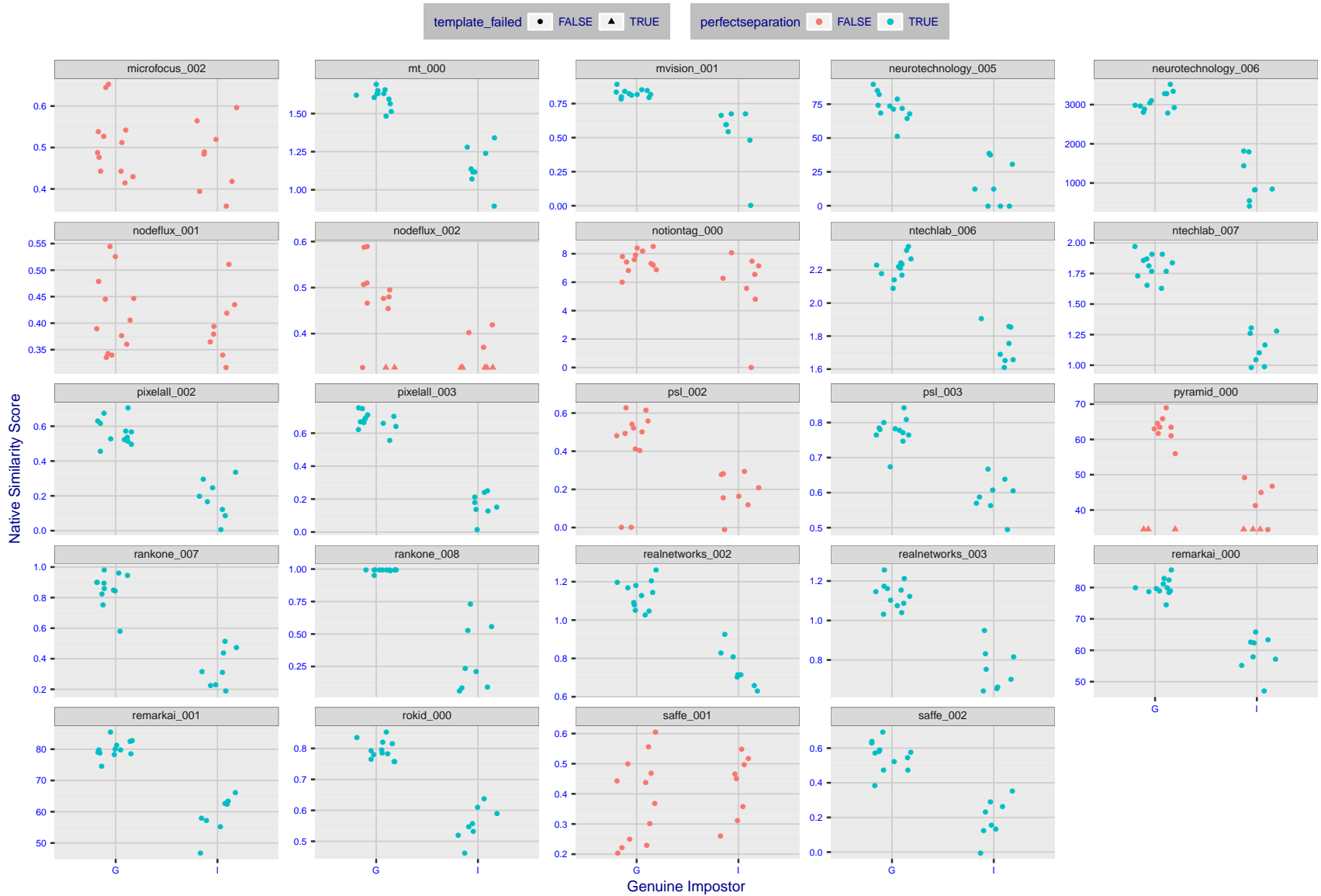


Figure 8: The Figure shows, in blue, algorithms that correctly separate the 12 genuine and 8 impostor pairs used in the May 2018 paper [Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms \(Phillips et al. \[1\]\)](#). In red are algorithms that are imperfect. Some algorithms fail only because they failed to make a template e.g. due to face detection failure (shown as a triangle). Others fail because the pairs were selected for that study because they had been difficult for three leading algorithms used in FRVT 2006. Caution: Given the small sample size (n=20) the figure may change substantially if larger or different sets were used. The images can be downloaded from the [Supplemental Information](#) page provided with that publication.

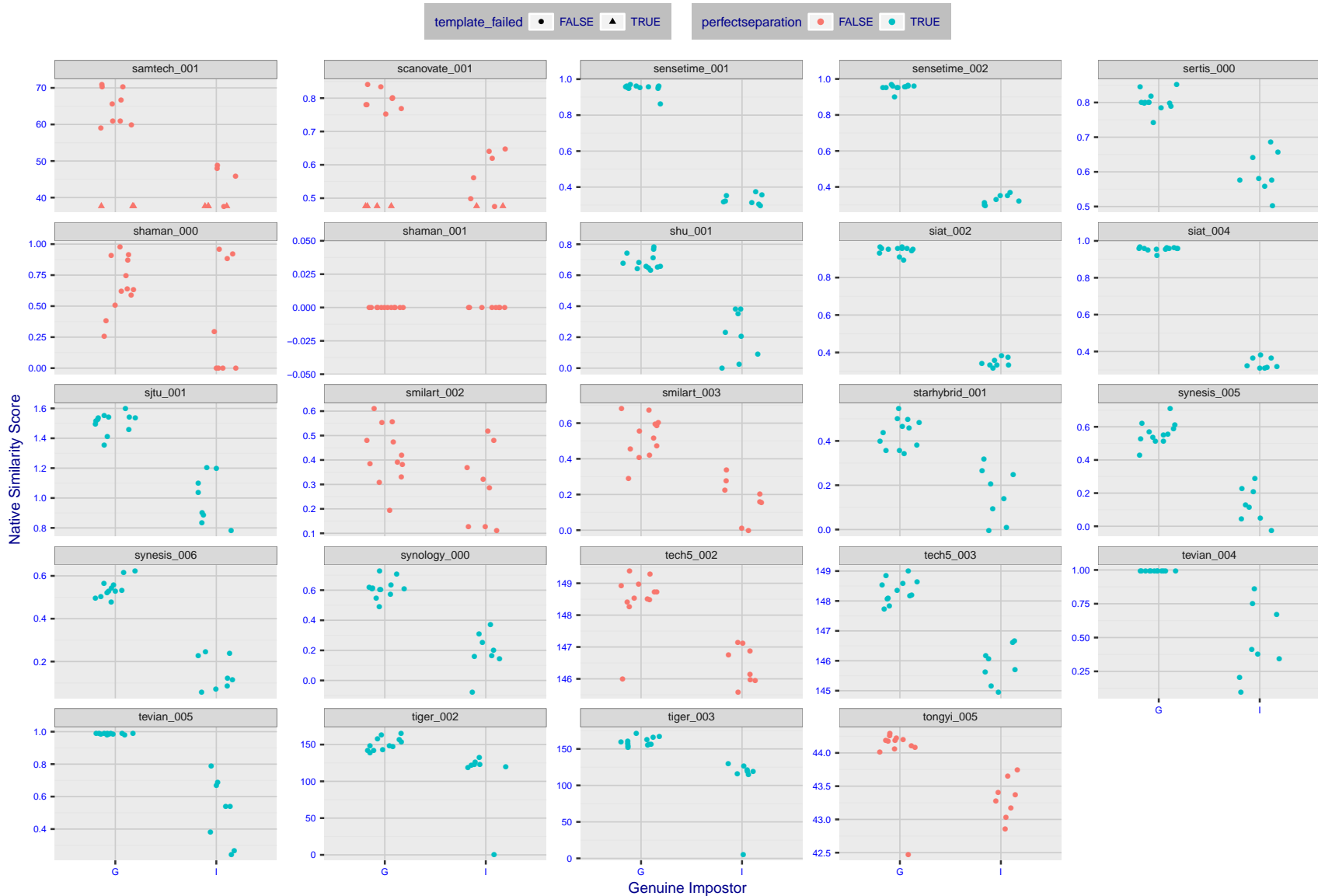


Figure 9: The Figure shows, in blue, algorithms that correctly separate the 12 genuine and 8 impostor pairs used in the May 2018 paper [Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms \(Phillips et al. \[1\]\)](#). In red are algorithms that are imperfect. Some algorithms fail only because they failed to make a template e.g. due to face detection failure (shown as a triangle). Others fail because the pairs were selected for that study because they had been difficult for three leading algorithms used in FRVT 2006. Caution: Given the small sample size (n=20) the figure may change substantially if larger or different sets were used. The images can be downloaded from the [Supplemental Information](#) page provided with that publication.



Figure 10: The Figure shows, in blue, algorithms that correctly separate the 12 genuine and 8 impostor pairs used in the May 2018 paper [Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms \(Phillips et al. \[1\]\)](#). In red are algorithms that are imperfect. Some algorithms fail only because they failed to make a template e.g. due to face detection failure (shown as a triangle). Others fail because the pairs were selected for that study because they had been difficult for three leading algorithms used in FRVT 2006. Caution: Given the small sample size (n=20) the figure may change substantially if larger or different sets were used. The images can be downloaded from the [Supplemental Information](#) page provided with that publication.

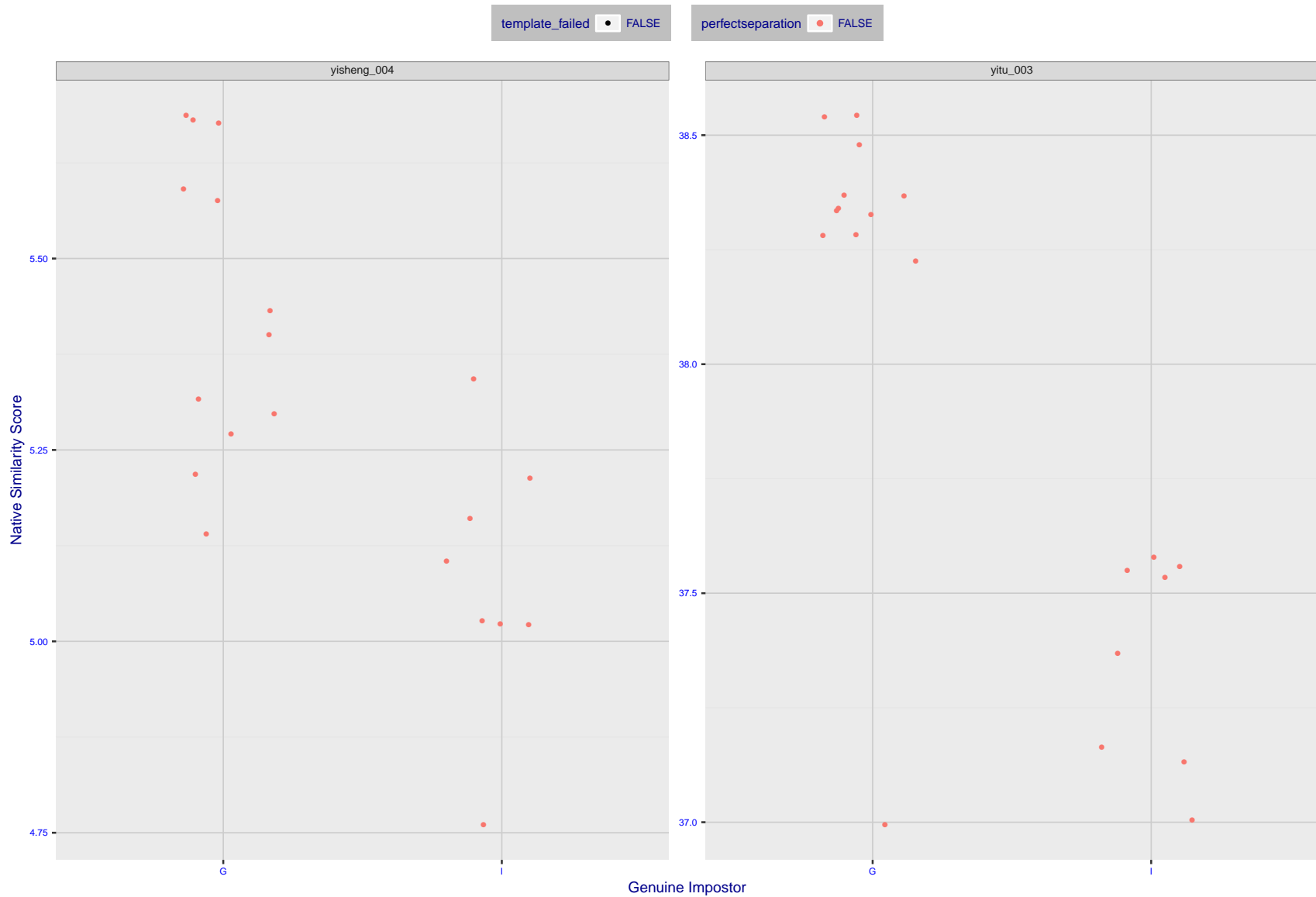


Figure 11: The Figure shows, in blue, algorithms that correctly separate the 12 genuine and 8 impostor pairs used in the May 2018 paper [Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms \(Phillips et al. \[1\]\)](#). In red are algorithms that are imperfect. Some algorithms fail only because they failed to make a template e.g. due to face detection failure (shown as a triangle). Others fail because the pairs were selected for that study because they had been difficult for three leading algorithms used in FRVT 2006. Caution: Given the small sample size (n=20) the figure may change substantially if larger or different sets were used. The images can be downloaded from the [Supplemental Information](#) page provided with that publication.

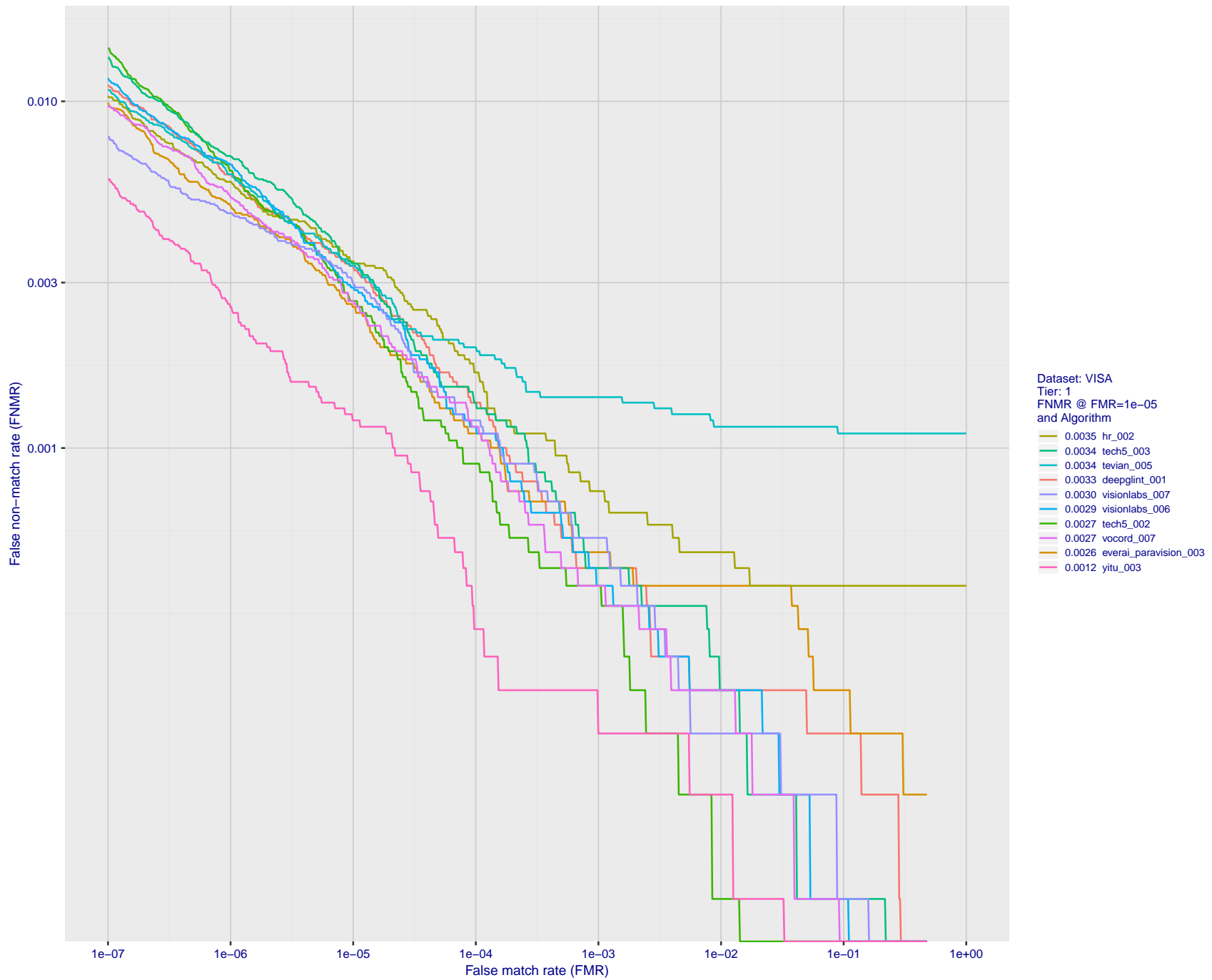


Figure 12: For the visa images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show many decades of FMR.

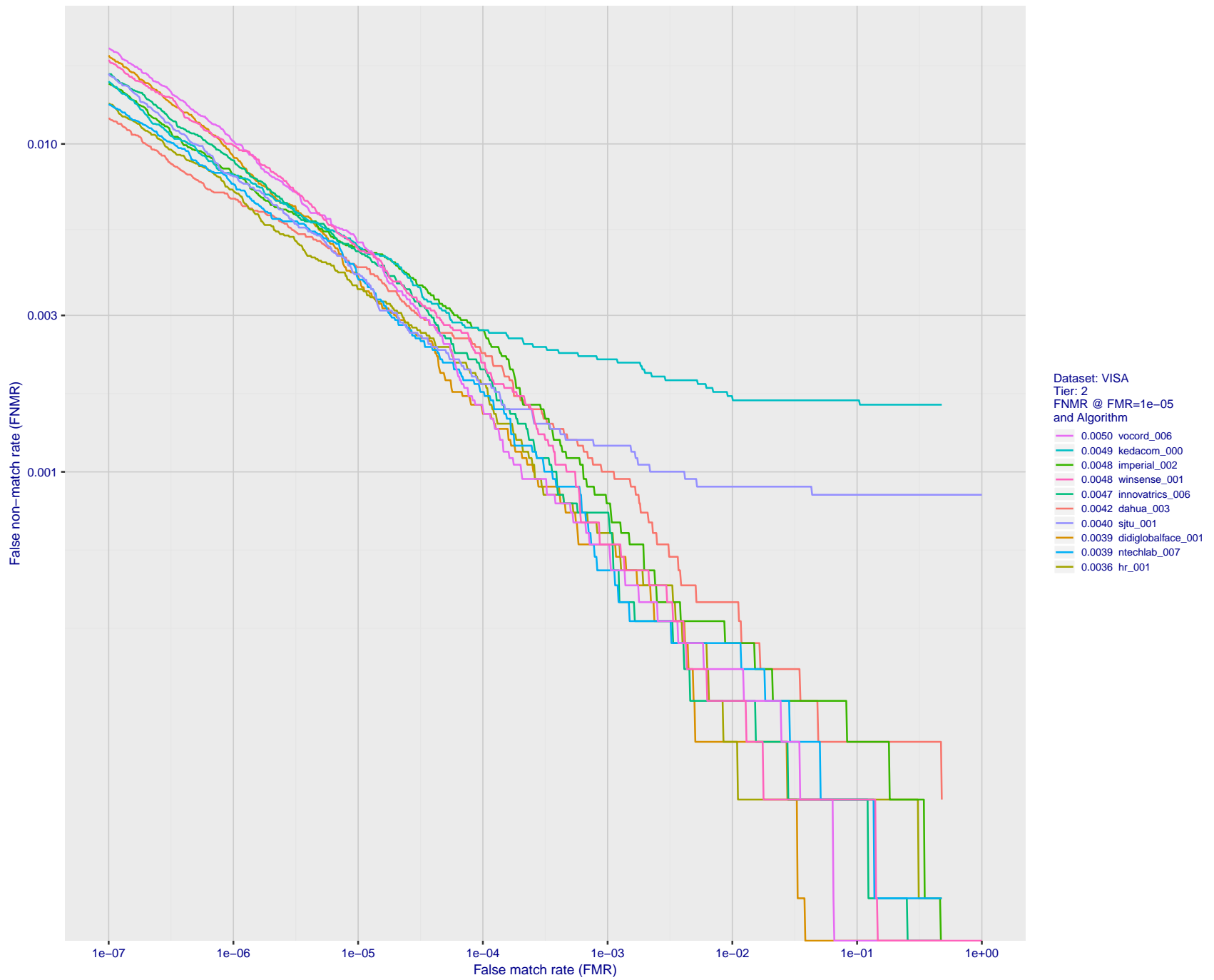


Figure 13: For the visa images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show many decades of FMR.

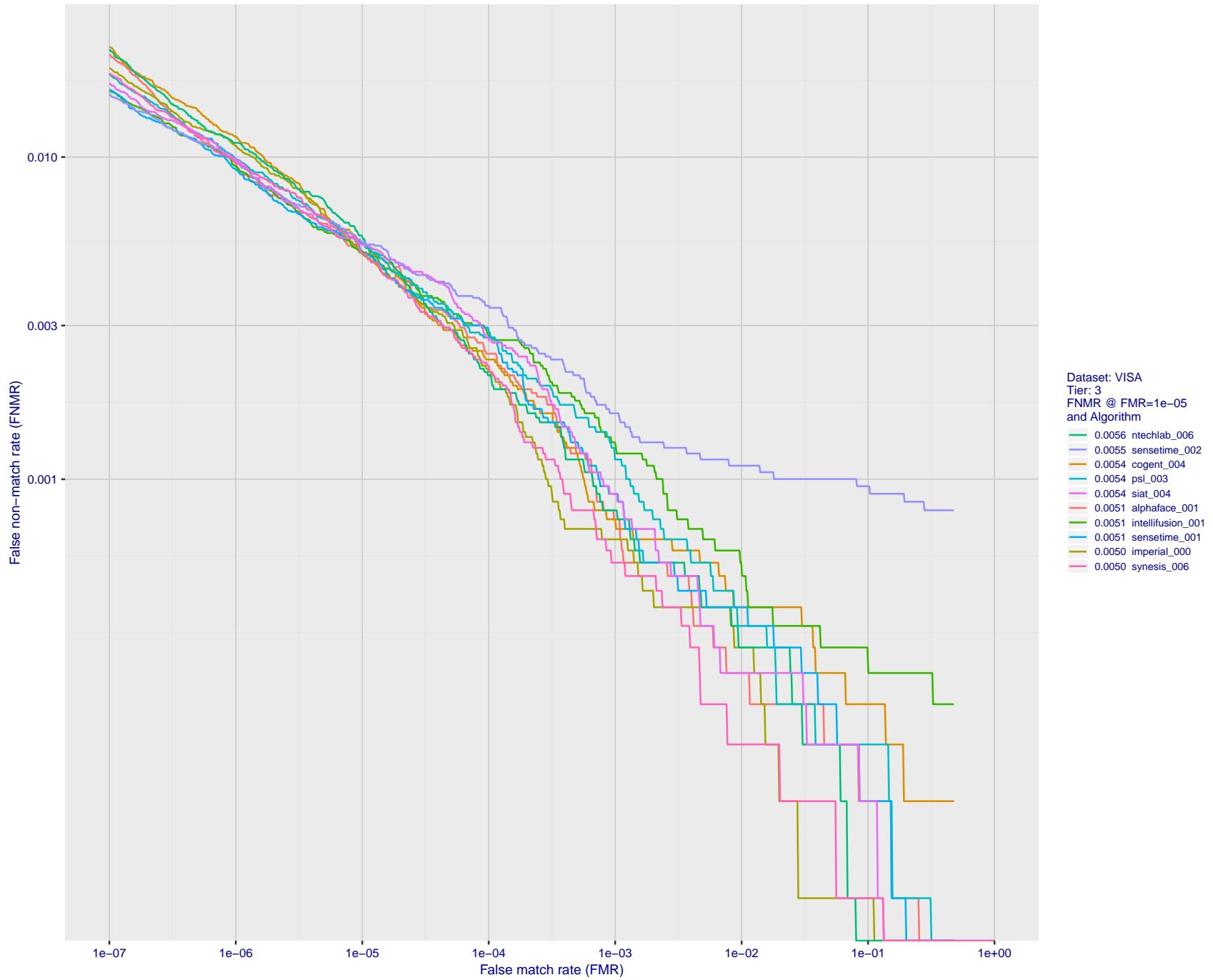


Figure 14: For the visa images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show many decades of FMR.



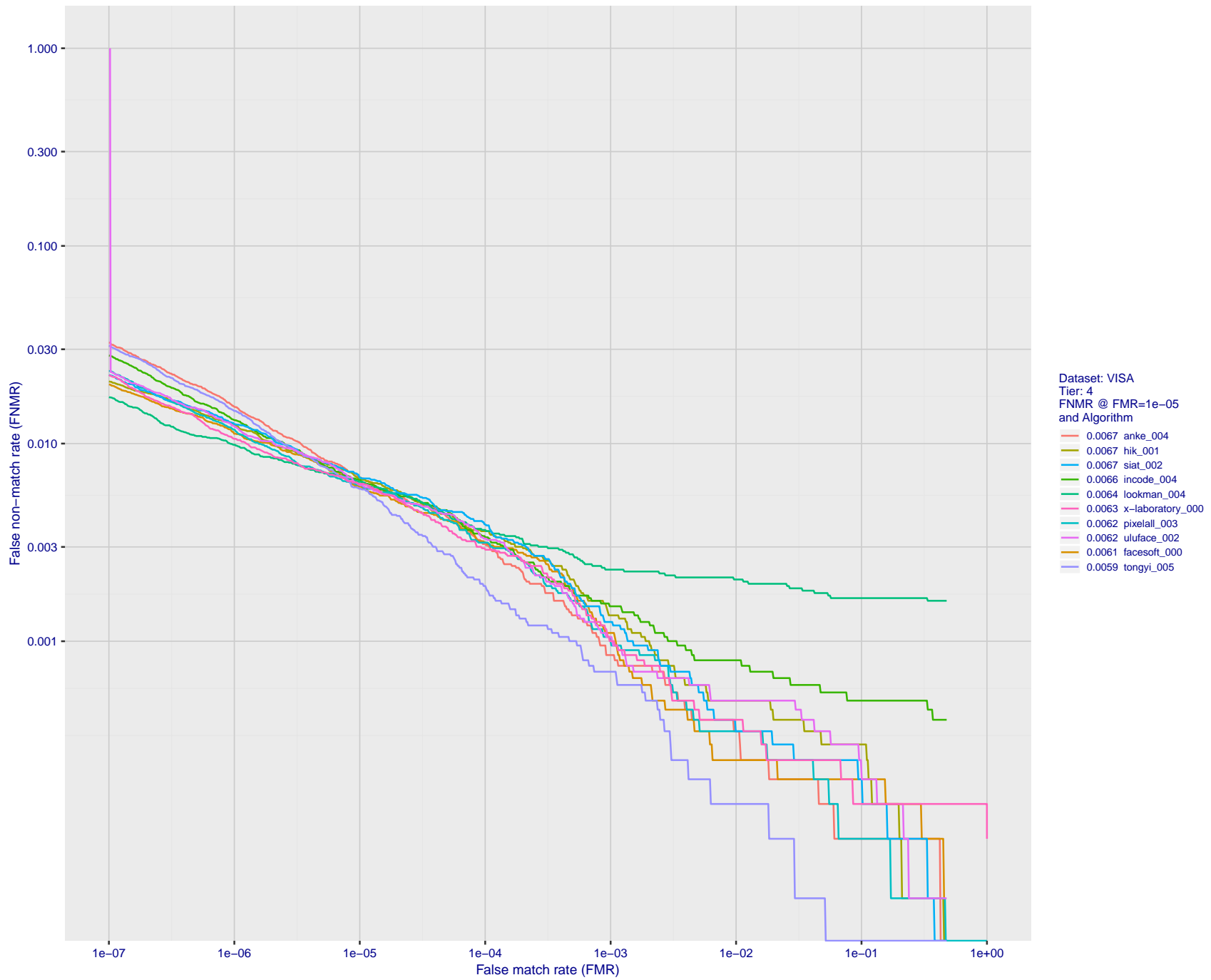
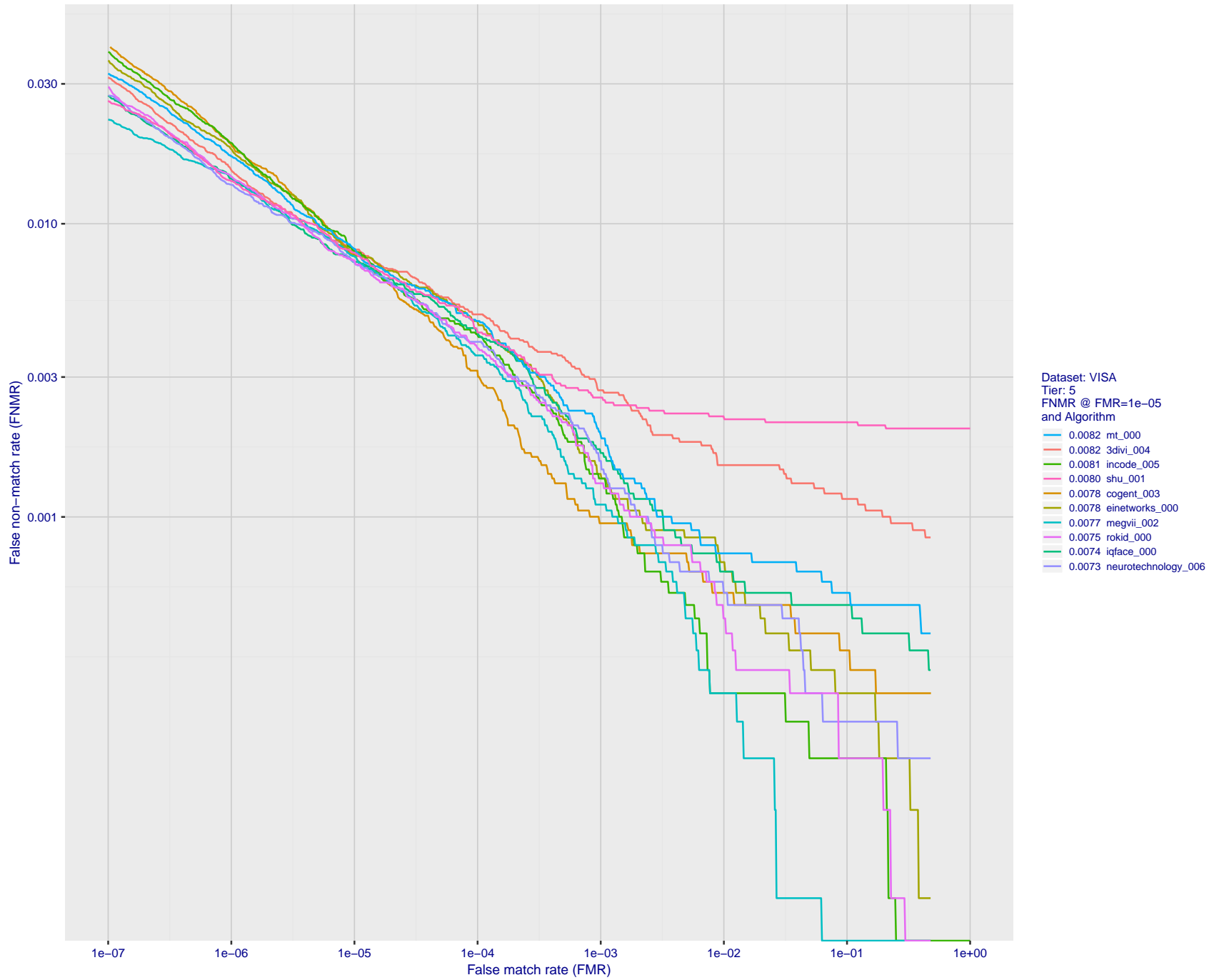


Figure 15: For the visa images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show many decades of FMR.



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 16: For the visa images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show many decades of FMR.

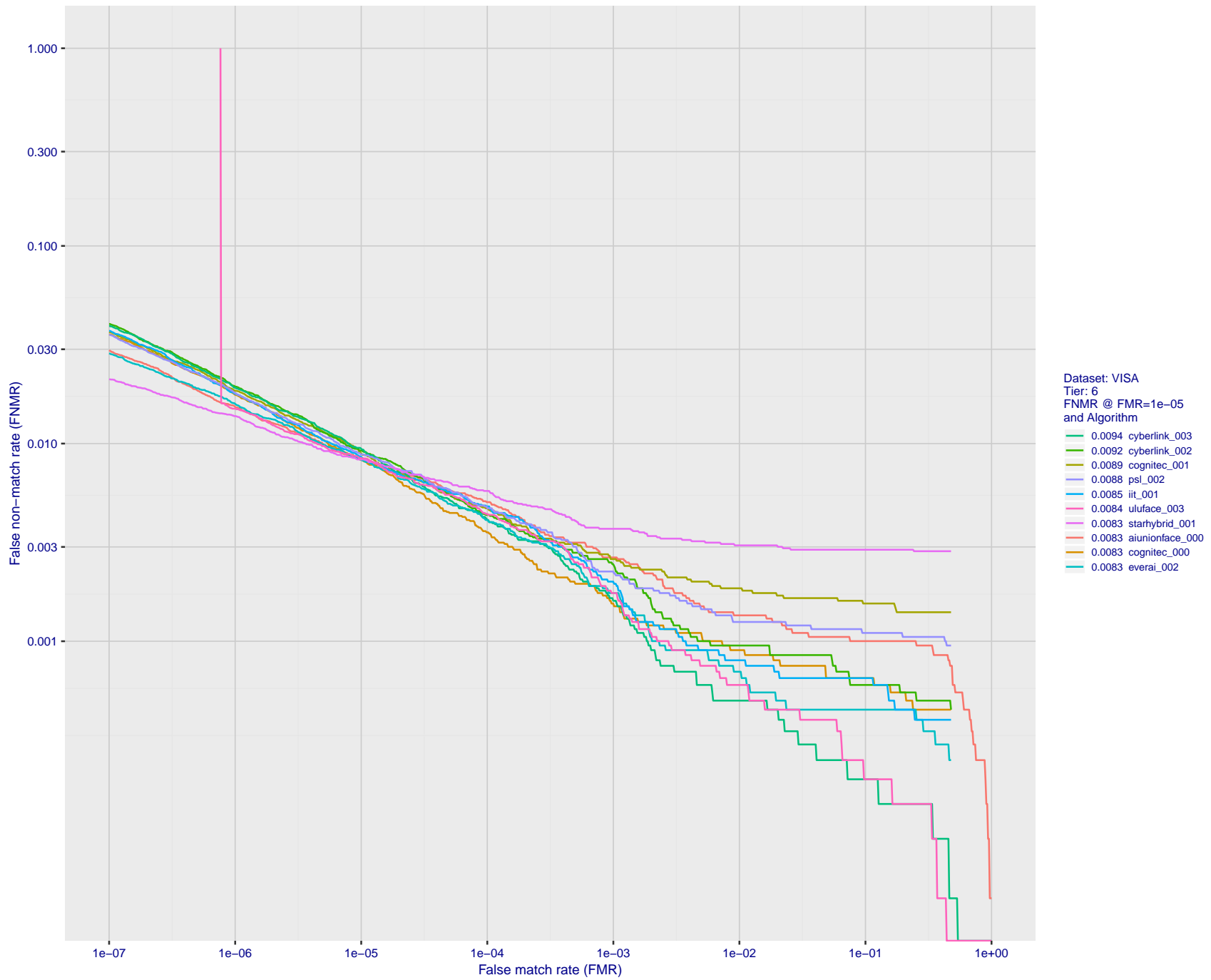


Figure 17: For the visa images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show many decades of FMR.

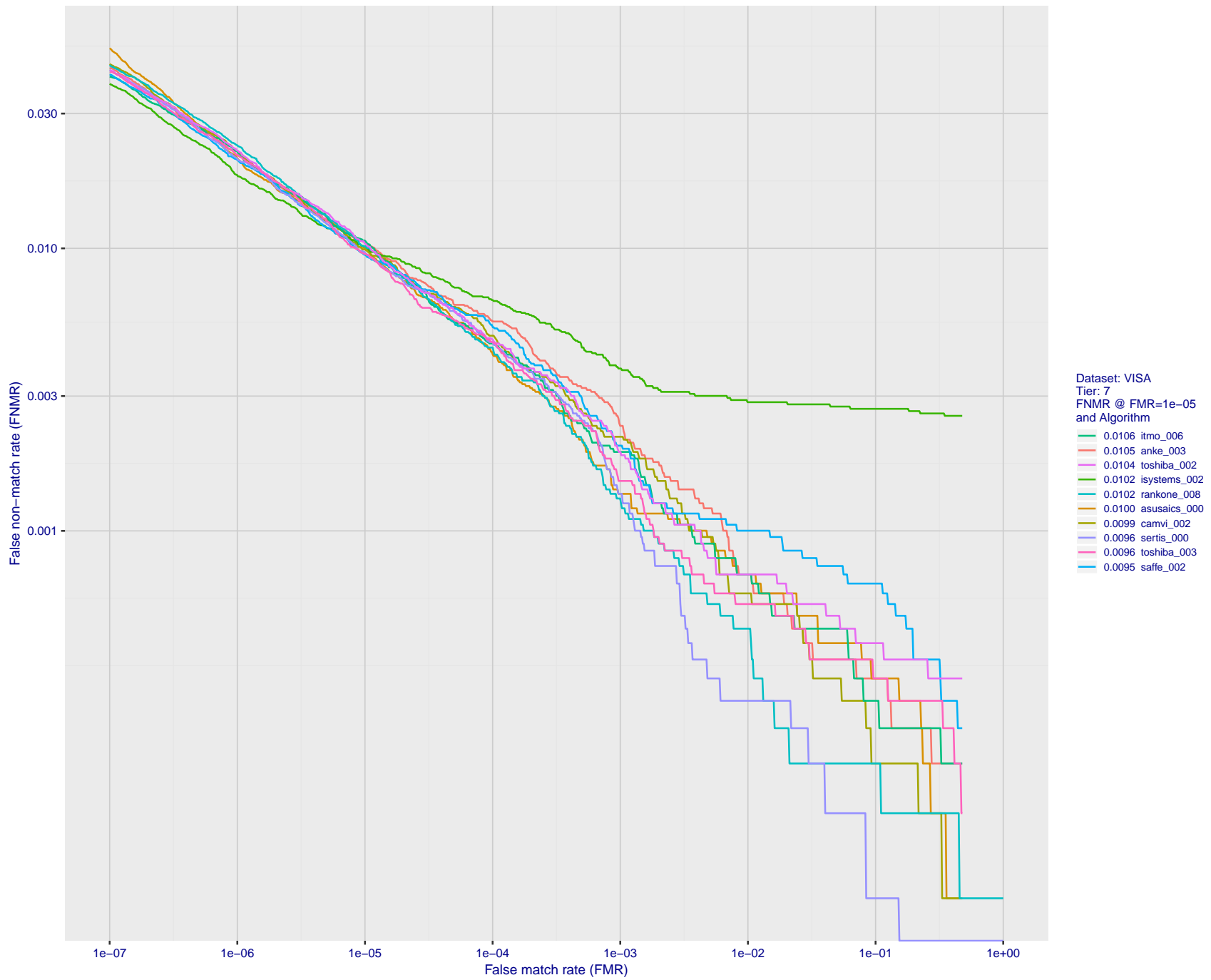


Figure 18: For the visa images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show many decades of FMR.

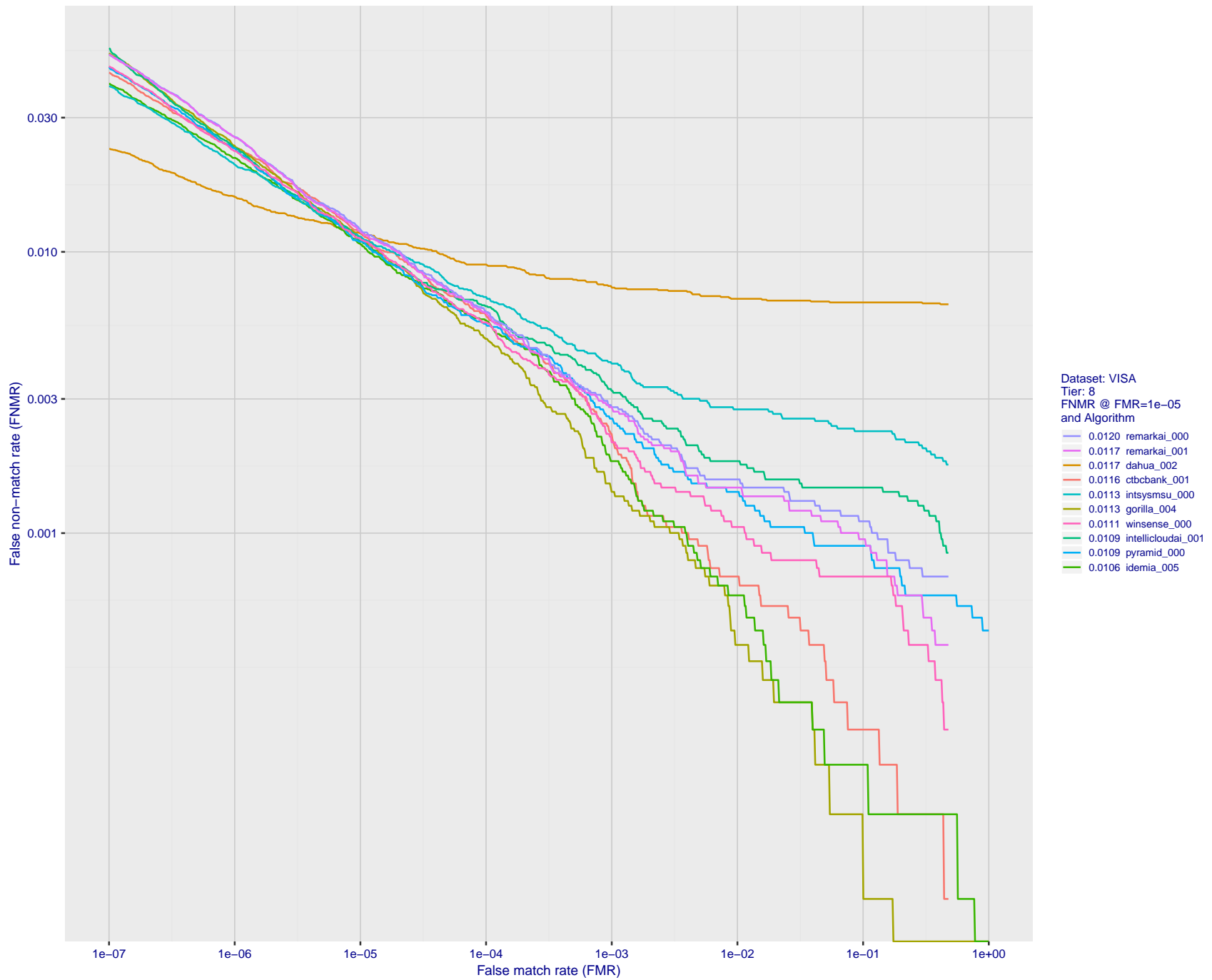
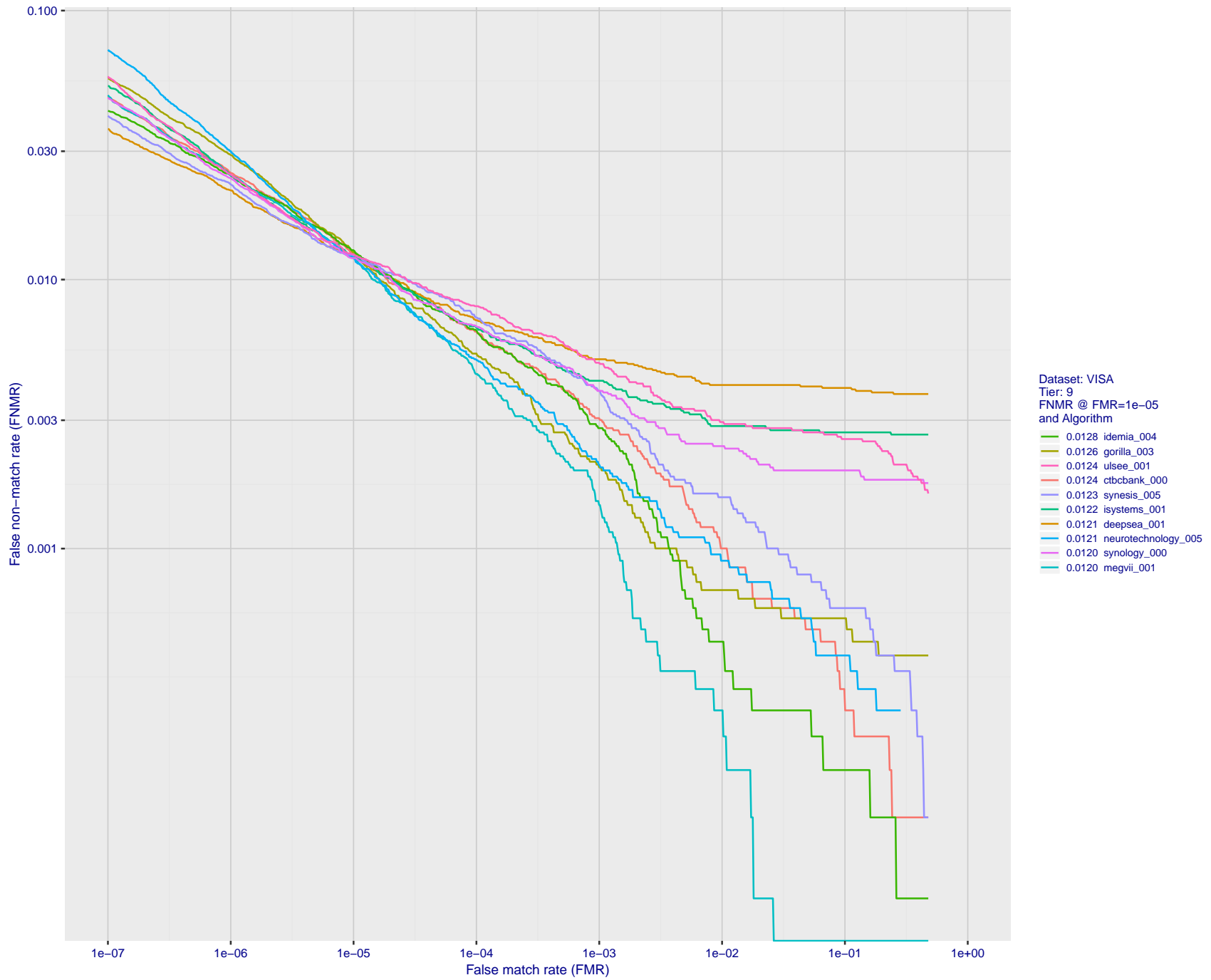


Figure 19: For the visa images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show many decades of FMR.



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 20: For the visa images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show many decades of FMR.

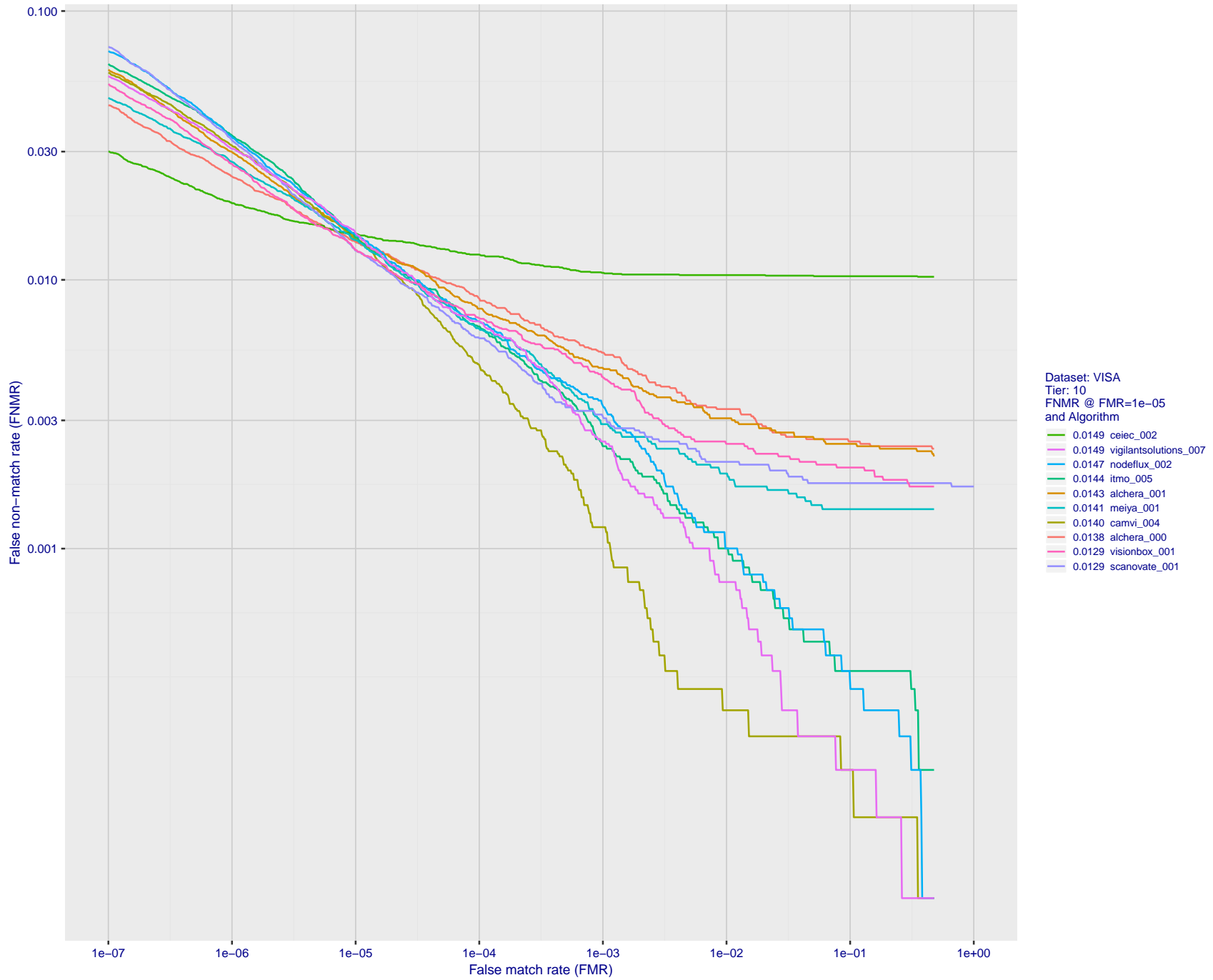


Figure 21: For the visa images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show many decades of FMR.

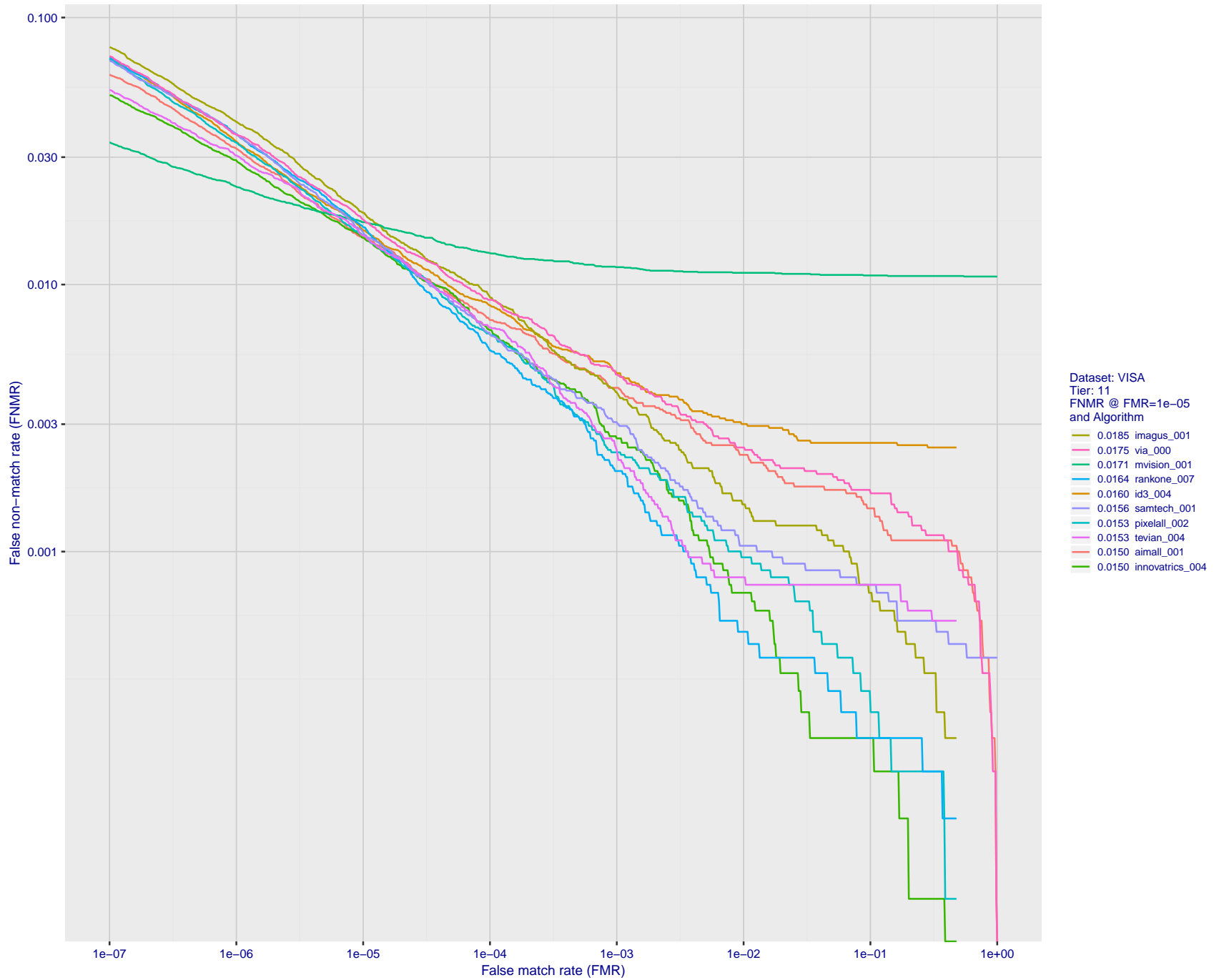


Figure 22: For the visa images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show many decades of FMR.



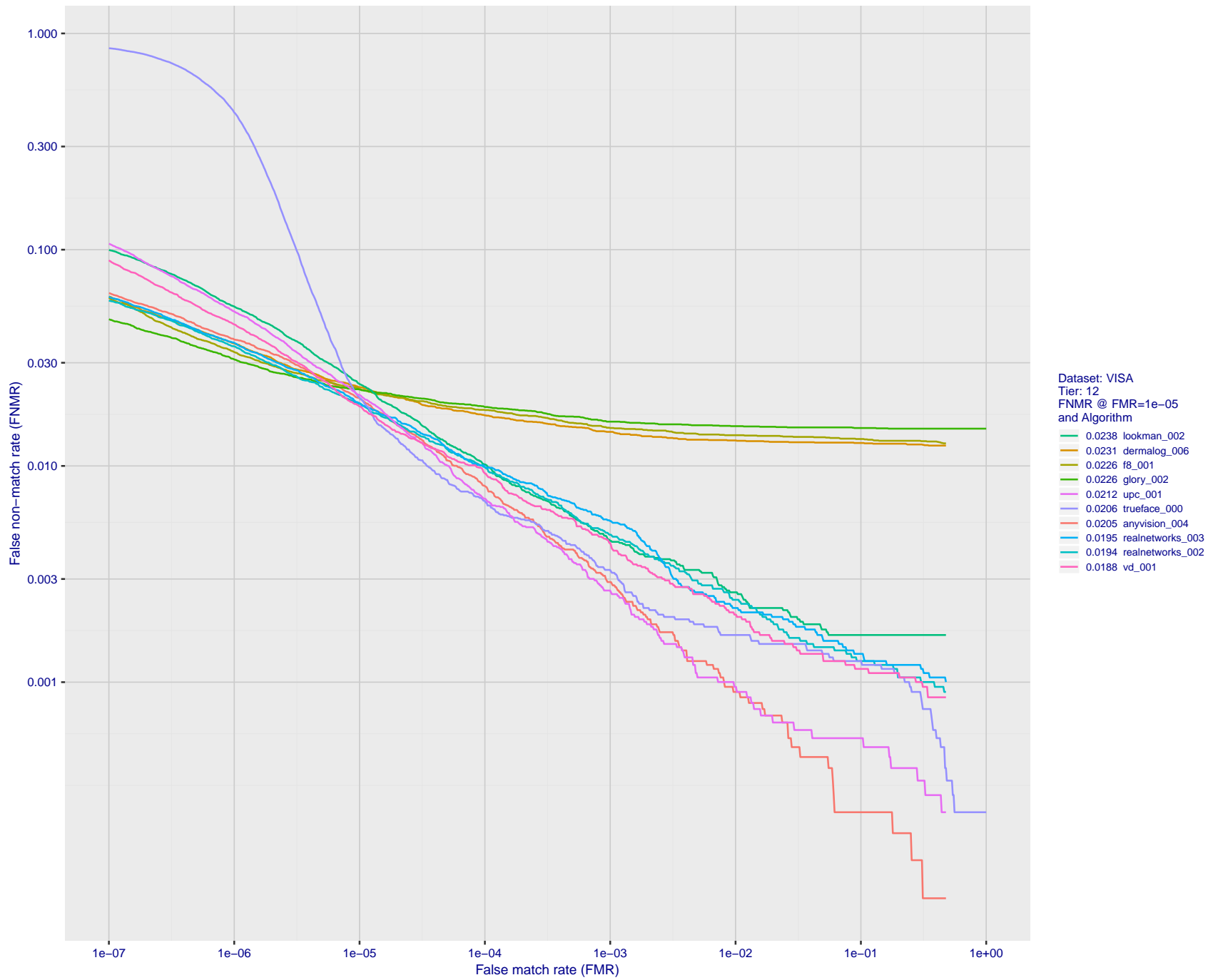


Figure 23: For the visa images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show many decades of FMR.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

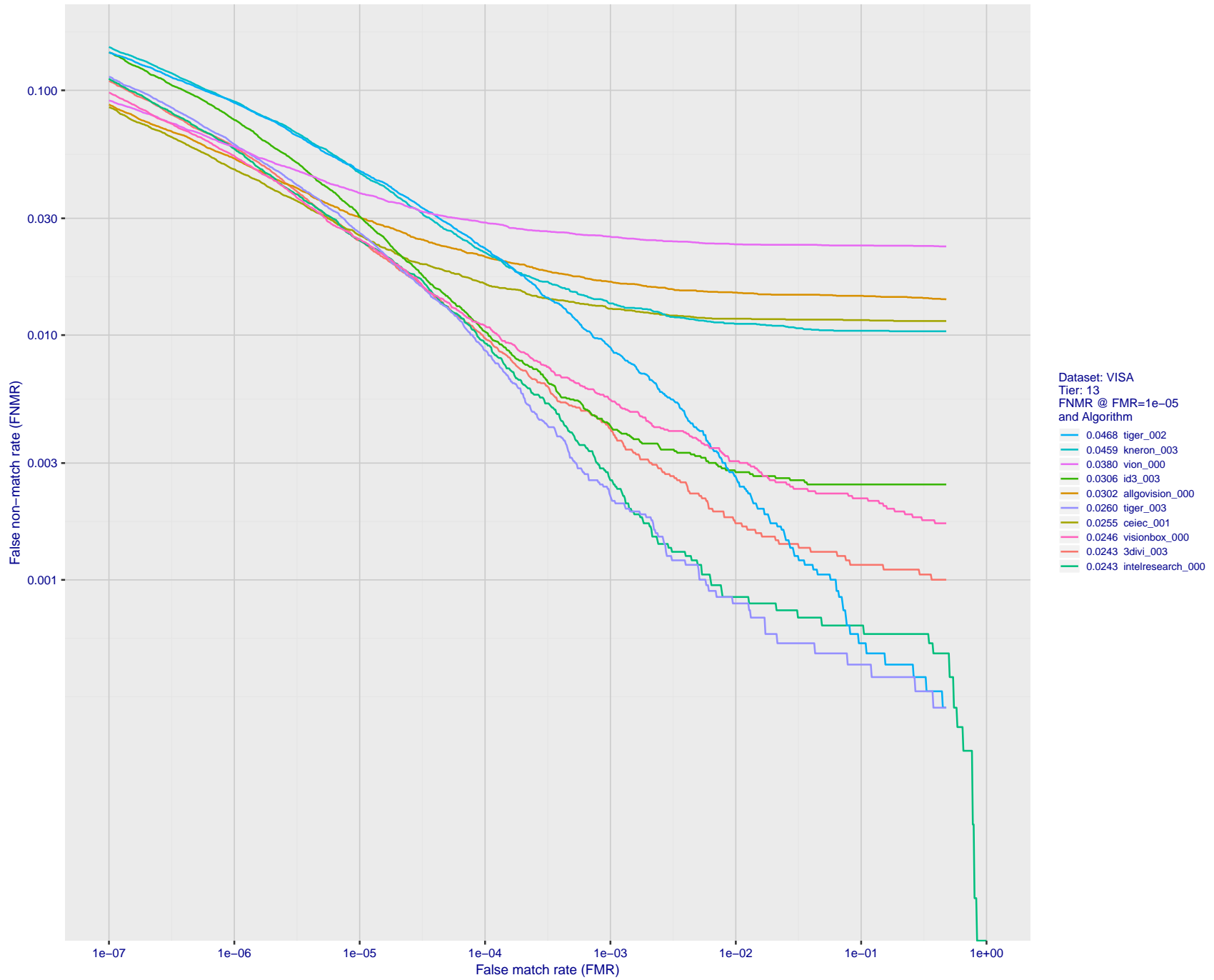


Figure 24: For the visa images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show many decades of FMR.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

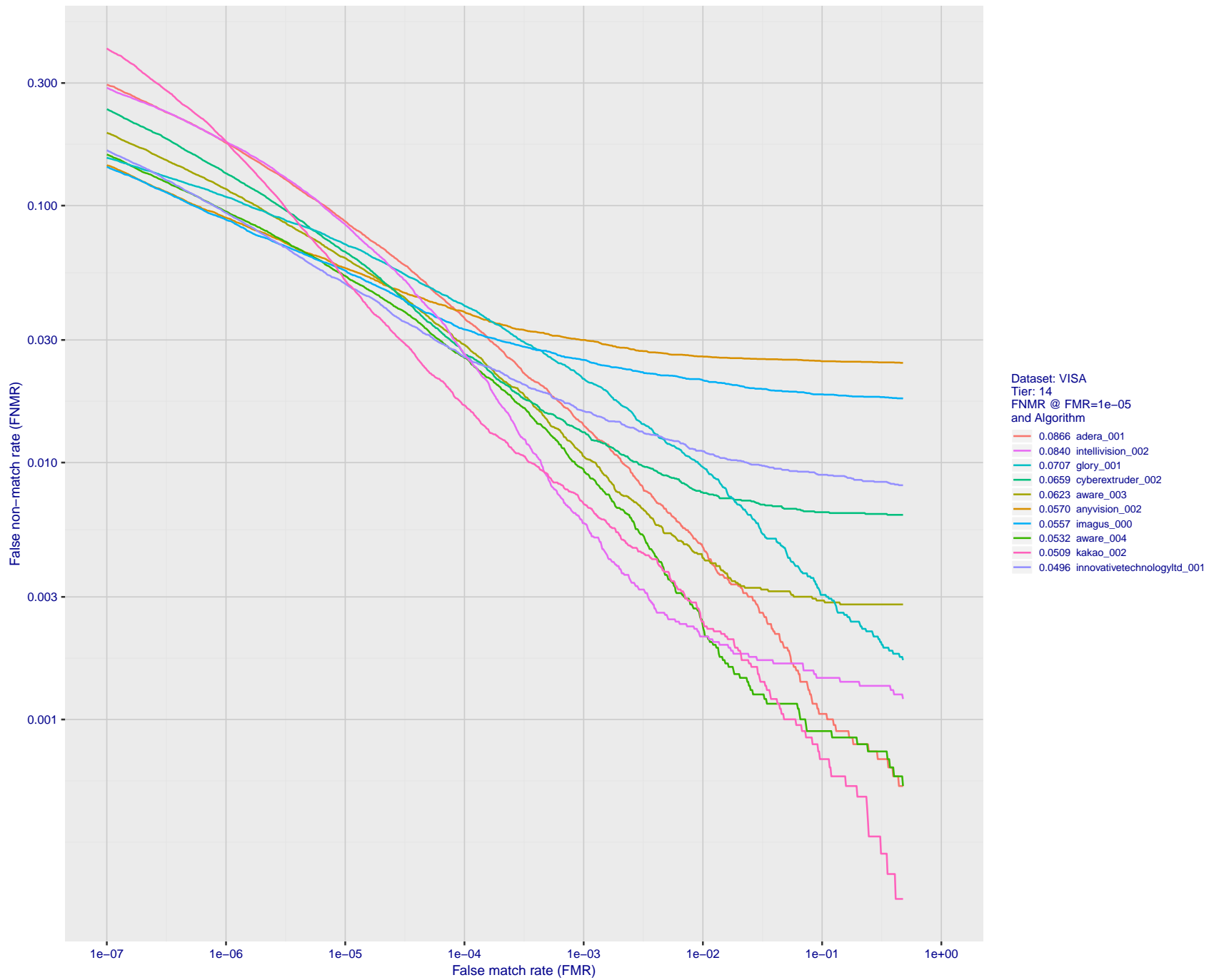


Figure 25: For the visa images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show many decades of FMR.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

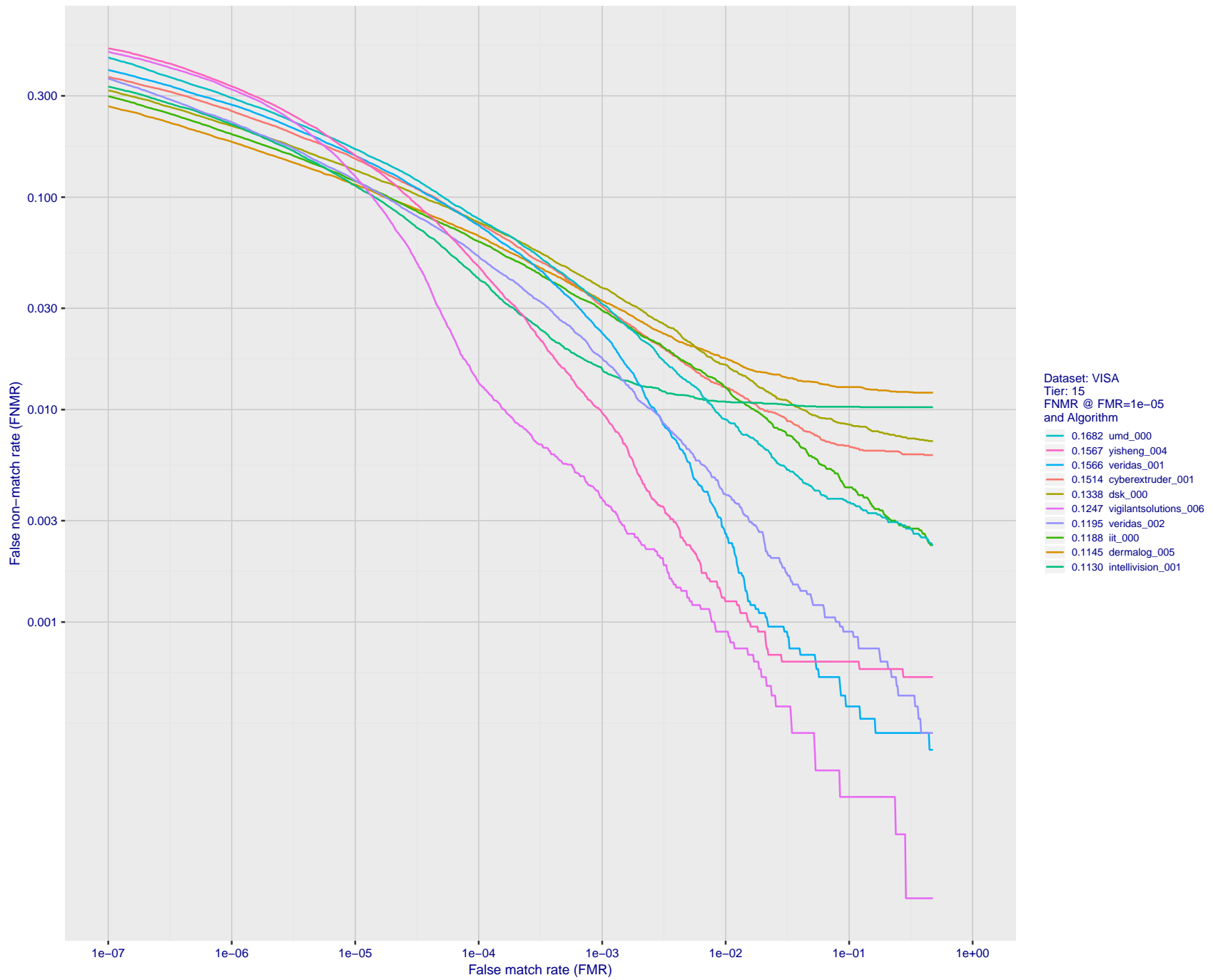


Figure 26: For the visa images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show many decades of FMR.

2019/11/19 11:24:36

FNMR(T)  
 FMR(T)  
 "False non-match rate"  
 "False match rate"

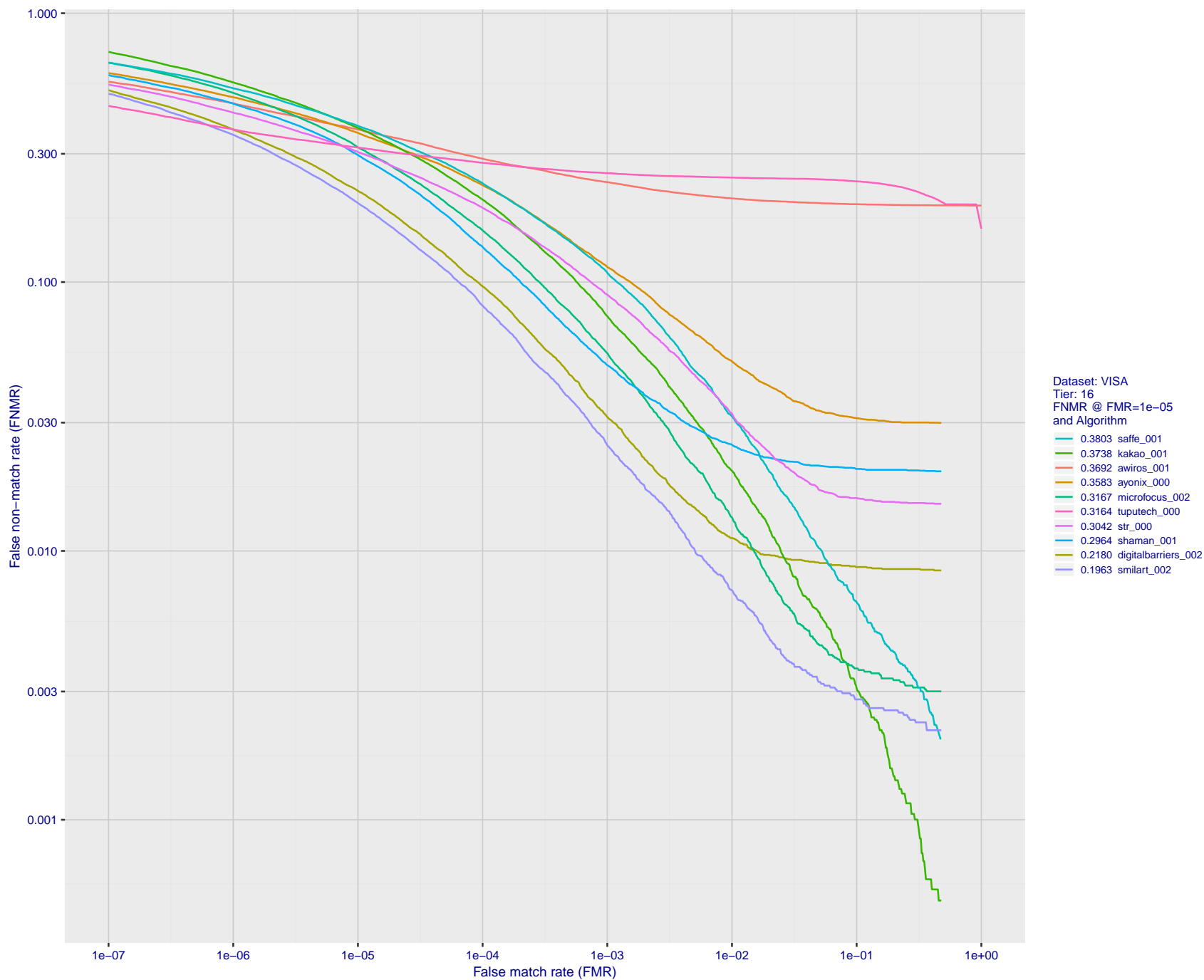


Figure 27: For the visa images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show many decades of FMR.

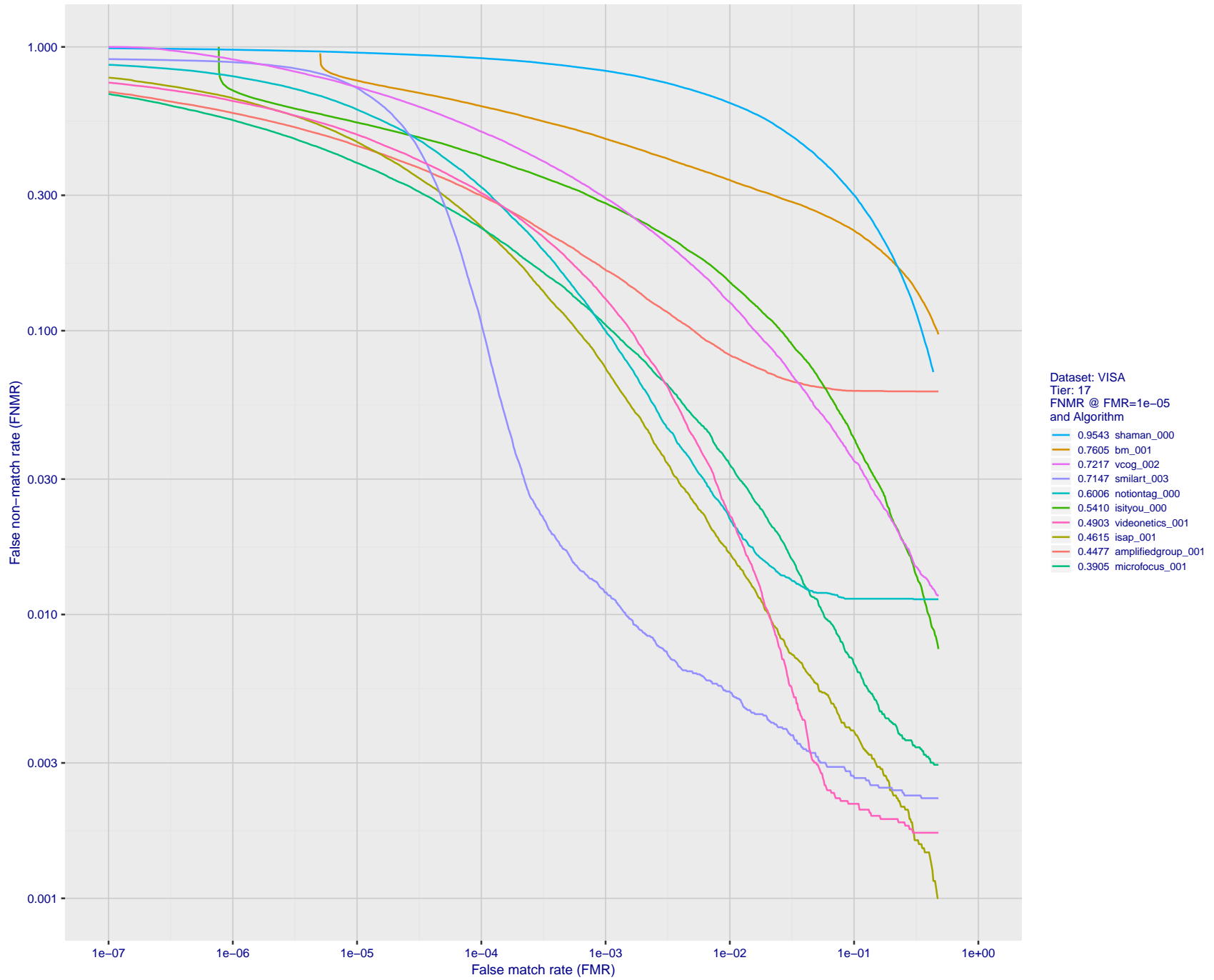


Figure 28: For the visa images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show many decades of FMR.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

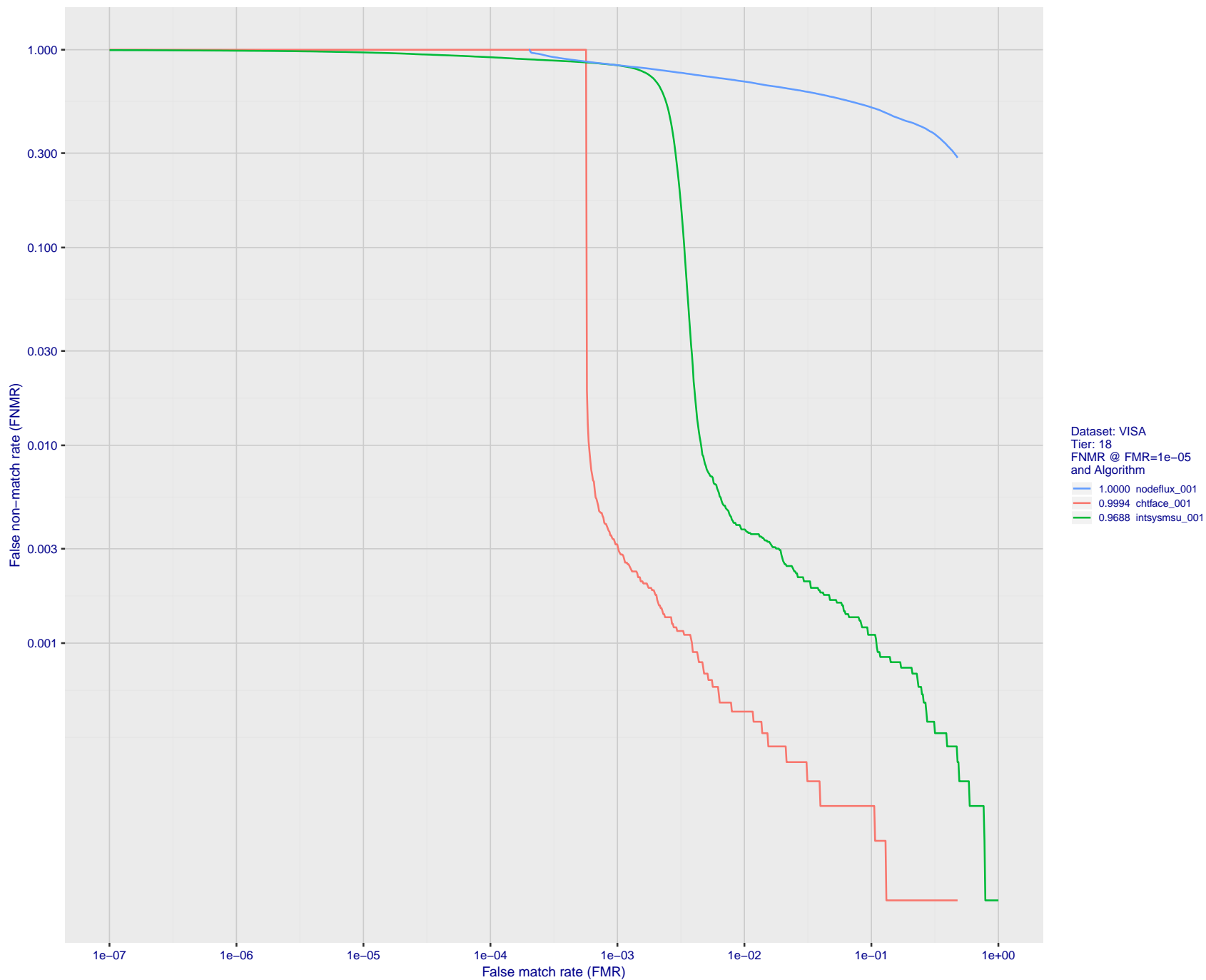


Figure 29: For the visa images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show many decades of FMR.

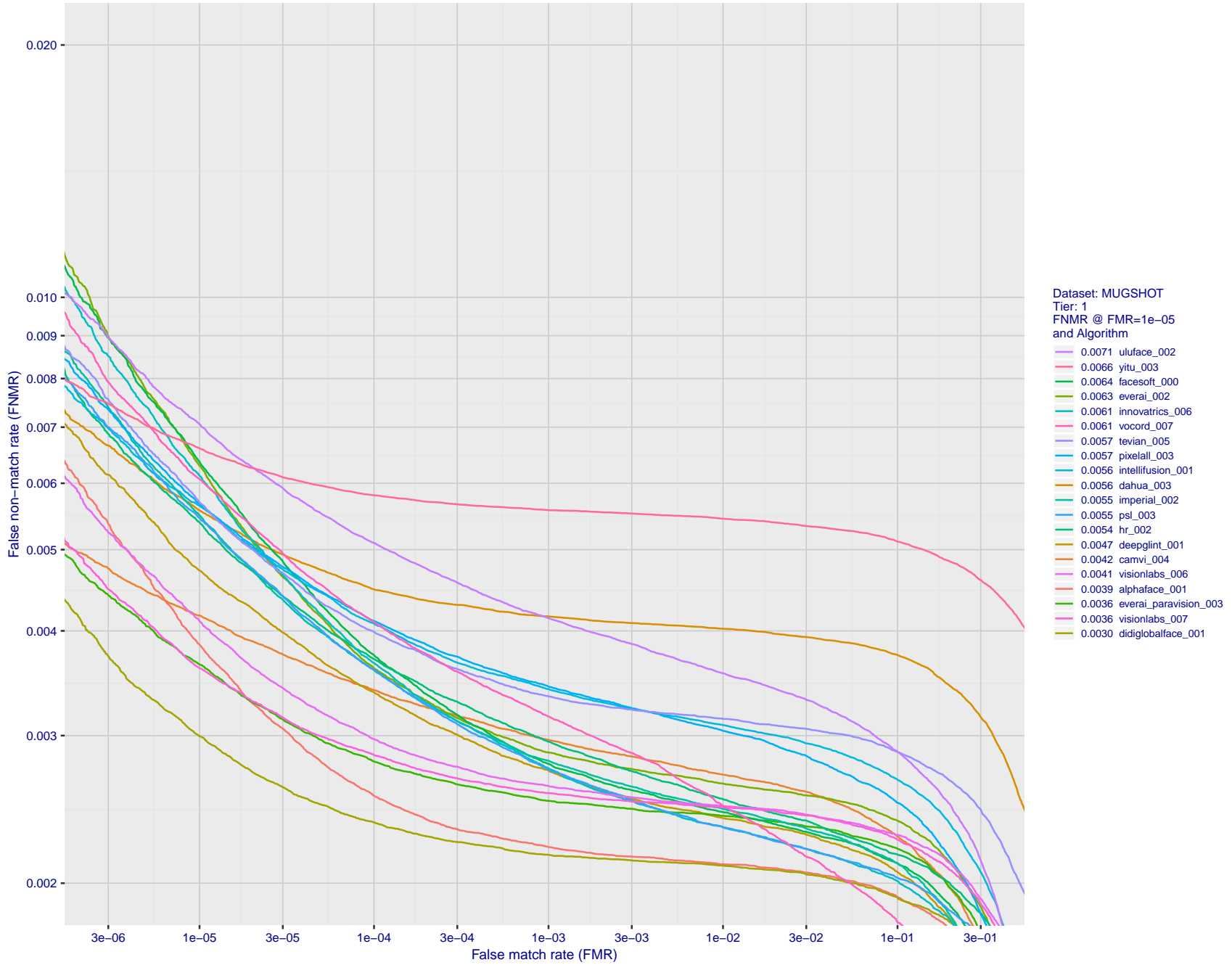


Figure 30: For the mugshot images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show decades of FMR.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"



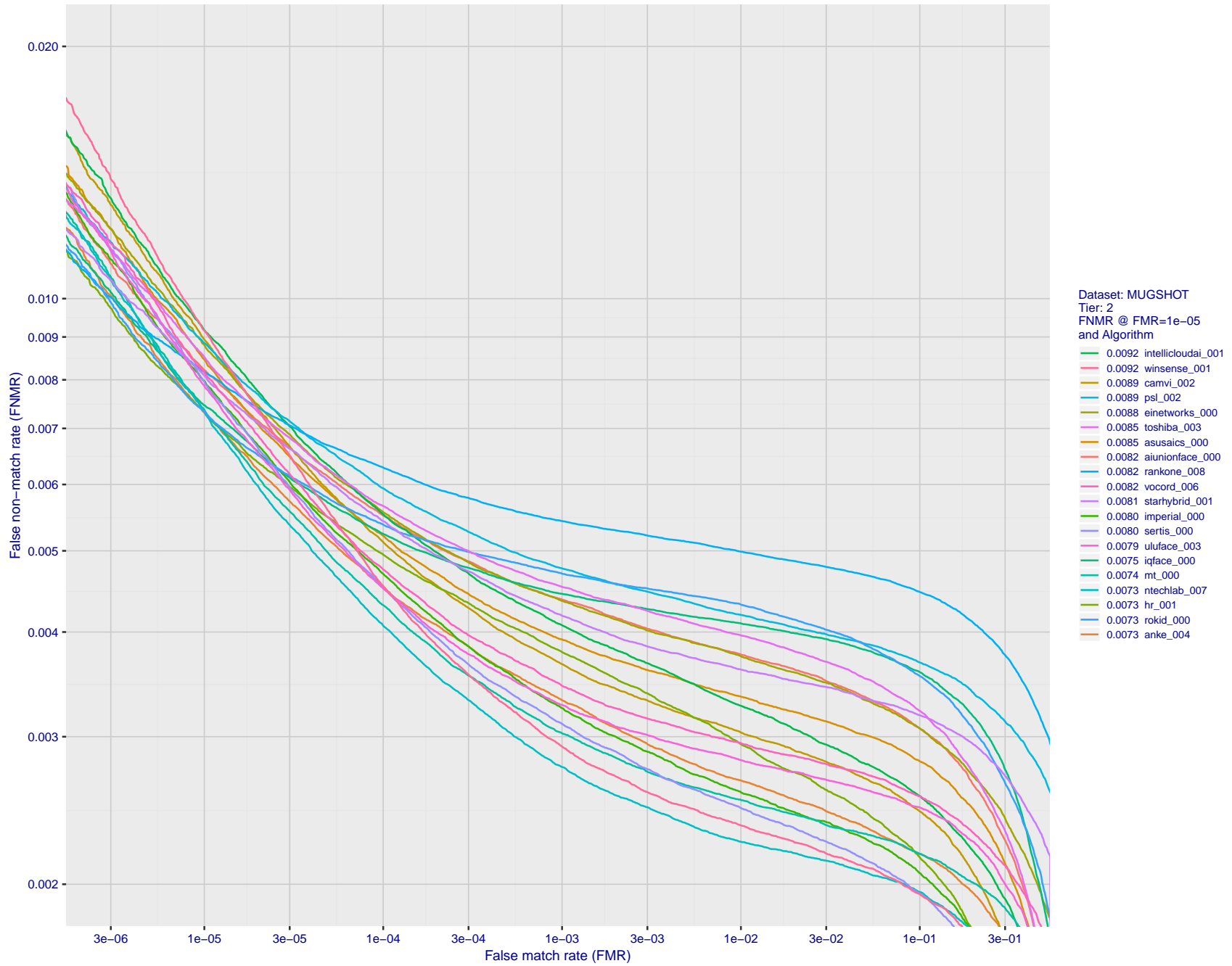


Figure 31: For the mugshot images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show decades of FMR.

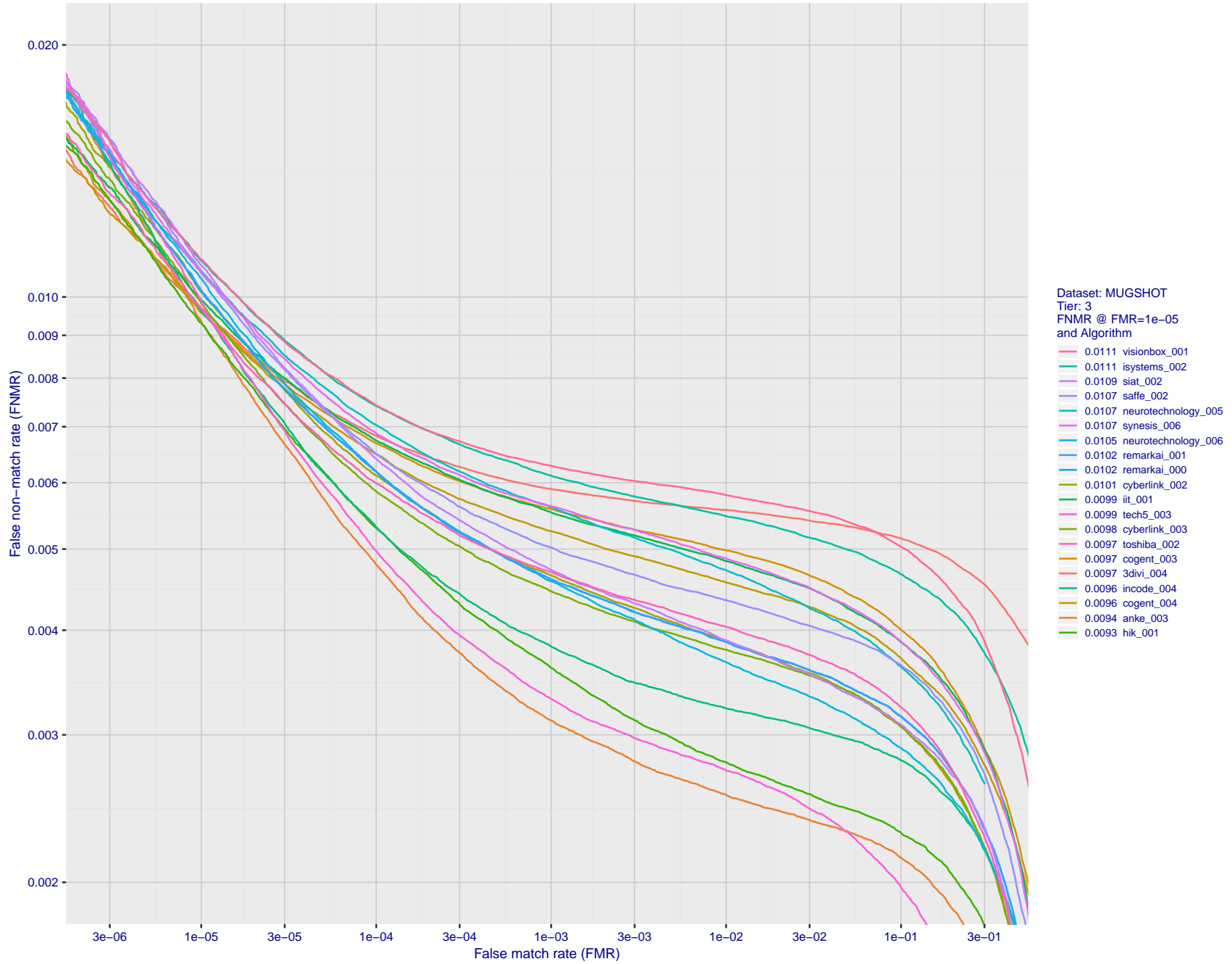


Figure 32: For the mugshot images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show decades of FMR.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

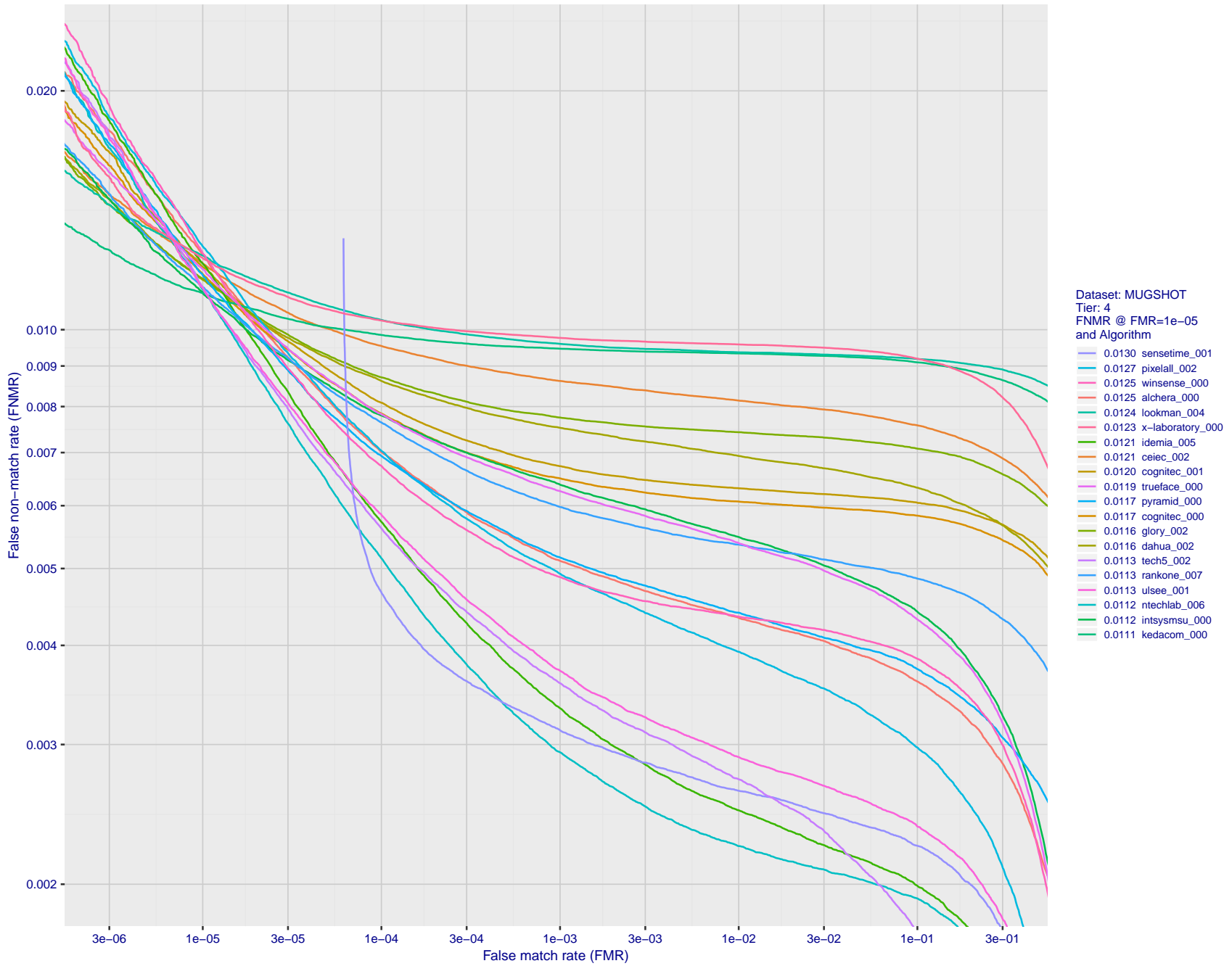
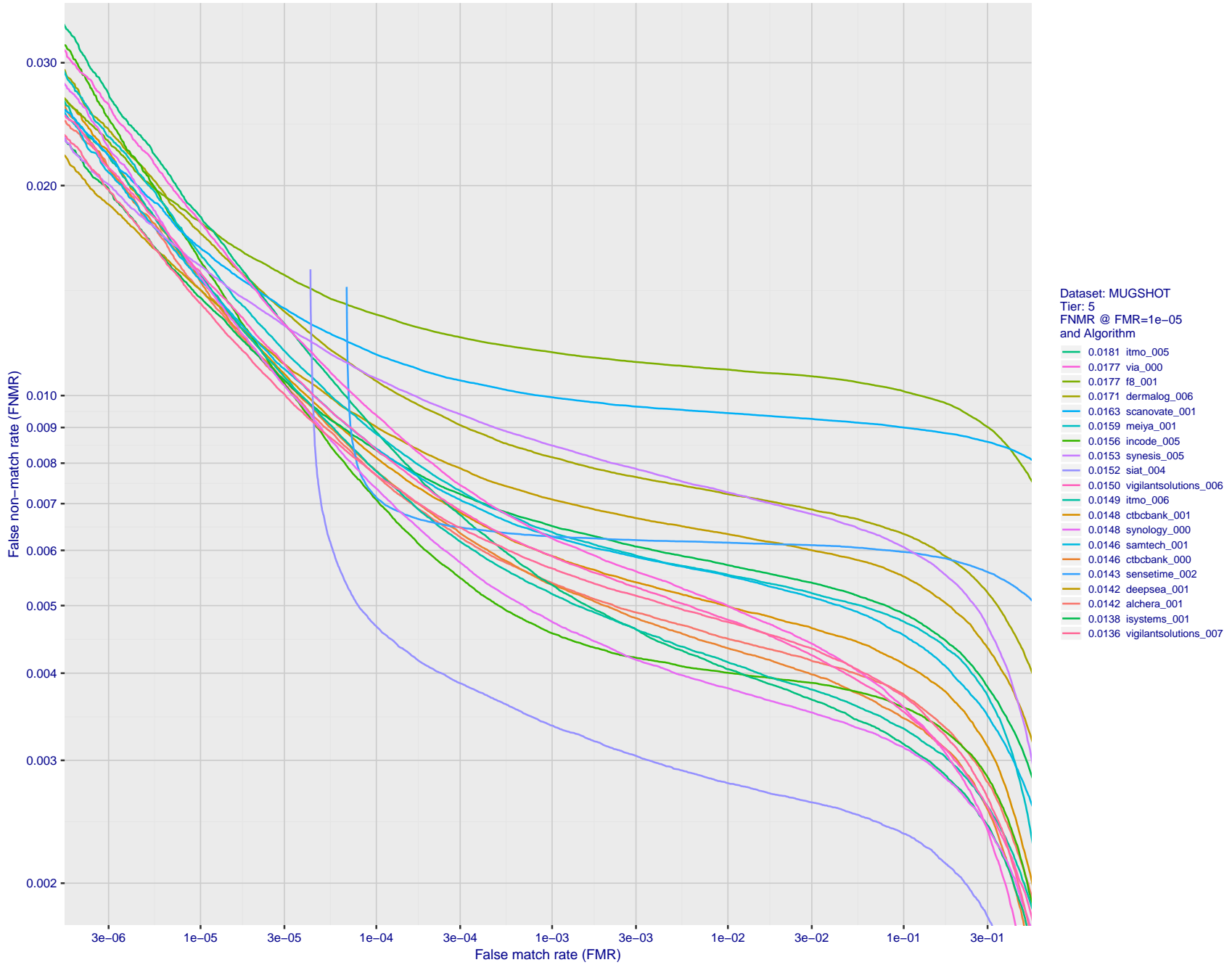
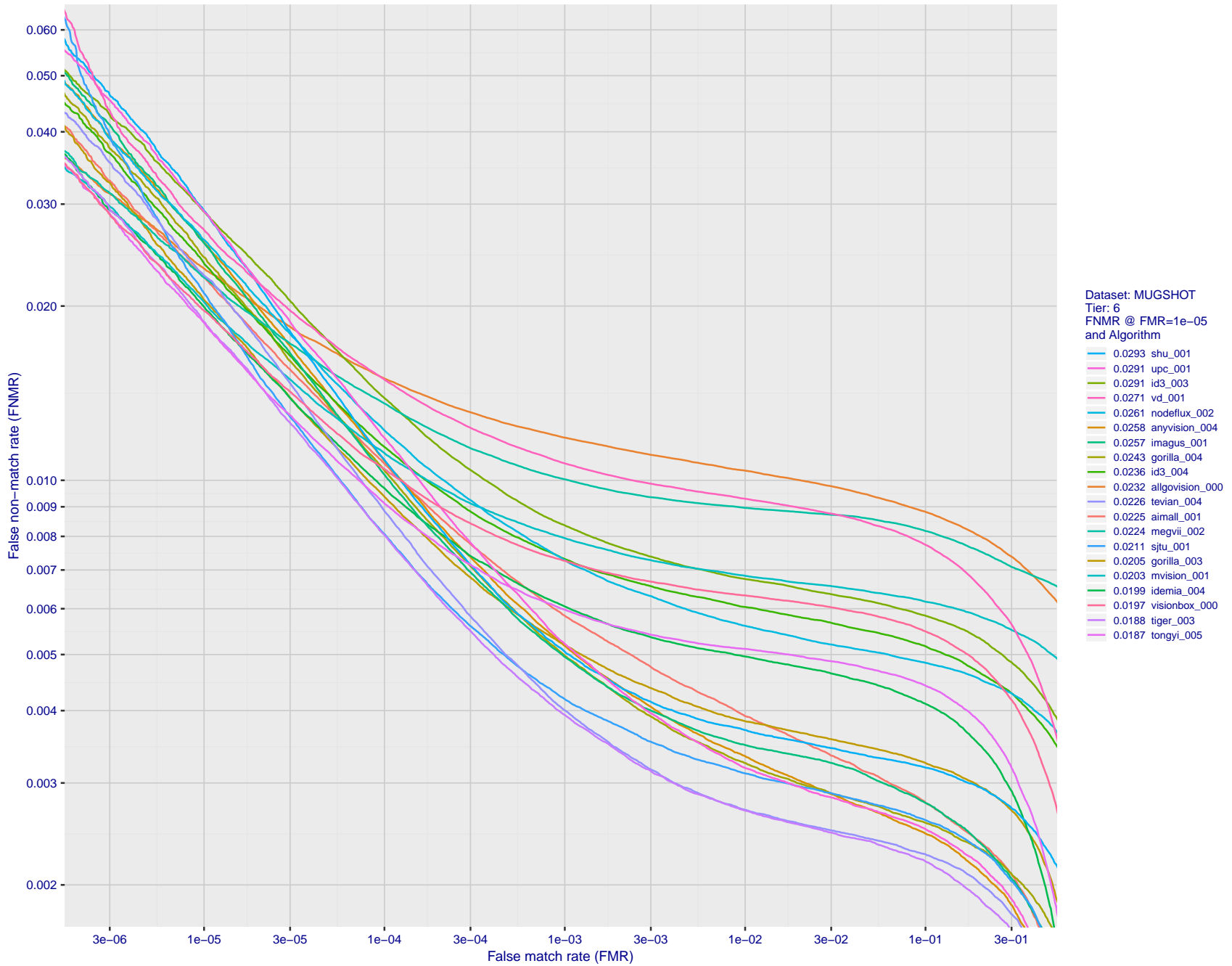


Figure 33: For the mugshot images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show decades of FMR.



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 34: For the mugshot images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold, T. The scales are logarithmic in order to show decades of FMR.



FNMR(T)  
 FMR(T)  
 "False non-match rate"  
 "False match rate"

Figure 35: For the mugshot images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold, T. The scales are logarithmic in order to show decades of FMR.

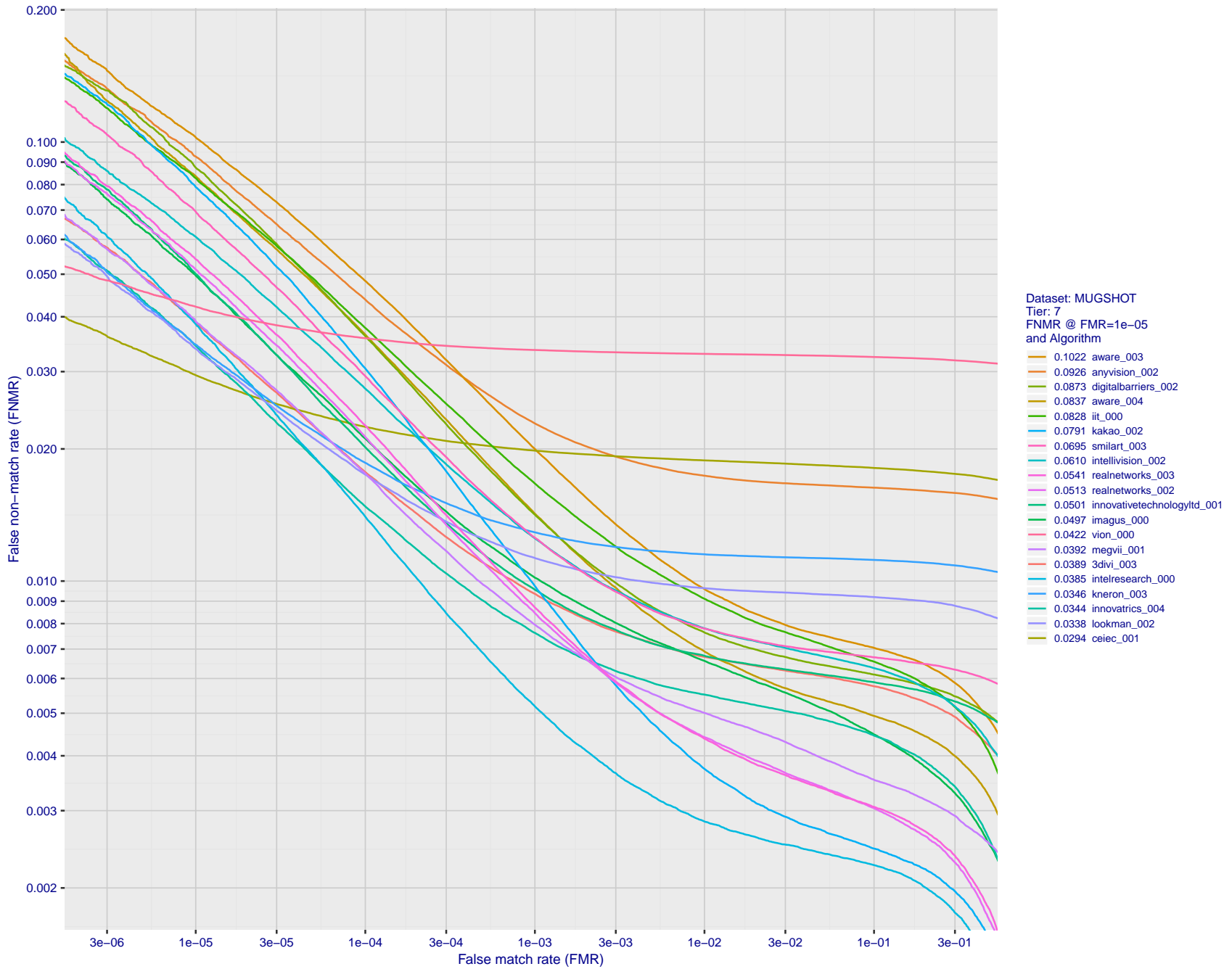


Figure 36: For the mugshot images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show decades of FMR.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

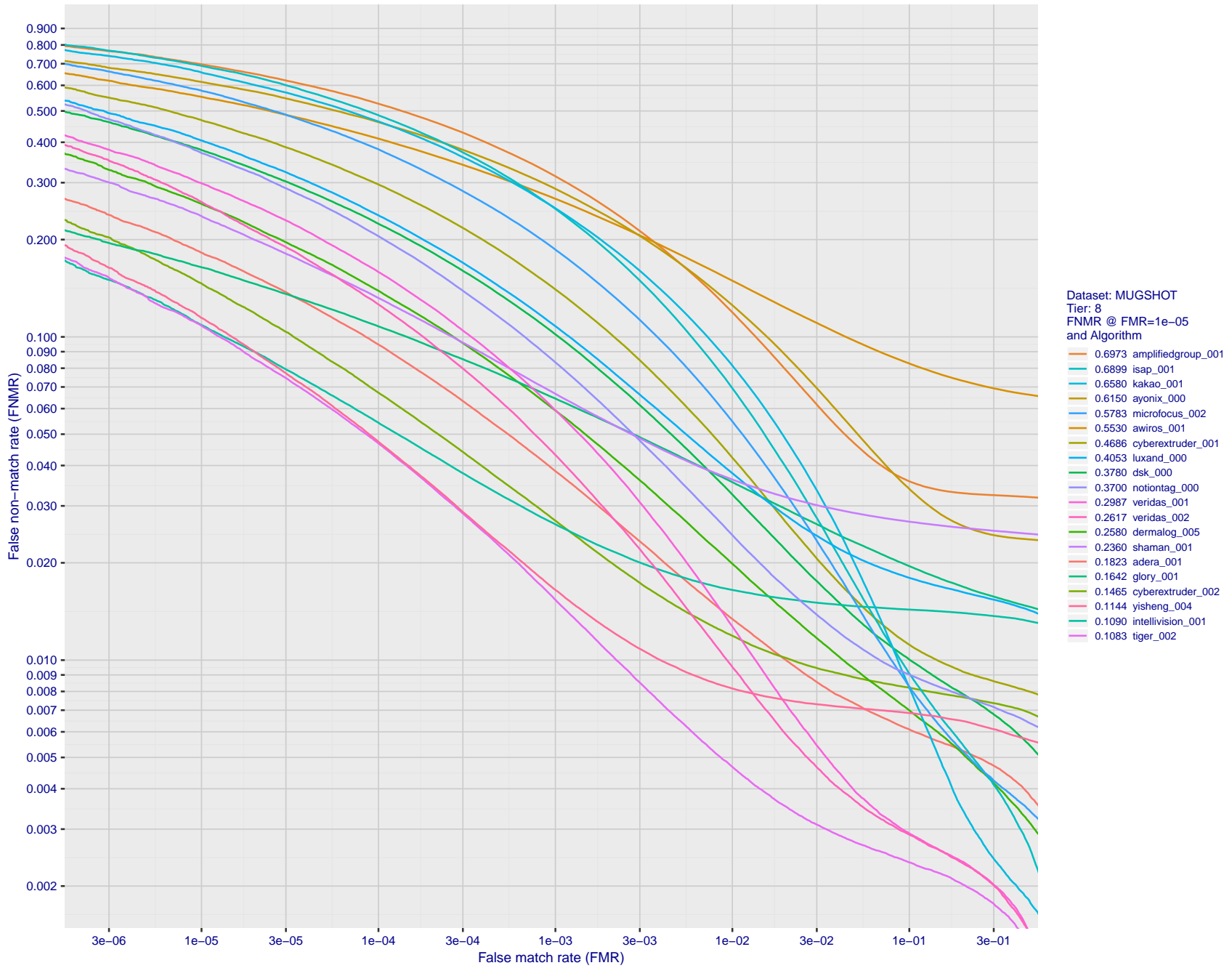


Figure 37: For the mugshot images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show decades of FMR.



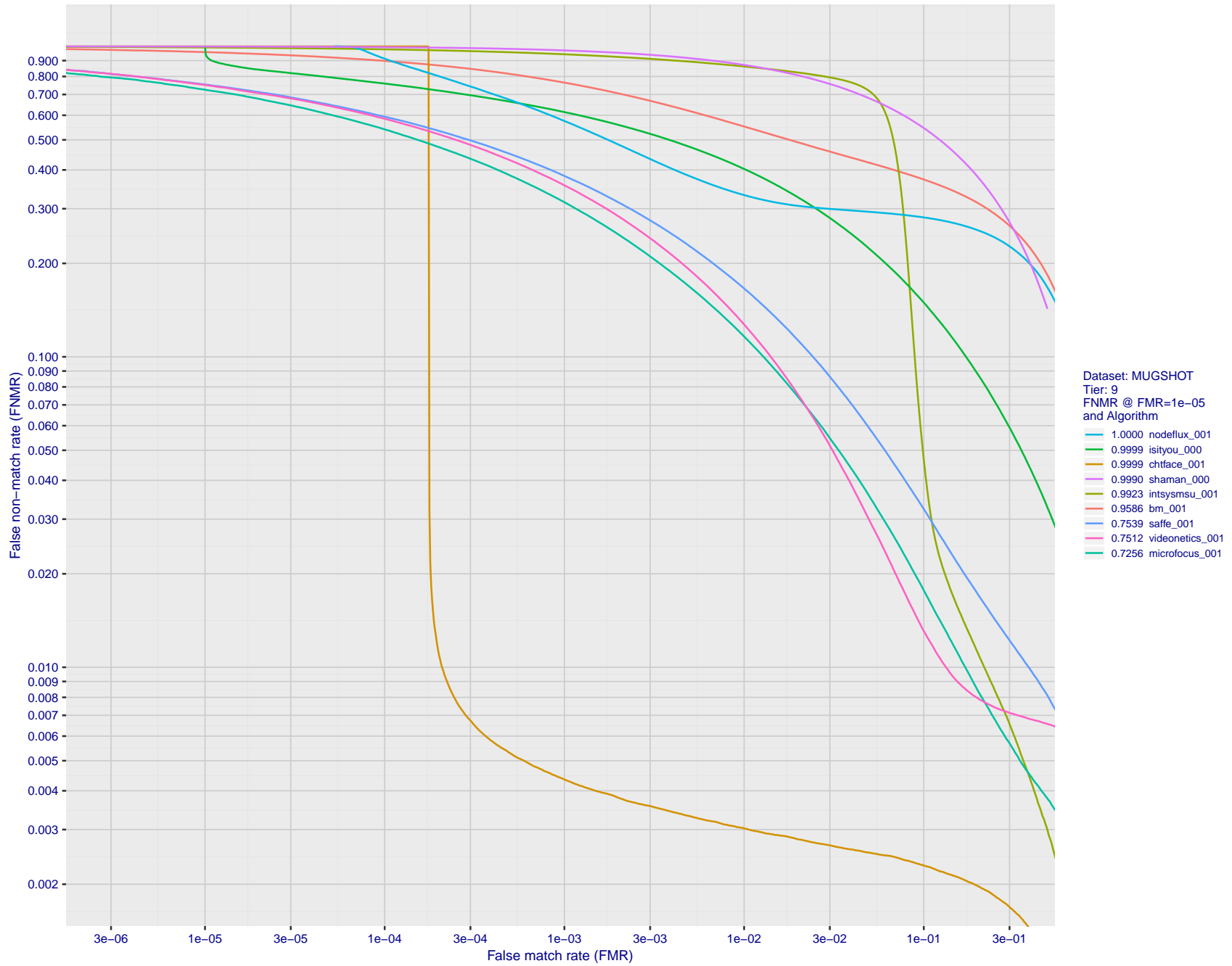
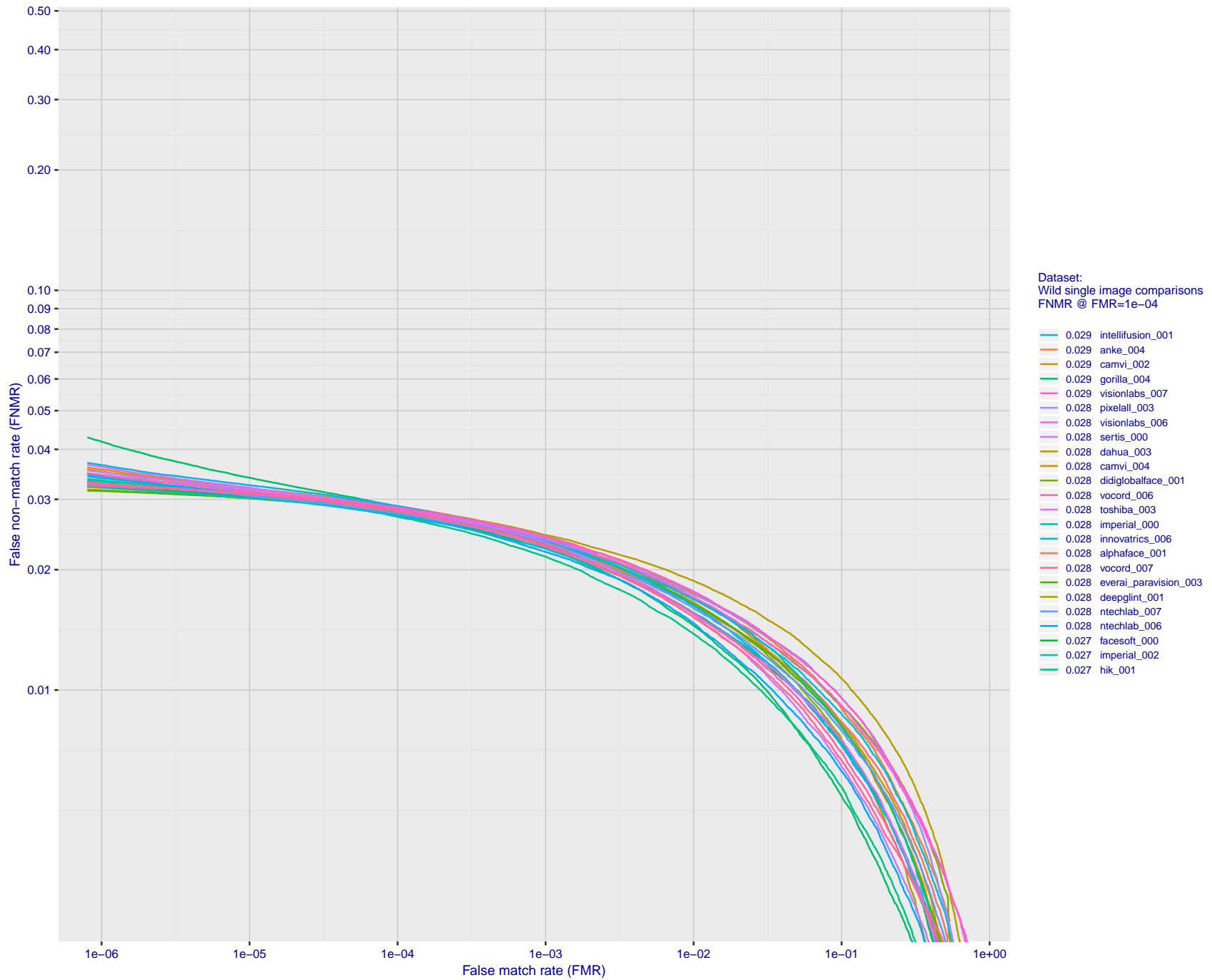


Figure 38: For the mugshot images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show decades of FMR.





FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 39: For the 2018 wild image comparisons, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show several decades of FMR.

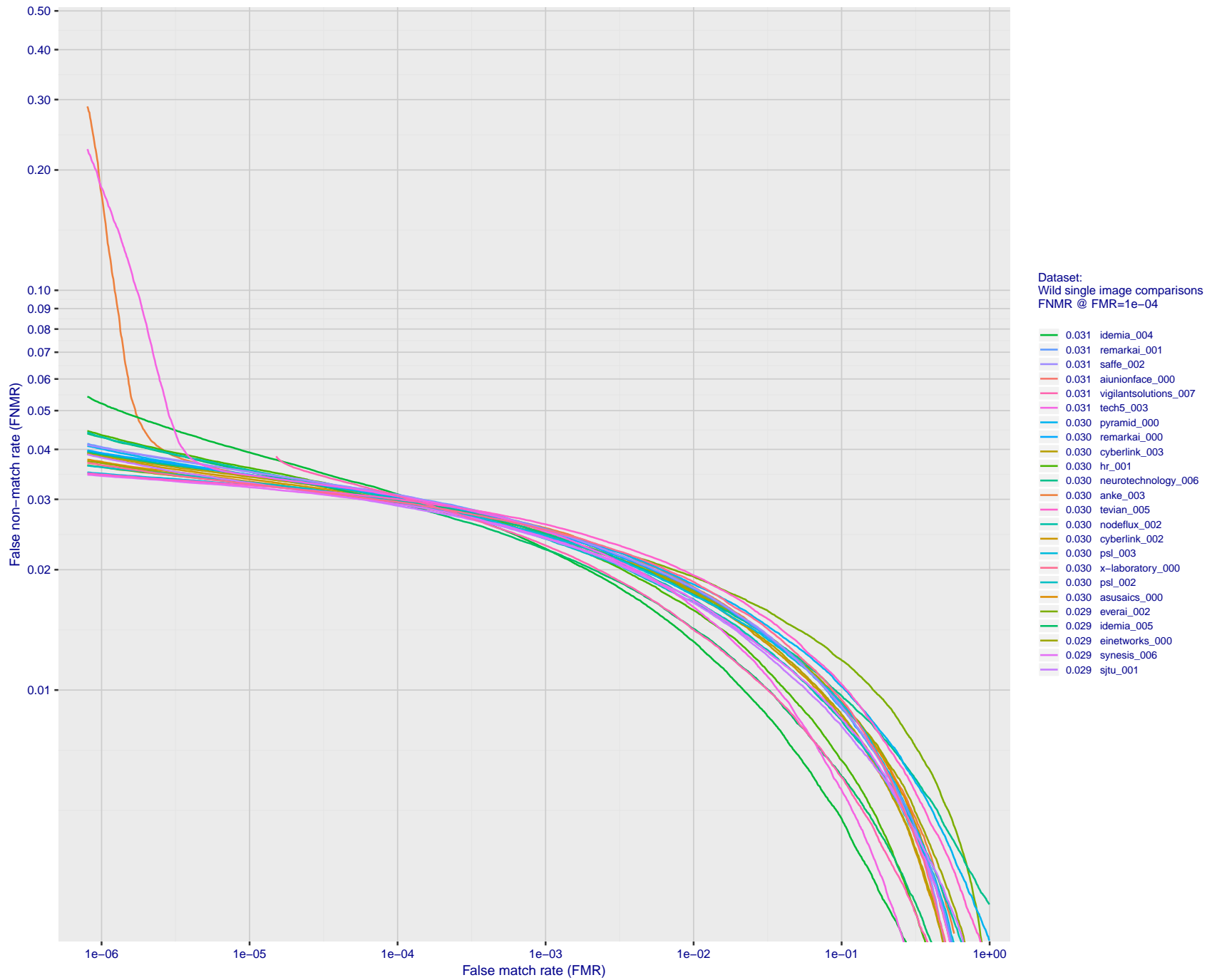
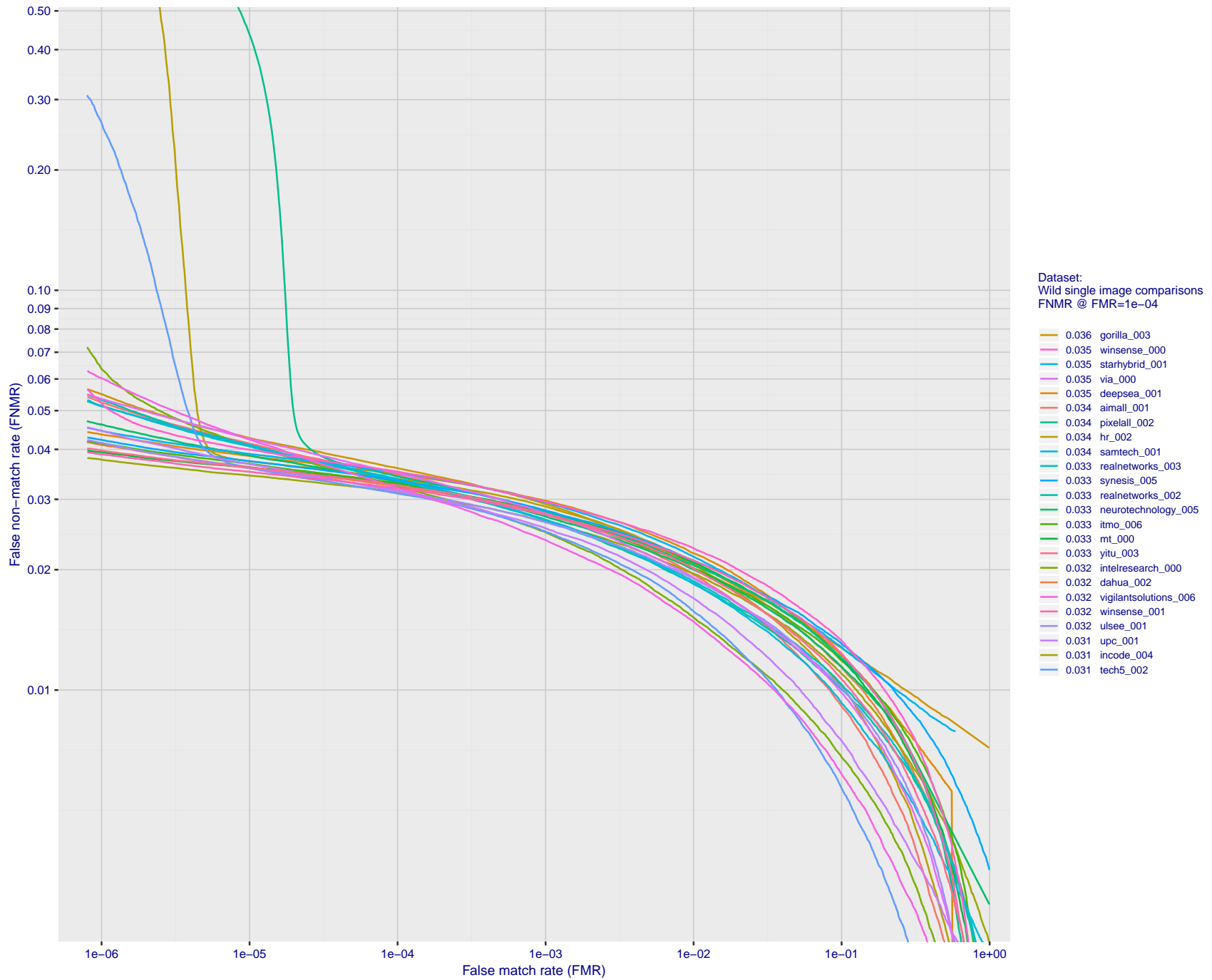


Figure 40: For the 2018 wild image comparisons, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show several decades of FMR.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 41: For the 2018 wild image comparisons, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show several decades of FMR.

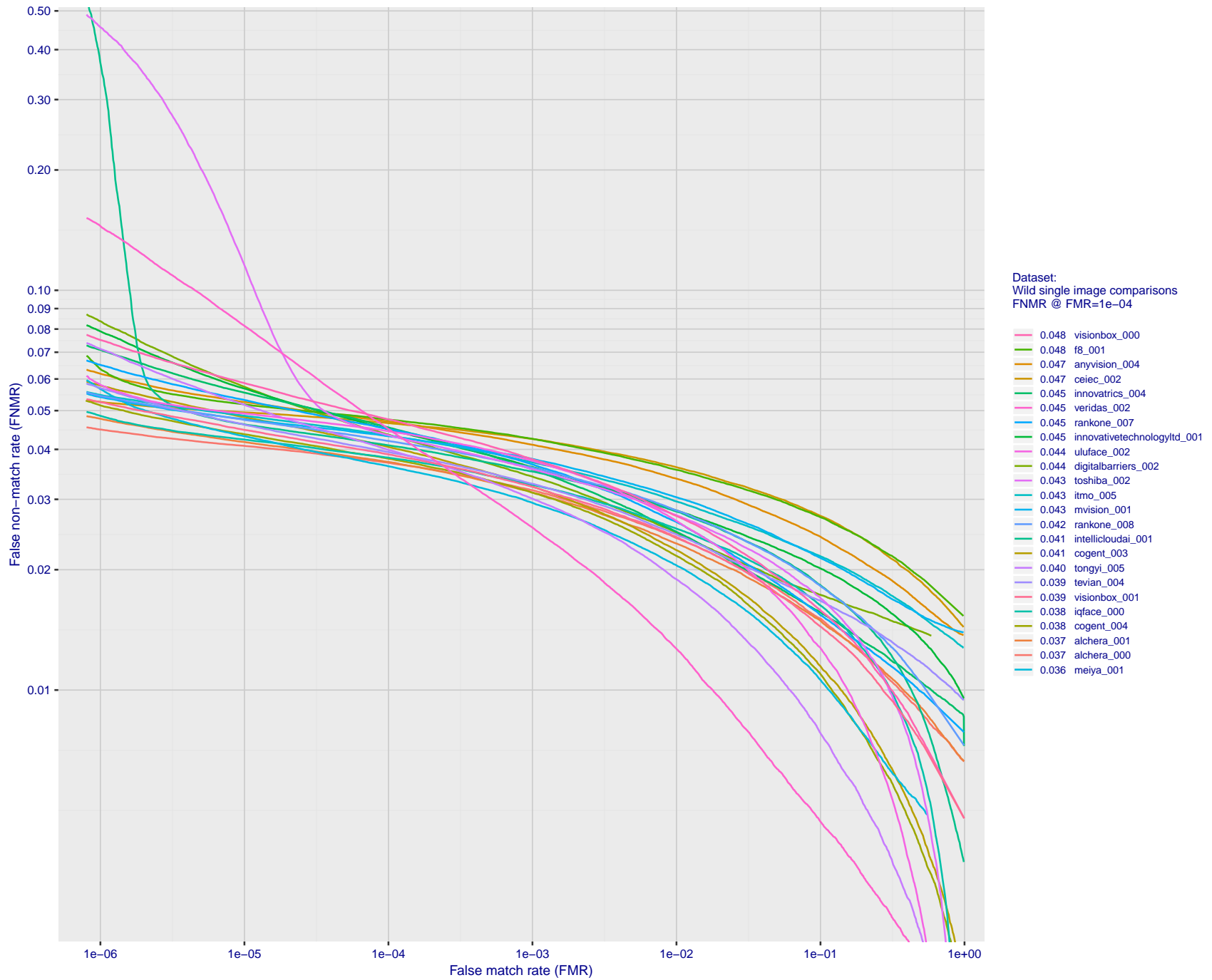


Figure 42: For the 2018 wild image comparisons, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show several decades of FMR.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

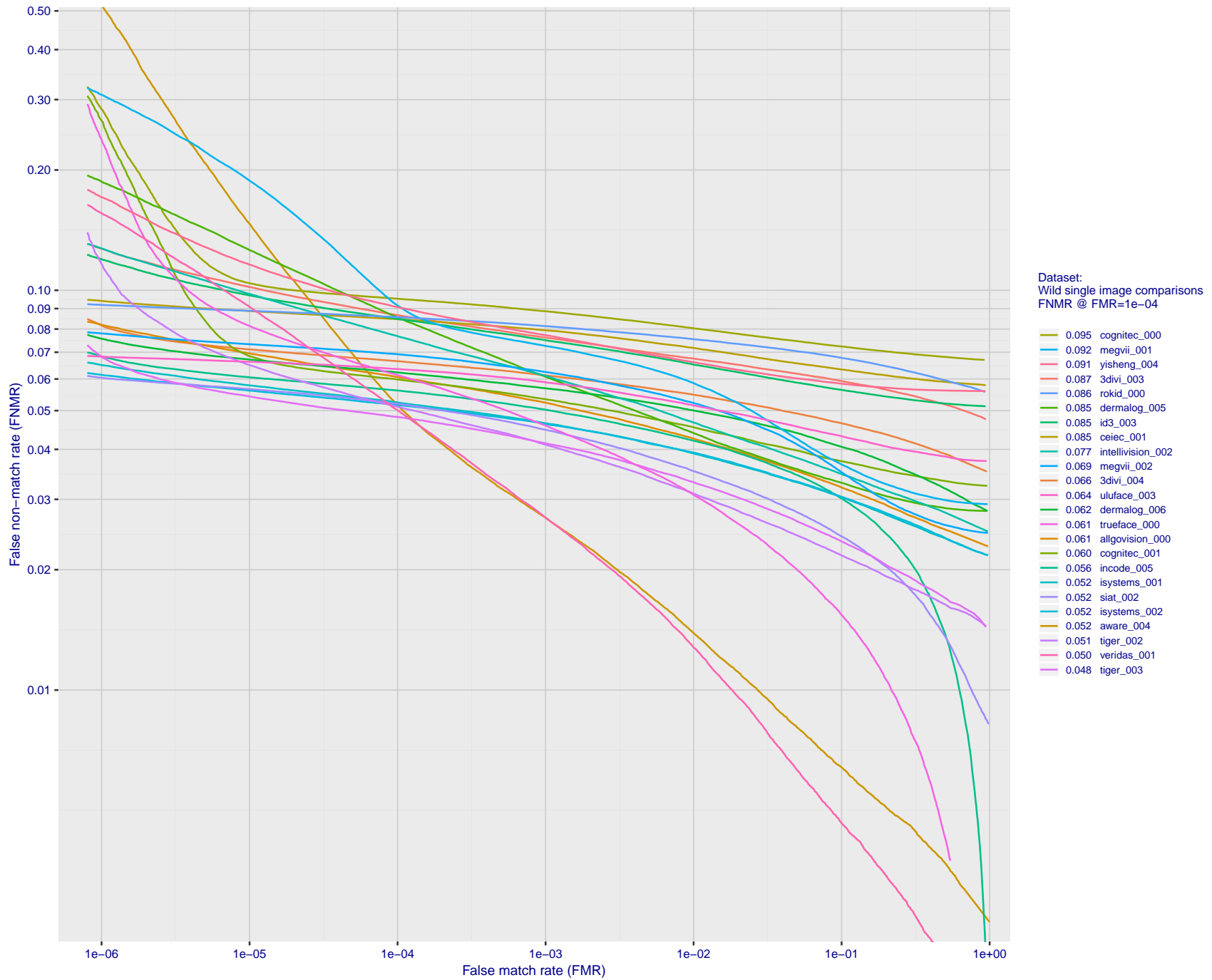


Figure 43: For the 2018 wild image comparisons, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold, T. The scales are logarithmic in order to show several decades of FMR.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

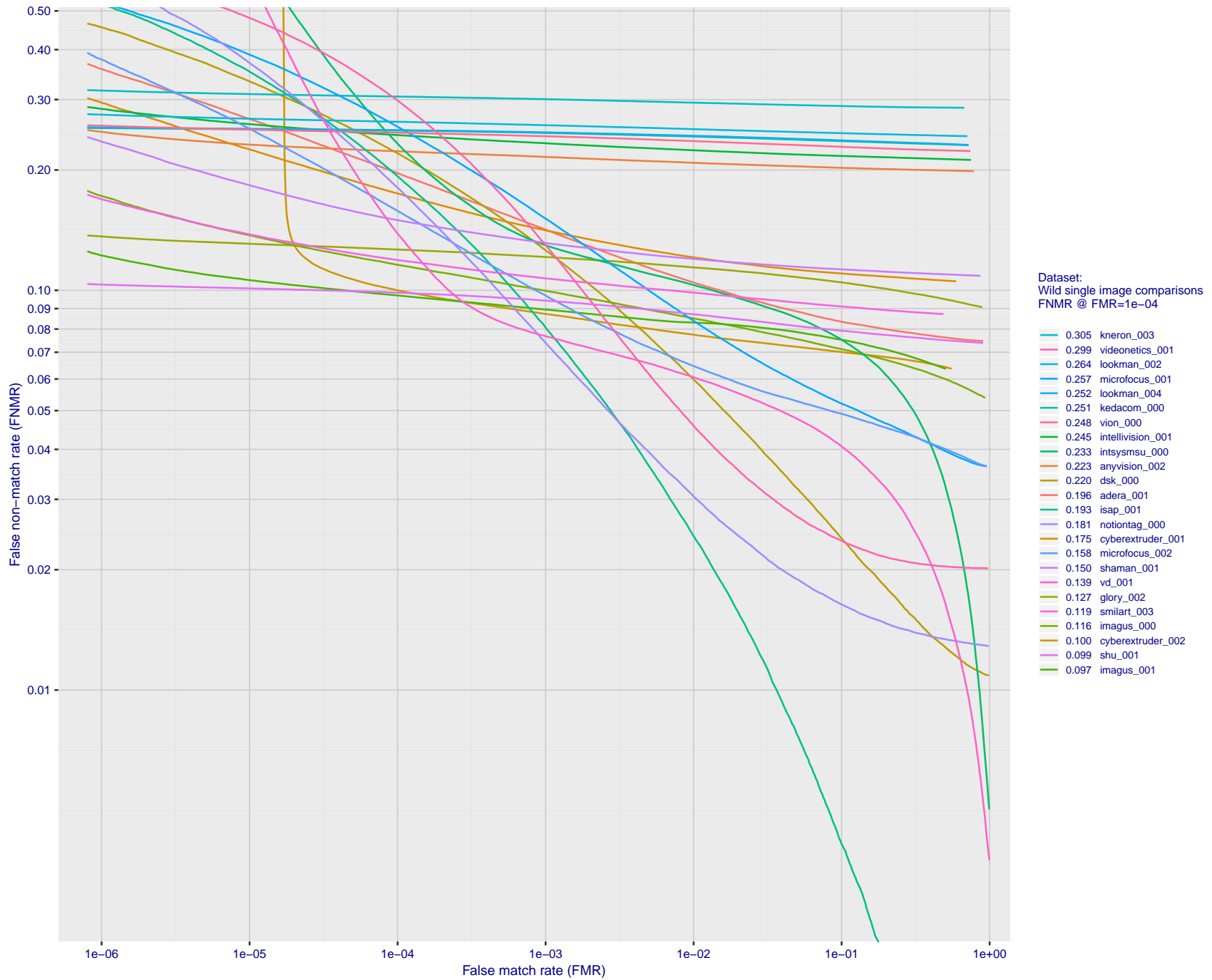


Figure 44: For the 2018 wild image comparisons, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold, T. The scales are logarithmic in order to show several decades of FMR.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

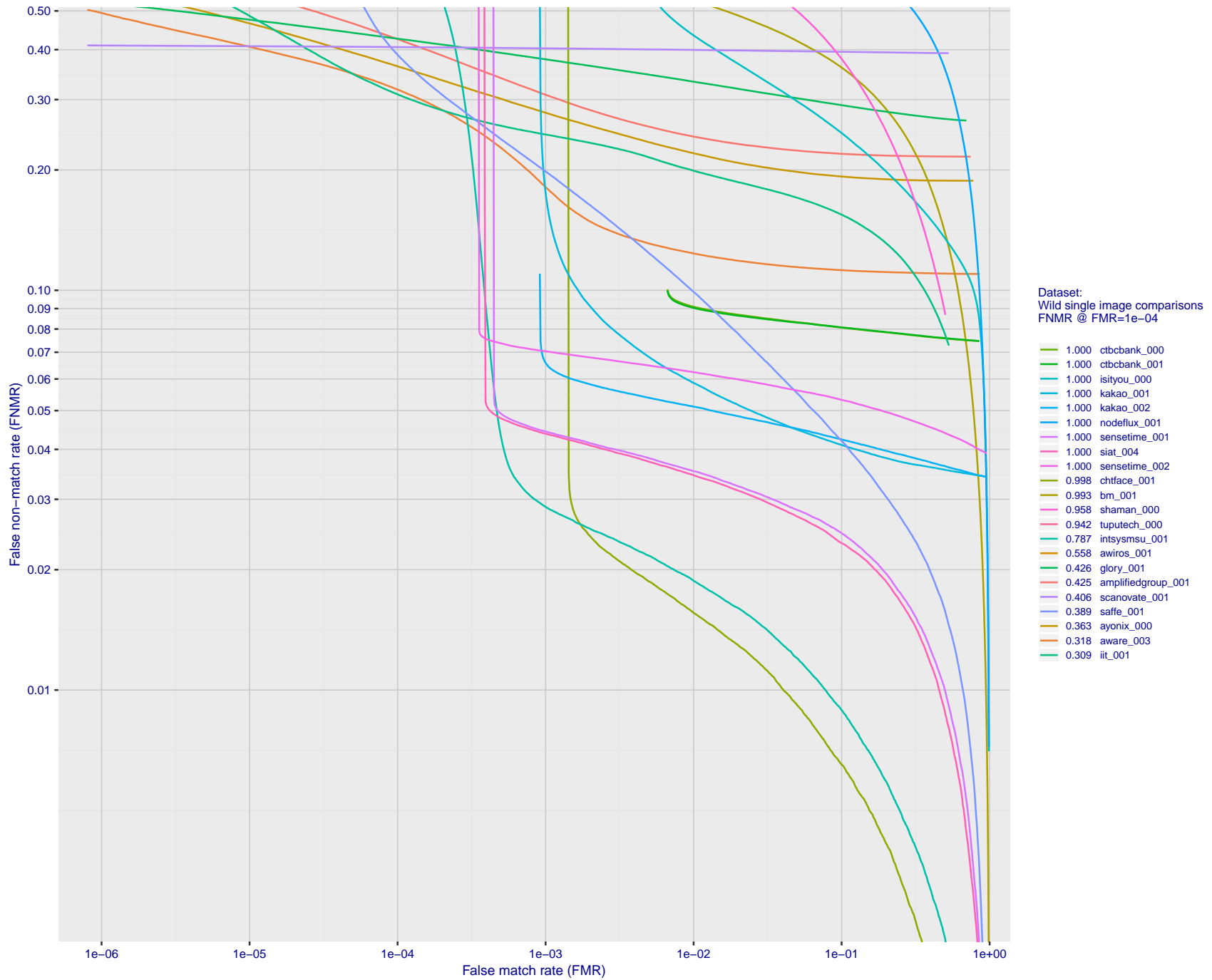


Figure 45: For the 2018 wild image comparisons, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold, T. The scales are logarithmic in order to show several decades of FMR.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

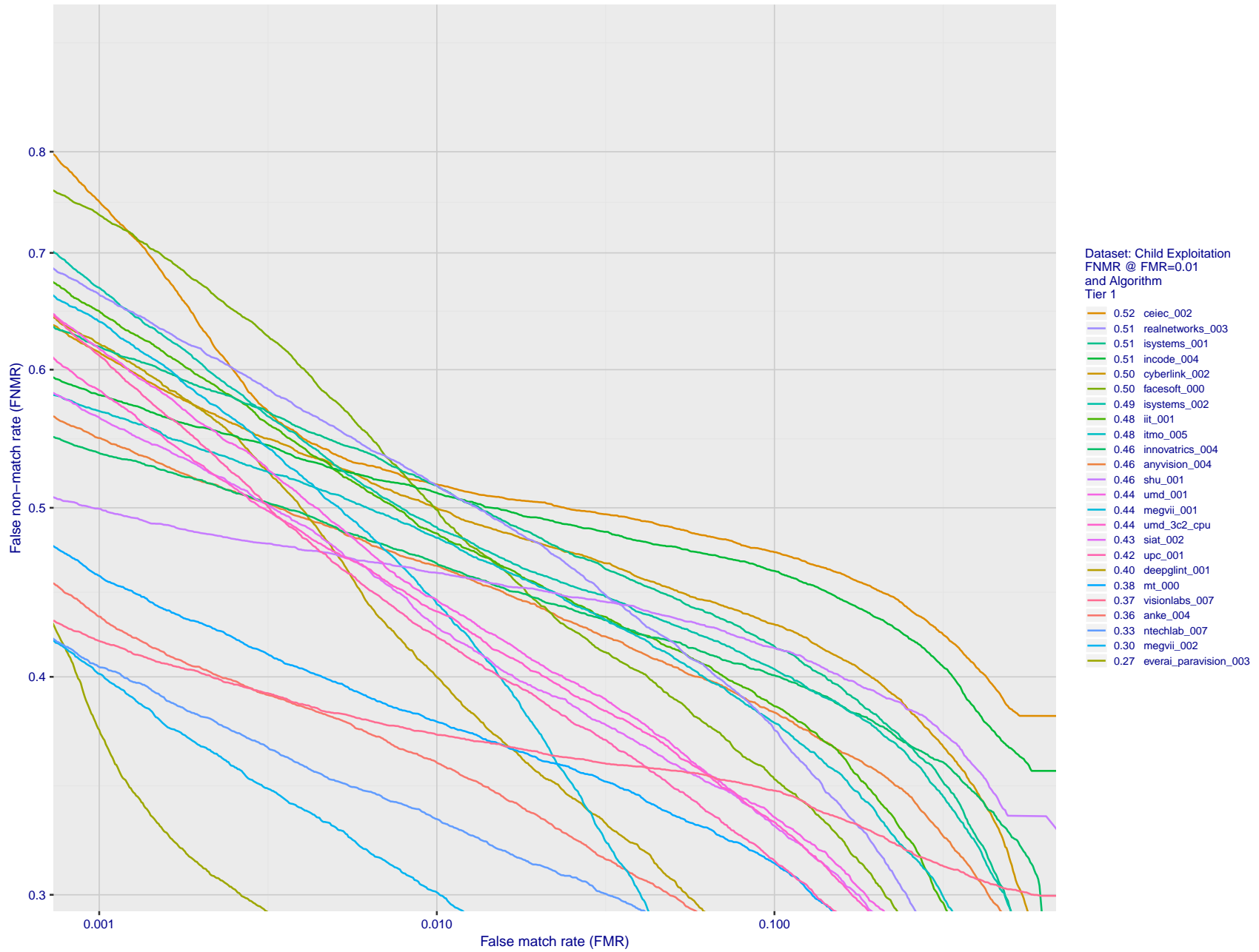


Figure 46: For child exploitation images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold, T. The scales are logarithmic in order to show many decades of FMR. Accuracy is poor because many images have adverse quality characteristics, and because detection and enrollment fails.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"



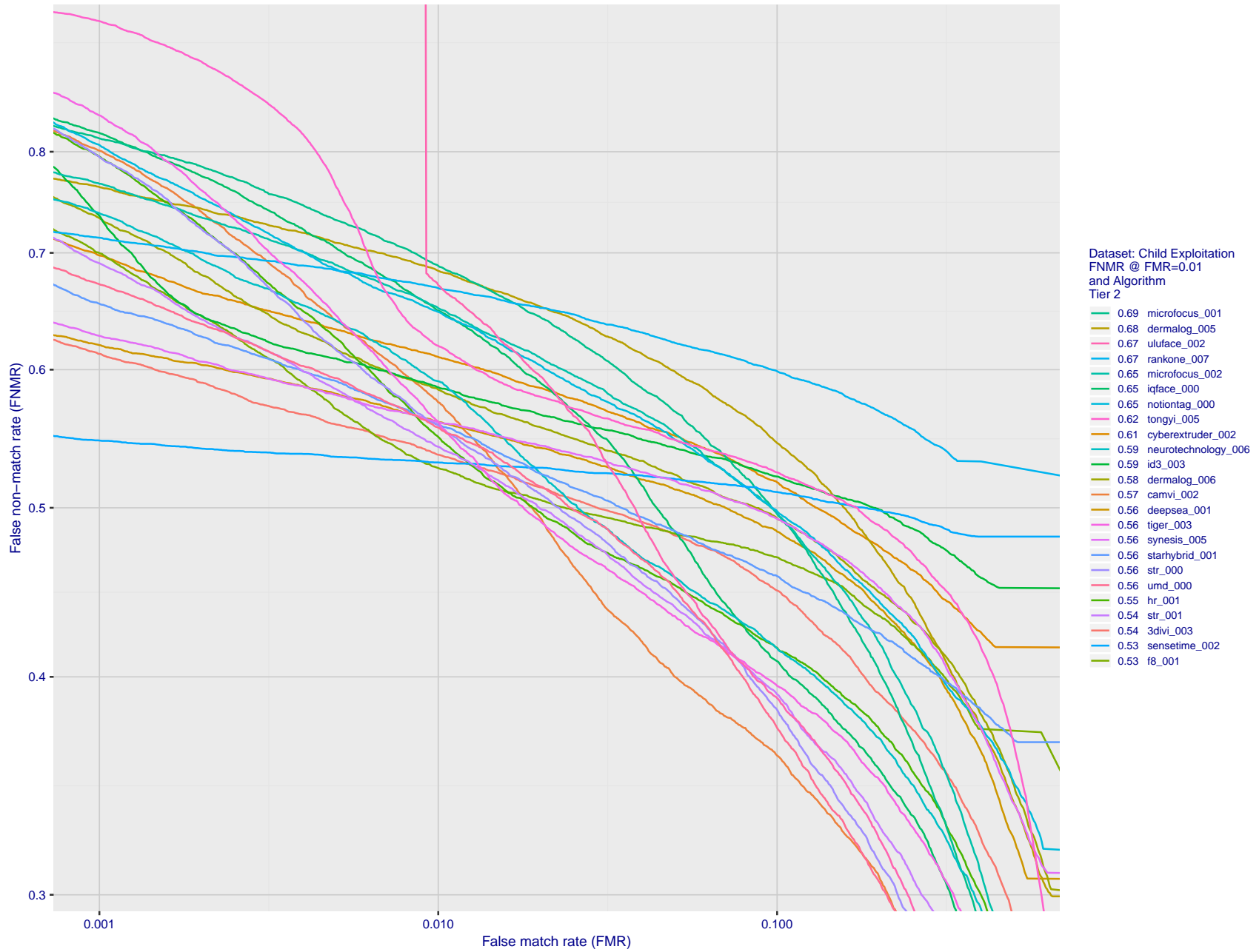


Figure 47: For child exploitation images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show many decades of FMR. Accuracy is poor because many images have adverse quality characteristics, and because detection and enrollment fails.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

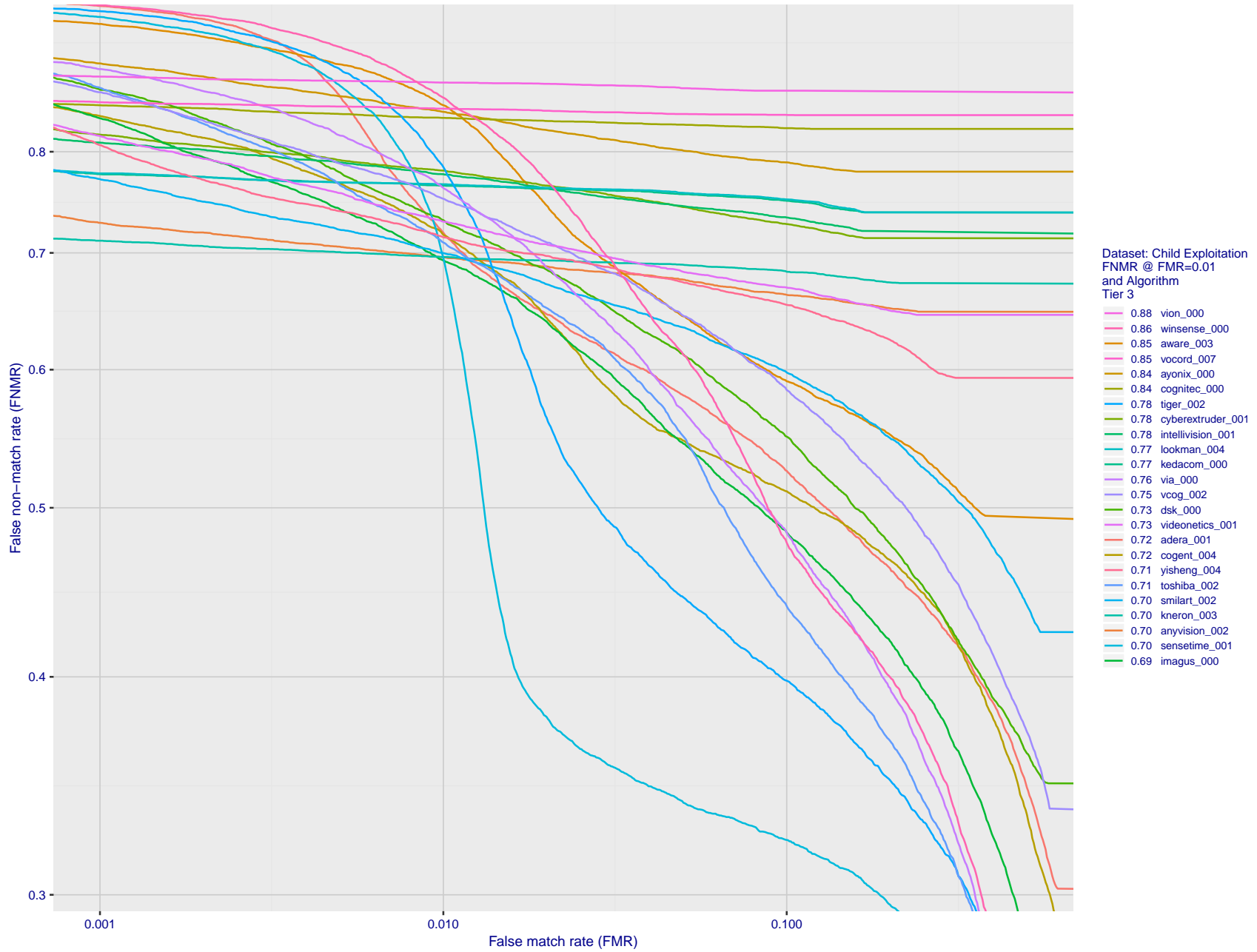
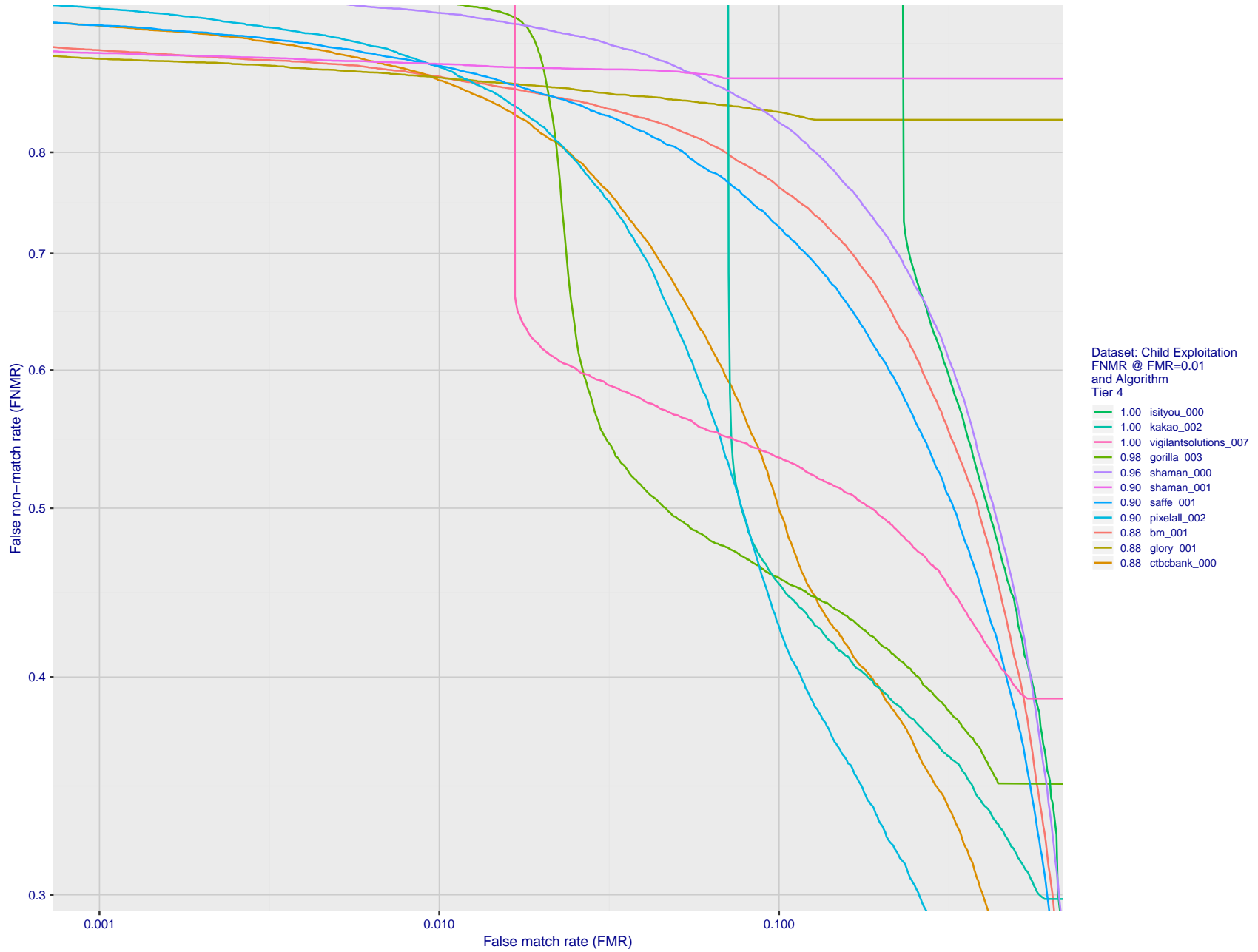


Figure 48: For child exploitation images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show many decades of FMR. Accuracy is poor because many images have adverse quality characteristics, and because detection and enrollment fails.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 49: For child exploitation images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold,  $T$ . The scales are logarithmic in order to show many decades of FMR. Accuracy is poor because many images have adverse quality characteristics, and because detection and enrollment fails.

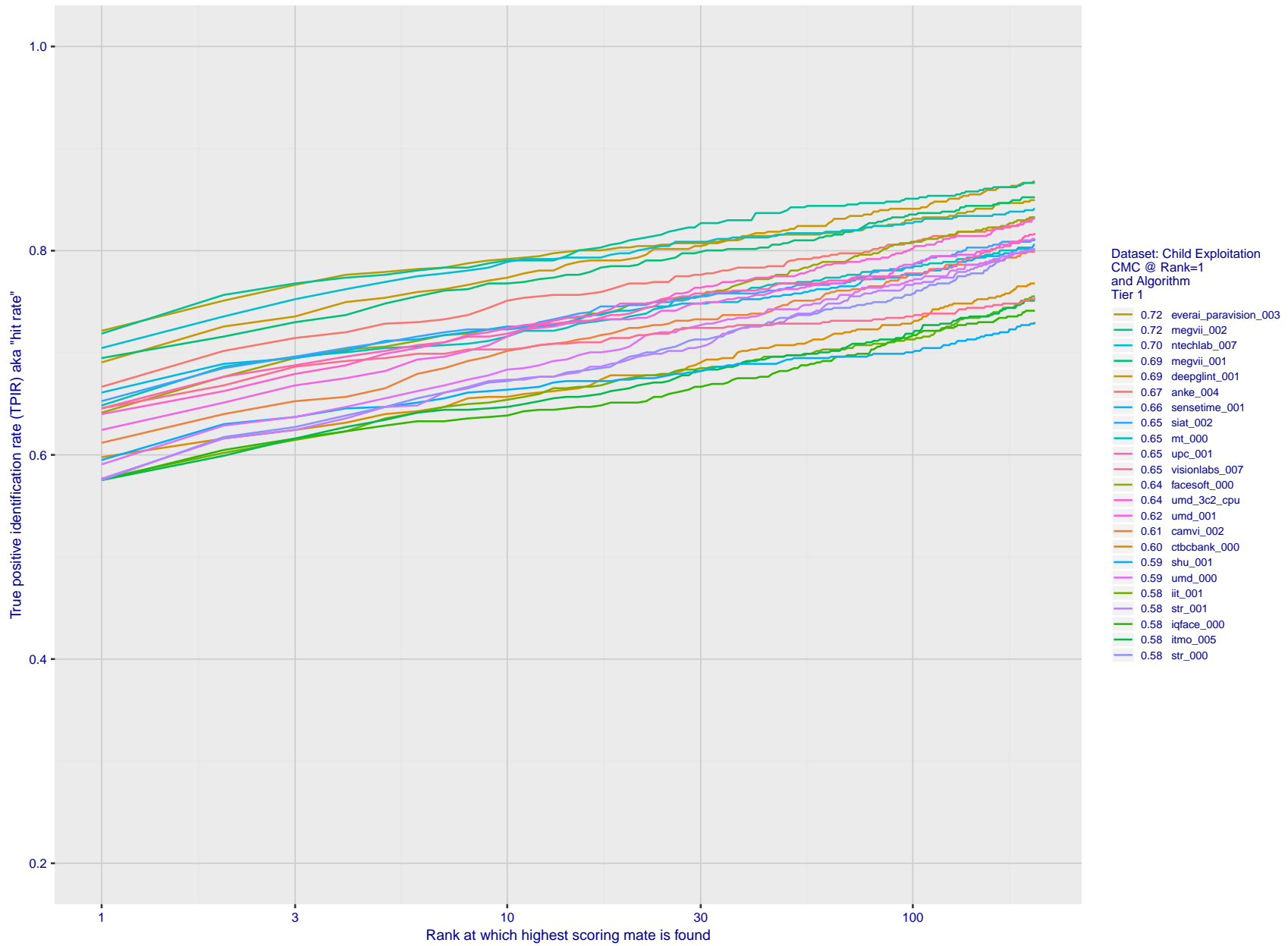


Figure 50: For child exploitation images, cumulative match characteristics (CMC) showing true positive identification rate vs. rank. This is simulation of a one-to-many search experiment - see discussion in section 3.2. The scales are logarithmic in order to show the effect of long candidate lists. Accuracy is poor but much improved relative to the 1:1 DETs of Fig. 49 because a search can succeed if any of a subject's several enrolled images matches the search image with a high score.

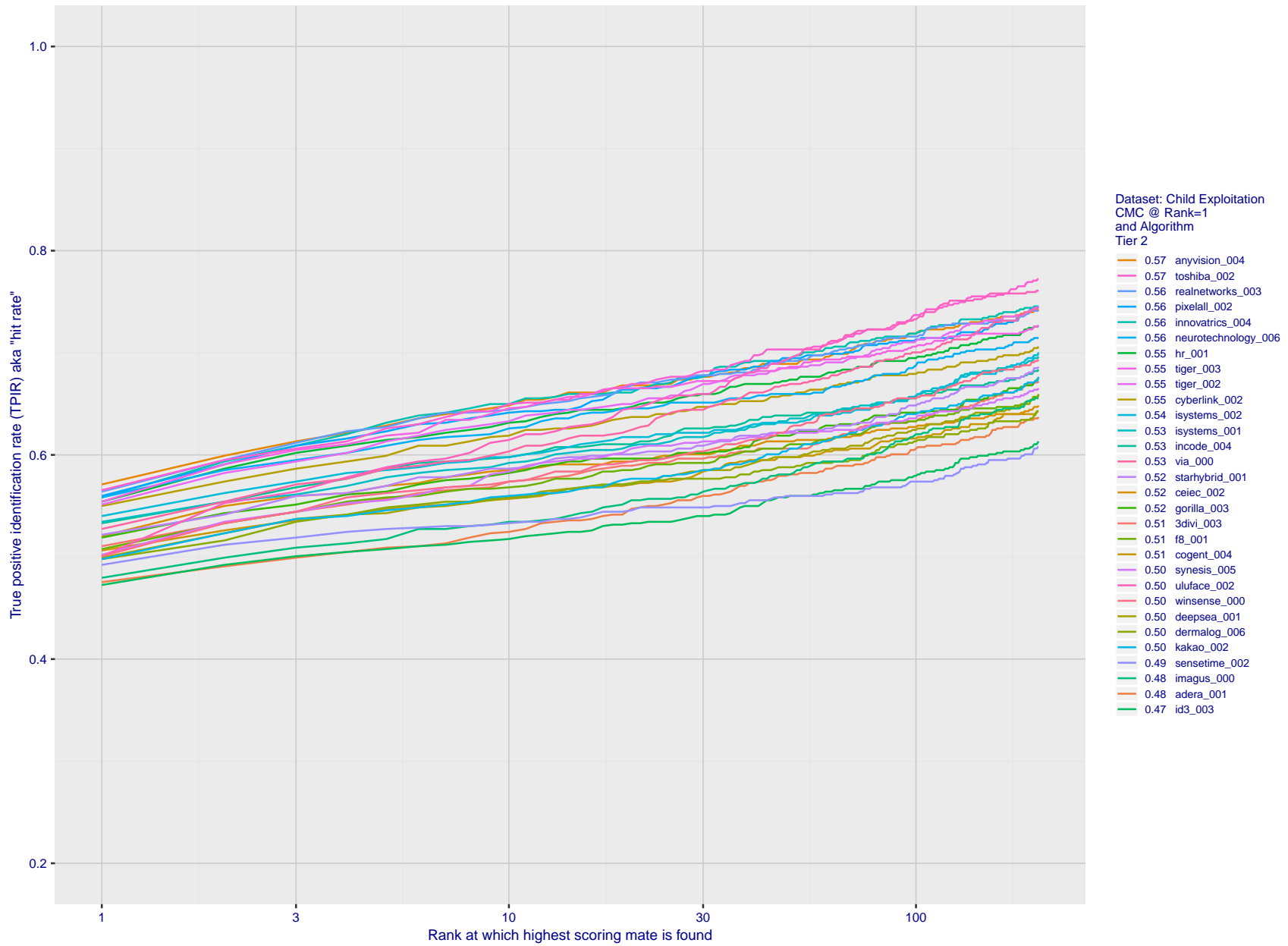


Figure 51: For child exploitation images, cumulative match characteristics (CMC) showing true positive identification rate vs. rank. This is simulation of a one-to-many search experiment - see discussion in section 3.2. The scales are logarithmic in order to show the effect of long candidate lists. Accuracy is poor but much improved relative to the 1:1 DETs of Fig. 49 because a search can succeed if any of a subject's several enrolled images matches the search image with a high score.

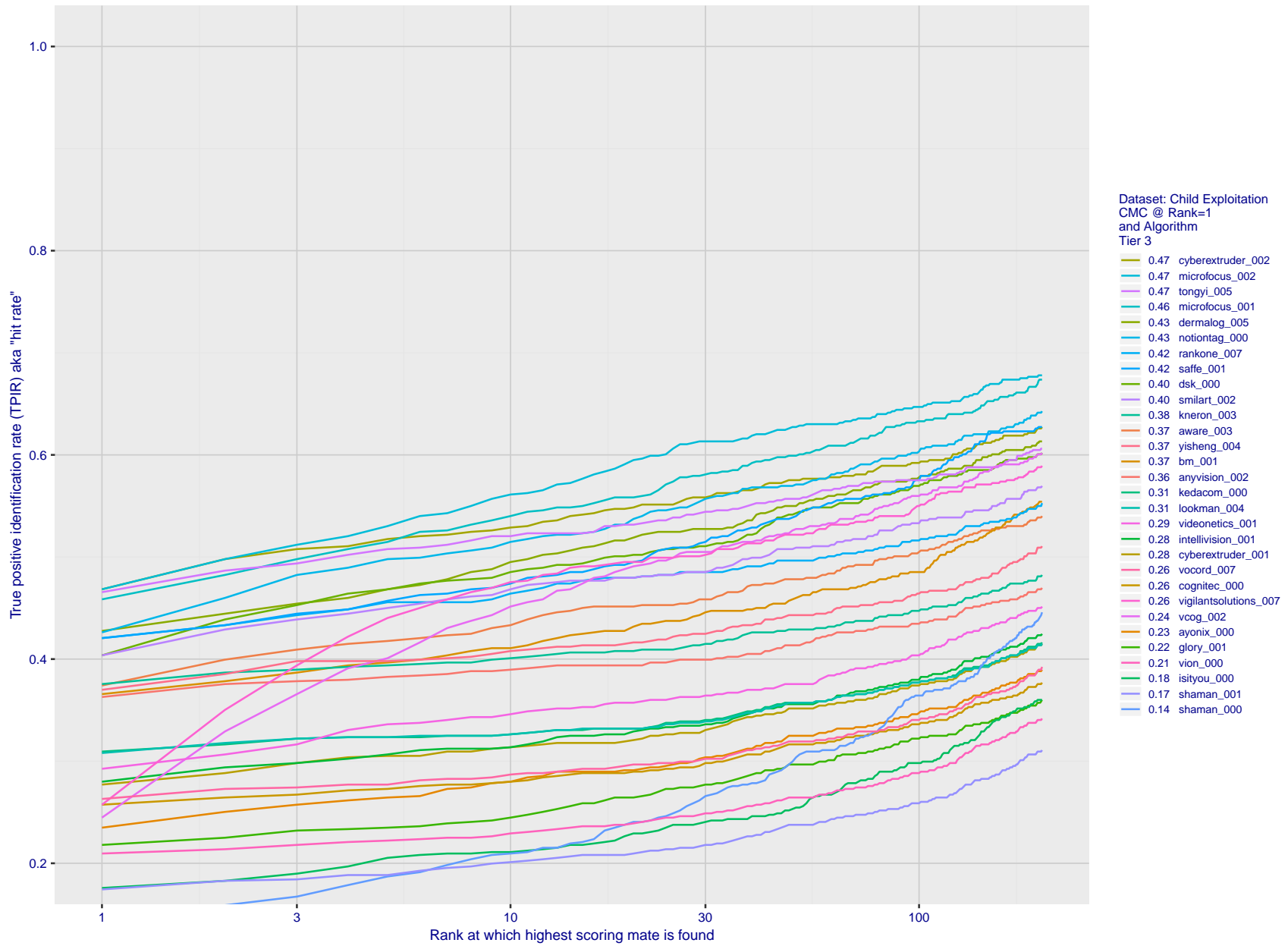
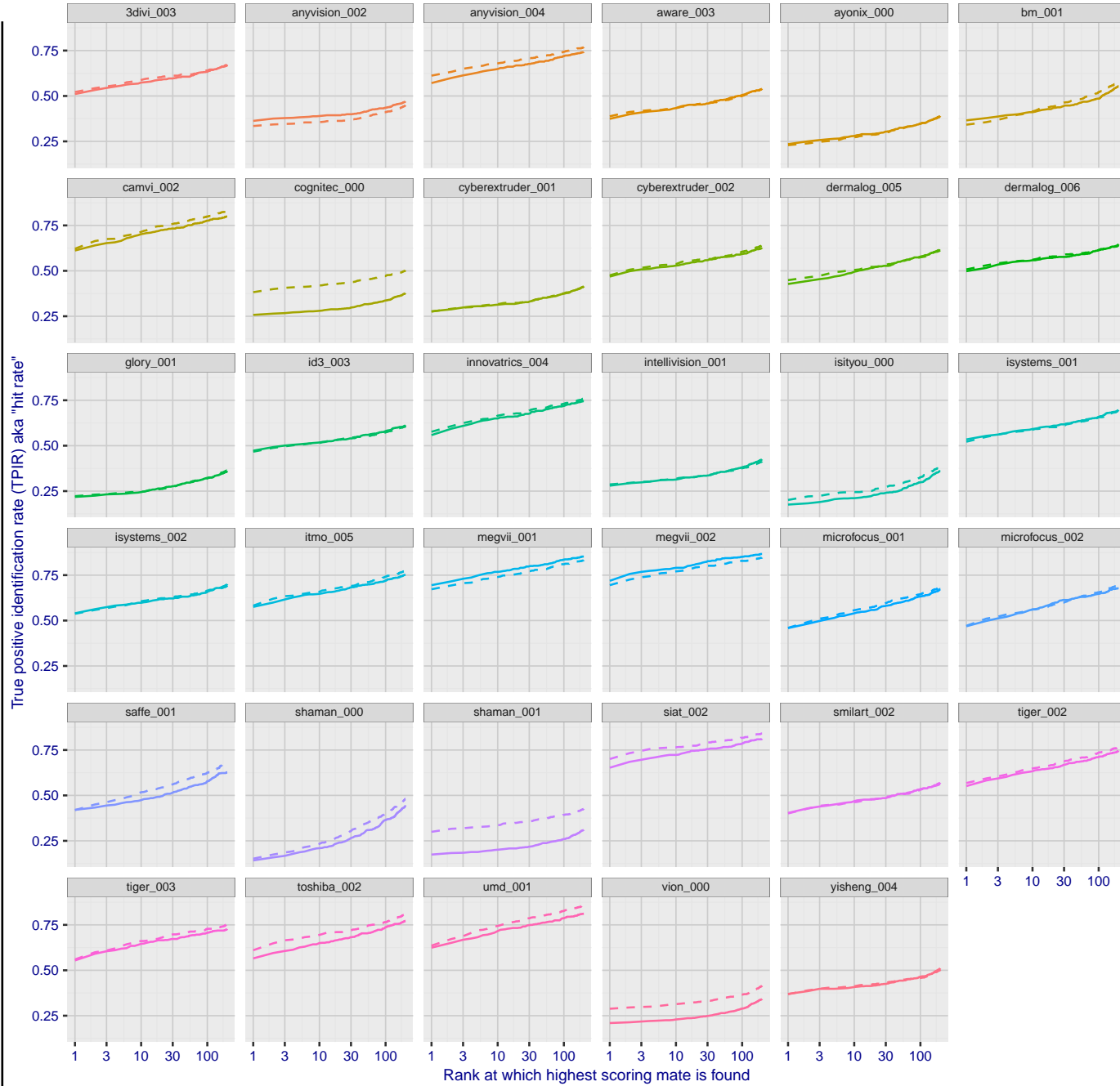


Figure 52: For child exploitation images, cumulative match characteristics (CMC) showing true positive identification rate vs. rank. This is simulation of a one-to-many search experiment - see discussion in section 3.2. The scales are logarithmic in order to show the effect of long candidate lists. Accuracy is poor but much improved relative to the 1:1 DETs of Fig. 49 because a search can succeed if any of a subject's several enrolled images matches the search image with a high score.



Dataset: Child Exploitation  
 CMC @ Rank=1 [cropped | uncropped] (delta improvement)  
 and Algorithm

- 0.70 | 0.65 (0.05) siat\_002
- 0.69 | 0.72 (-0.02) megvii\_002
- 0.67 | 0.69 (-0.02) megvii\_001
- 0.64 | 0.62 (0.01) umd\_001
- 0.62 | 0.61 (0.01) camvi\_002
- 0.61 | 0.57 (0.04) anyvision\_004
- 0.61 | 0.57 (0.05) toshiba\_002
- 0.58 | 0.58 (0.01) itmo\_005
- 0.58 | 0.56 (0.02) innovatrics\_004
- 0.57 | 0.55 (0.02) tiger\_002
- 0.56 | 0.55 (0.01) tiger\_003
- 0.54 | 0.54 (0.00) isystems\_002
- 0.52 | 0.51 (0.01) 3divi\_003
- 0.52 | 0.53 (-0.01) isystems\_001
- 0.51 | 0.50 (0.01) dermalog\_006
- 0.48 | 0.47 (0.01) cyberextruder\_002
- 0.47 | 0.47 (0.00) microfocus\_002
- 0.47 | 0.47 (-0.01) id3\_003
- 0.46 | 0.46 (0.00) microfocus\_001
- 0.45 | 0.43 (0.02) dermalog\_005
- 0.42 | 0.42 (0.00) saffe\_001
- 0.40 | 0.40 (0.00) smilart\_002
- 0.39 | 0.37 (0.01) aware\_003
- 0.38 | 0.26 (0.13) cognitec\_000
- 0.37 | 0.37 (0.00) yisheng\_004
- 0.34 | 0.37 (-0.02) bm\_001
- 0.33 | 0.36 (-0.03) anyvision\_002
- 0.30 | 0.17 (0.13) shaman\_001
- 0.29 | 0.21 (0.08) vion\_000
- 0.29 | 0.28 (0.01) intellivision\_001
- 0.28 | 0.28 (0.00) cyberextruder\_001
- 0.23 | 0.23 (-0.01) ayonix\_000
- 0.22 | 0.22 (0.00) glory\_001
- 0.20 | 0.18 (0.03) isityou\_000
- 0.15 | 0.14 (0.01) shaman\_000

Study  
 - - cropped  
 — uncropped

FNMR(T)  
 FMR(T)  
 "False non-match rate"  
 "False match rate"

Figure 53: For child exploitation images, cumulative match characteristics (CMC) showing true positive identification rate vs. rank for two cases: 1. Whole image provided to the algorithm; 2. Human annotated rectangular region, cropped and provided to the algorithm. The difference between the traces is associated with detection of difficult faces, and fine localization.

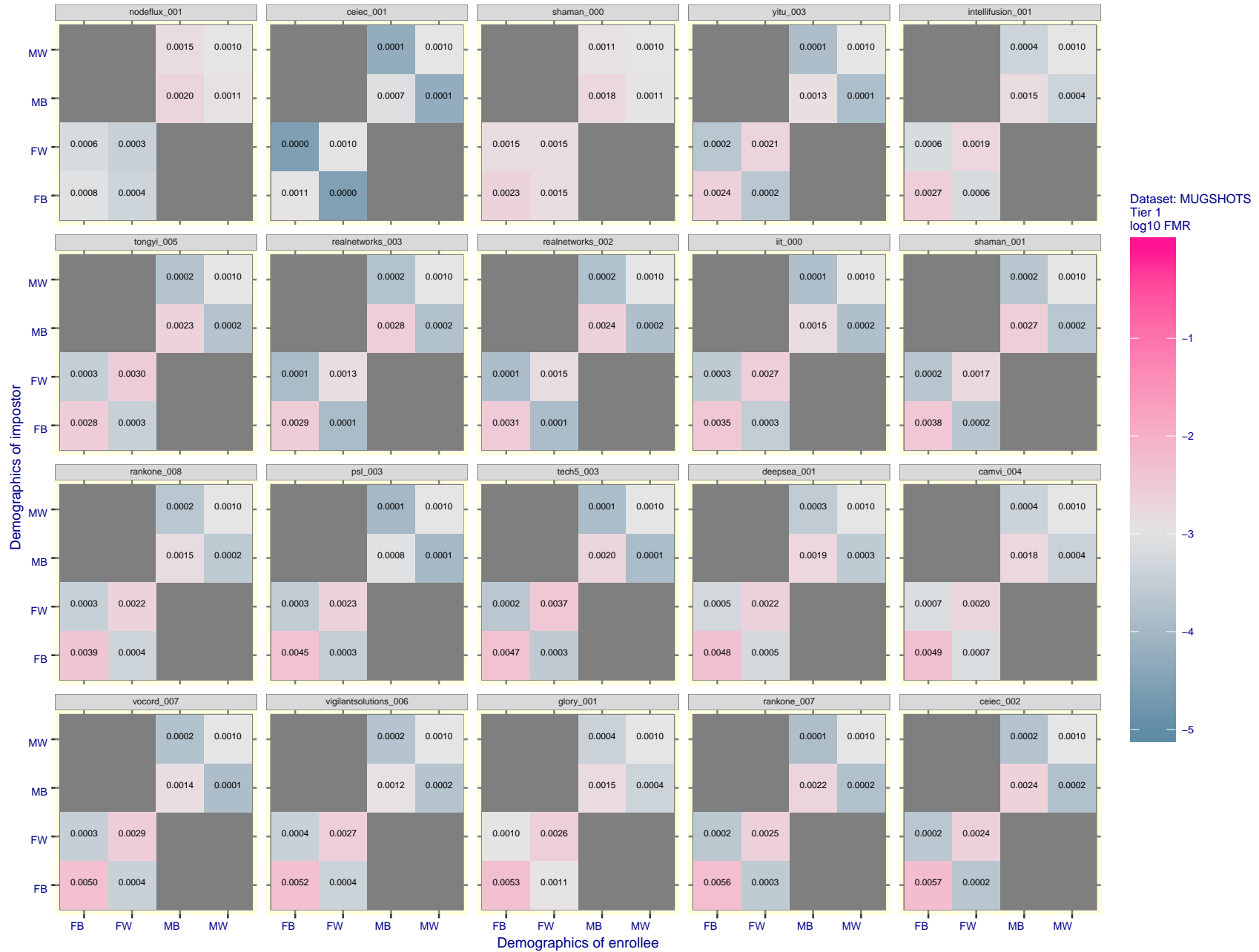


Figure 54: For the mugshot images, FMR for same-sex impostor pairs of images annotated with codes for black female, black male, white female, white male. The threshold is set for each algorithm to give FMR = 0.001 for white males which is the demographic that usually gives the lowest FMR. This means the top right box is the same color in all panels. The panels are sorted over multiple pages in order of FMR on black females, which is the demographic that usually gives the highest FMR.



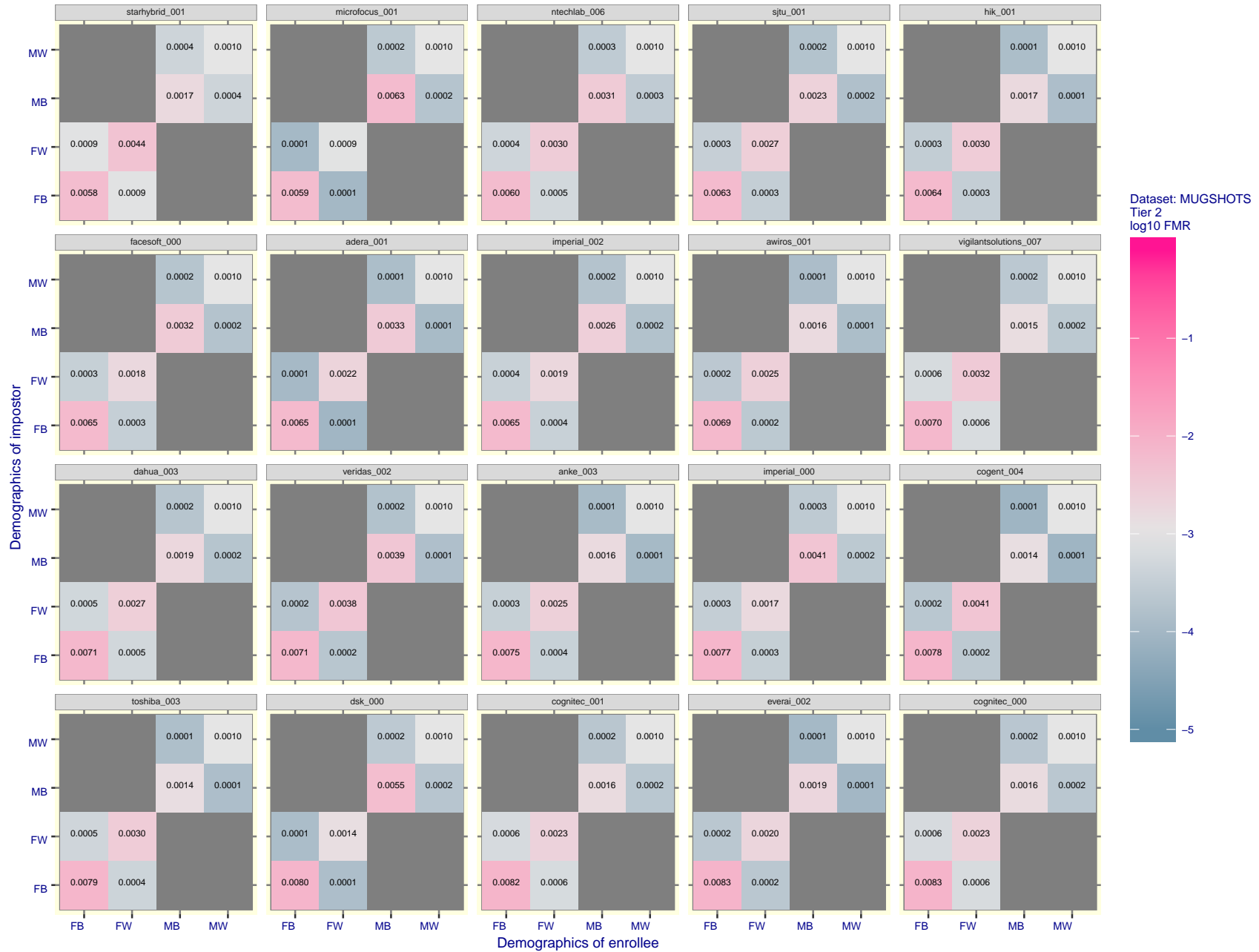


Figure 55: For the mugshot images, FMR for same-sex impostor pairs of images annotated with codes for black female, black male, white female, white male. The threshold is set for each algorithm to give FMR = 0.001 for white males which is the demographic that usually gives the lowest FMR. This means the top right box is the same color in all panels. The panels are sorted over multiple pages in order of FMR on black females, which is the demographic that usually gives the highest FMR.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

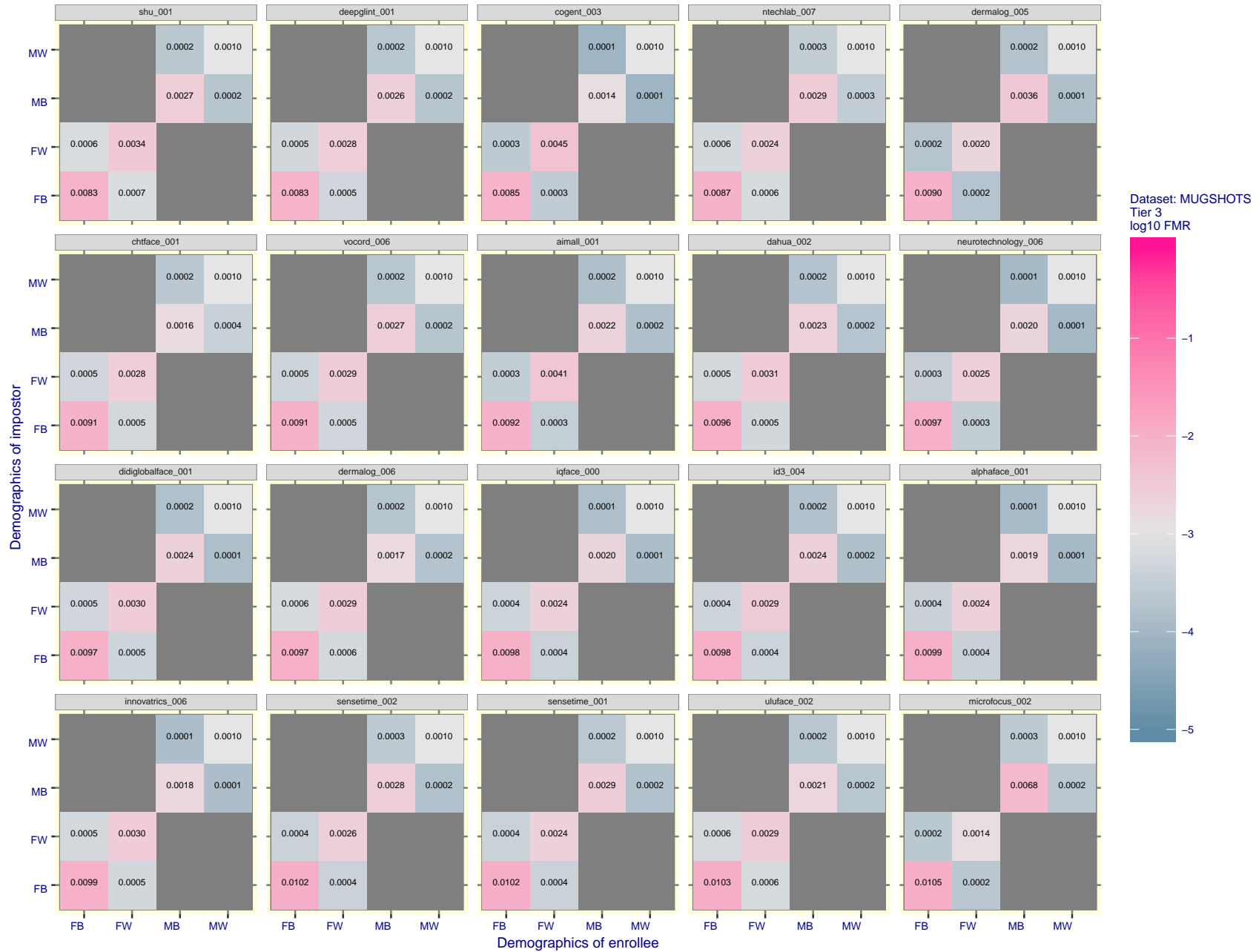


Figure 56: For the mugshot images, FMR for same-sex impostor pairs of images annotated with codes for black female, black male, white female, white male. The threshold is set for each algorithm to give FMR = 0.001 for white males which is the demographic that usually gives the lowest FMR. This means the top right box is the same color in all panels. The panels are sorted over multiple pages in order of FMR on black females, which is the demographic that usually gives the highest FMR.

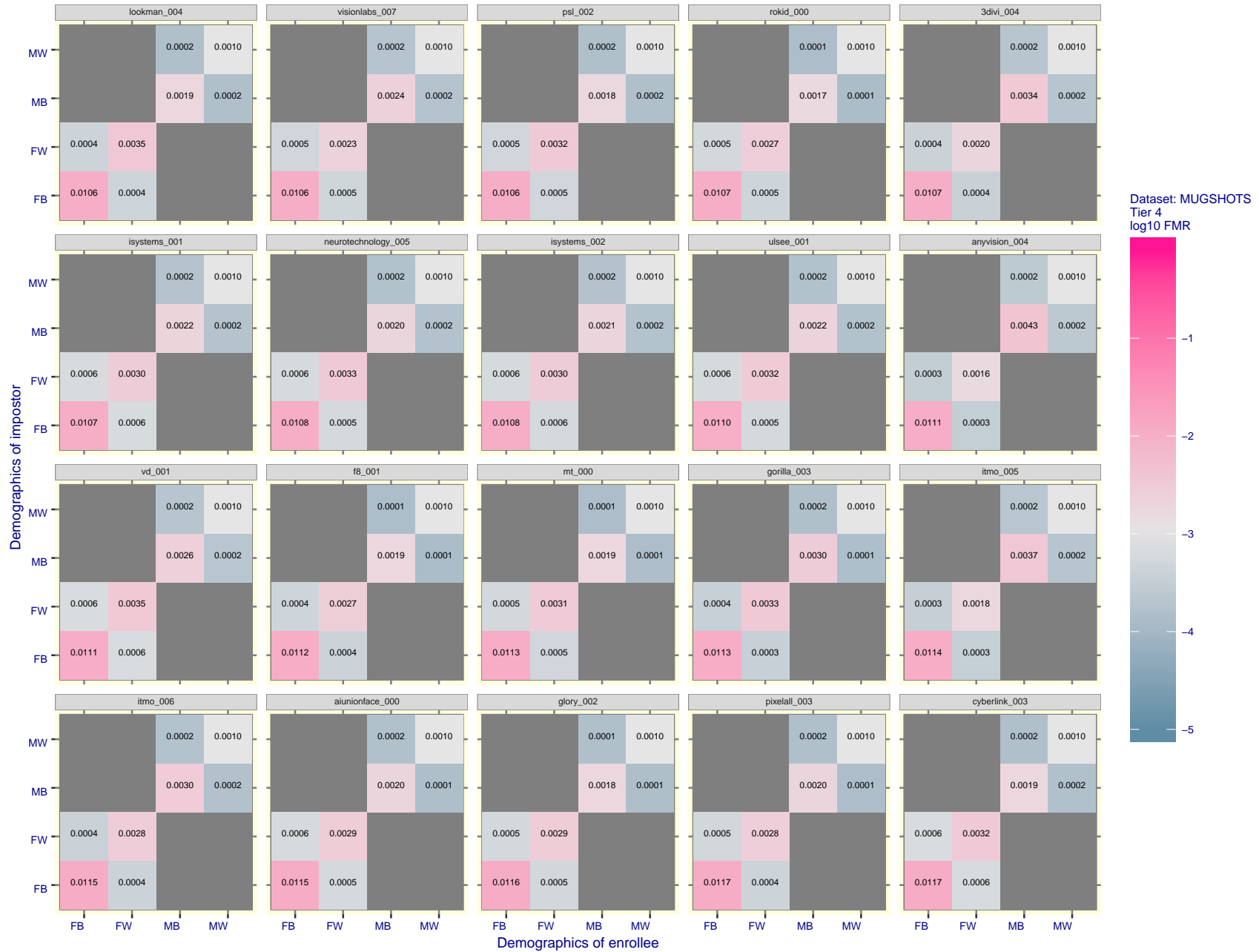


Figure 57: For the mugshot images, FMR for same-sex impostor pairs of images annotated with codes for black female, black male, white female, white male. The threshold is set for each algorithm to give FMR = 0.001 for white males which is the demographic that usually gives the lowest FMR. This means the top right box is the same color in all panels. The panels are sorted over multiple pages in order of FMR on black females, which is the demographic that usually gives the highest FMR.

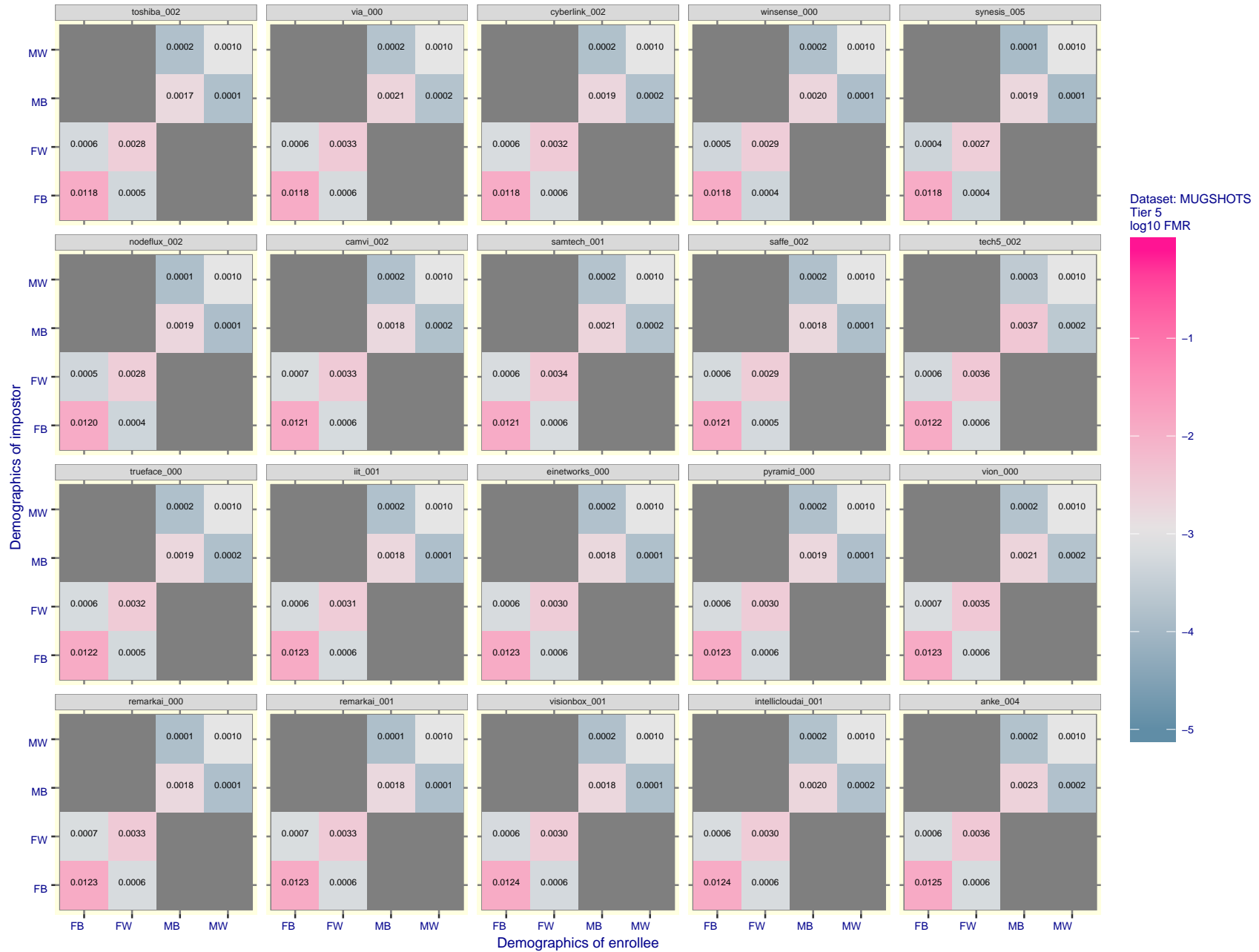


Figure 58: For the mugshot images, FMR for same-sex impostor pairs of images annotated with codes for black female, black male, white female, white male. The threshold is set for each algorithm to give FMR = 0.001 for white males which is the demographic that usually gives the lowest FMR. This means the top right box is the same color in all panels. The panels are sorted over multiple pages in order of FMR on black females, which is the demographic that usually gives the highest FMR.

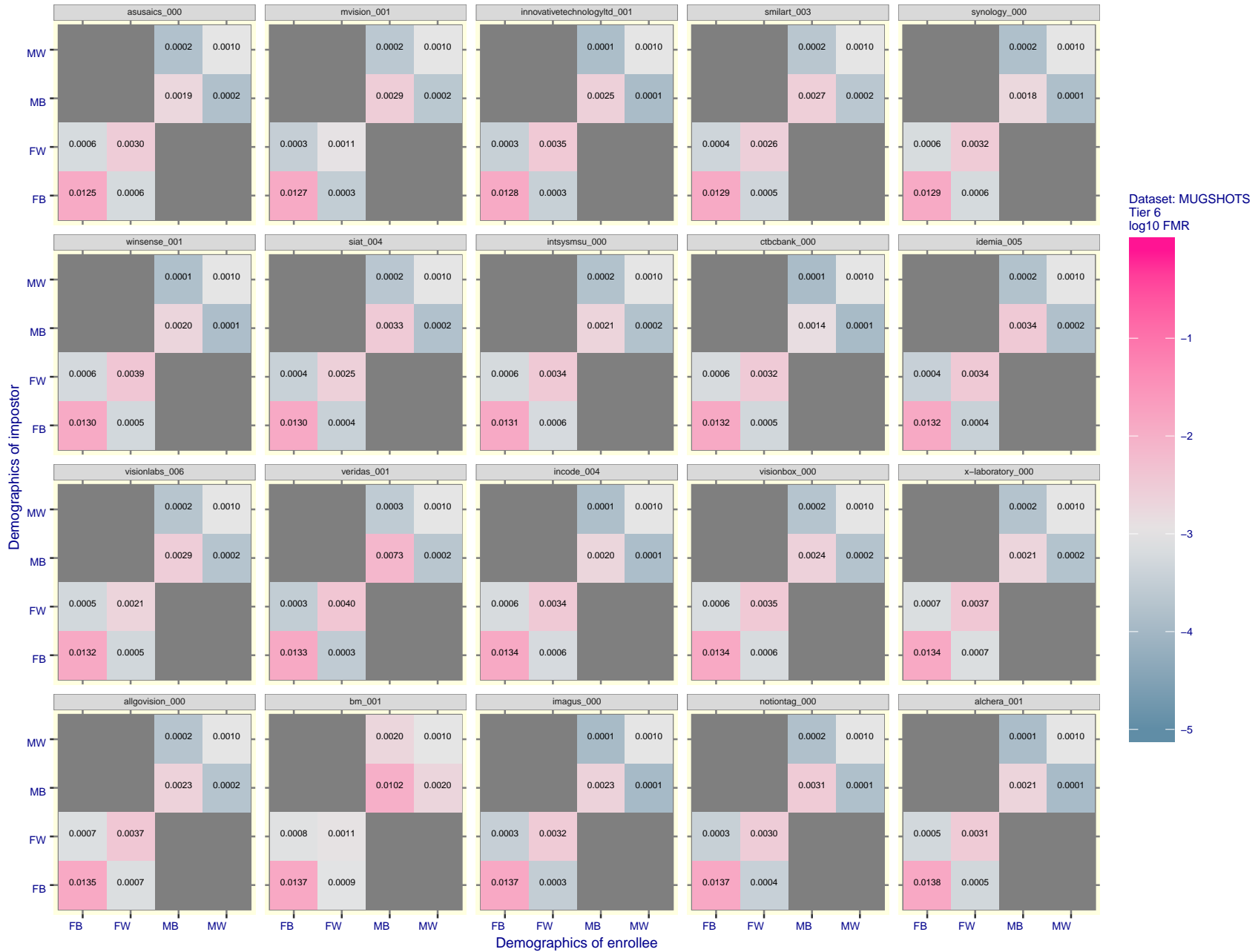


Figure 59: For the mugshot images, FMR for same-sex impostor pairs of images annotated with codes for black female, black male, white female, white male. The threshold is set for each algorithm to give FMR = 0.001 for white males which is the demographic that usually gives the lowest FMR. This means the top right box is the same color in all panels. The panels are sorted over multiple pages in order of FMR on black females, which is the demographic that usually gives the highest FMR.

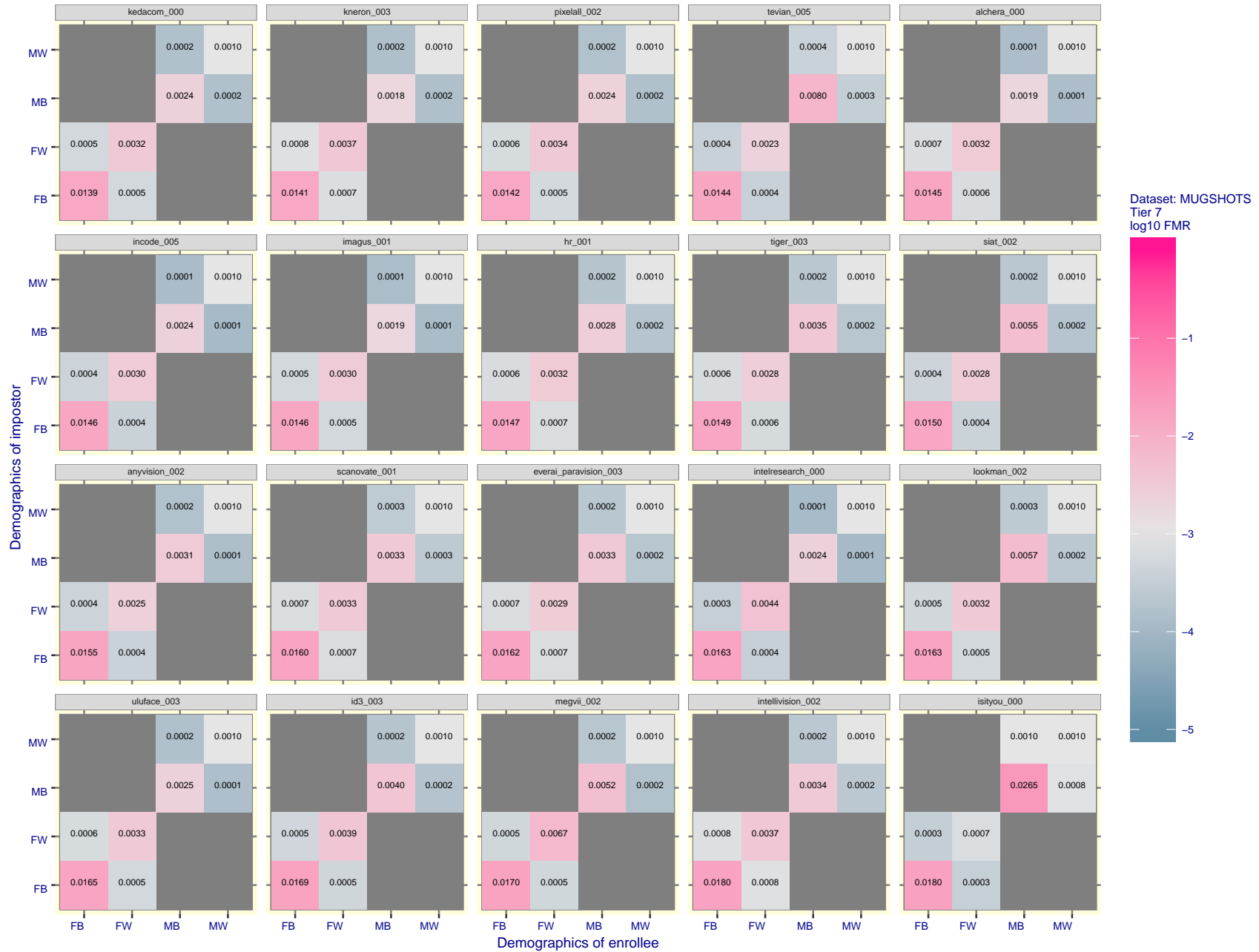


Figure 60: For the mugshot images, FMR for same-sex impostor pairs of images annotated with codes for black female, black male, white female, white male. The threshold is set for each algorithm to give FMR = 0.001 for white males which is the demographic that usually gives the lowest FMR. This means the top right box is the same color in all panels. The panels are sorted over multiple pages in order of FMR on black females, which is the demographic that usually gives the highest FMR.

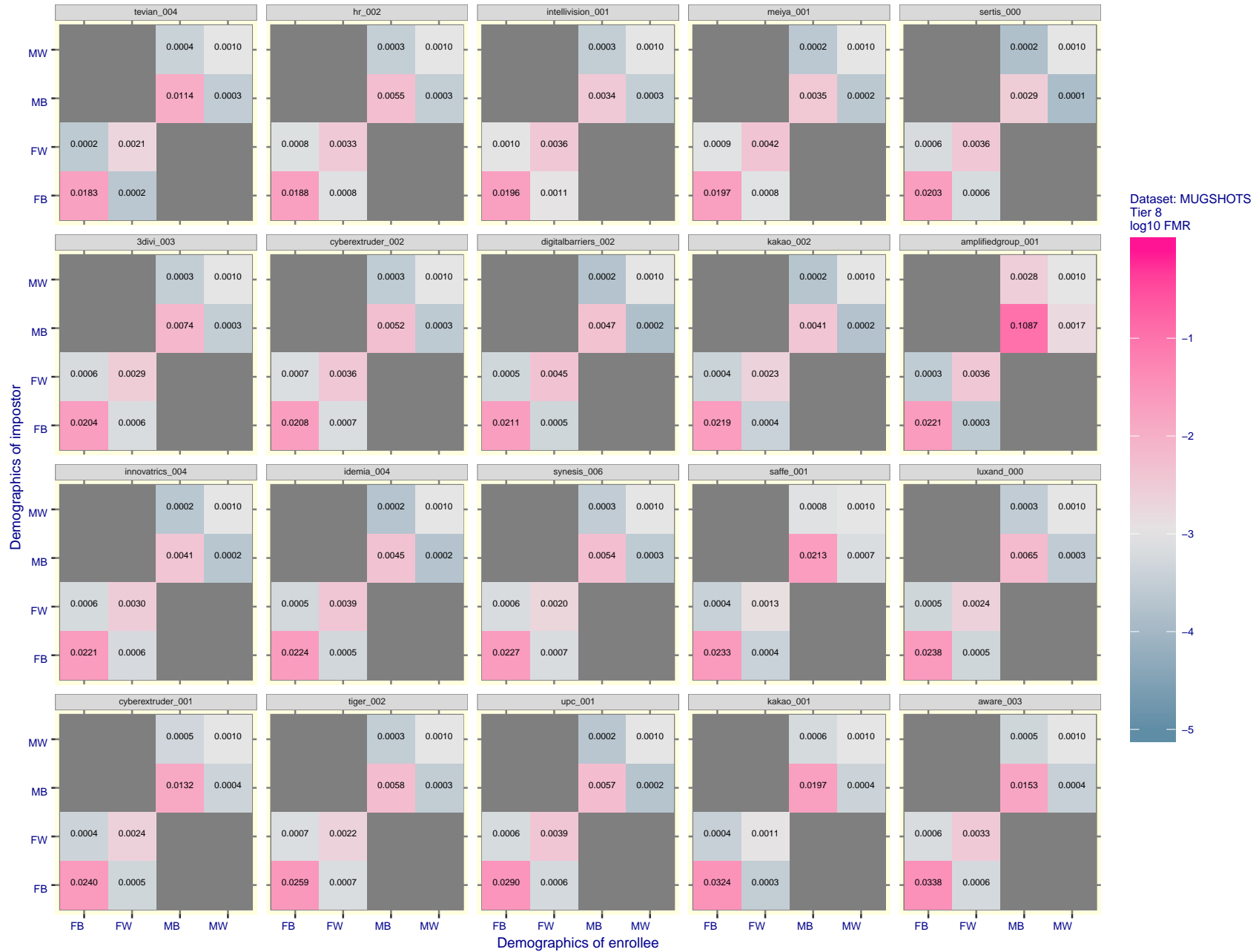
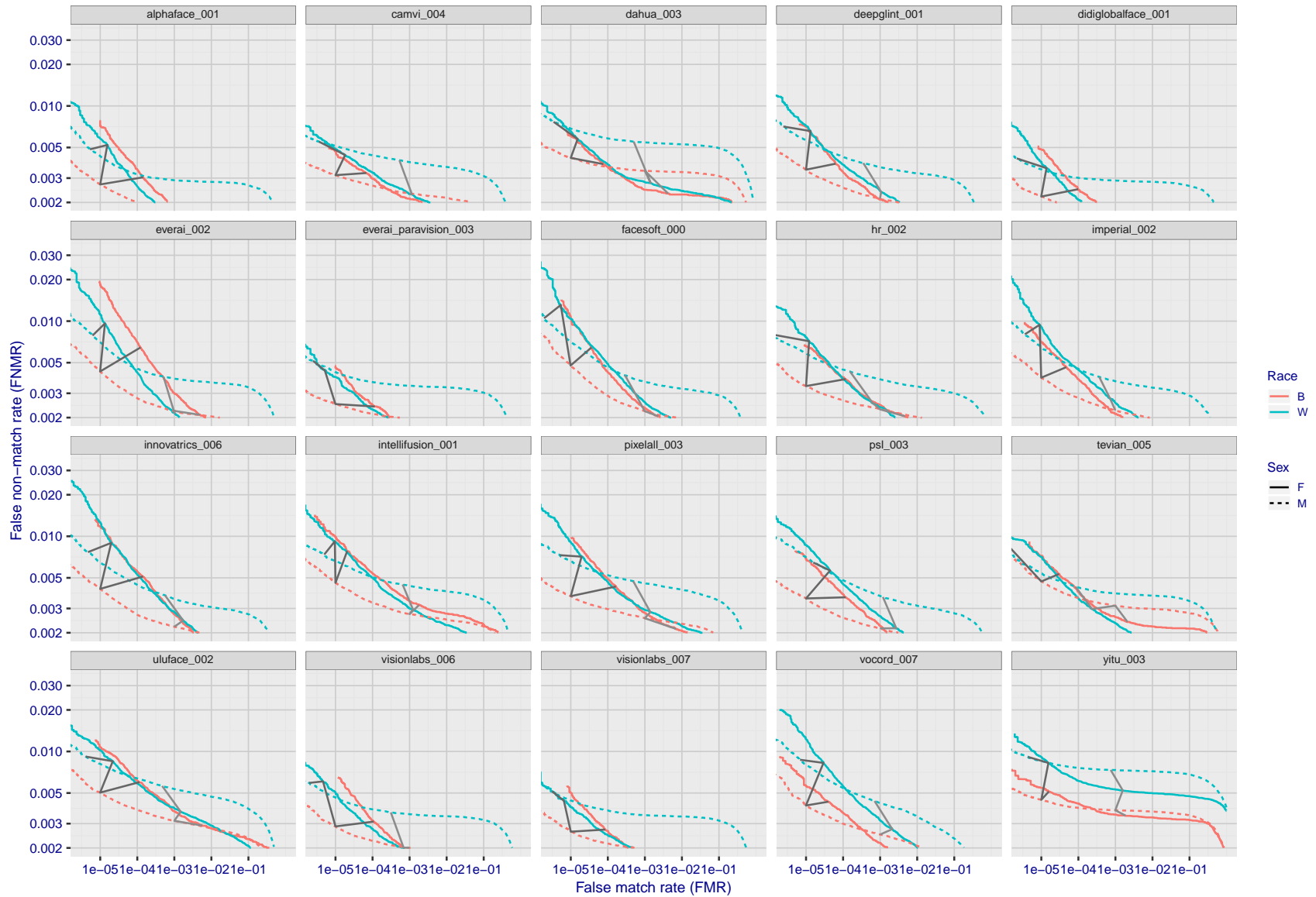


Figure 61: For the mugshot images, FMR for same-sex impostor pairs of images annotated with codes for black female, black male, white female, white male. The threshold is set for each algorithm to give FMR = 0.001 for white males which is the demographic that usually gives the lowest FMR. This means the top right box is the same color in all panels. The panels are sorted over multiple pages in order of FMR on black females, which is the demographic that usually gives the highest FMR.



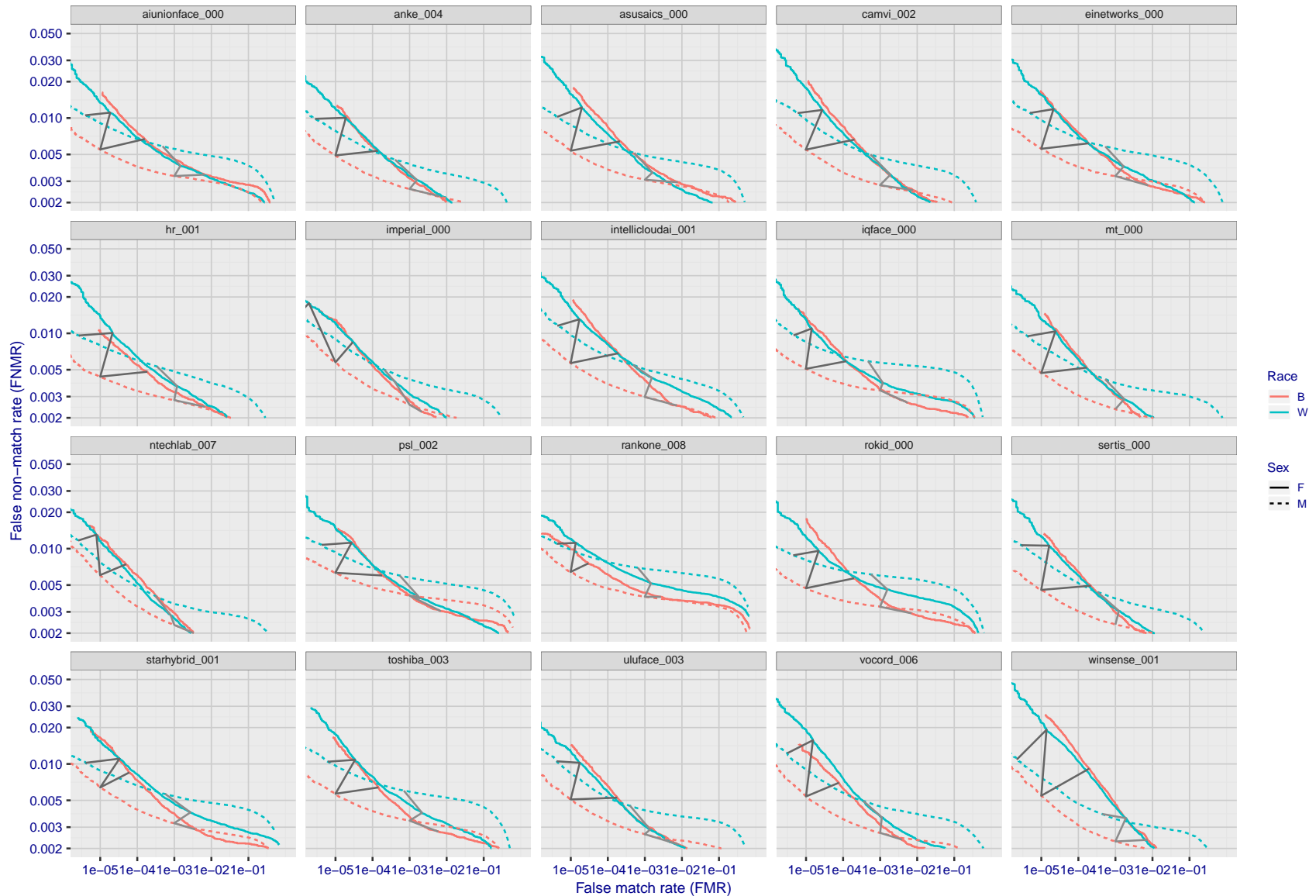
Figure 62: For the mugshot images, FMR for same-sex impostor pairs of images annotated with codes for black female, black male, white female, white male. The threshold is set for each algorithm to give FMR = 0.001 for white males which is the demographic that usually gives the lowest FMR. This means the top right box is the same color in all panels. The panels are sorted over multiple pages in order of FMR on black females, which is the demographic that usually gives the highest FMR.





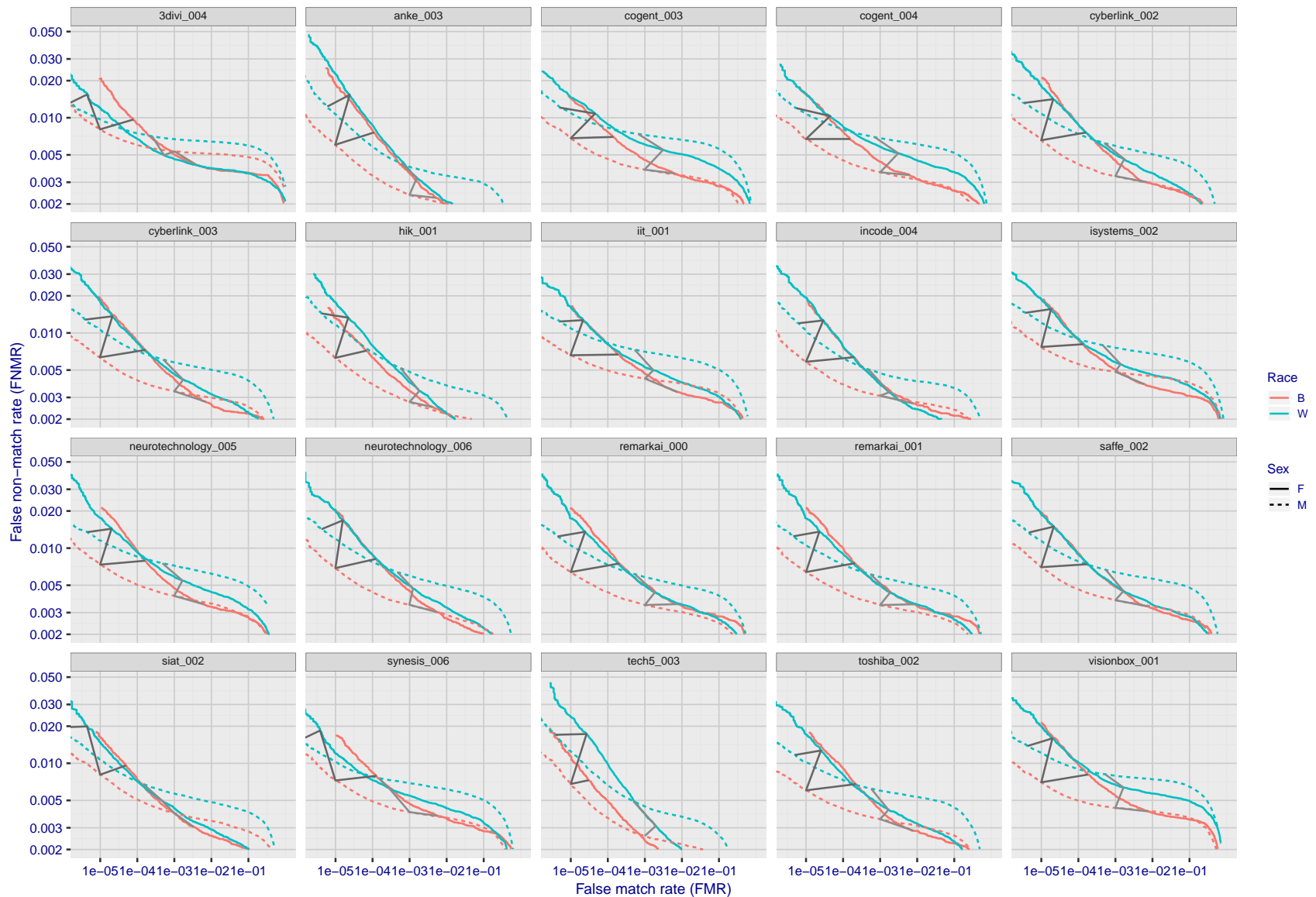
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 63: For the mugshot images, error tradeoff characteristics for white females, black females, black males and white males. The Z-shaped grey lines correspond to fixed thresholds, showing both FNMR and FMR vary at one T value. Note: Many of the plots will naively be read as saying women gives worse error rates than men because the solid traces lie above the dotted ones. However, this is misleading and incomplete: The grey lines show the traces reveal horizontal shifts. Thus for the cogent-003 algorithm FNMR for men is higher than for women at a fixed threshold but, at the same time, FMR is higher for women - see Figure 94. As access control systems almost always operate at a fixed threshold, the naive interpretation is incorrect.



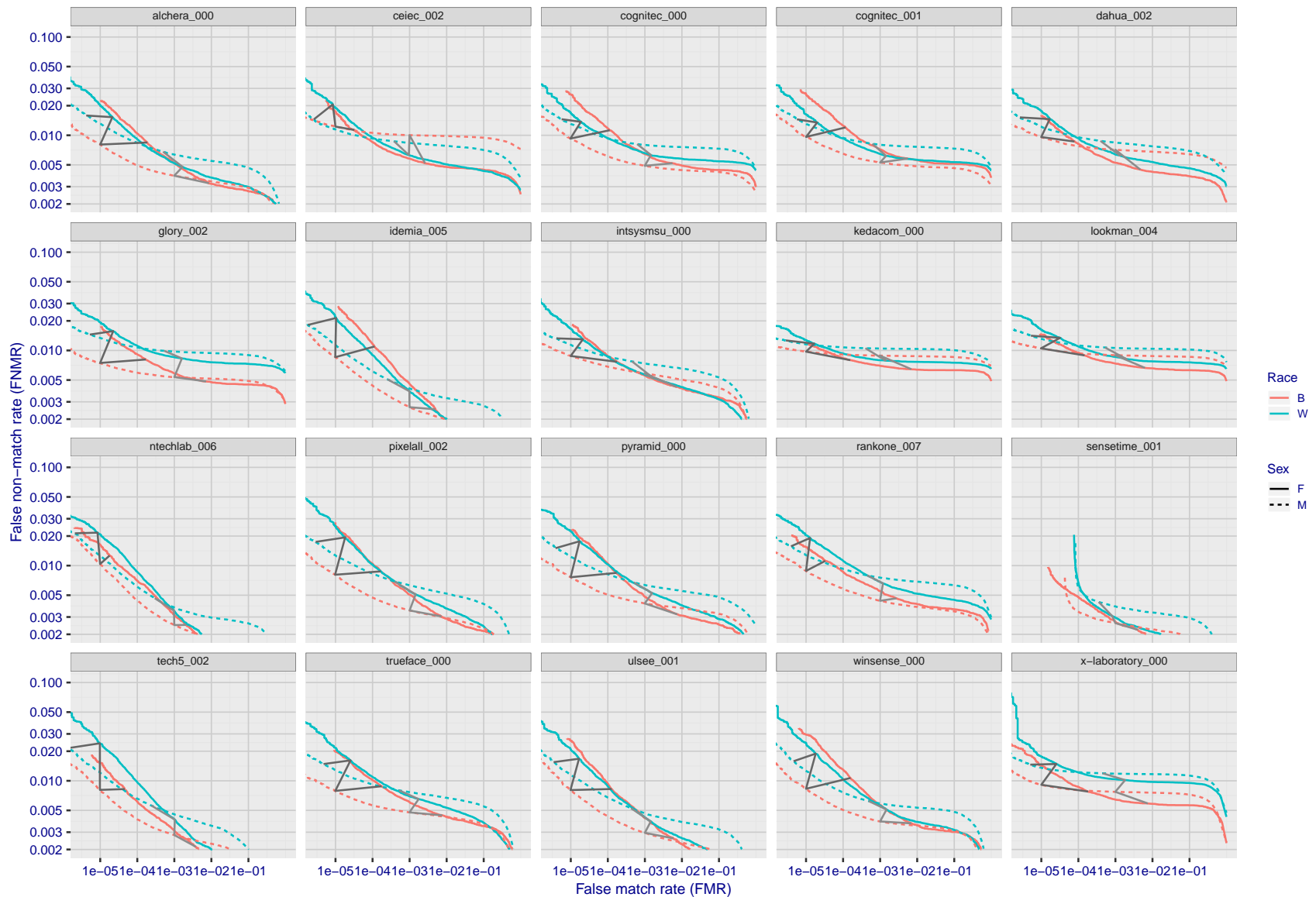
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 64: For the mugshot images, error tradeoff characteristics for white females, black females, black males and white males. The Z-shaped grey lines correspond to fixed thresholds, showing both FNMR and FMR vary at one  $T$  value. Note: Many of the plots will naively be read as saying women gives worse error rates than men because the solid traces lie above the dotted ones. However, this is misleading and incomplete: The grey lines show the traces reveal horizontal shifts. Thus for the cogent-003 algorithm FNMR for men is higher than for women at a fixed threshold but, at the same time, FMR is higher for women - see Figure 94. As access control systems almost always operate at a fixed threshold, the naive interpretation is incorrect.



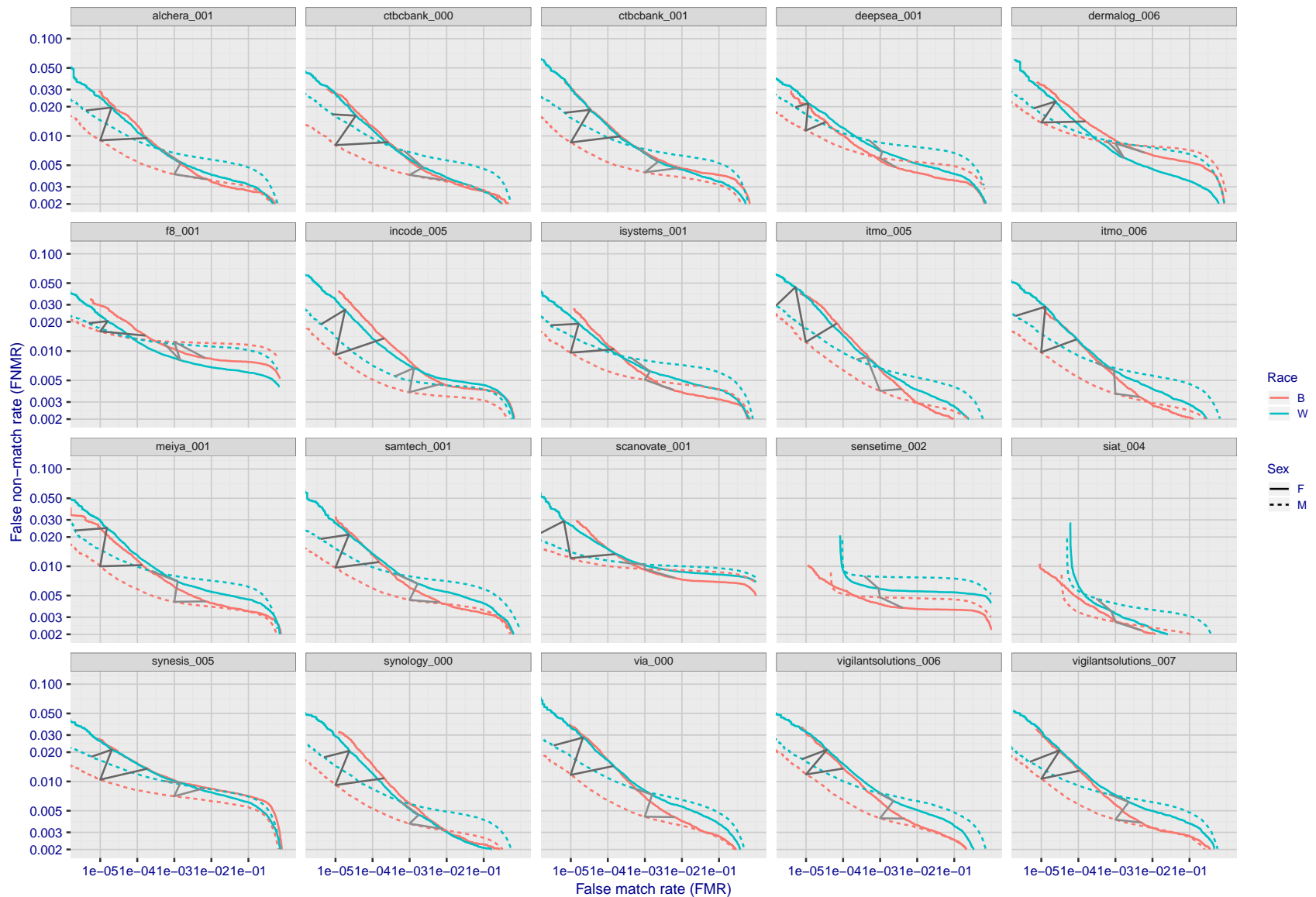
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 65: For the mugshot images, error tradeoff characteristics for white females, black females, black males and white males. The Z-shaped grey lines correspond to fixed thresholds, showing both FNMR and FMR vary at one  $T$  value. Note: Many of the plots will naively be read as saying women gives worse error rates than men because the solid traces lie above the dotted ones. However, this is misleading and incomplete: The grey lines show the traces reveal horizontal shifts. Thus for the cogent-003 algorithm FNMR for men is higher than for women at a fixed threshold but, at the same time, FMR is higher for women - see Figure 94. As access control systems almost always operate at a fixed threshold, the naive interpretation is incorrect.



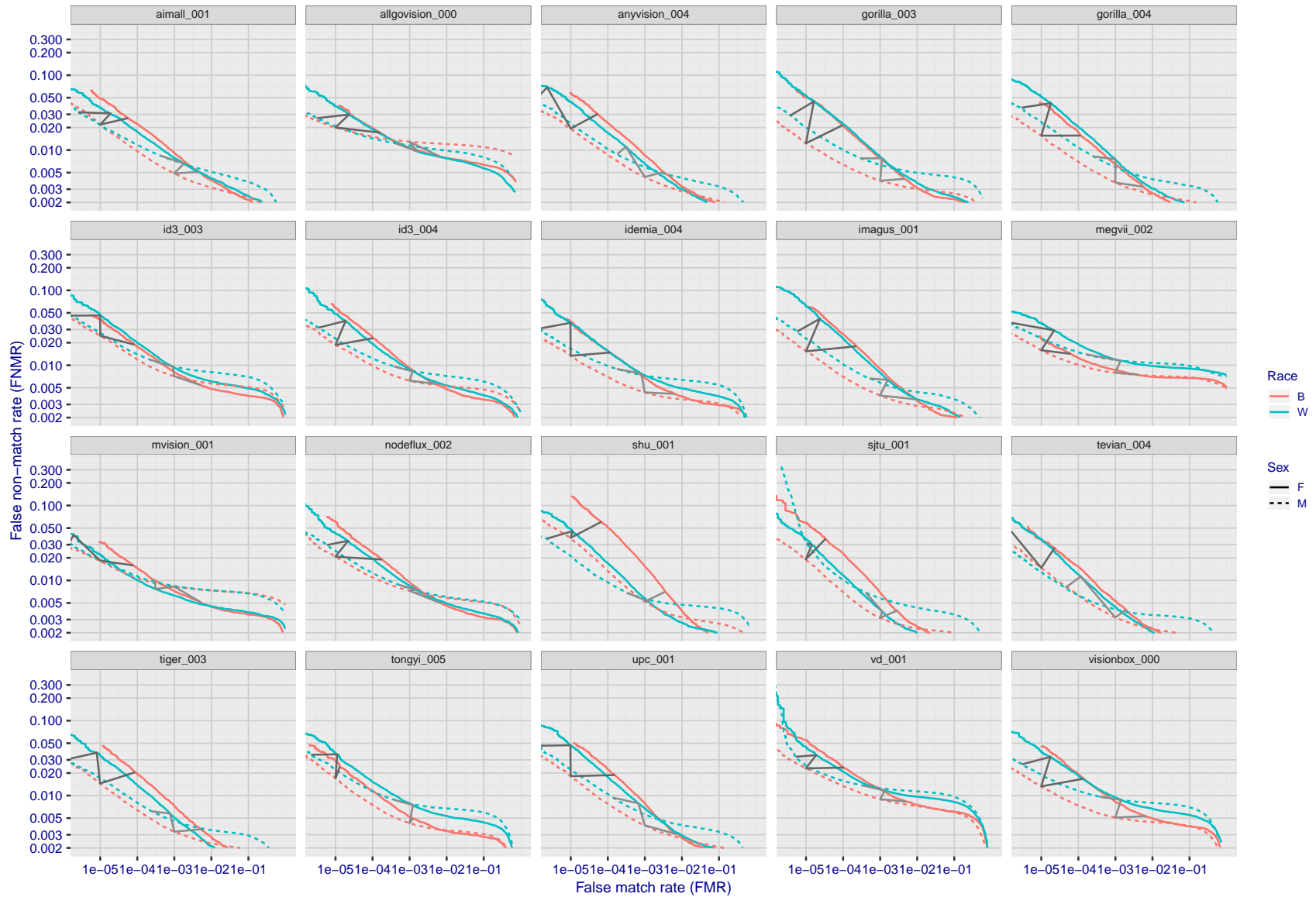
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 66: For the mugshot images, error tradeoff characteristics for white females, black females, black males and white males. The Z-shaped grey lines correspond to fixed thresholds, showing both FNMR and FMR vary at one  $T$  value. Note: Many of the plots will naively be read as saying women gives worse error rates than men because the solid traces lie above the dotted ones. However, this is misleading and incomplete: The grey lines show the traces reveal horizontal shifts. Thus for the cogent-003 algorithm FNMR for men is higher than for women at a fixed threshold but, at the same time, FMR is higher for women - see Figure 94. As access control systems almost always operate at a fixed threshold, the naive interpretation is incorrect.



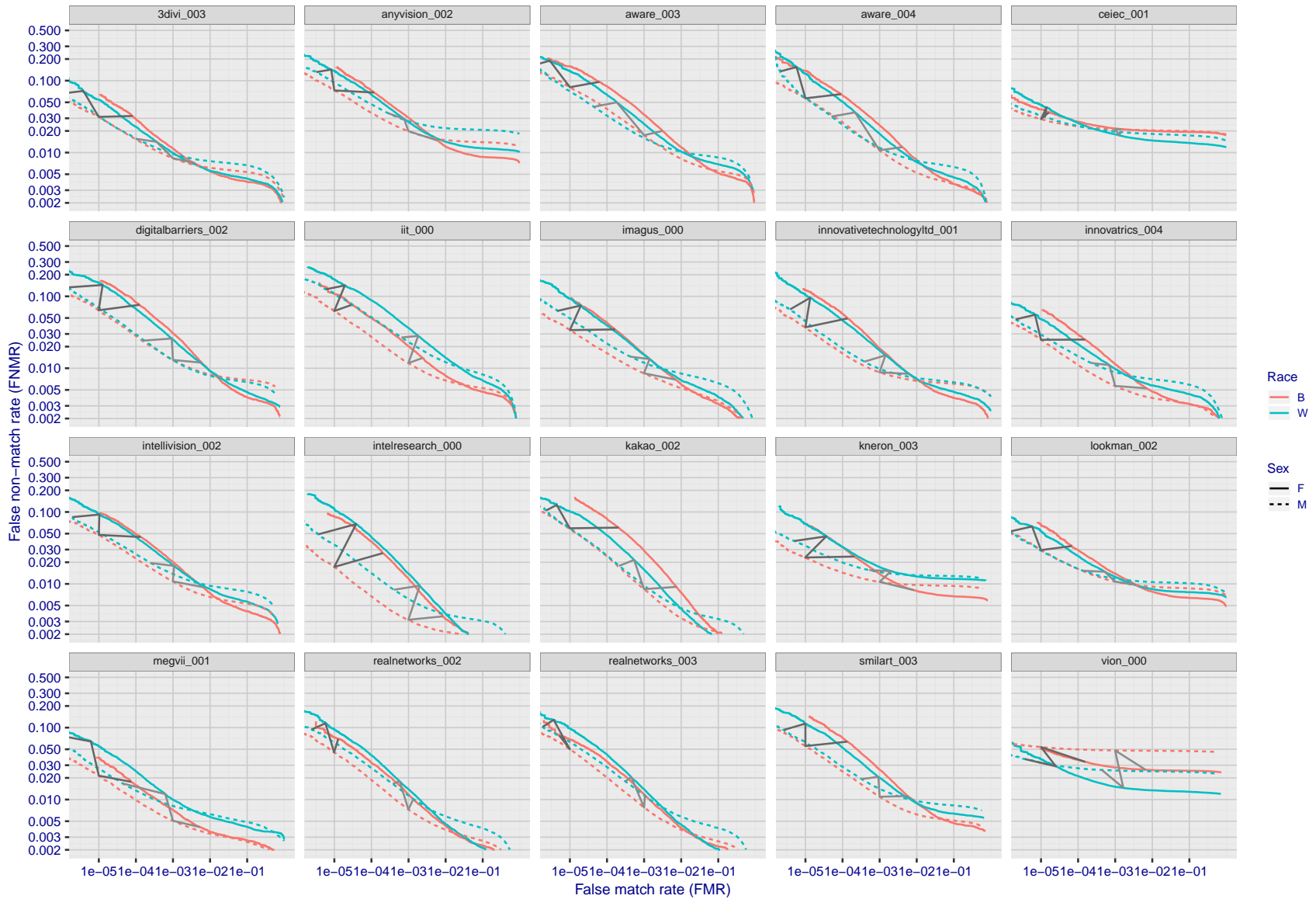
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 67: For the mugshot images, error tradeoff characteristics for white females, black females, black males and white males. The Z-shaped grey lines correspond to fixed thresholds, showing both FNMR and FMR vary at one T value. Note: Many of the plots will naively be read as saying women gives worse error rates than men because the solid traces lie above the dotted ones. However, this is misleading and incomplete: The grey lines show the traces reveal horizontal shifts. Thus for the cogent-003 algorithm FNMR for men is higher than for women at a fixed threshold but, at the same time, FMR is higher for women - see Figure 94. As access control systems almost always operate at a fixed threshold, the naive interpretation is incorrect.



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 68: For the mugshot images, error tradeoff characteristics for white females, black females, black males and white males. The Z-shaped grey lines correspond to fixed thresholds, showing both FNMR and FMR vary at one  $T$  value. Note: Many of the plots will naively be read as saying women gives worse error rates than men because the solid traces lie above the dotted ones. However, this is misleading and incomplete: The grey lines show the traces reveal horizontal shifts. Thus for the cogent-003 algorithm FNMR for men is higher than for women at a fixed threshold but, at the same time, FMR is higher for women - see Figure 94. As access control systems almost always operate at a fixed threshold, the naive interpretation is incorrect.



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 69: For the mugshot images, error tradeoff characteristics for white females, black females, black males and white males. The Z-shaped grey lines correspond to fixed thresholds, showing both FNMR and FMR vary at one T value. Note: Many of the plots will naively be read as saying women gives worse error rates than men because the solid traces lie above the dotted ones. However, this is misleading and incomplete: The grey lines show the traces reveal horizontal shifts. Thus for the cogent-003 algorithm FNMR for men is higher than for women at a fixed threshold but, at the same time, FMR is higher for women - see Figure 94. As access control systems almost always operate at a fixed threshold, the naive interpretation is incorrect.



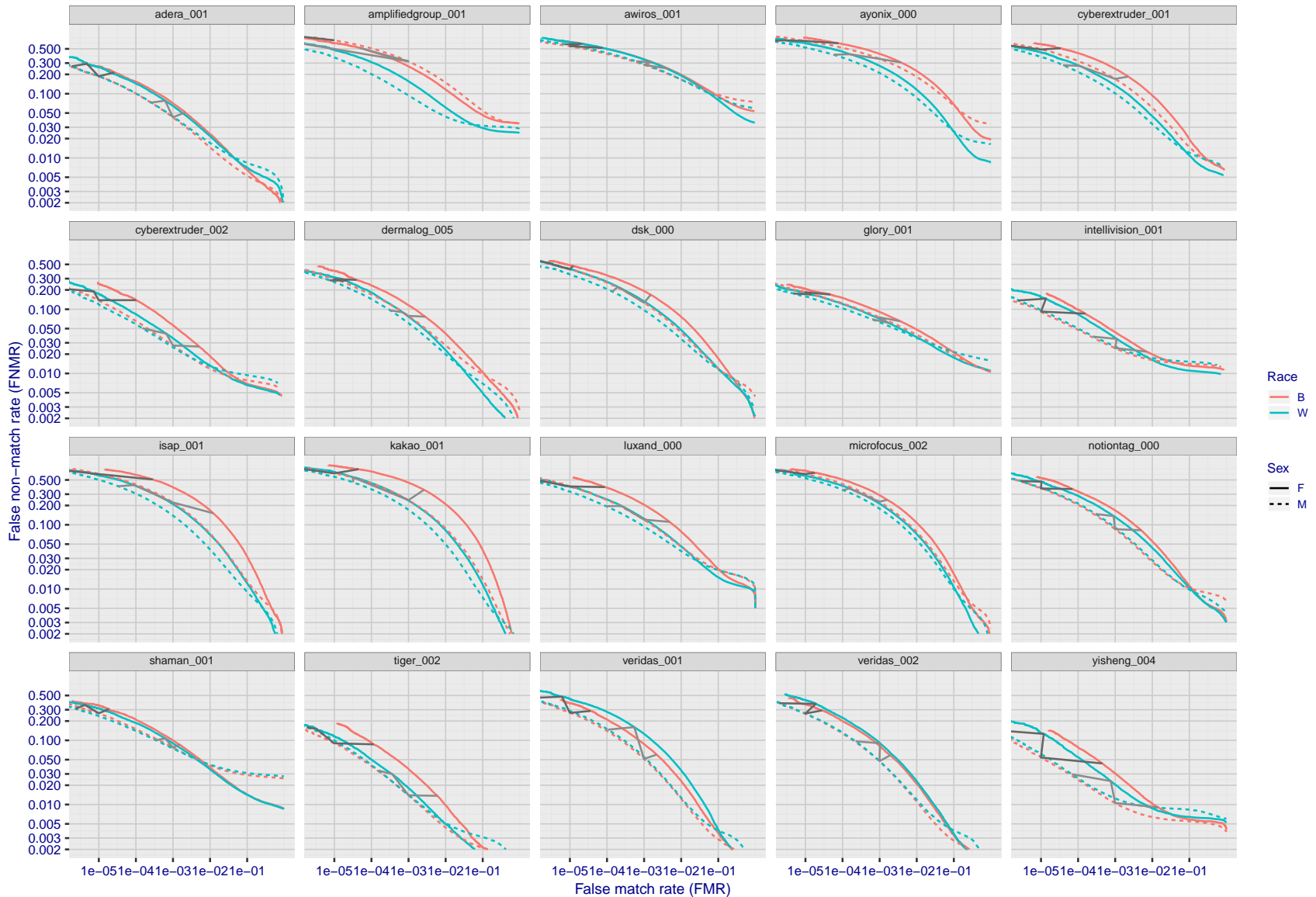
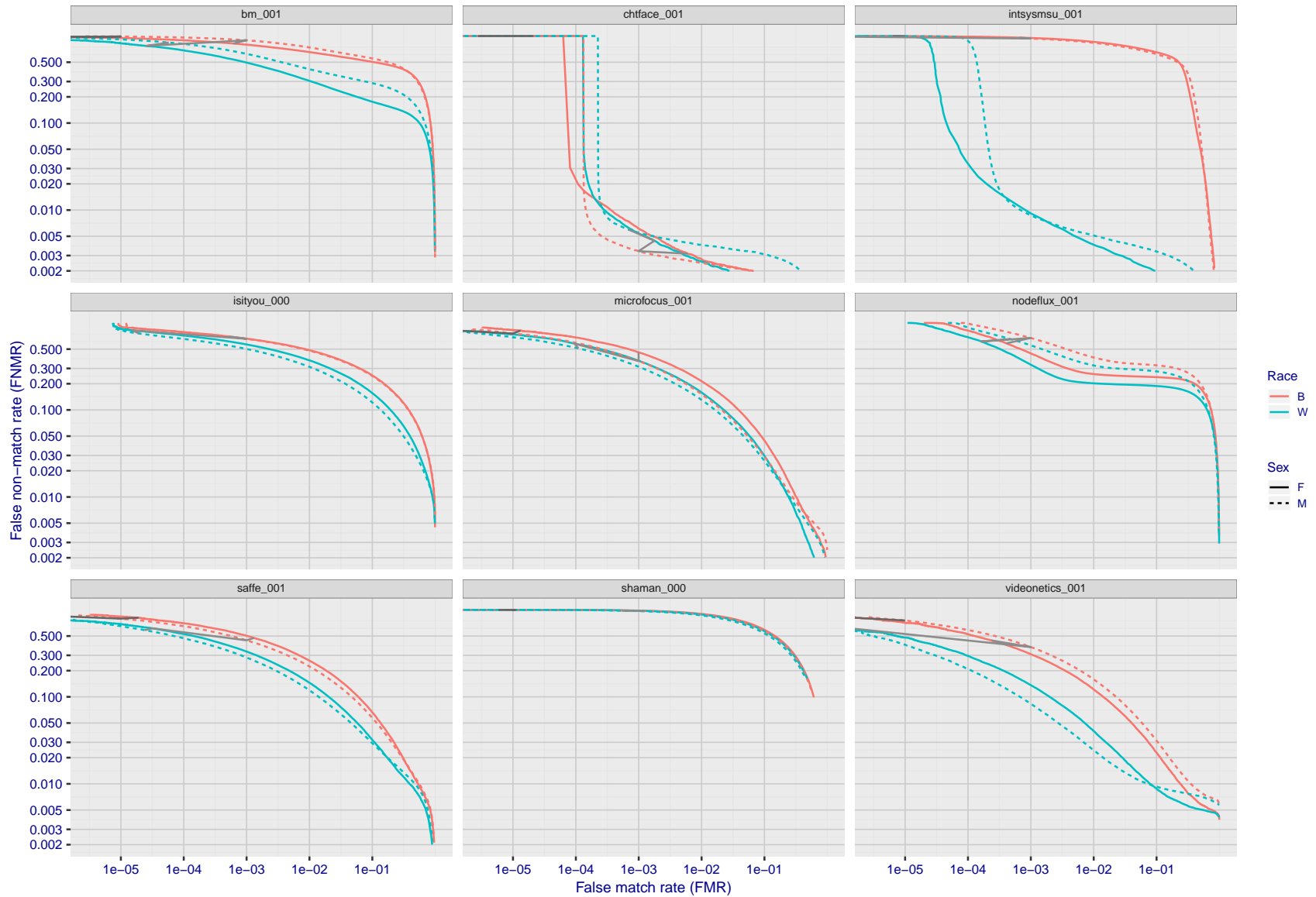


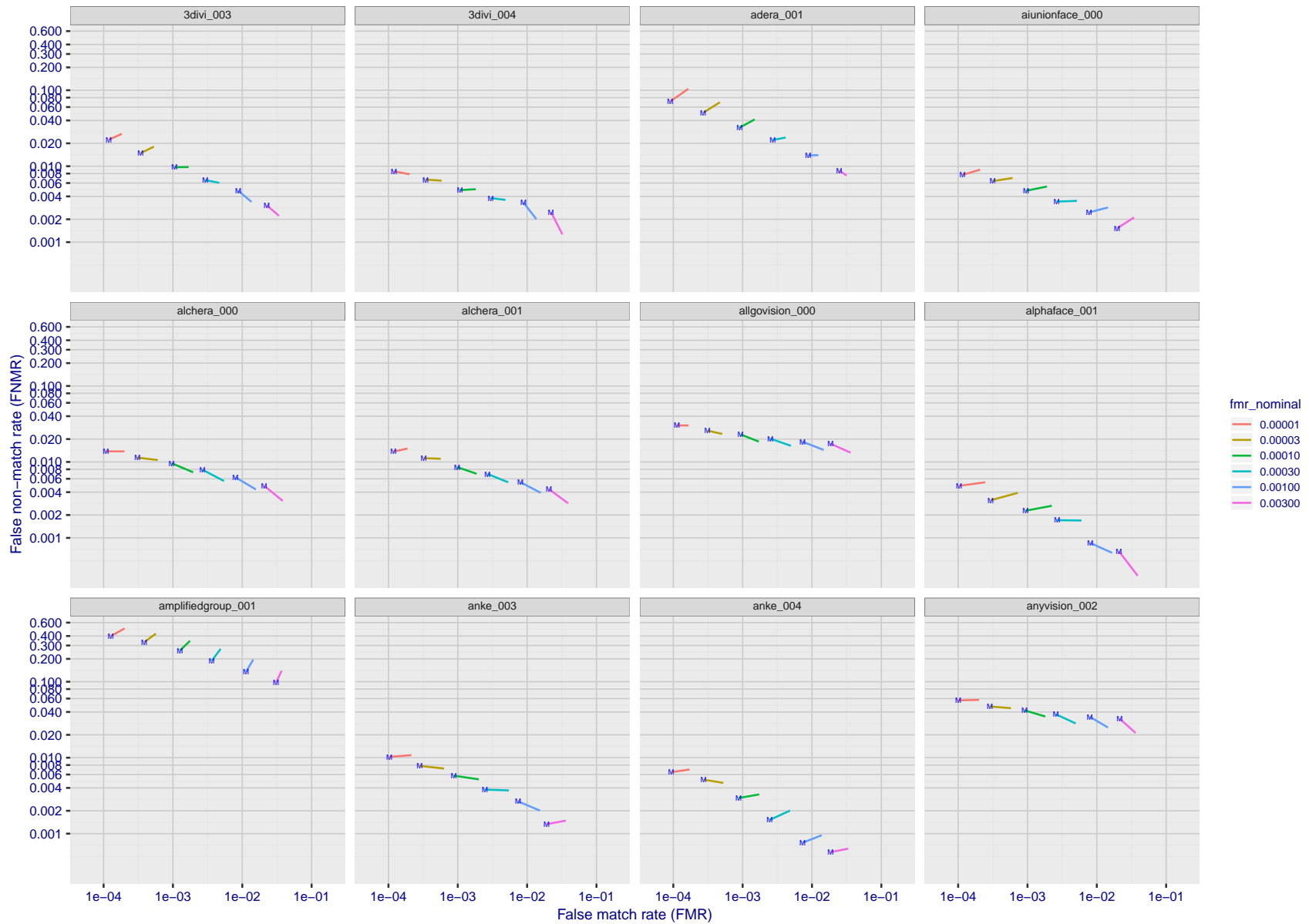
Figure 70: For the mugshot images, error tradeoff characteristics for white females, black females, black males and white males. The Z-shaped grey lines correspond to fixed thresholds, showing both FNMR and FMR vary at one  $T$  value. Note: Many of the plots will naively be read as saying women gives worse error rates than men because the solid traces lie above the dotted ones. However, this is misleading and incomplete: The grey lines show the traces reveal horizontal shifts. Thus for the cogent-003 algorithm FNMR for men is higher than for women at a fixed threshold but, at the same time, FMR is higher for women - see Figure 94. As access control systems almost always operate at a fixed threshold, the naive interpretation is incorrect.





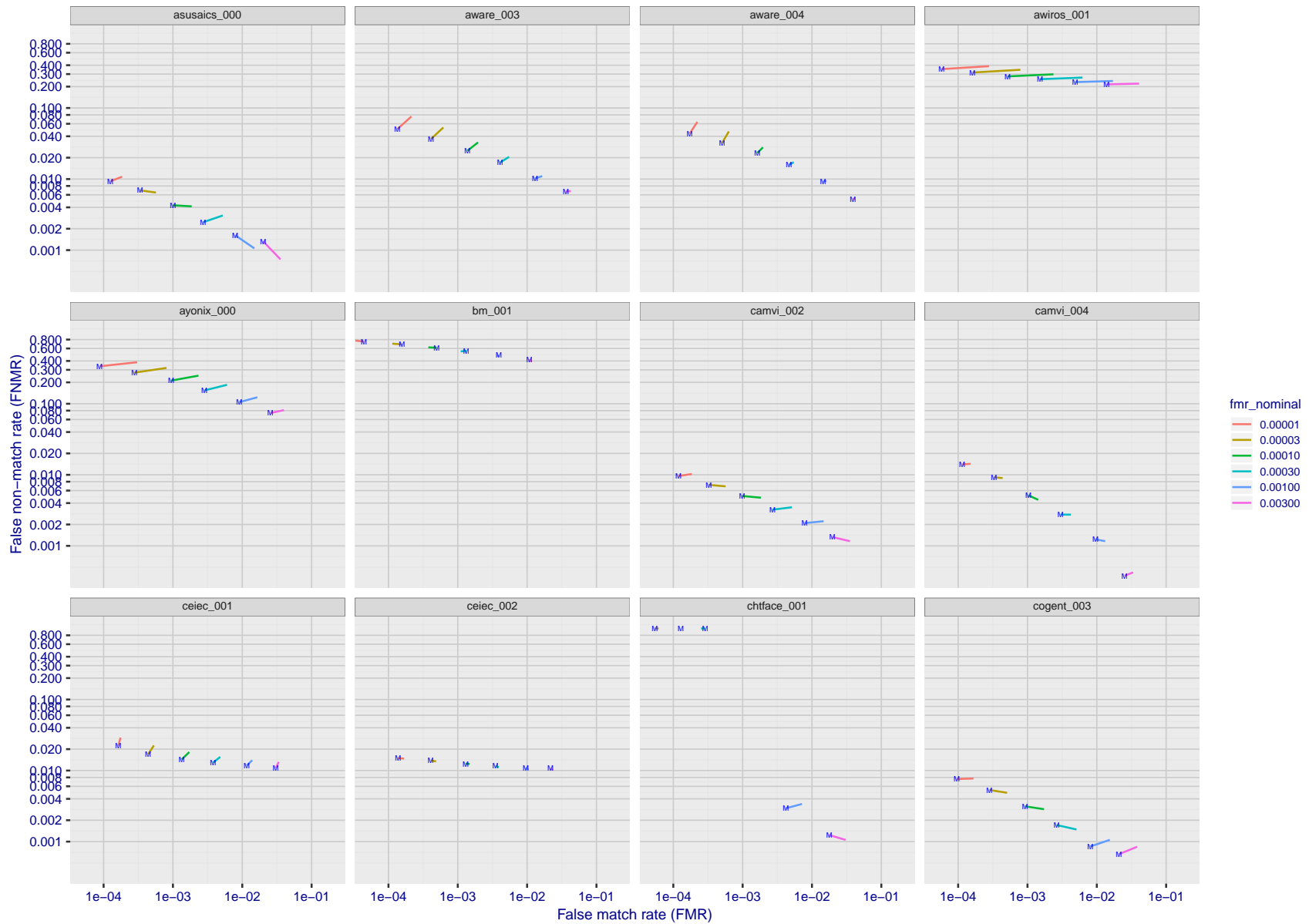
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 71: For the mugshot images, error tradeoff characteristics for white females, black females, black males and white males. The Z-shaped grey lines correspond to fixed thresholds, showing both FNMR and FMR vary at one T value. Note: Many of the plots will naively be read as saying women gives worse error rates than men because the solid traces lie above the dotted ones. However, this is misleading and incomplete: The grey lines show the traces reveal horizontal shifts. Thus for the cogent-003 algorithm FNMR for men is higher than for women at a fixed threshold but, at the same time, FMR is higher for women - see Figure 94. As access control systems almost always operate at a fixed threshold, the naive interpretation is incorrect.



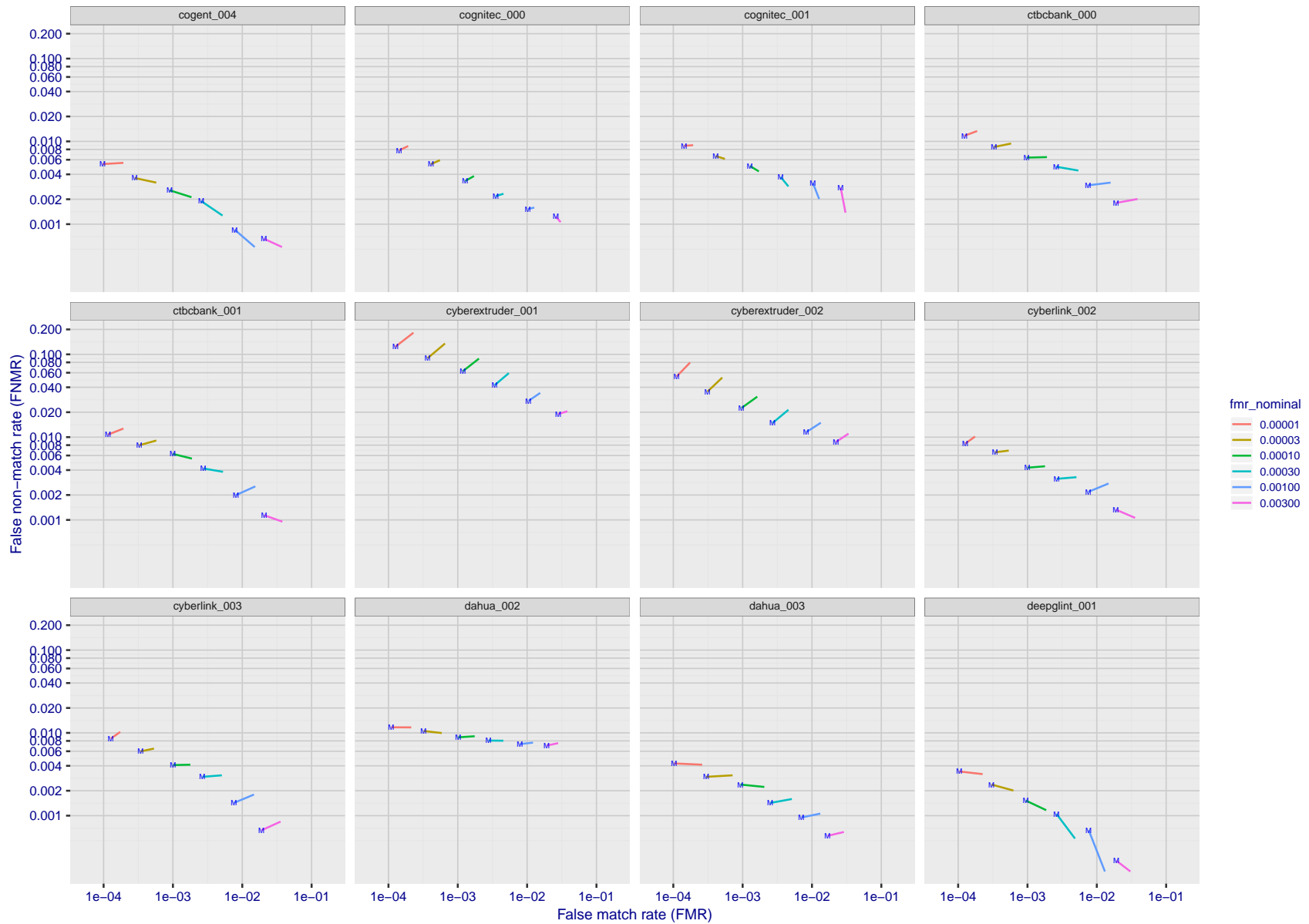
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 72: For the visa images, FNMR and FMR at six operating points along the DET characteristic. At each point a line is drawn between  $(FMR, FNMR)_{MALE}$  and  $(FMR, FNMR)_{FEMALE}$  showing how which sex has lower FMR and/or FNMR. The "M" label denotes male, the other end of the line corresponds to female. The six operating thresholds are selected to give the nominal false match rates given in the legend, and are computed over all impostor pairs regardless of age, sex, and place of birth. The plotted FMR values are broadly an order of magnitude larger than the nominal rates because FMR is computed over demographically-matched impostor pairs i.e individuals of the same sex, from the same geographic region (see section 3.6.1), and the same age group (see section 3.6.2).



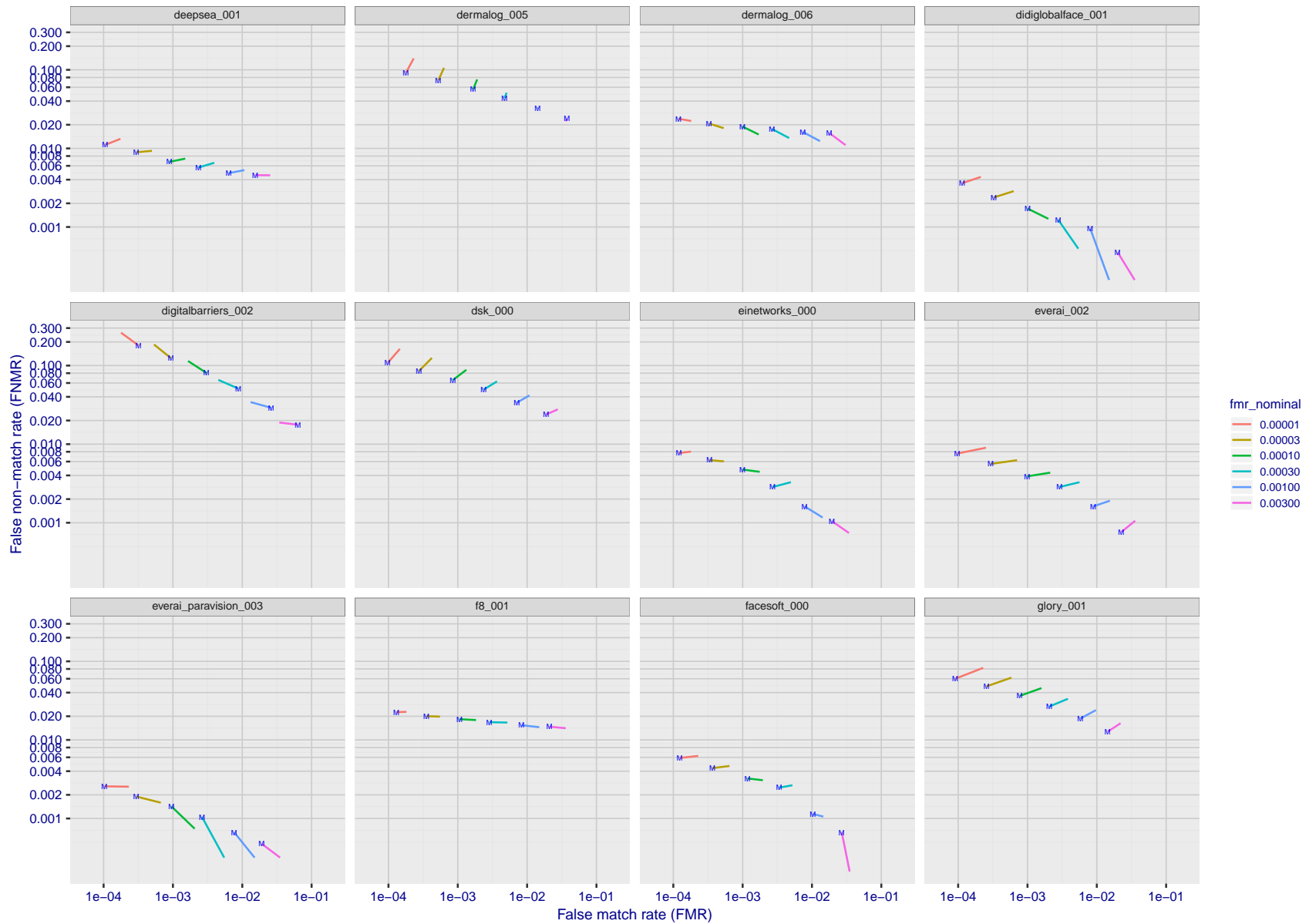
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 73: For the visa images, FNMR and FMR at six operating points along the DET characteristic. At each point a line is drawn between  $(FMR, FNMR)_{MALE}$  and  $(FMR, FNMR)_{FEMALE}$  showing how which sex has lower FMR and/or FNMR. The "M" label denotes male, the other end of the line corresponds to female. The six operating thresholds are selected to give the nominal false match rates given in the legend, and are computed over all impostor pairs regardless of age, sex, and place of birth. The plotted FMR values are broadly an order of magnitude larger than the nominal rates because FMR is computed over demographically-matched impostor pairs i.e individuals of the same sex, from the same geographic region (see section 3.6.1), and the same age group (see section 3.6.2).



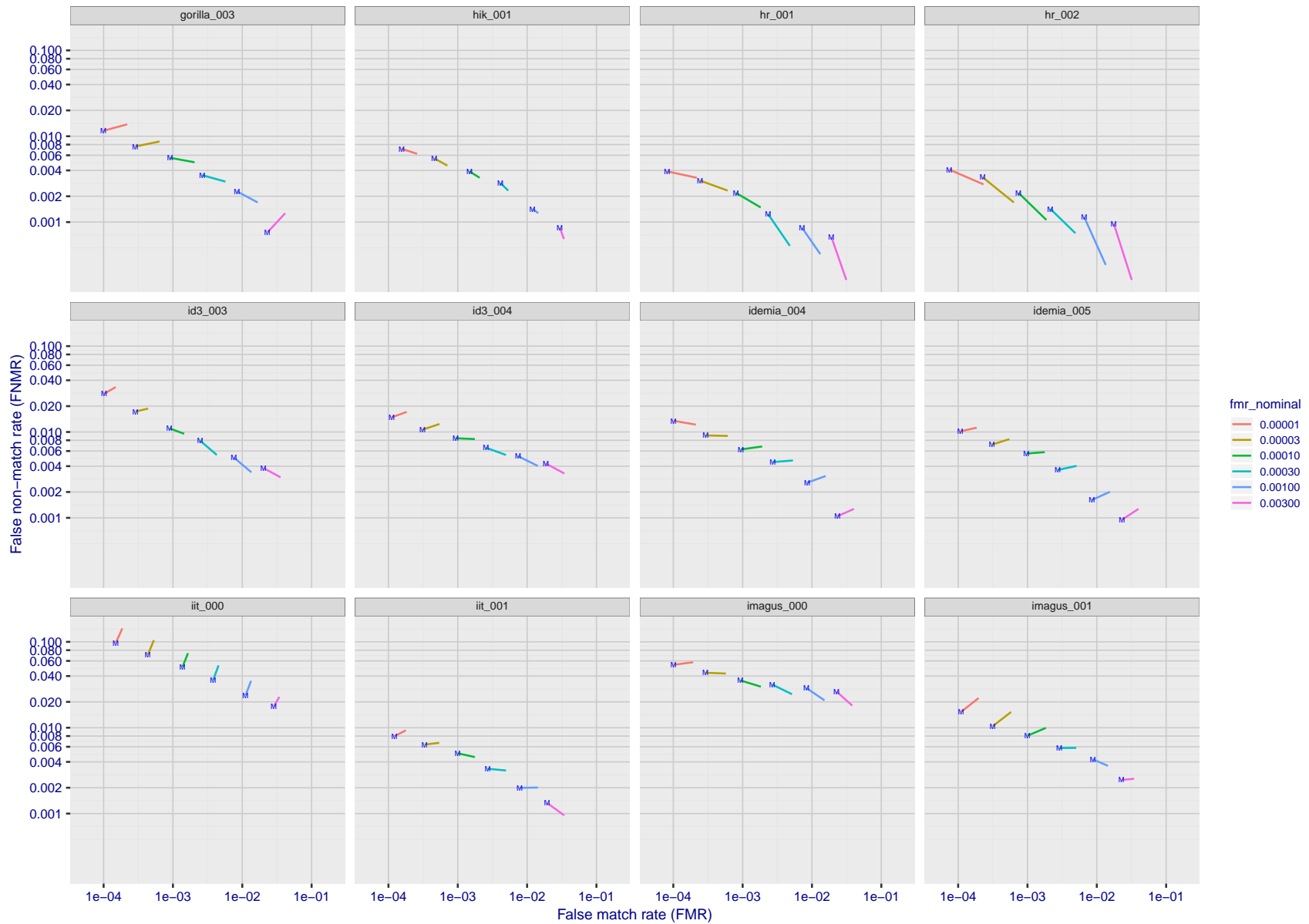
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 74: For the visa images, FNMR and FMR at six operating points along the DET characteristic. At each point a line is drawn between  $(FMR, FNMR)_{MALE}$  and  $(FMR, FNMR)_{FEMALE}$  showing how which sex has lower FMR and/or FNMR. The "M" label denotes male, the other end of the line corresponds to female. The six operating thresholds are selected to give the nominal false match rates given in the legend, and are computed over all impostor pairs regardless of age, sex, and place of birth. The plotted FMR values are broadly an order of magnitude larger than the nominal rates because FMR is computed over demographically-matched impostor pairs i.e individuals of the same sex, from the same geographic region (see section 3.6.1), and the same age group (see section 3.6.2).



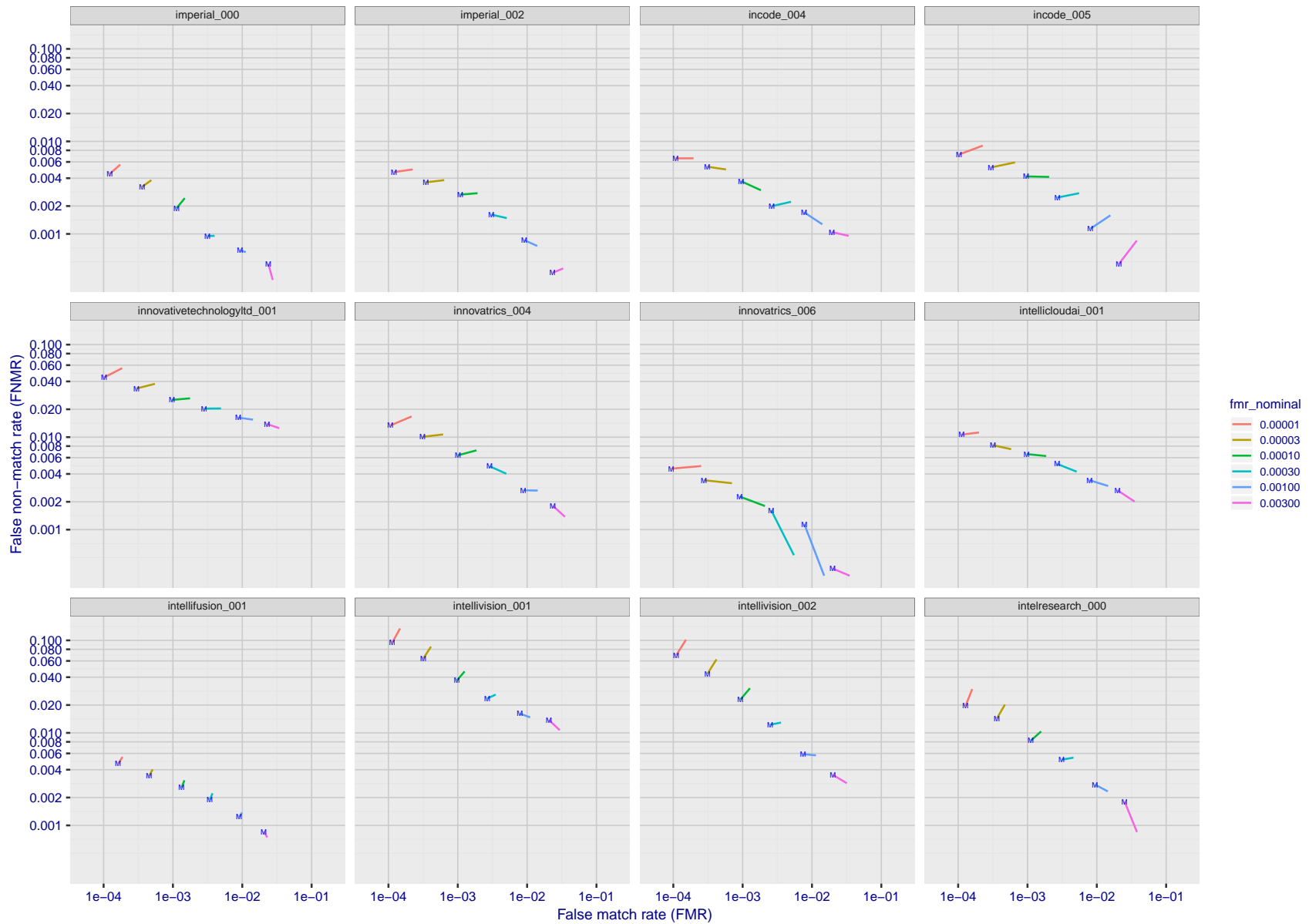
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 75: For the visa images, FNMR and FMR at six operating points along the DET characteristic. At each point a line is drawn between  $(FMR, FNMR)_{MALE}$  and  $(FMR, FNMR)_{FEMALE}$  showing how which sex has lower FMR and/or FNMR. The "M" label denotes male, the other end of the line corresponds to female. The six operating thresholds are selected to give the nominal false match rates given in the legend, and are computed over all impostor pairs regardless of age, sex, and place of birth. The plotted FMR values are broadly an order of magnitude larger than the nominal rates because FMR is computed over demographically-matched impostor pairs i.e individuals of the same sex, from the same geographic region (see section 3.6.1), and the same age group (see section 3.6.2).



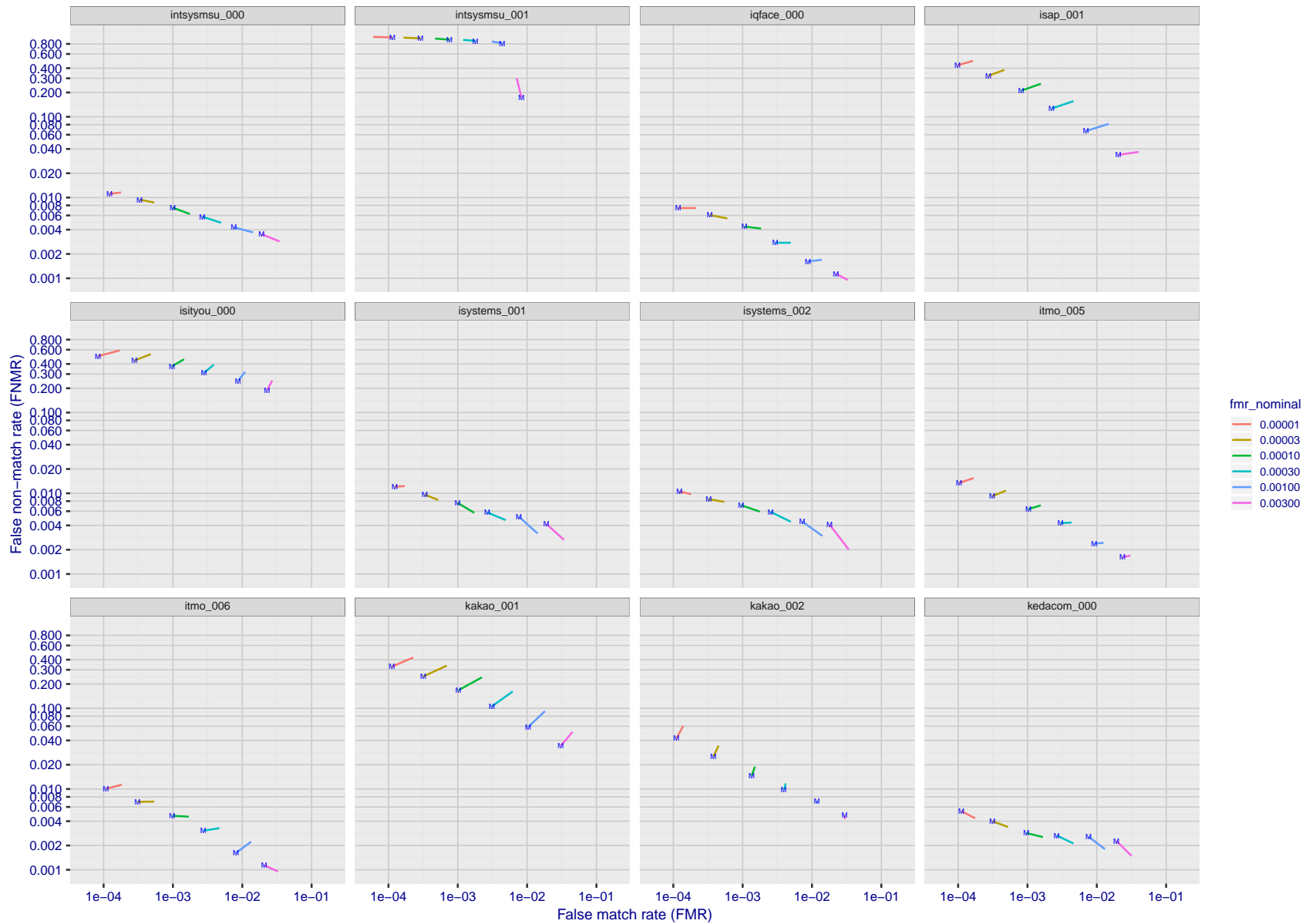
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 76: For the visa images, FNMR and FMR at six operating points along the DET characteristic. At each point a line is drawn between  $(FMR, FNMR)_{MALE}$  and  $(FMR, FNMR)_{FEMALE}$  showing how which sex has lower FMR and/or FNMR. The "M" label denotes male, the other end of the line corresponds to female. The six operating thresholds are selected to give the nominal false match rates given in the legend, and are computed over all impostor pairs regardless of age, sex, and place of birth. The plotted FMR values are broadly an order of magnitude larger than the nominal rates because FMR is computed over demographically-matched impostor pairs i.e individuals of the same sex, from the same geographic region (see section 3.6.1), and the same age group (see section 3.6.2).



FNMR(T)  
 FMR(T)  
 "False non-match rate"  
 "False match rate"

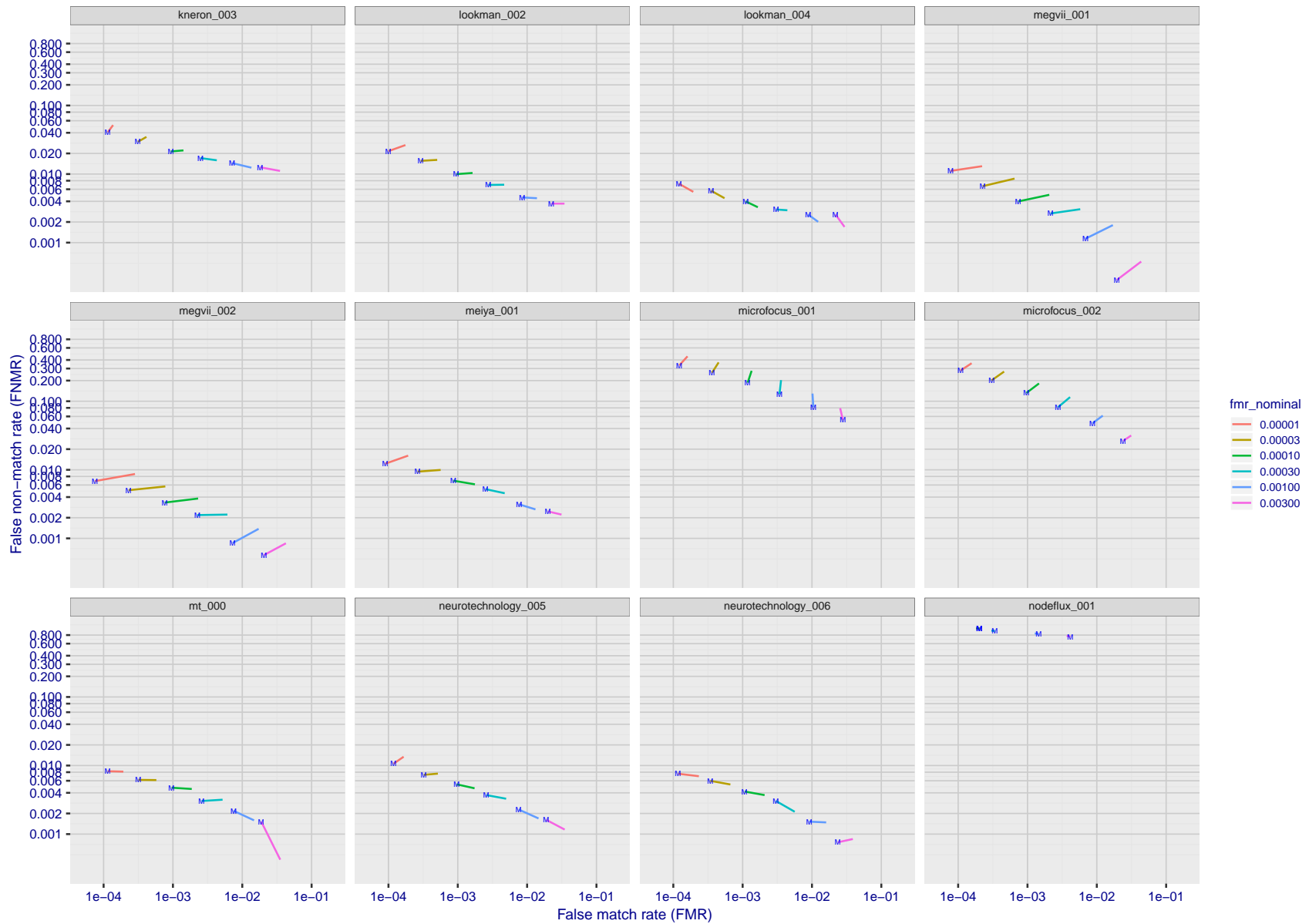
Figure 77: For the visa images, FNMR and FMR at six operating points along the DET characteristic. At each point a line is drawn between  $(FMR, FNMR)_{MALE}$  and  $(FMR, FNMR)_{FEMALE}$  showing how which sex has lower FMR and/or FNMR. The "M" label denotes male, the other end of the line corresponds to female. The six operating thresholds are selected to give the nominal false match rates given in the legend, and are computed over all impostor pairs regardless of age, sex, and place of birth. The plotted FMR values are broadly an order of magnitude larger than the nominal rates because FMR is computed over demographically-matched impostor pairs i.e individuals of the same sex, from the same geographic region (see section 3.6.1), and the same age group (see section 3.6.2).



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

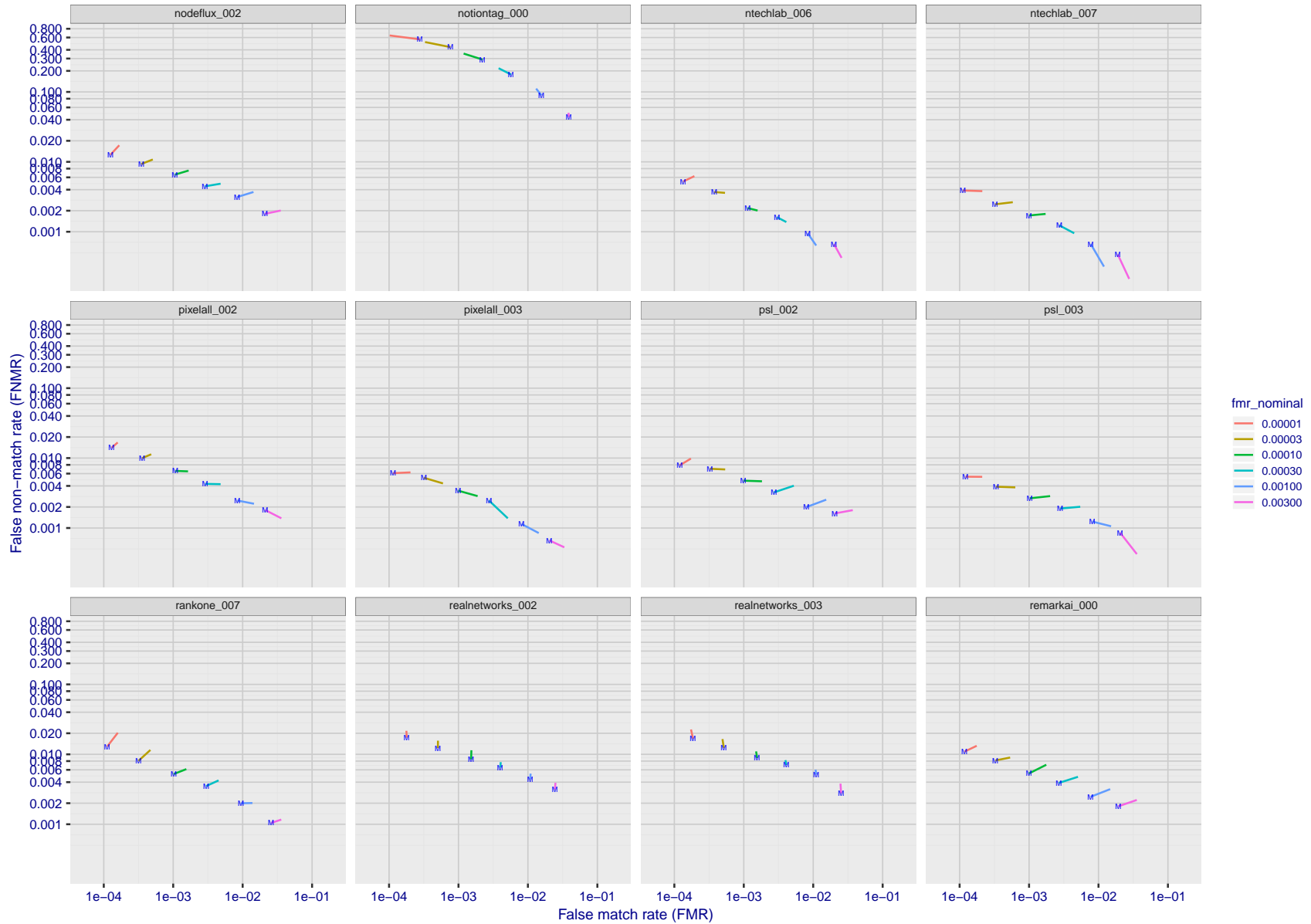
Figure 78: For the visa images, FNMR and FMR at six operating points along the DET characteristic. At each point a line is drawn between  $(FMR, FNMR)_{MALE}$  and  $(FMR, FNMR)_{FEMALE}$  showing how which sex has lower FMR and/or FNMR. The "M" label denotes male, the other end of the line corresponds to female. The six operating thresholds are selected to give the nominal false match rates given in the legend, and are computed over all impostor pairs regardless of age, sex, and place of birth. The plotted FMR values are broadly an order of magnitude larger than the nominal rates because FMR is computed over demographically-matched impostor pairs i.e individuals of the same sex, from the same geographic region (see section 3.6.1), and the same age group (see section 3.6.2).





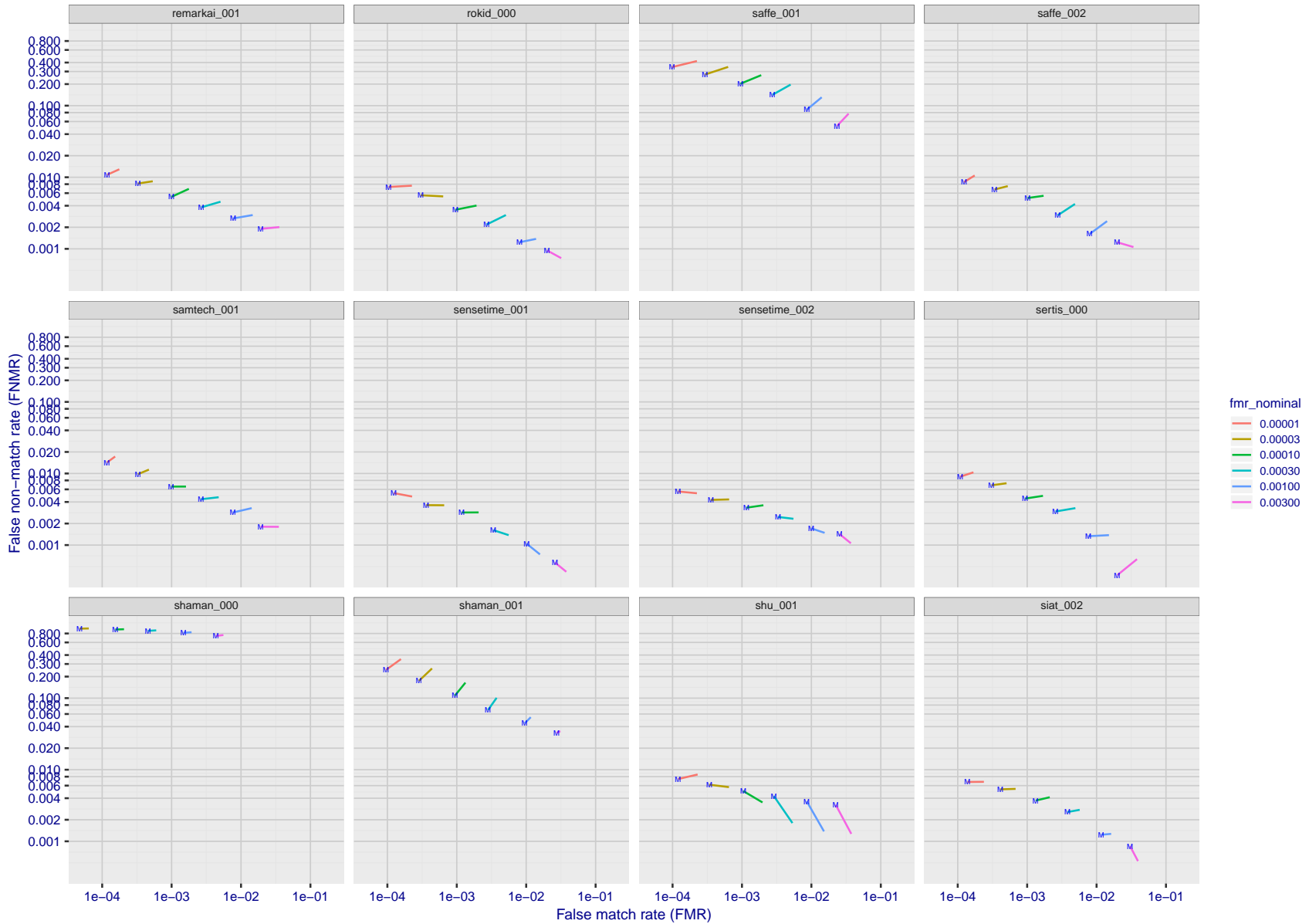
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 79: For the visa images, FNMR and FMR at six operating points along the DET characteristic. At each point a line is drawn between  $(FMR, FNMR)_{MALE}$  and  $(FMR, FNMR)_{FEMALE}$  showing how which sex has lower FMR and/or FNMR. The "M" label denotes male, the other end of the line corresponds to female. The six operating thresholds are selected to give the nominal false match rates given in the legend, and are computed over all impostor pairs regardless of age, sex, and place of birth. The plotted FMR values are broadly an order of magnitude larger than the nominal rates because FMR is computed over demographically-matched impostor pairs i.e individuals of the same sex, from the same geographic region (see section 3.6.1), and the same age group (see section 3.6.2).



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 80: For the visa images, FNMR and FMR at six operating points along the DET characteristic. At each point a line is drawn between  $(FMR, FNMR)_{\text{MALE}}$  and  $(FMR, FNMR)_{\text{FEMALE}}$  showing how which sex has lower FMR and/or FNMR. The "M" label denotes male, the other end of the line corresponds to female. The six operating thresholds are selected to give the nominal false match rates given in the legend, and are computed over all impostor pairs regardless of age, sex, and place of birth. The plotted FMR values are broadly an order of magnitude larger than the nominal rates because FMR is computed over demographically-matched impostor pairs i.e individuals of the same sex, from the same geographic region (see section 3.6.1), and the same age group (see section 3.6.2).



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 81: For the visa images, FNMR and FMR at six operating points along the DET characteristic. At each point a line is drawn between  $(FMR, FNMR)_{MALE}$  and  $(FMR, FNMR)_{FEMALE}$  showing how which sex has lower FMR and/or FNMR. The "M" label denotes male, the other end of the line corresponds to female. The six operating thresholds are selected to give the nominal false match rates given in the legend, and are computed over all impostor pairs regardless of age, sex, and place of birth. The plotted FMR values are broadly an order of magnitude larger than the nominal rates because FMR is computed over demographically-matched impostor pairs i.e individuals of the same sex, from the same geographic region (see section 3.6.1), and the same age group (see section 3.6.2).

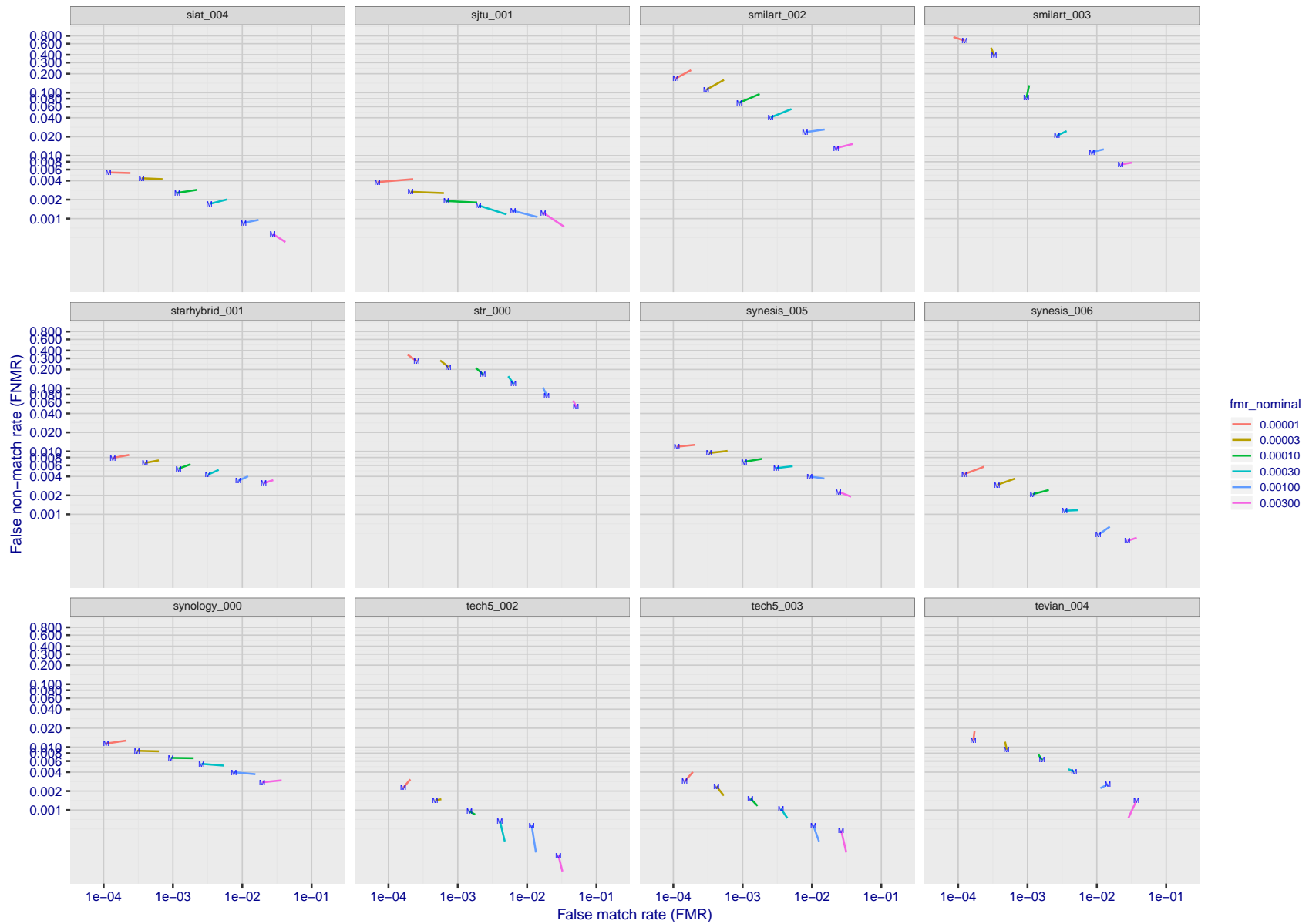
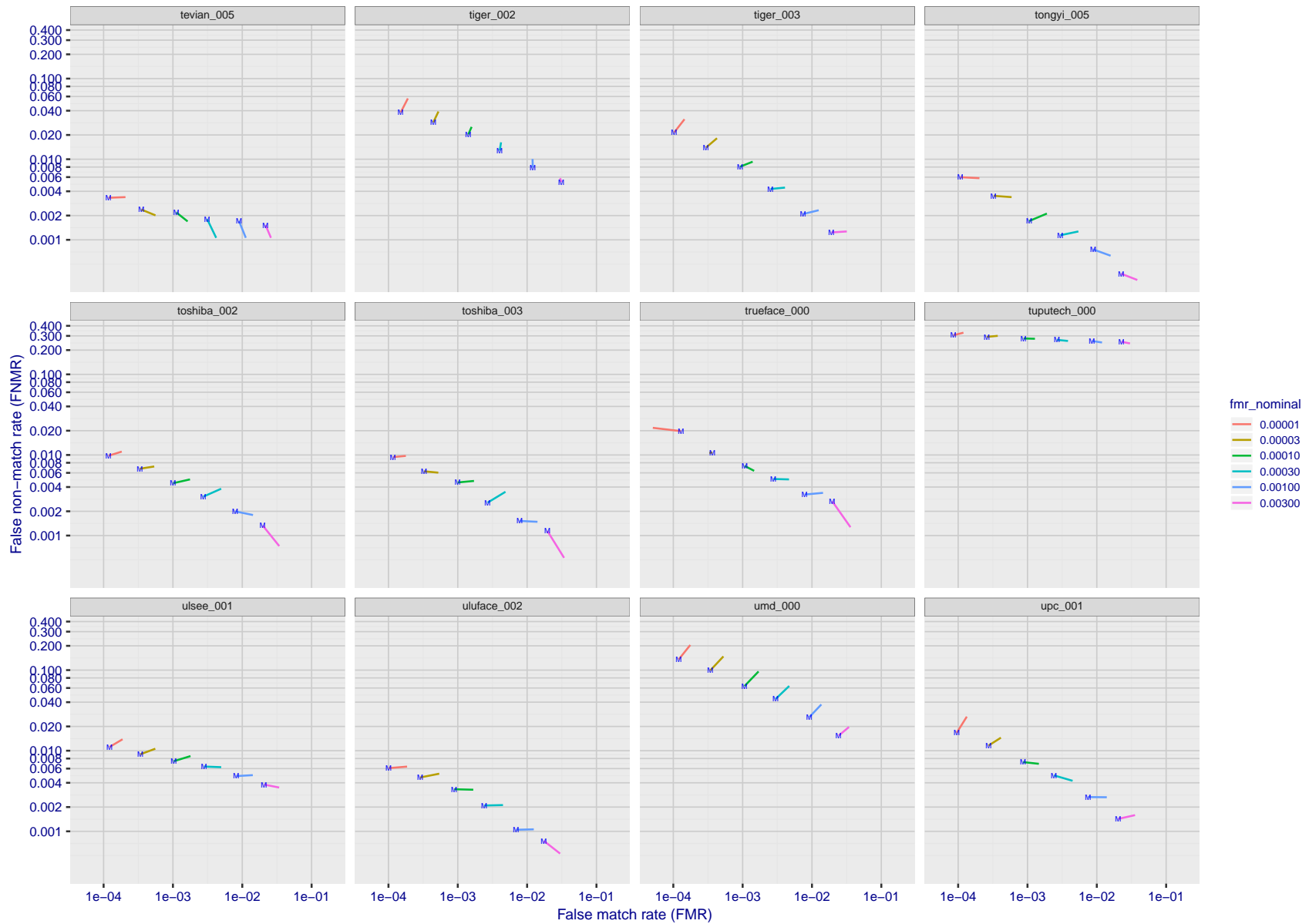
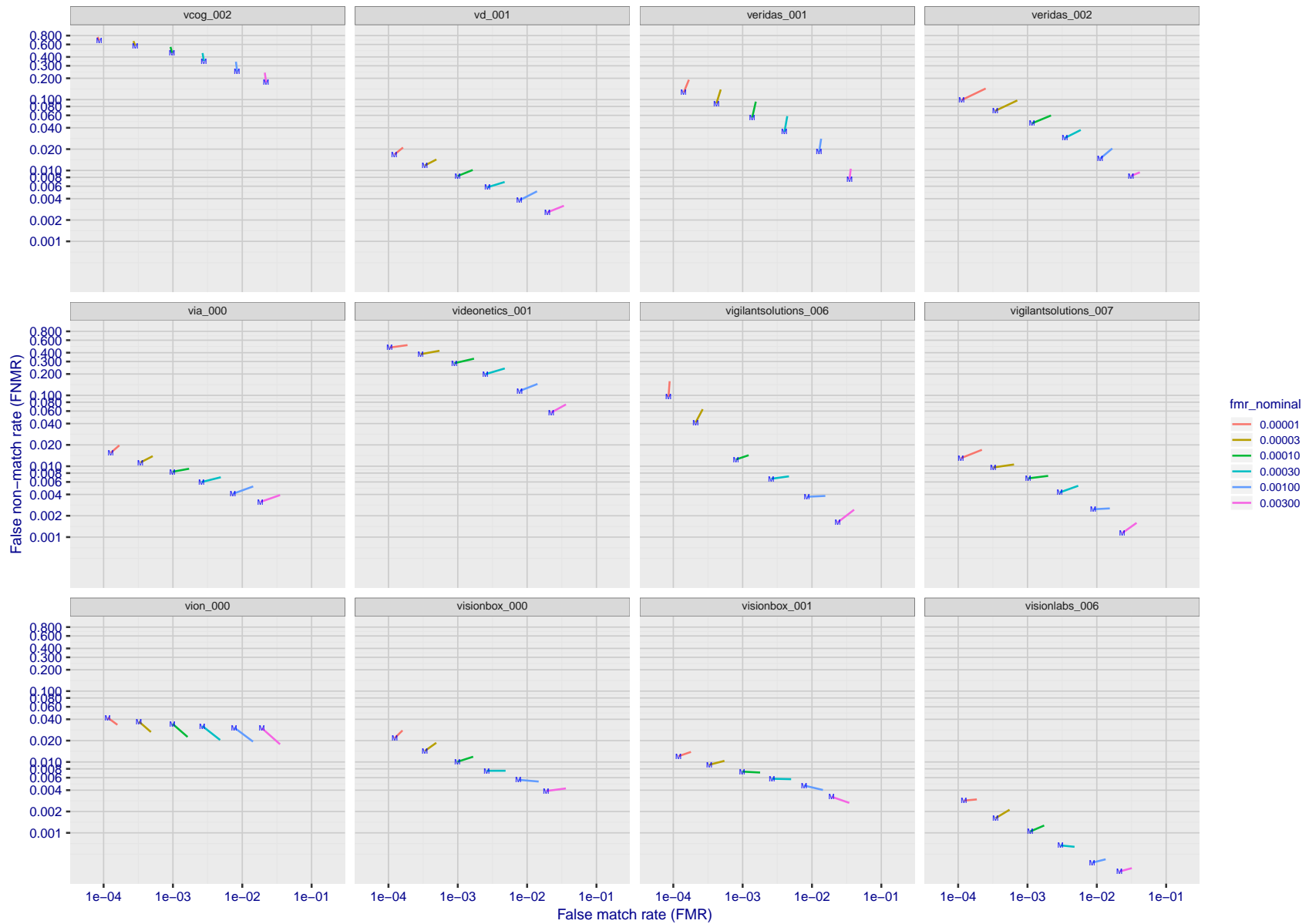


Figure 82: For the visa images, FNMR and FMR at six operating points along the DET characteristic. At each point a line is drawn between  $(FMR, FNMR)_{MALE}$  and  $(FMR, FNMR)_{FEMALE}$  showing how which sex has lower FMR and/or FNMR. The "M" label denotes male, the other end of the line corresponds to female. The six operating thresholds are selected to give the nominal false match rates given in the legend, and are computed over all impostor pairs regardless of age, sex, and place of birth. The plotted FMR values are broadly an order of magnitude larger than the nominal rates because FMR is computed over demographically-matched impostor pairs i.e individuals of the same sex, from the same geographic region (see section 3.6.1), and the same age group (see section 3.6.2).



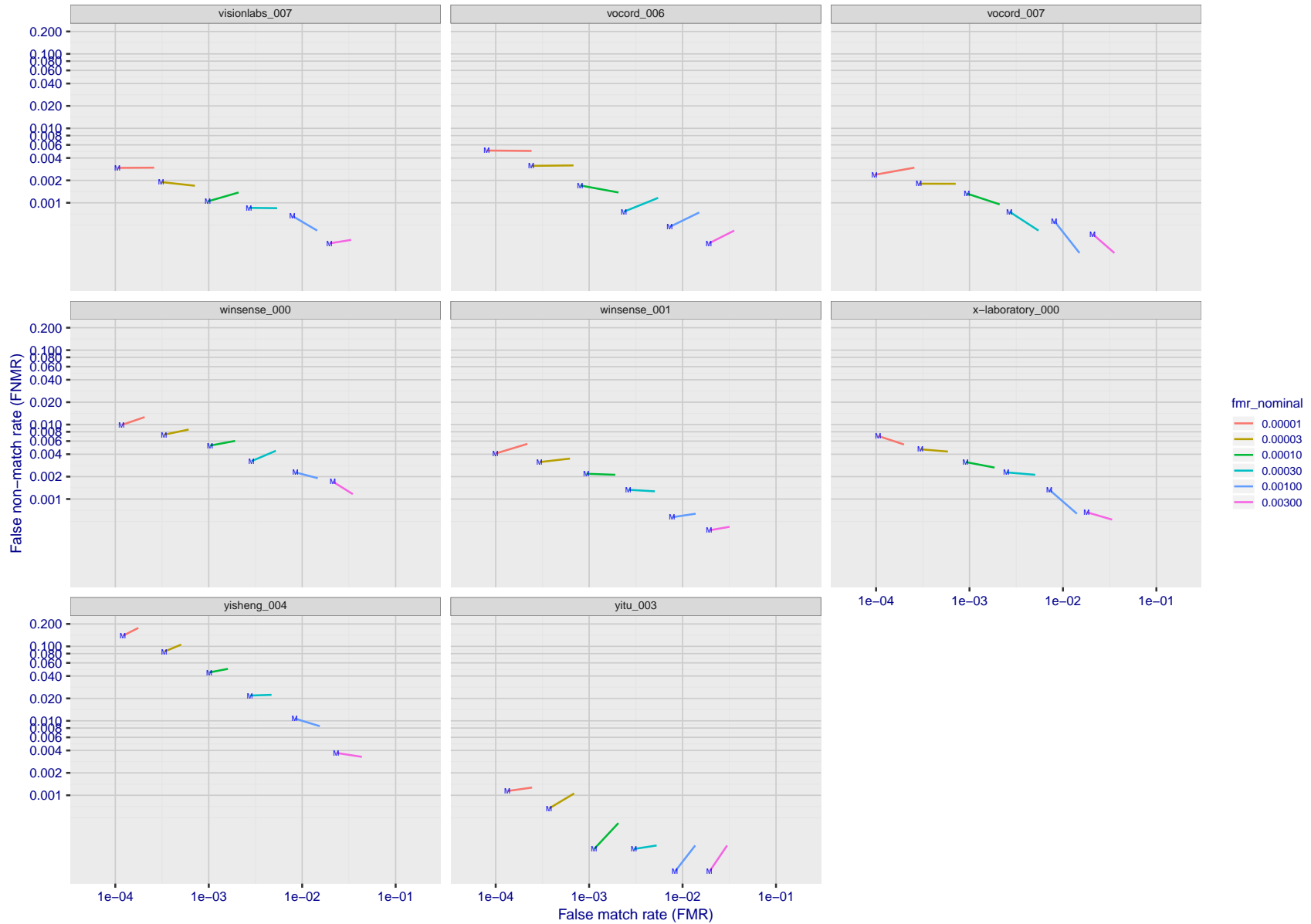
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 83: For the visa images, FNMR and FMR at six operating points along the DET characteristic. At each point a line is drawn between  $(FMR, FNMR)_{MALE}$  and  $(FMR, FNMR)_{FEMALE}$  showing how which sex has lower FMR and/or FNMR. The "M" label denotes male, the other end of the line corresponds to female. The six operating thresholds are selected to give the nominal false match rates given in the legend, and are computed over all impostor pairs regardless of age, sex, and place of birth. The plotted FMR values are broadly an order of magnitude larger than the nominal rates because FMR is computed over demographically-matched impostor pairs i.e individuals of the same sex, from the same geographic region (see section 3.6.1), and the same age group (see section 3.6.2).



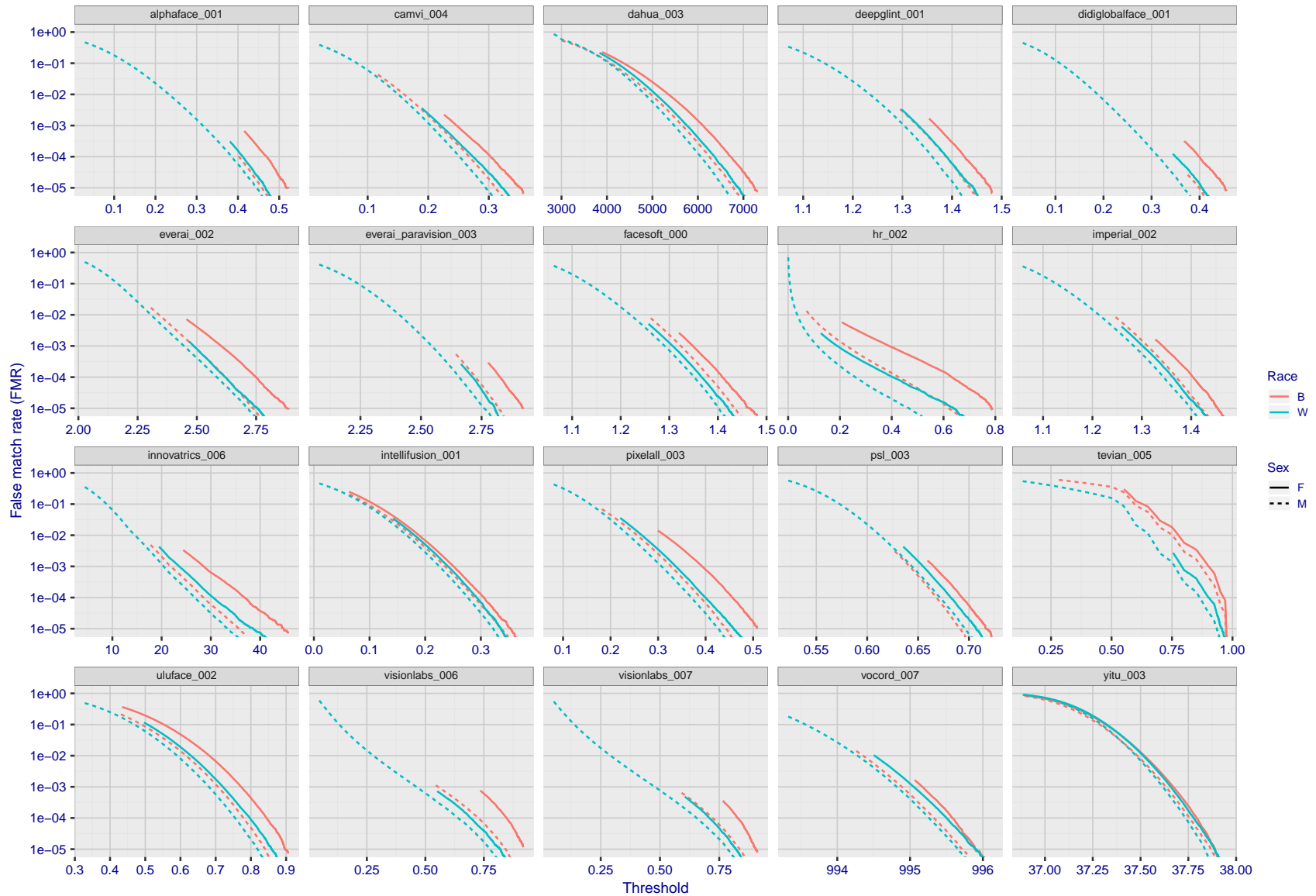
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 84: For the visa images, FNMR and FMR at six operating points along the DET characteristic. At each point a line is drawn between  $(FMR, FNMR)_{MALE}$  and  $(FMR, FNMR)_{FEMALE}$  showing how which sex has lower FMR and/or FNMR. The "M" label denotes male, the other end of the line corresponds to female. The six operating thresholds are selected to give the nominal false match rates given in the legend, and are computed over all impostor pairs regardless of age, sex, and place of birth. The plotted FMR values are broadly an order of magnitude larger than the nominal rates because FMR is computed over demographically-matched impostor pairs i.e individuals of the same sex, from the same geographic region (see section 3.6.1), and the same age group (see section 3.6.2).



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

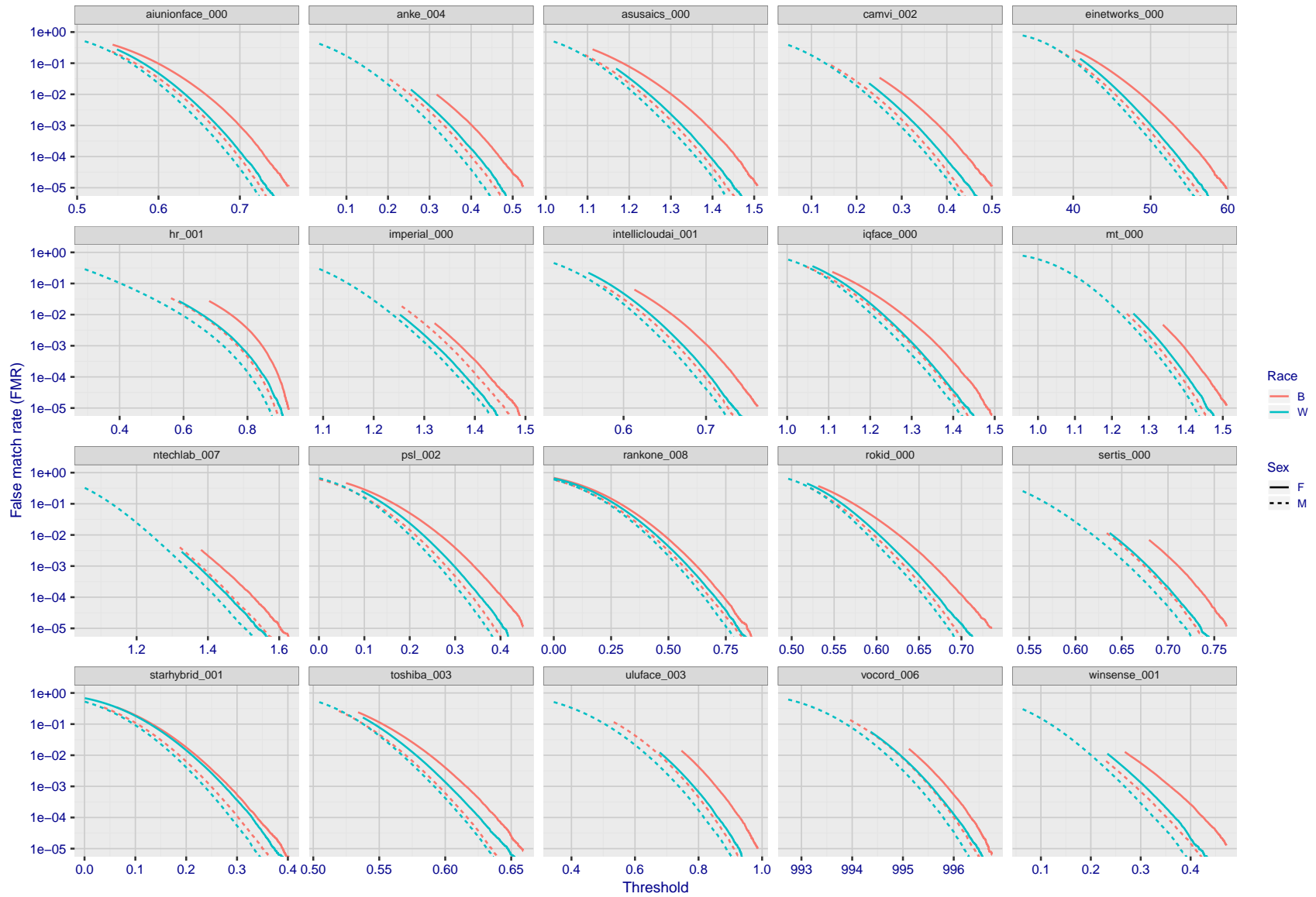
Figure 85: For the visa images, FNMR and FMR at six operating points along the DET characteristic. At each point a line is drawn between  $(FMR, FNMR)_{MALE}$  and  $(FMR, FNMR)_{FEMALE}$  showing how which sex has lower FMR and/or FNMR. The "M" label denotes male, the other end of the line corresponds to female. The six operating thresholds are selected to give the nominal false match rates given in the legend, and are computed over all impostor pairs regardless of age, sex, and place of birth. The plotted FMR values are broadly an order of magnitude larger than the nominal rates because FMR is computed over demographically-matched impostor pairs i.e individuals of the same sex, from the same geographic region (see section 3.6.1), and the same age group (see section 3.6.2).



FNMR(T)  
 FMR(T)  
 "False non-match rate"  
 "False match rate"

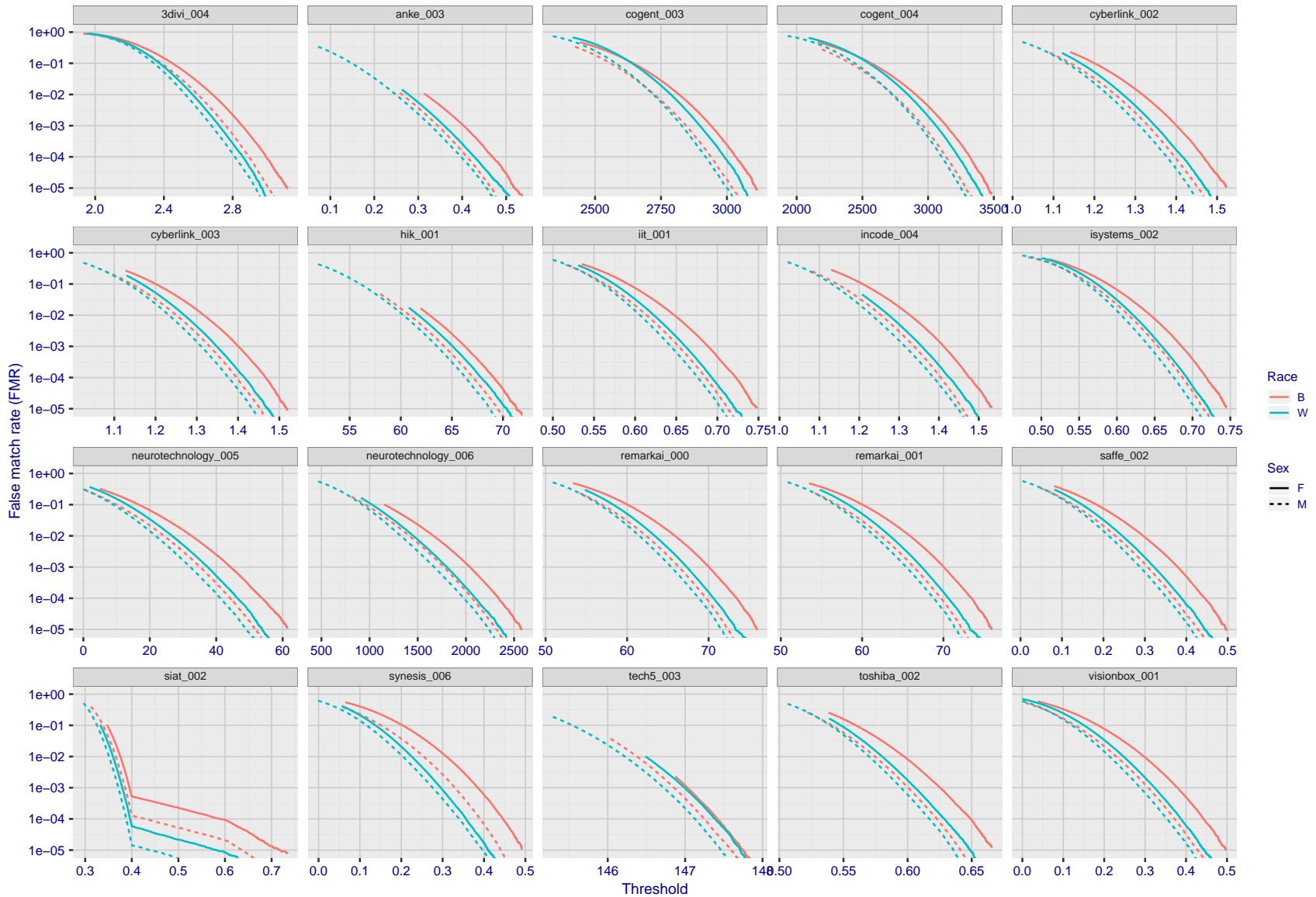
Figure 86: For the mugshot images, the false match calibration curves show false match rate vs. threshold. Separate curves appear for white females, black females, black males and white males.





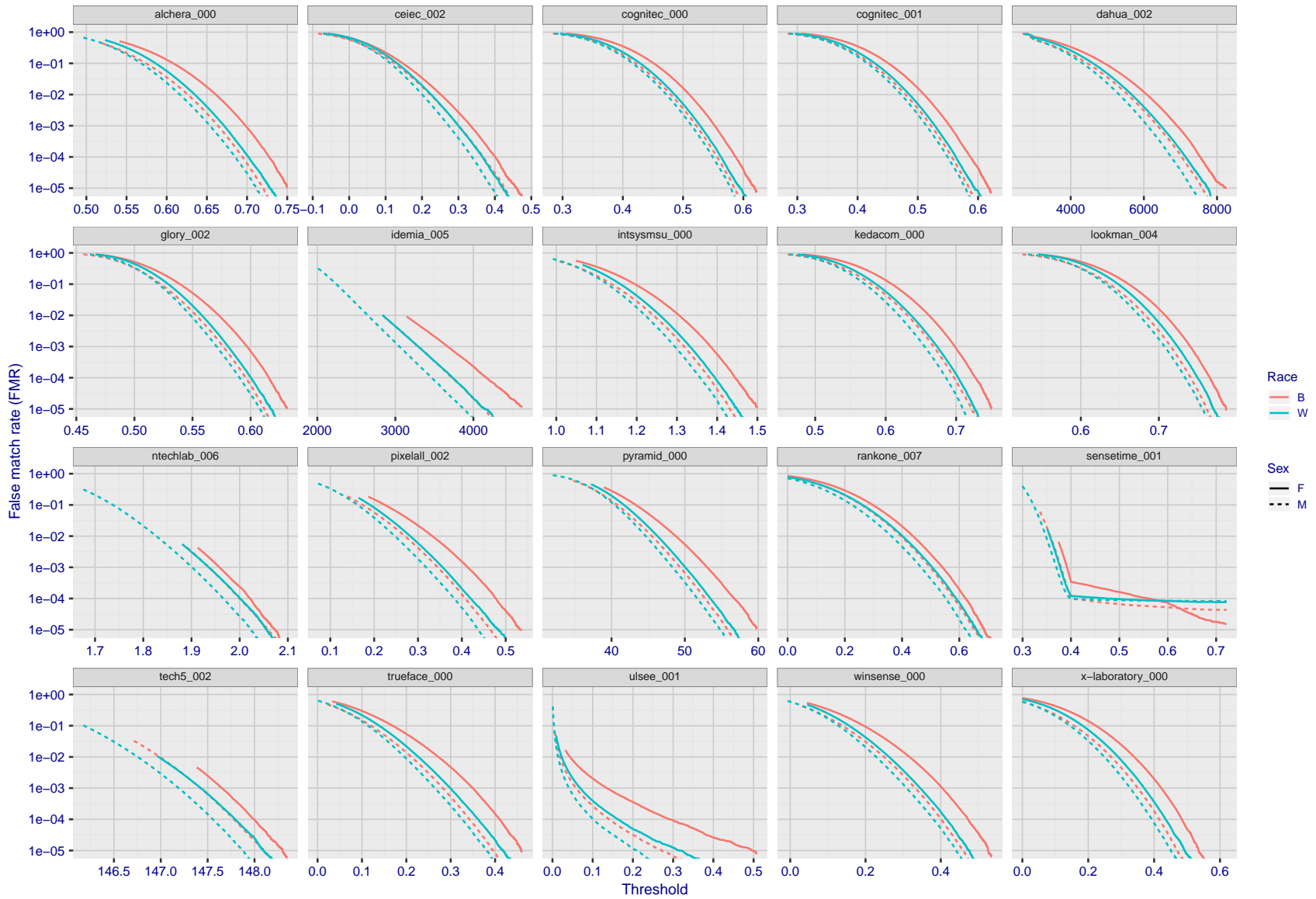
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 87: For the mugshot images, the false match calibration curves show false match rate vs. threshold. Separate curves appear for white females, black females, black males and white males.



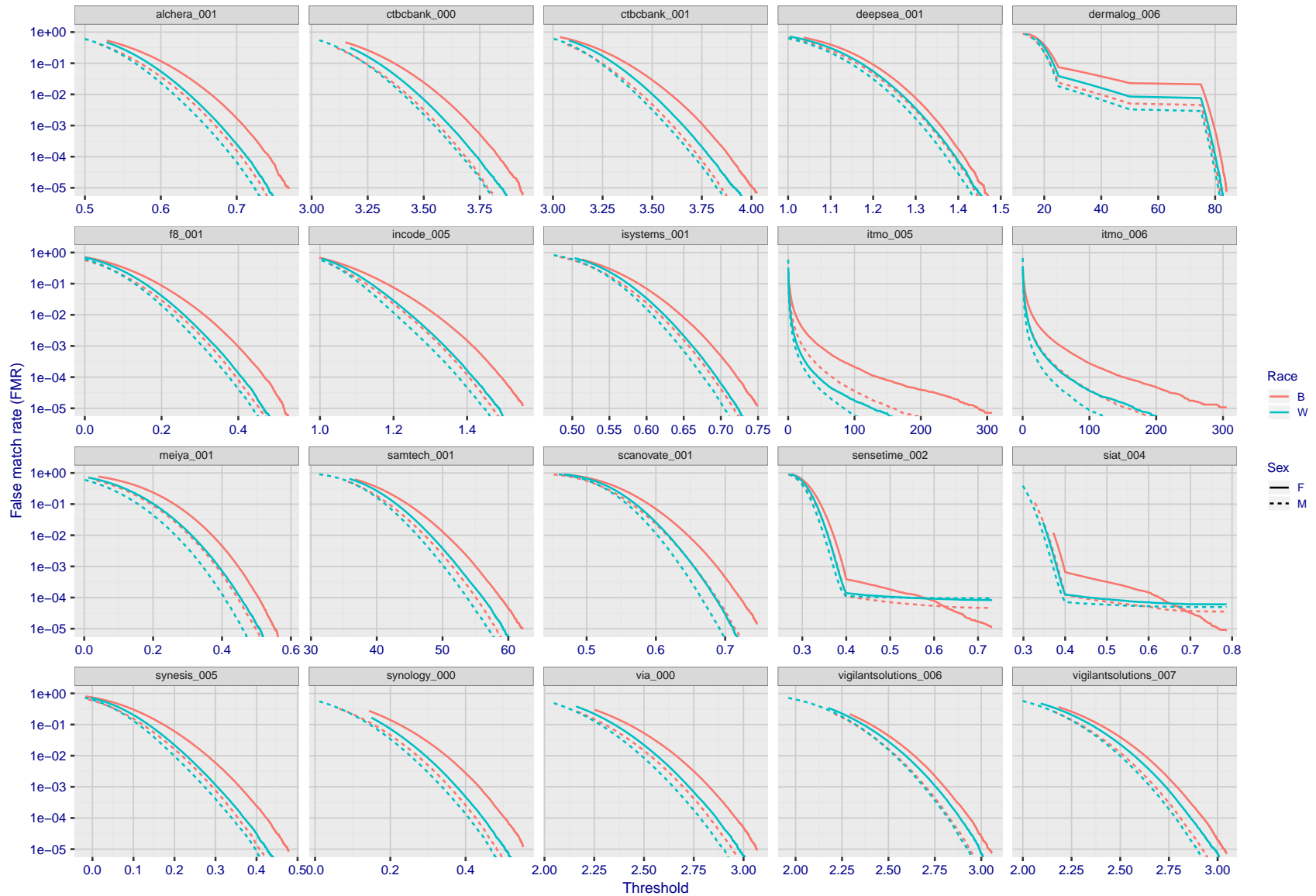
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 88: For the mugshot images, the false match calibration curves show false match rate vs. threshold. Separate curves appear for white females, black females, black males and white males.



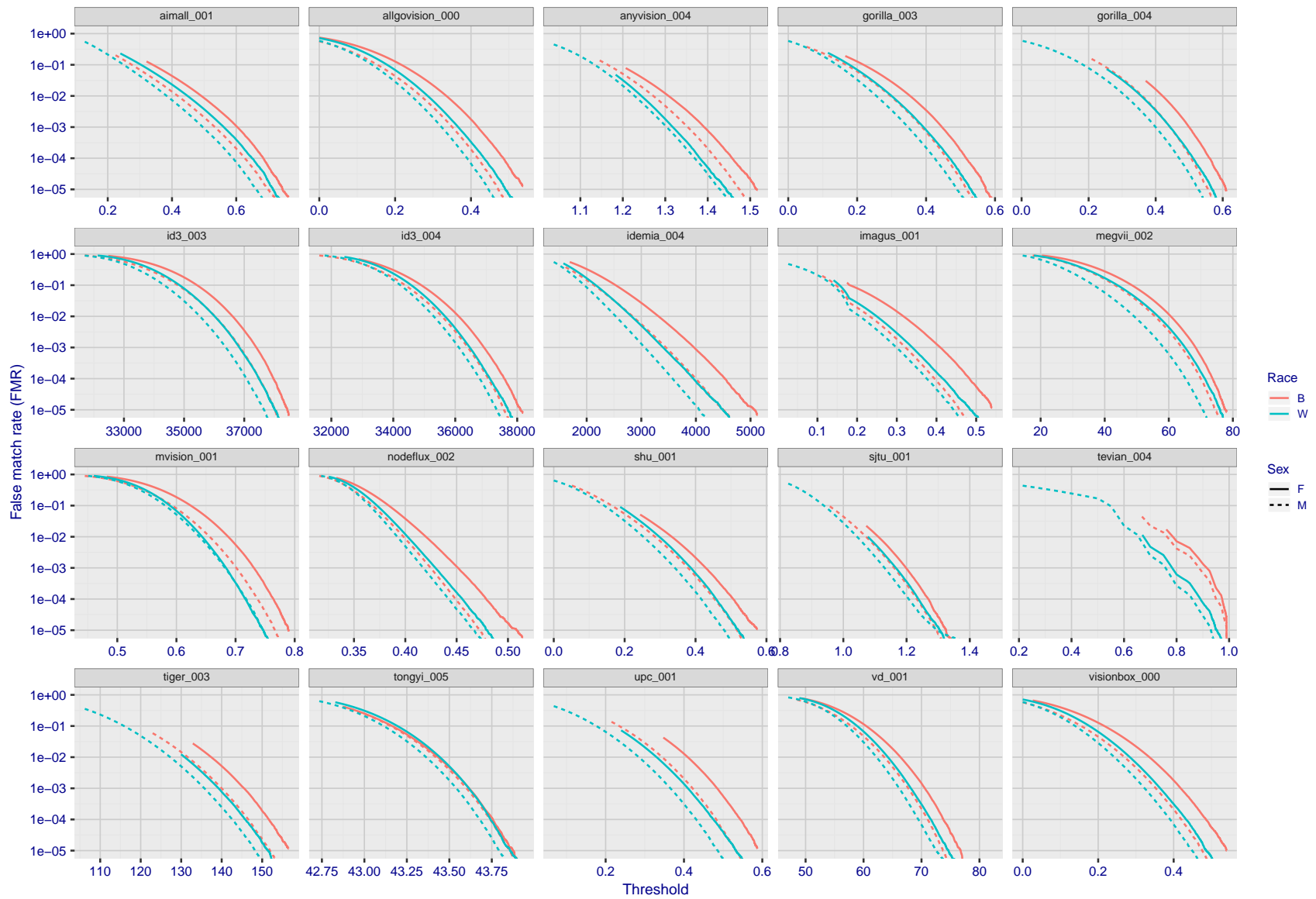
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 89: For the mugshot images, the false match calibration curves show false match rate vs. threshold. Separate curves appear for white females, black females, black males and white males.



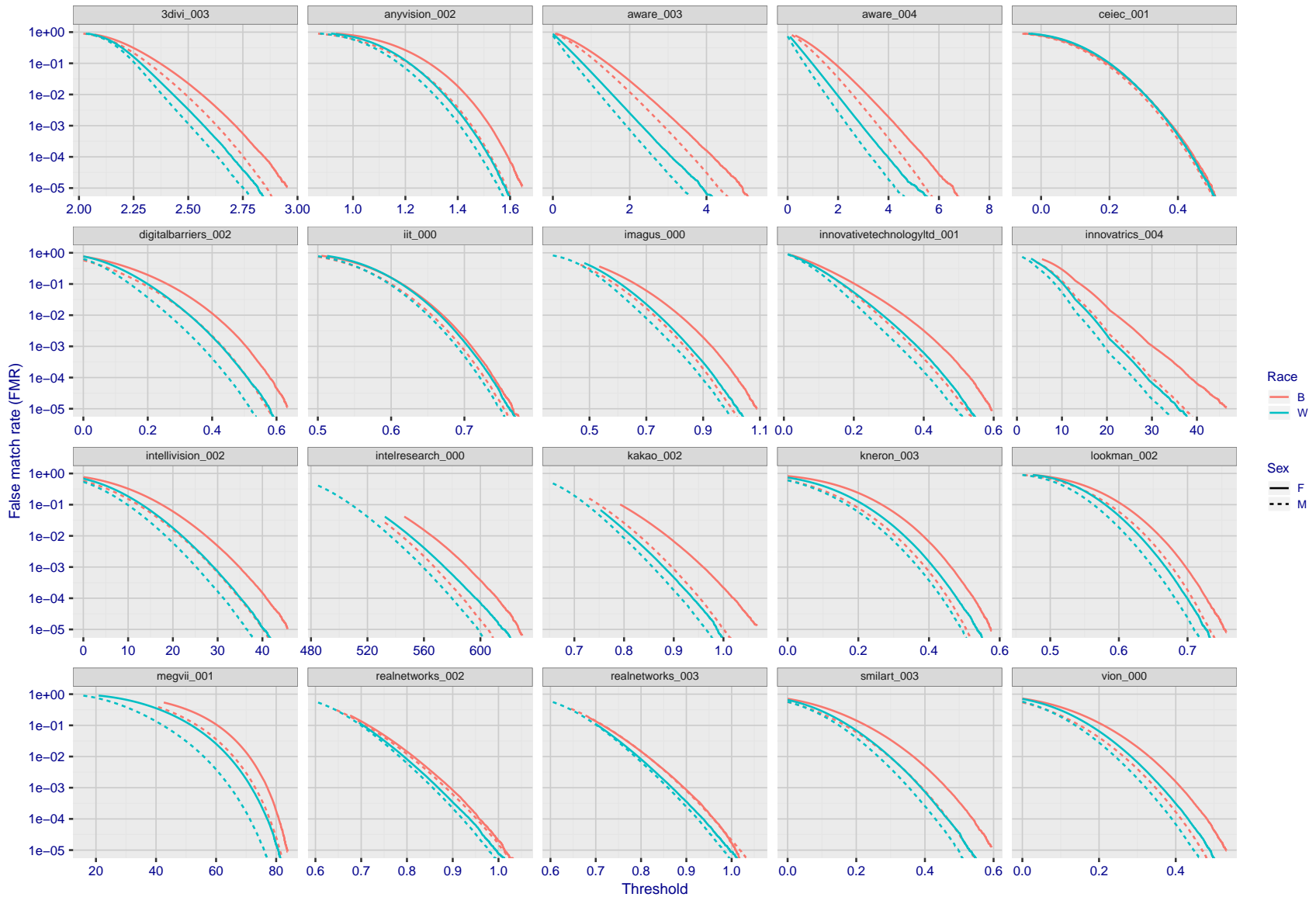
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 90: For the mugshot images, the false match calibration curves show false match rate vs. threshold. Separate curves appear for white females, black females, black males and white males.



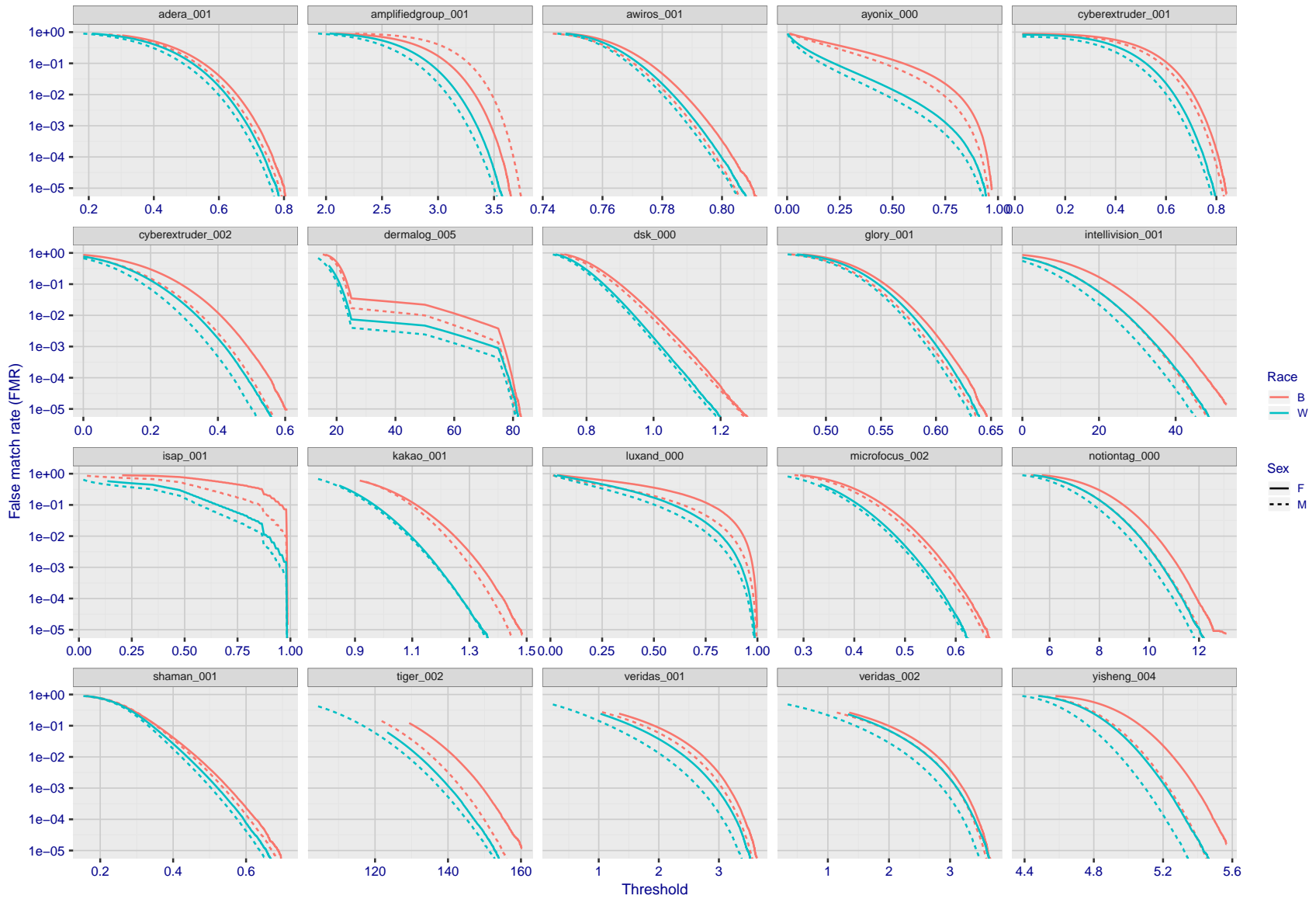
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 91: For the mugshot images, the false match calibration curves show false match rate vs. threshold. Separate curves appear for white females, black females, black males and white males.



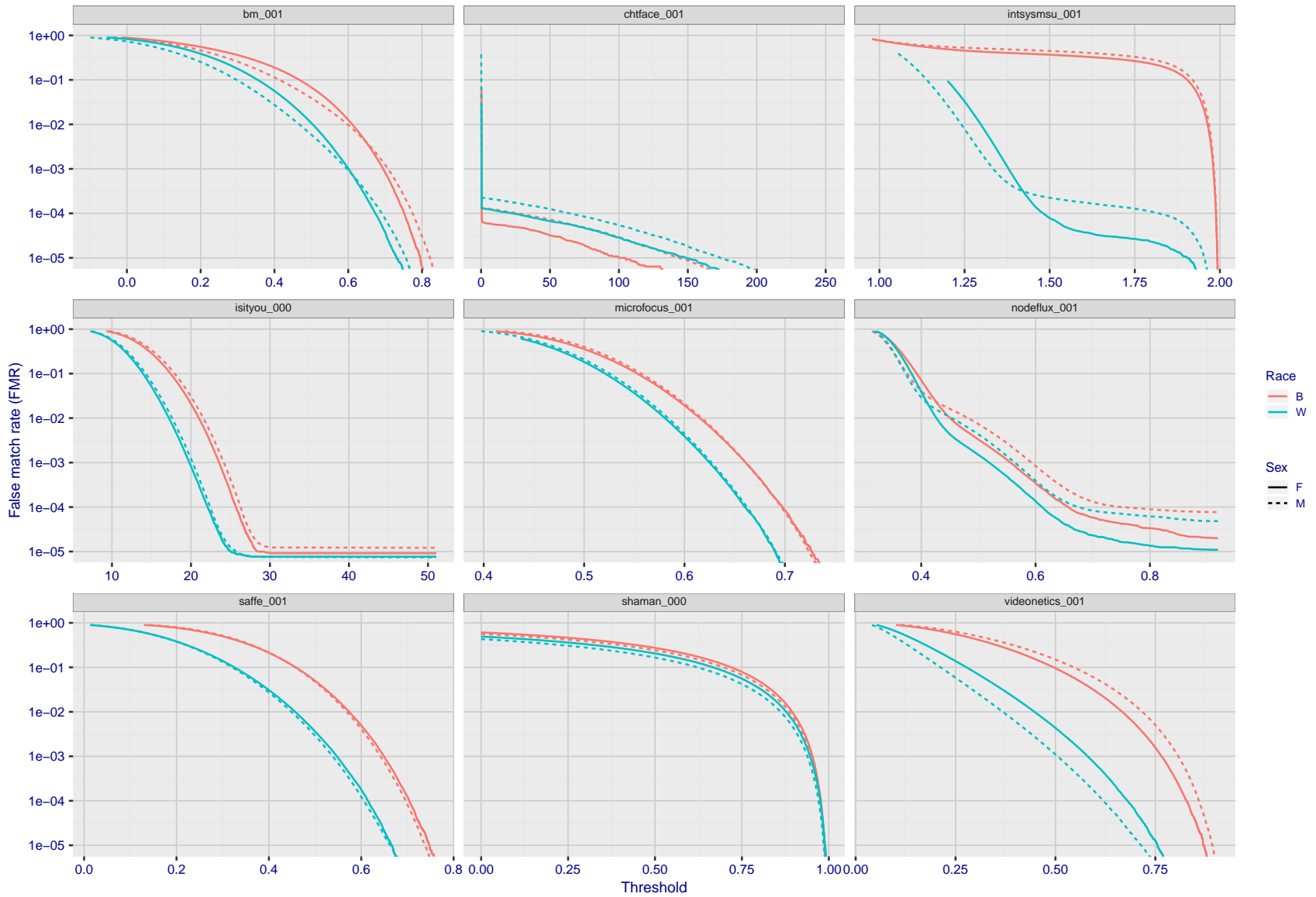
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 92: For the mugshot images, the false match calibration curves show false match rate vs. threshold. Separate curves appear for white females, black females, black males and white males.



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 93: For the mugshot images, the false match calibration curves show false match rate vs. threshold. Separate curves appear for white females, black females, black males and white males.



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 94: For the mugshot images, the false match calibration curves show false match rate vs. threshold. Separate curves appear for white females, black females, black males and white males.



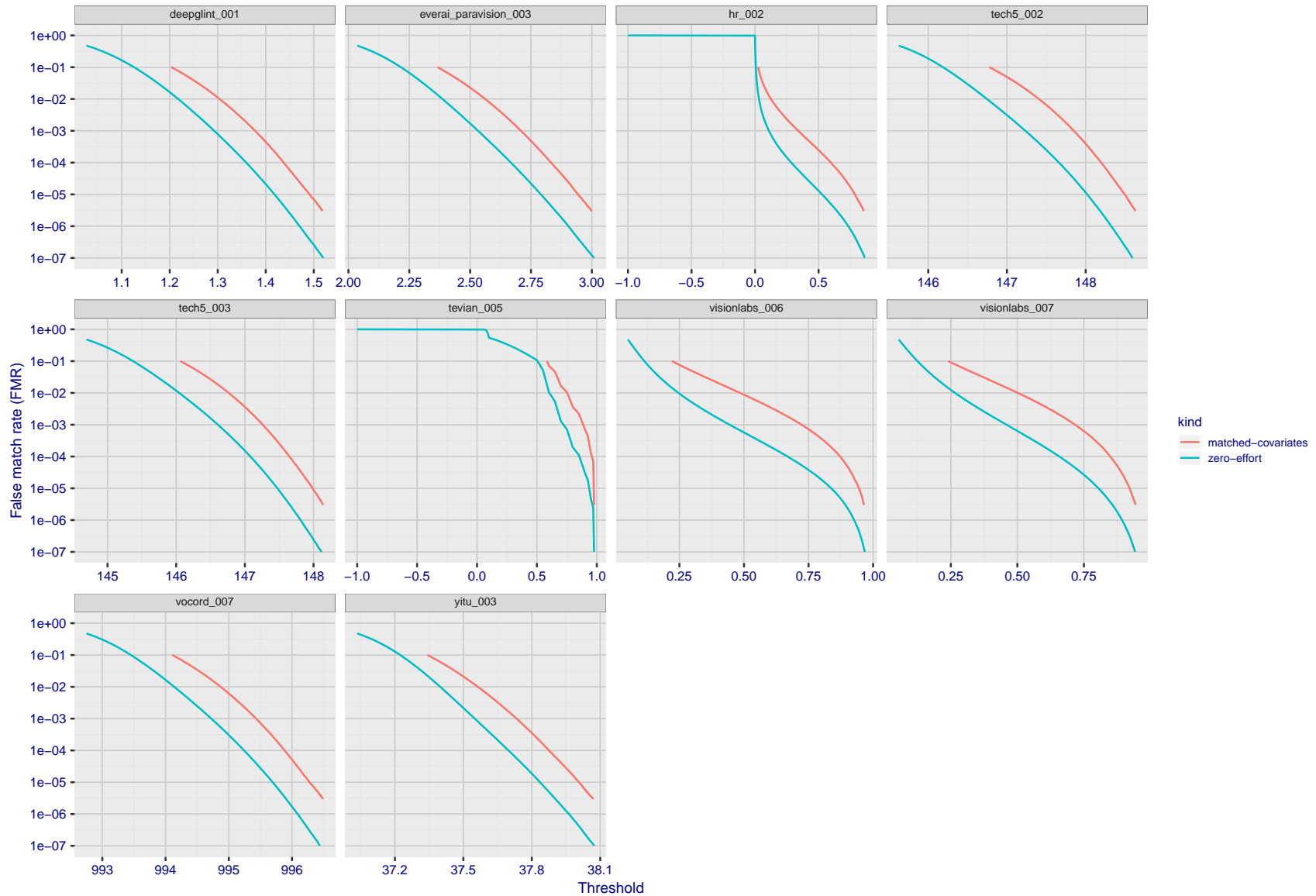
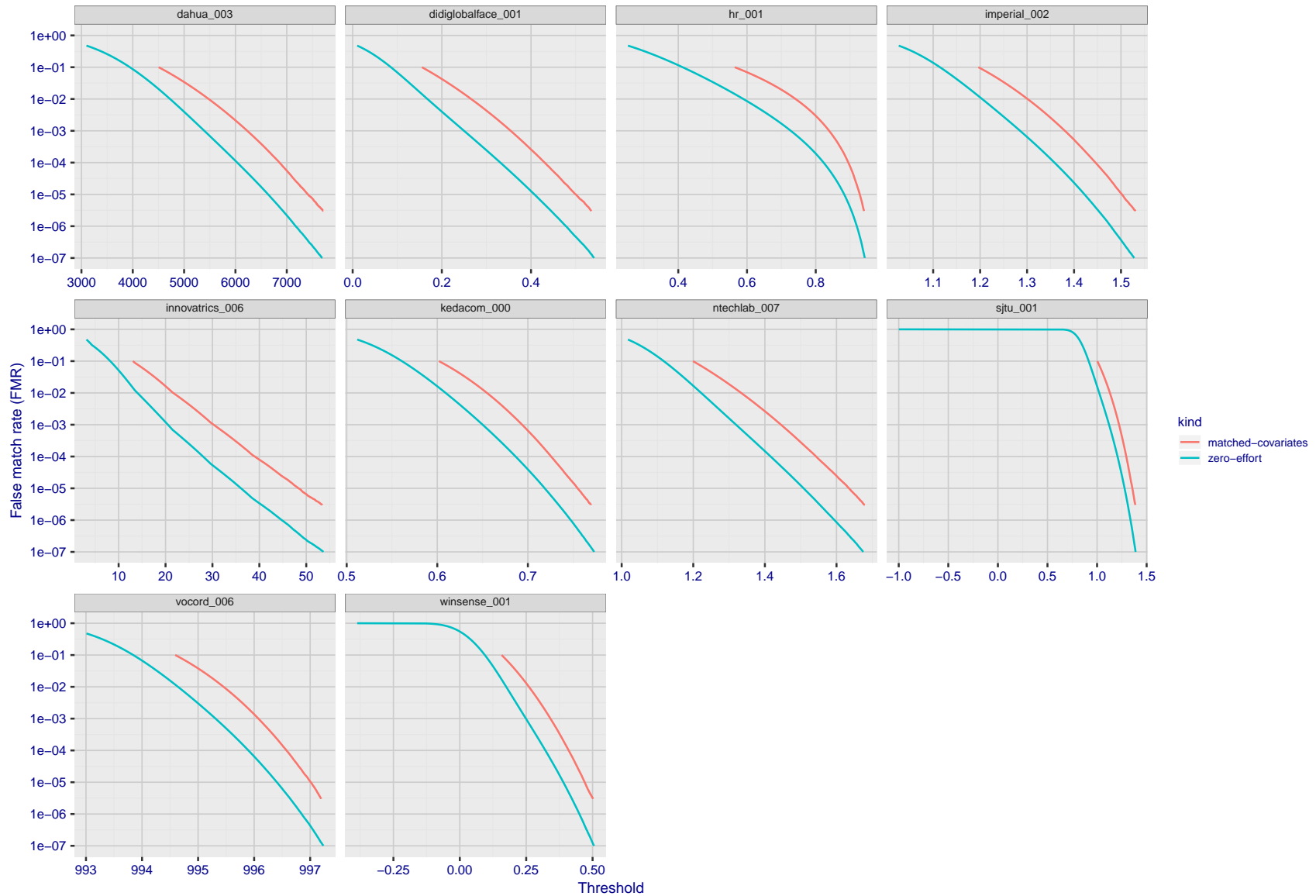
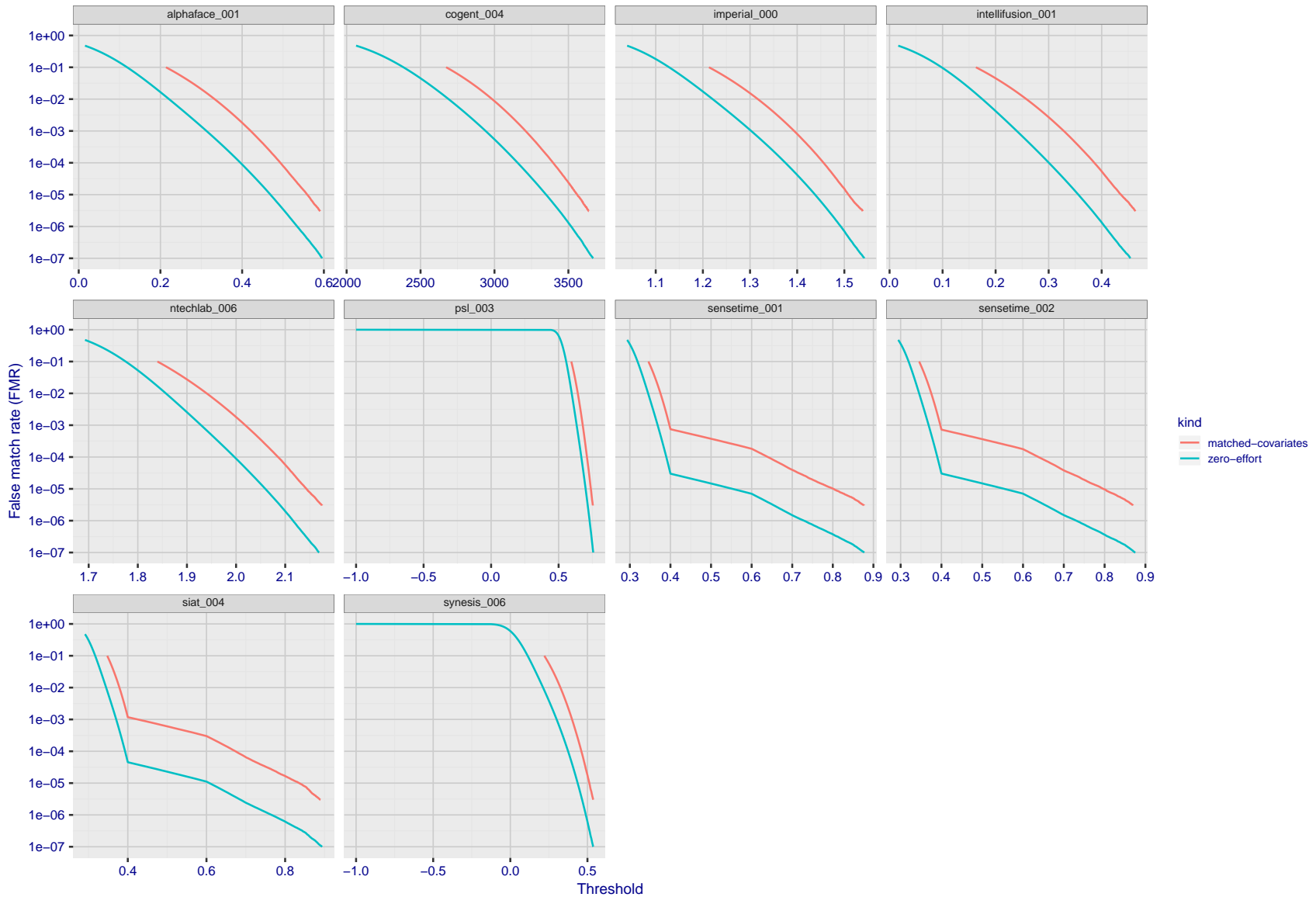


Figure 95: For the visa images, the false match calibration curves show FMR vs. threshold,  $T$ . The blue (lower) curves are for zero-effort impostors (i.e. comparing all images against all). The red (upper) curves are for persons of the same-sex, same-age, and same national-origin. This shows that FMR is underestimated (by a factor of 10 or more) by using a zero-effort impostor calculation to calibrate  $T$ . As shown later (sec. 3.6), FMR is higher for demographic-matched impostors.



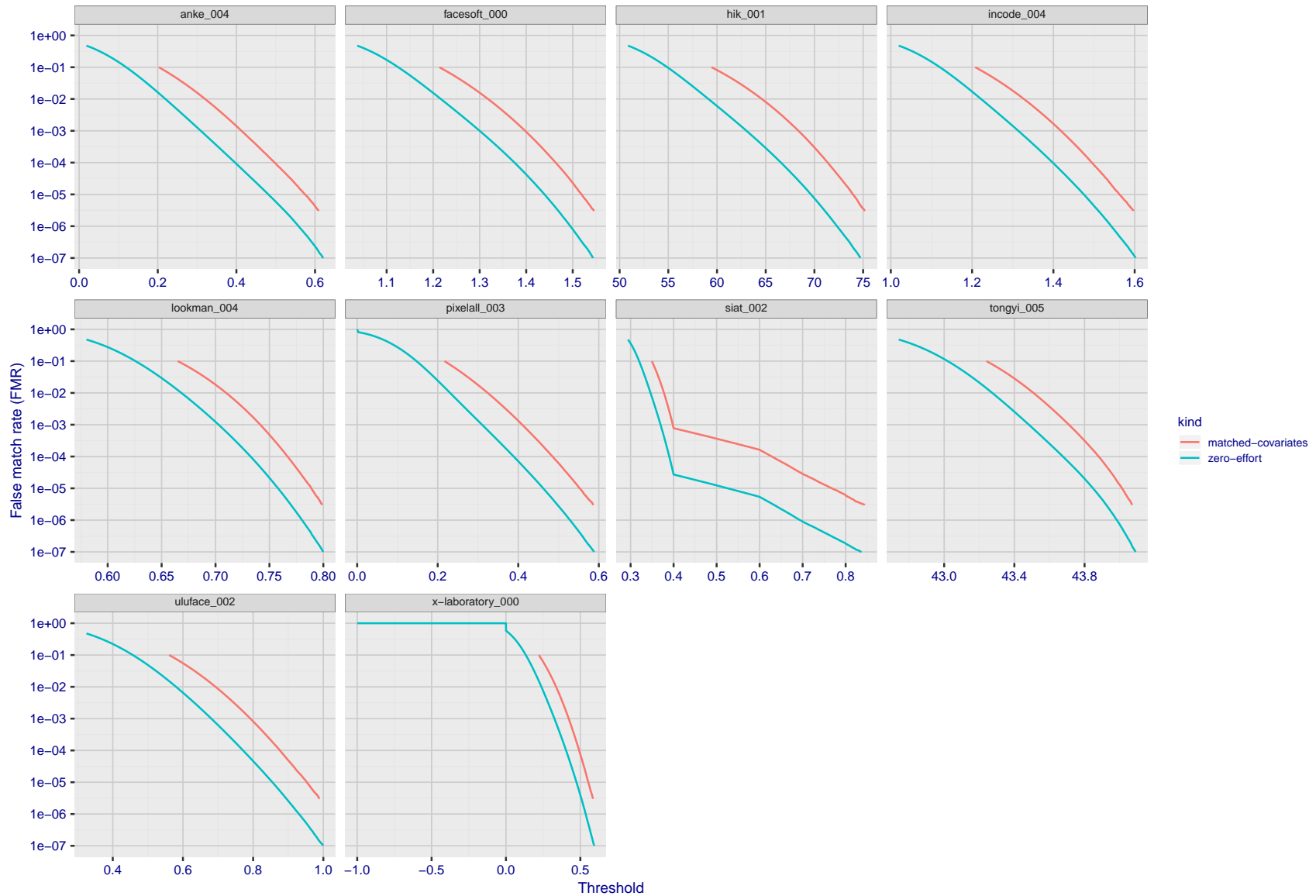
FNMR(T)  
 FMR(T)  
 "False non-match rate"  
 "False match rate"

Figure 96: For the visa images, the false match calibration curves show FMR vs. threshold,  $T$ . The blue (lower) curves are for zero-effort impostors (i.e. comparing all images against all). The red (upper) curves are for persons of the same-sex, same-age, and same national-origin. This shows that FMR is underestimated (by a factor of 10 or more) by using a zero-effort impostor calculation to calibrate  $T$ . As shown later (sec. 3.6), FMR is higher for demographic-matched impostors.



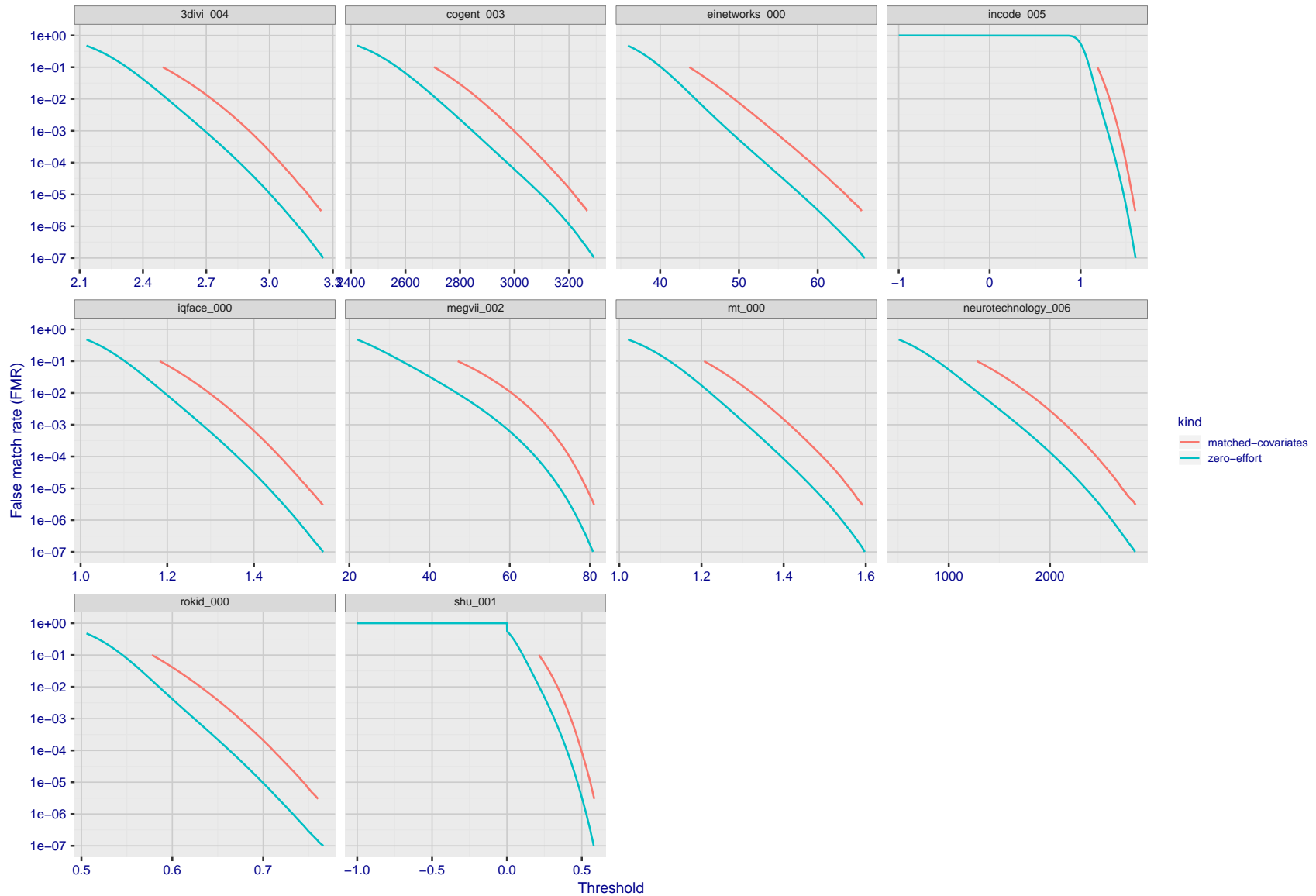
FNMR(T)  
 FMR(T)  
 "False non-match rate"  
 "False match rate"

Figure 97: For the visa images, the false match calibration curves show FMR vs. threshold,  $T$ . The blue (lower) curves are for zero-effort impostors (i.e. comparing all images against all). The red (upper) curves are for persons of the same-sex, same-age, and same national-origin. This shows that FMR is underestimated (by a factor of 10 or more) by using a zero-effort impostor calculation to calibrate  $T$ . As shown later (sec. 3.6), FMR is higher for demographic-matched impostors.



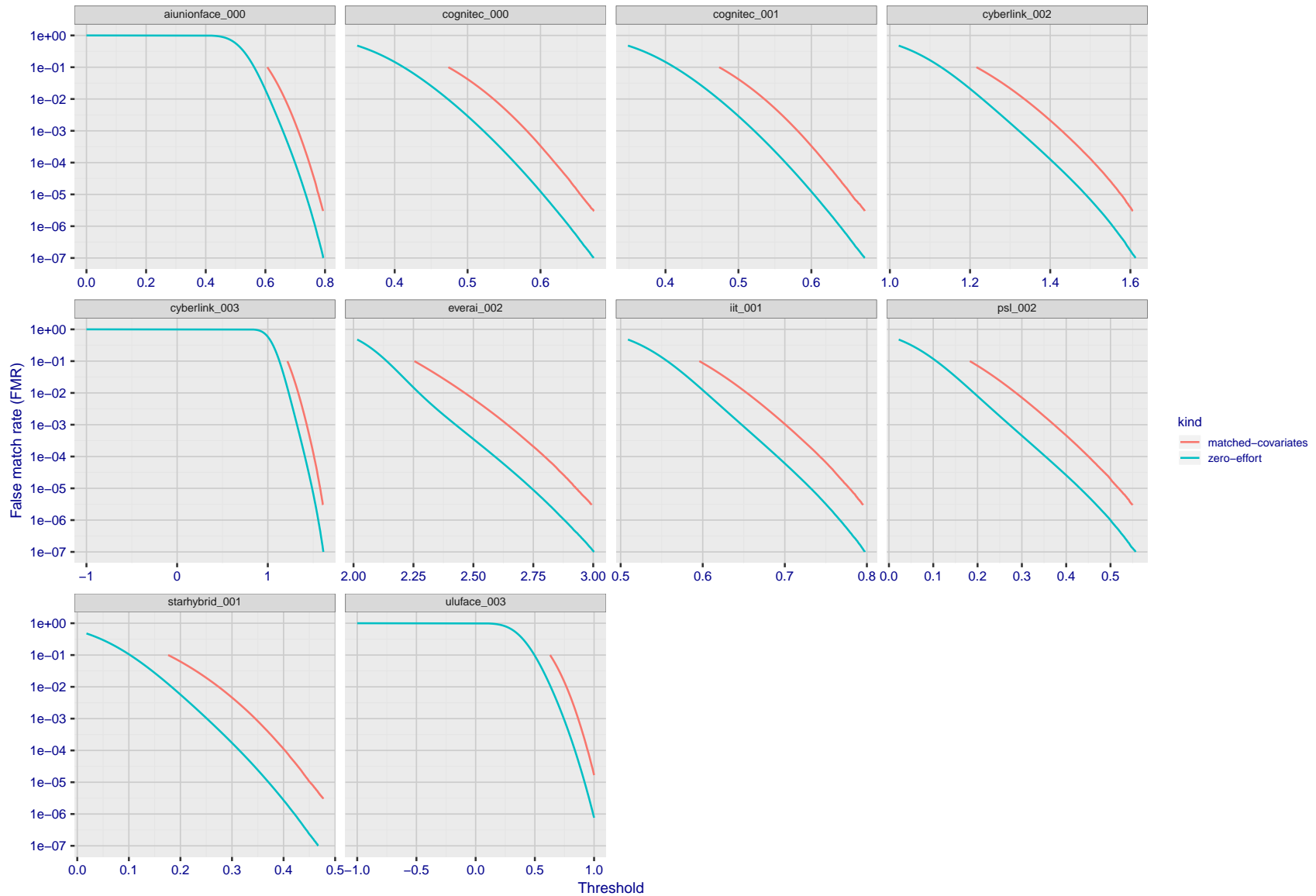
FNMR(T)  
 FMR(T)  
 "False non-match rate"  
 "False match rate"

Figure 98: For the visa images, the false match calibration curves show FMR vs. threshold,  $T$ . The blue (lower) curves are for zero-effort impostors (i.e. comparing all images against all). The red (upper) curves are for persons of the same-sex, same-age, and same national-origin. This shows that FMR is underestimated (by a factor of 10 or more) by using a zero-effort impostor calculation to calibrate  $T$ . As shown later (sec. 3.6), FMR is higher for demographic-matched impostors.



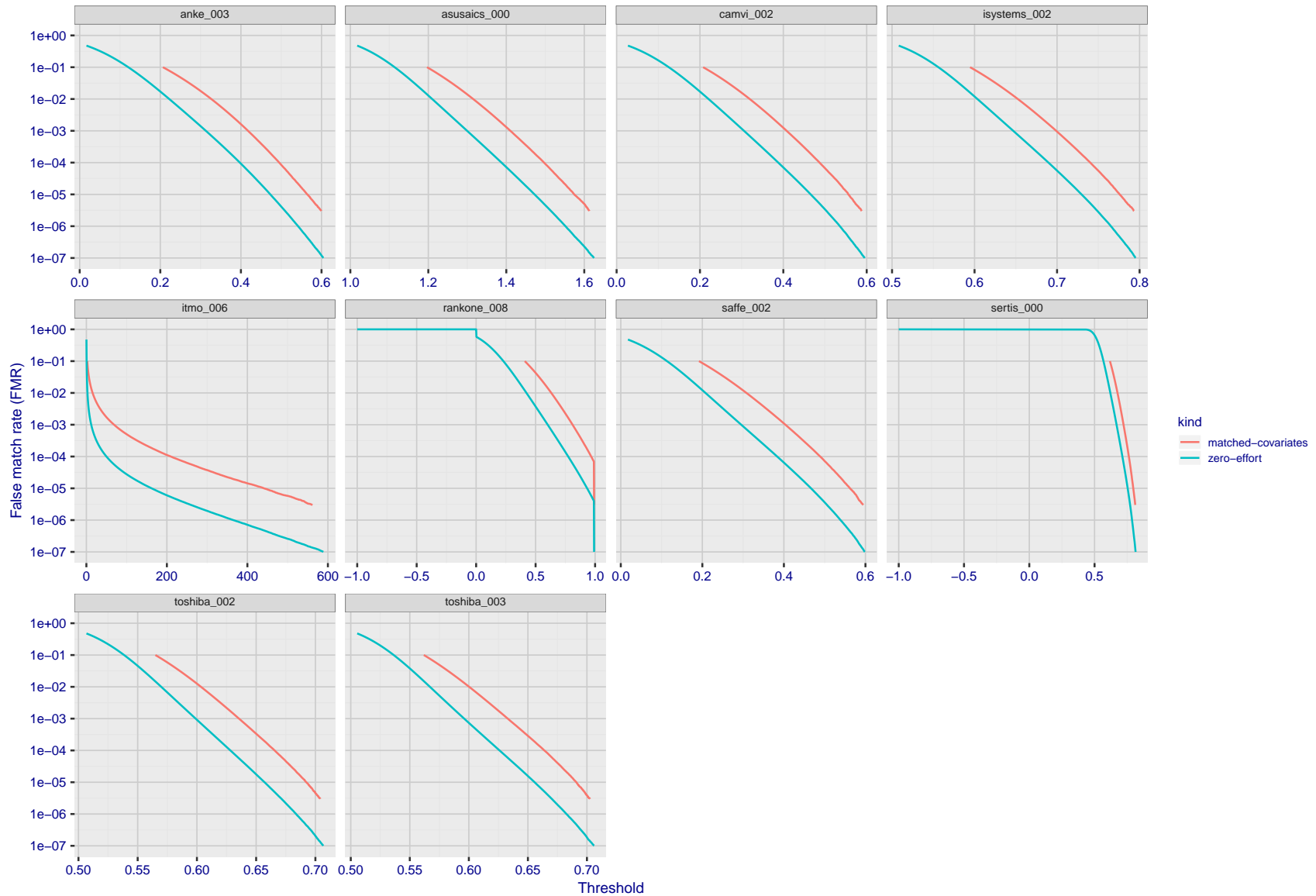
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 99: For the visa images, the false match calibration curves show FMR vs. threshold,  $T$ . The blue (lower) curves are for zero-effort impostors (i.e. comparing all images against all). The red (upper) curves are for persons of the same-sex, same-age, and same national-origin. This shows that FMR is underestimated (by a factor of 10 or more) by using a zero-effort impostor calculation to calibrate  $T$ . As shown later (sec. 3.6), FMR is higher for demographic-matched impostors.



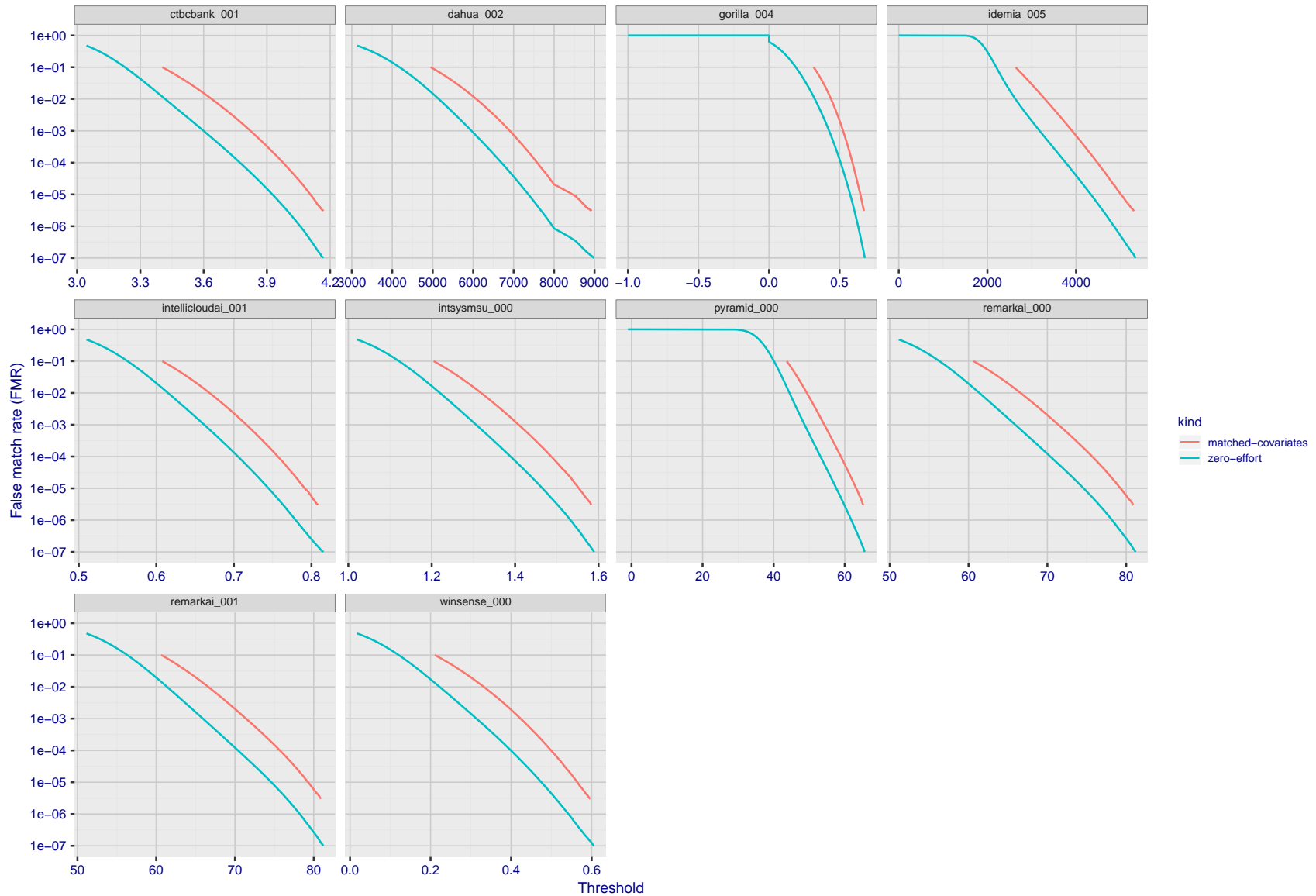
FNMR(T)  
 FMR(T)  
 "False non-match rate"  
 "False match rate"

Figure 100: For the visa images, the false match calibration curves show FMR vs. threshold,  $T$ . The blue (lower) curves are for zero-effort impostors (i.e. comparing all images against all). The red (upper) curves are for persons of the same-sex, same-age, and same national-origin. This shows that FMR is underestimated (by a factor of 10 or more) by using a zero-effort impostor calculation to calibrate  $T$ . As shown later (sec. 3.6), FMR is higher for demographic-matched impostors.



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

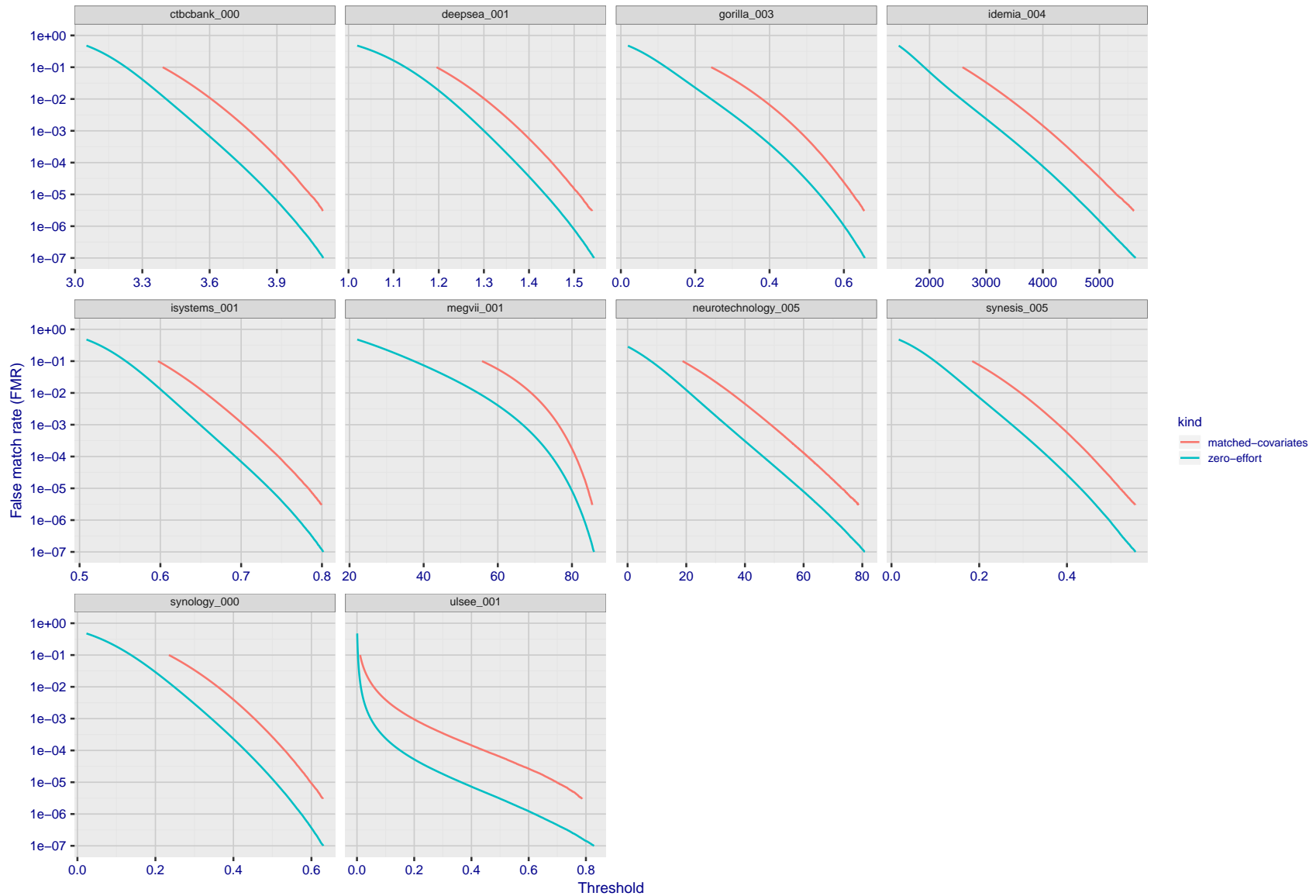
Figure 101: For the visa images, the false match calibration curves show FMR vs. threshold,  $T$ . The blue (lower) curves are for zero-effort impostors (i.e. comparing all images against all). The red (upper) curves are for persons of the same-sex, same-age, and same national-origin. This shows that FMR is underestimated (by a factor of 10 or more) by using a zero-effort impostor calculation to calibrate  $T$ . As shown later (sec. 3.6), FMR is higher for demographic-matched impostors.



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

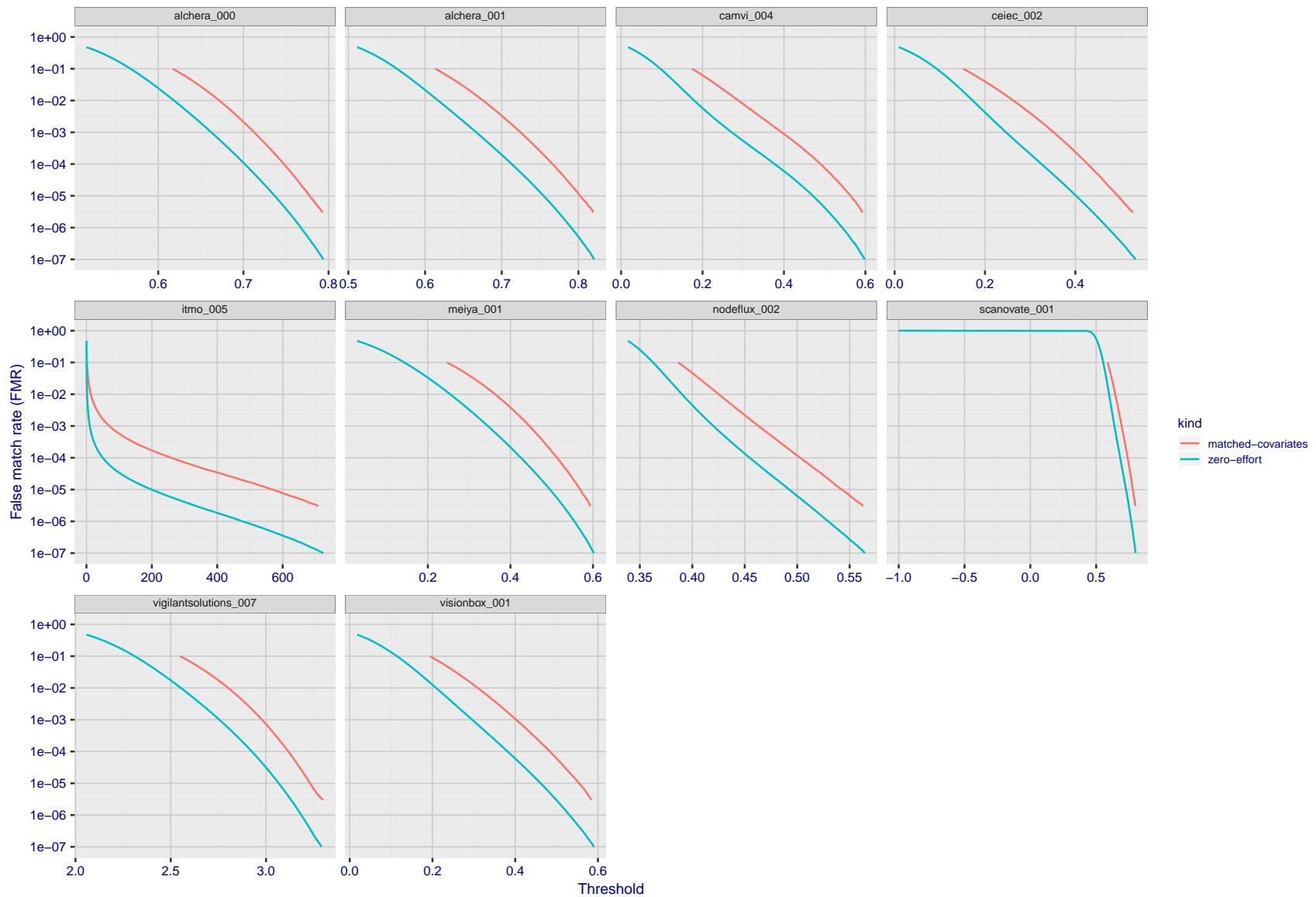
Figure 102: For the visa images, the false match calibration curves show FMR vs. threshold,  $T$ . The blue (lower) curves are for zero-effort impostors (i.e. comparing all images against all). The red (upper) curves are for persons of the same-sex, same-age, and same national-origin. This shows that FMR is underestimated (by a factor of 10 or more) by using a zero-effort impostor calculation to calibrate  $T$ . As shown later (sec. 3.6), FMR is higher for demographic-matched impostors.





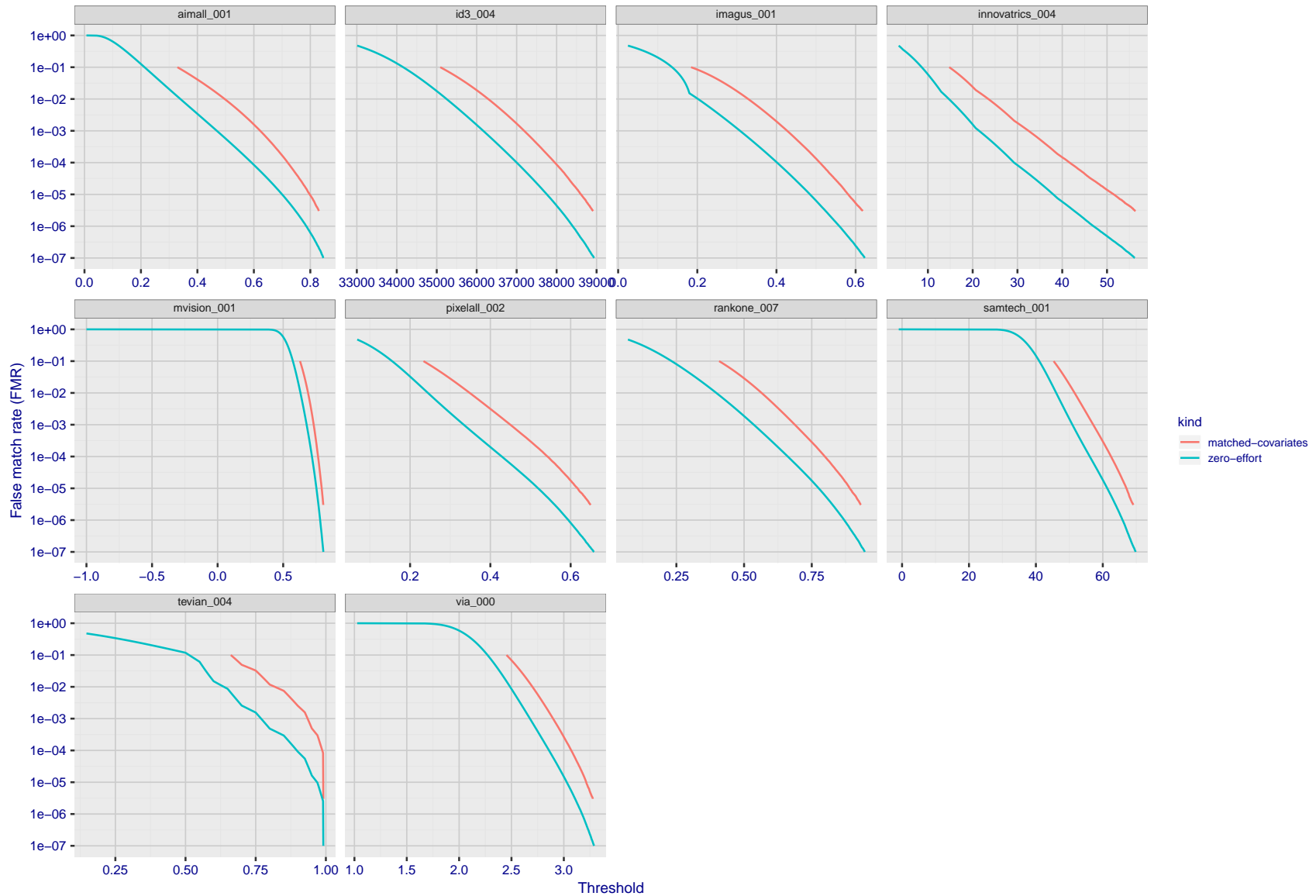
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 103: For the visa images, the false match calibration curves show FMR vs. threshold,  $T$ . The blue (lower) curves are for zero-effort impostors (i.e. comparing all images against all). The red (upper) curves are for persons of the same-sex, same-age, and same national-origin. This shows that FMR is underestimated (by a factor of 10 or more) by using a zero-effort impostor calculation to calibrate  $T$ . As shown later (sec. 3.6), FMR is higher for demographic-matched impostors.



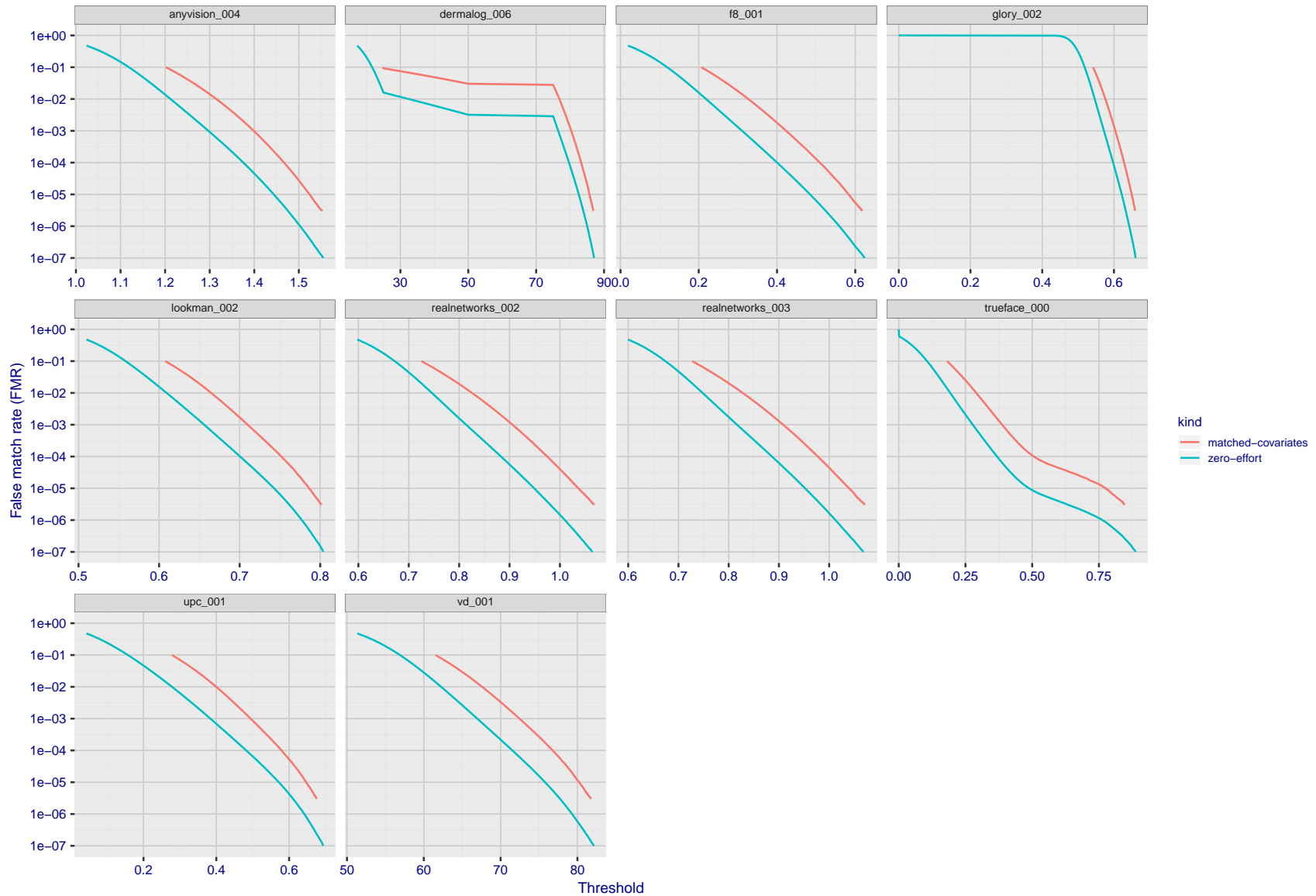
FNMR(T)  
 FMR(T)  
 "False non-match rate"  
 "False match rate"

Figure 104: For the visa images, the false match calibration curves show FMR vs. threshold,  $T$ . The blue (lower) curves are for zero-effort impostors (i.e. comparing all images against all). The red (upper) curves are for persons of the same-sex, same-age, and same national-origin. This shows that FMR is underestimated (by a factor of 10 or more) by using a zero-effort impostor calculation to calibrate  $T$ . As shown later (sec. 3.6), FMR is higher for demographic-matched impostors.



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 105: For the visa images, the false match calibration curves show FMR vs. threshold,  $T$ . The blue (lower) curves are for zero-effort impostors (i.e. comparing all images against all). The red (upper) curves are for persons of the same-sex, same-age, and same national-origin. This shows that FMR is underestimated (by a factor of 10 or more) by using a zero-effort impostor calculation to calibrate  $T$ . As shown later (sec. 3.6), FMR is higher for demographic-matched impostors.



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 106: For the visa images, the false match calibration curves show FMR vs. threshold,  $T$ . The blue (lower) curves are for zero-effort impostors (i.e. comparing all images against all). The red (upper) curves are for persons of the same-sex, same-age, and same national-origin. This shows that FMR is underestimated (by a factor of 10 or more) by using a zero-effort impostor calculation to calibrate  $T$ . As shown later (sec. 3.6), FMR is higher for demographic-matched impostors.

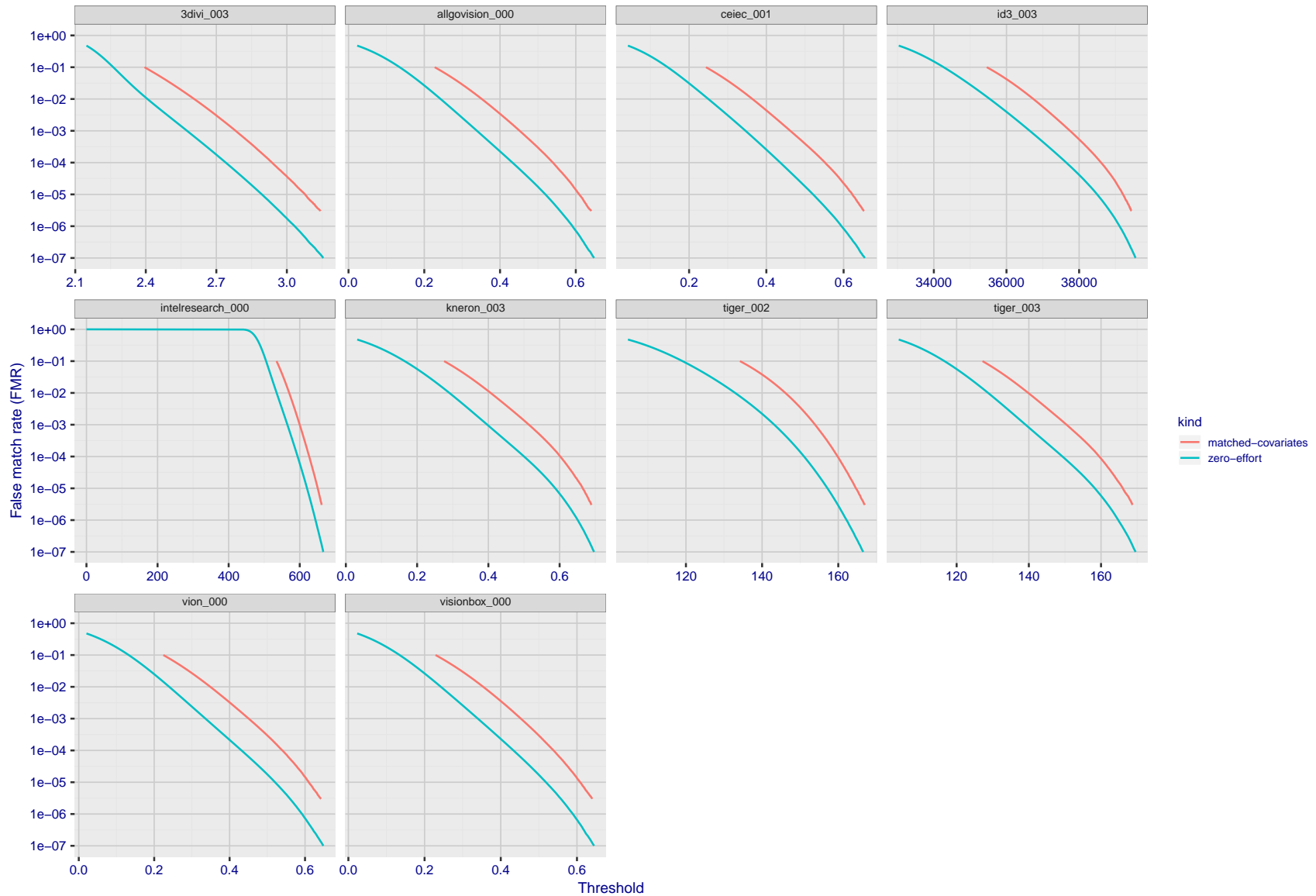
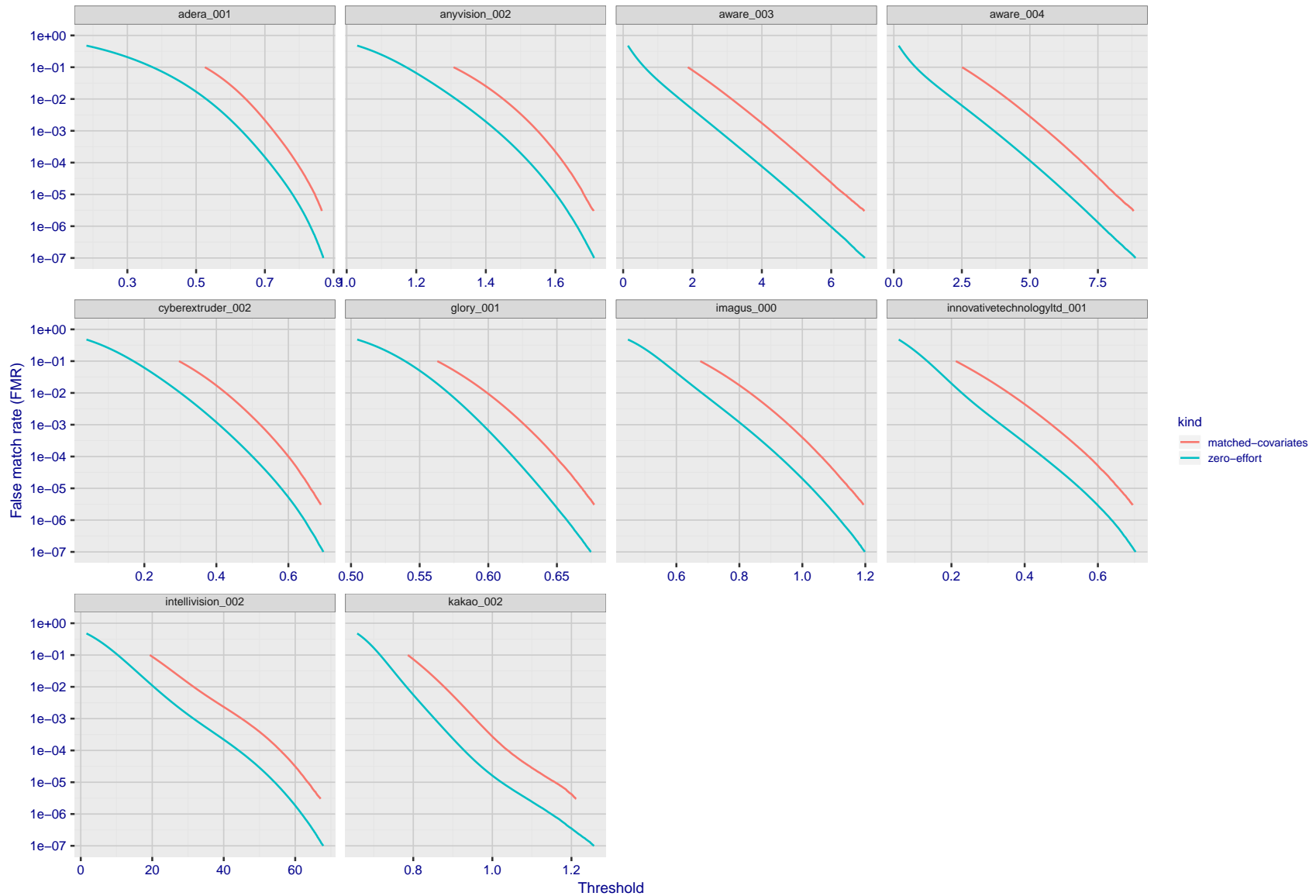
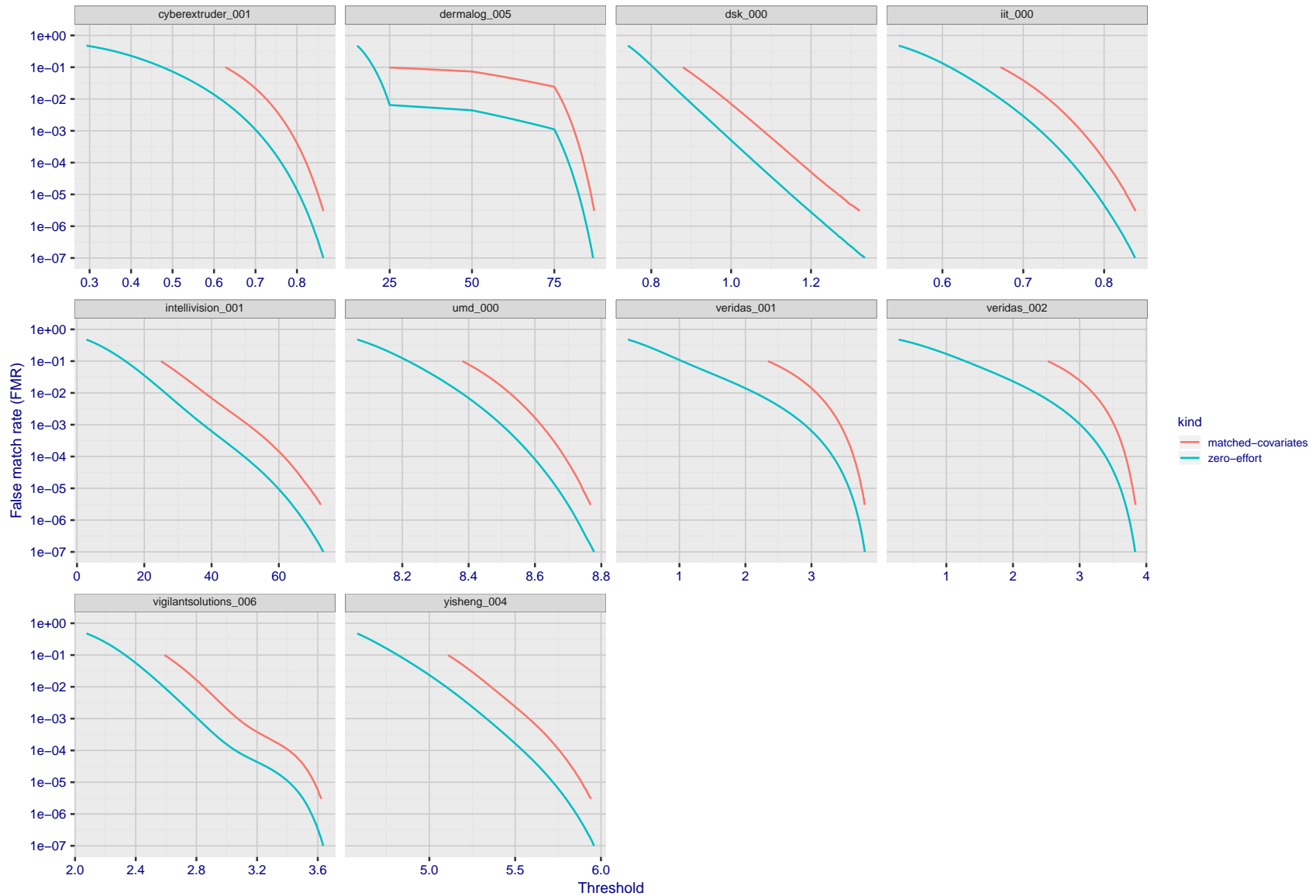


Figure 107: For the visa images, the false match calibration curves show FMR vs. threshold,  $T$ . The blue (lower) curves are for zero-effort impostors (i.e. comparing all images against all). The red (upper) curves are for persons of the same-sex, same-age, and same national-origin. This shows that FMR is underestimated (by a factor of 10 or more) by using a zero-effort impostor calculation to calibrate  $T$ . As shown later (sec. 3.6), FMR is higher for demographic-matched impostors.



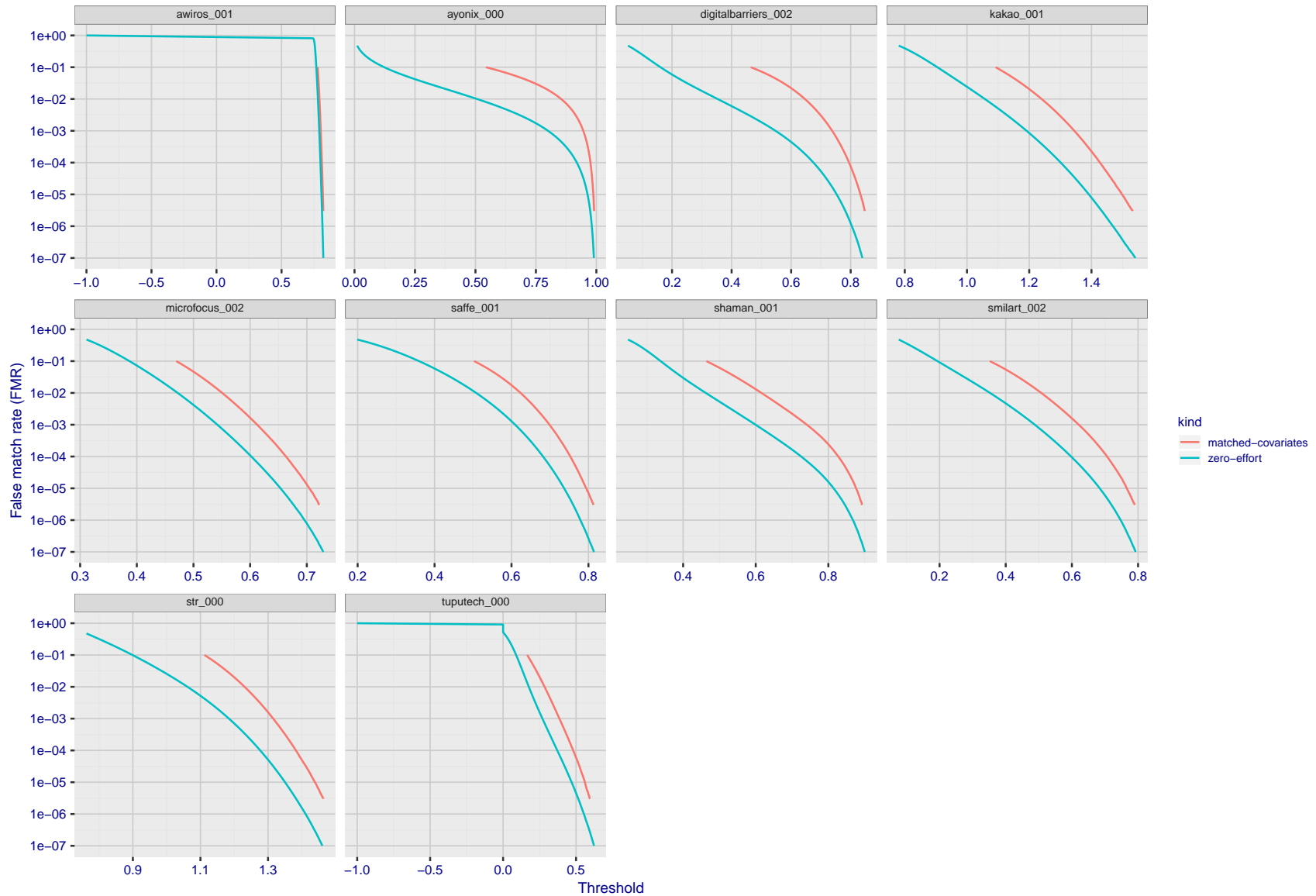
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 108: For the visa images, the false match calibration curves show FMR vs. threshold,  $T$ . The blue (lower) curves are for zero-effort impostors (i.e. comparing all images against all). The red (upper) curves are for persons of the same-sex, same-age, and same national-origin. This shows that FMR is underestimated (by a factor of 10 or more) by using a zero-effort impostor calculation to calibrate  $T$ . As shown later (sec. 3.6), FMR is higher for demographic-matched impostors.



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

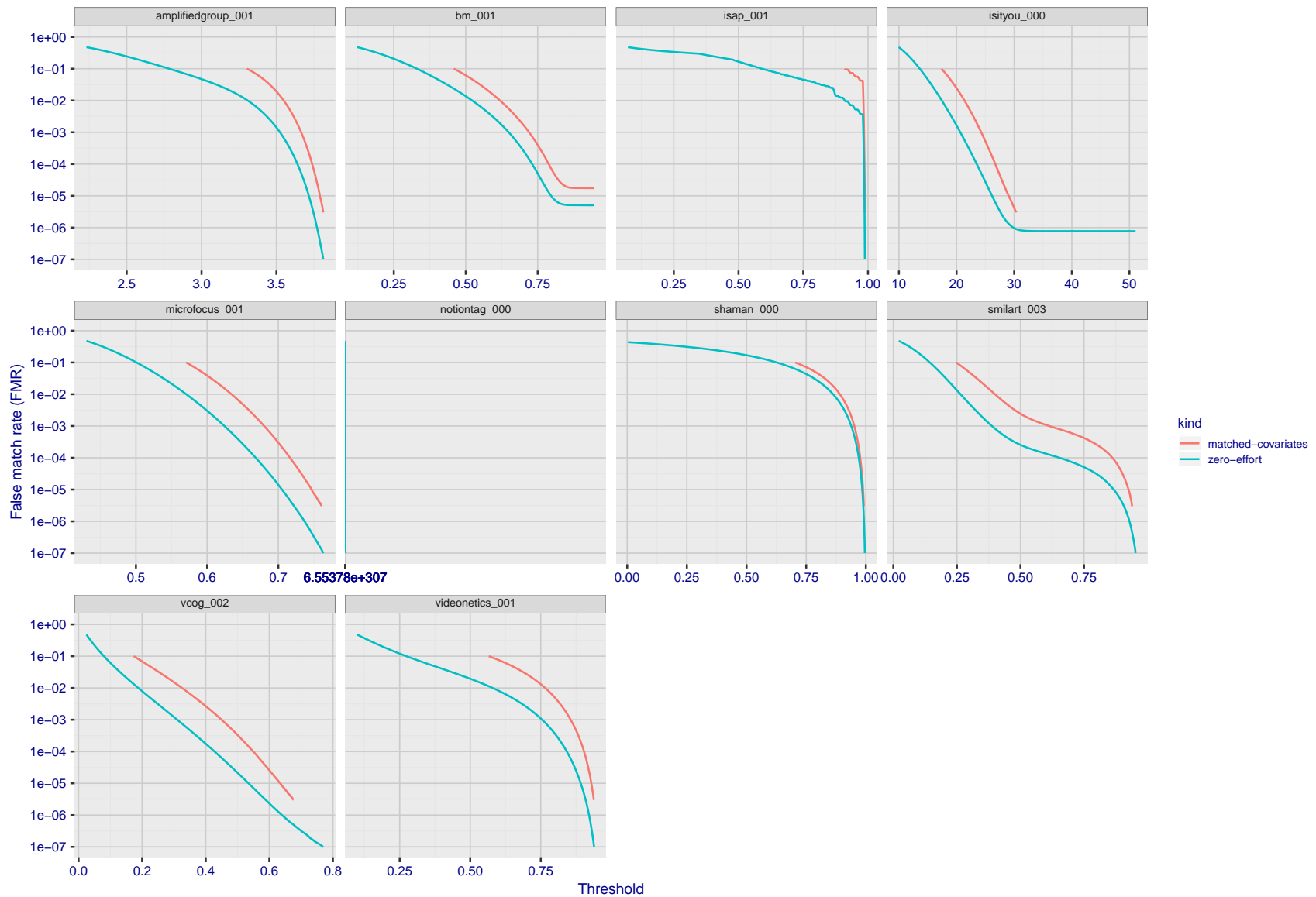
Figure 109: For the visa images, the false match calibration curves show FMR vs. threshold,  $T$ . The blue (lower) curves are for zero-effort impostors (i.e. comparing all images against all). The red (upper) curves are for persons of the same-sex, same-age, and same national-origin. This shows that FMR is underestimated (by a factor of 10 or more) by using a zero-effort impostor calculation to calibrate  $T$ . As shown later (sec. 3.6), FMR is higher for demographic-matched impostors.



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 110: For the visa images, the false match calibration curves show FMR vs. threshold,  $T$ . The blue (lower) curves are for zero-effort impostors (i.e. comparing all images against all). The red (upper) curves are for persons of the same-sex, same-age, and same national-origin. This shows that FMR is underestimated (by a factor of 10 or more) by using a zero-effort impostor calculation to calibrate  $T$ . As shown later (sec. 3.6), FMR is higher for demographic-matched impostors.





FNMR(T)  
 FMR(T)  
 "False non-match rate"  
 "False match rate"

Figure 111: For the visa images, the false match calibration curves show FMR vs. threshold,  $T$ . The blue (lower) curves are for zero-effort impostors (i.e. comparing all images against all). The red (upper) curves are for persons of the same-sex, same-age, and same national-origin. This shows that FMR is underestimated (by a factor of 10 or more) by using a zero-effort impostor calculation to calibrate  $T$ . As shown later (sec. 3.6), FMR is higher for demographic-matched impostors.

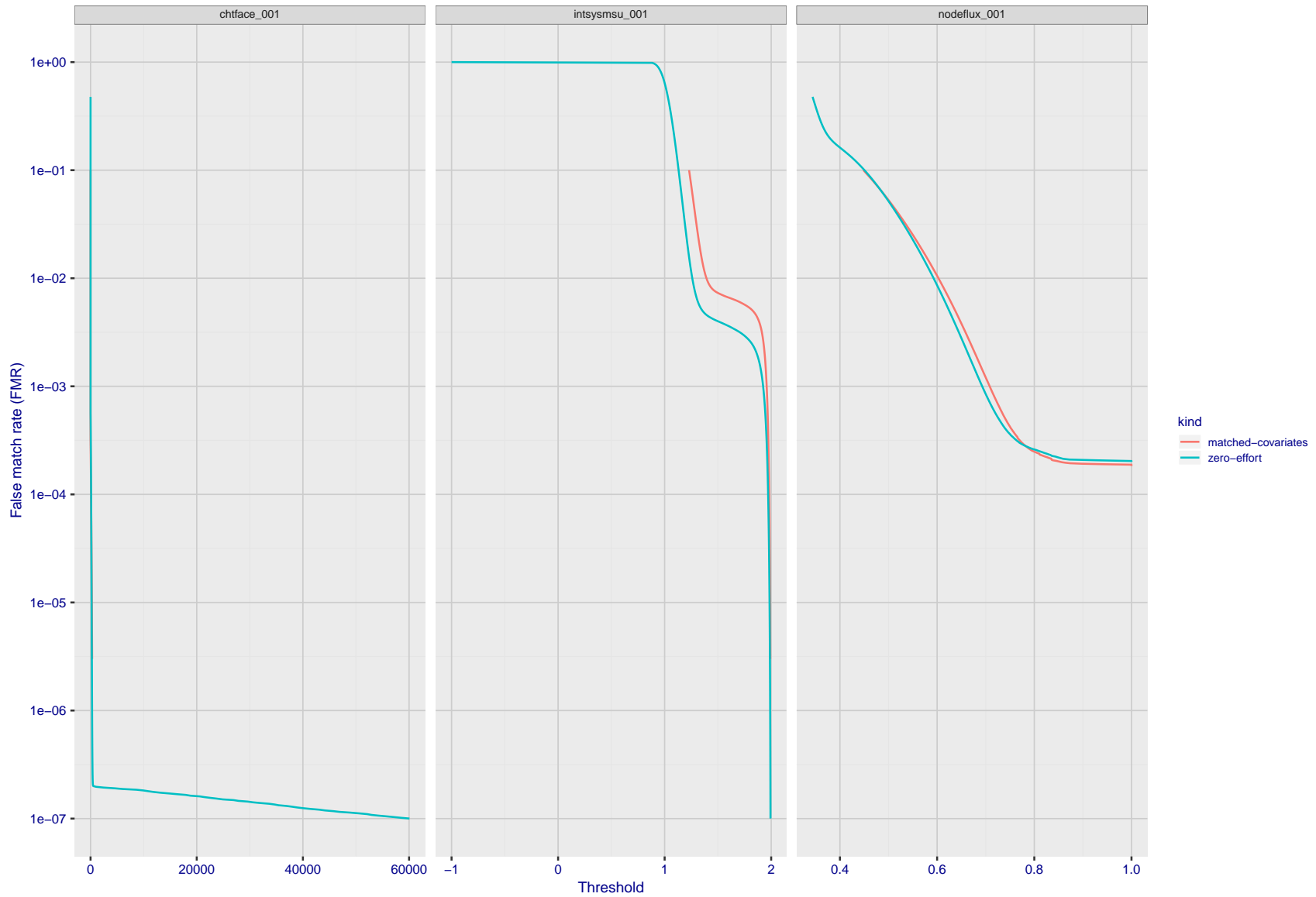
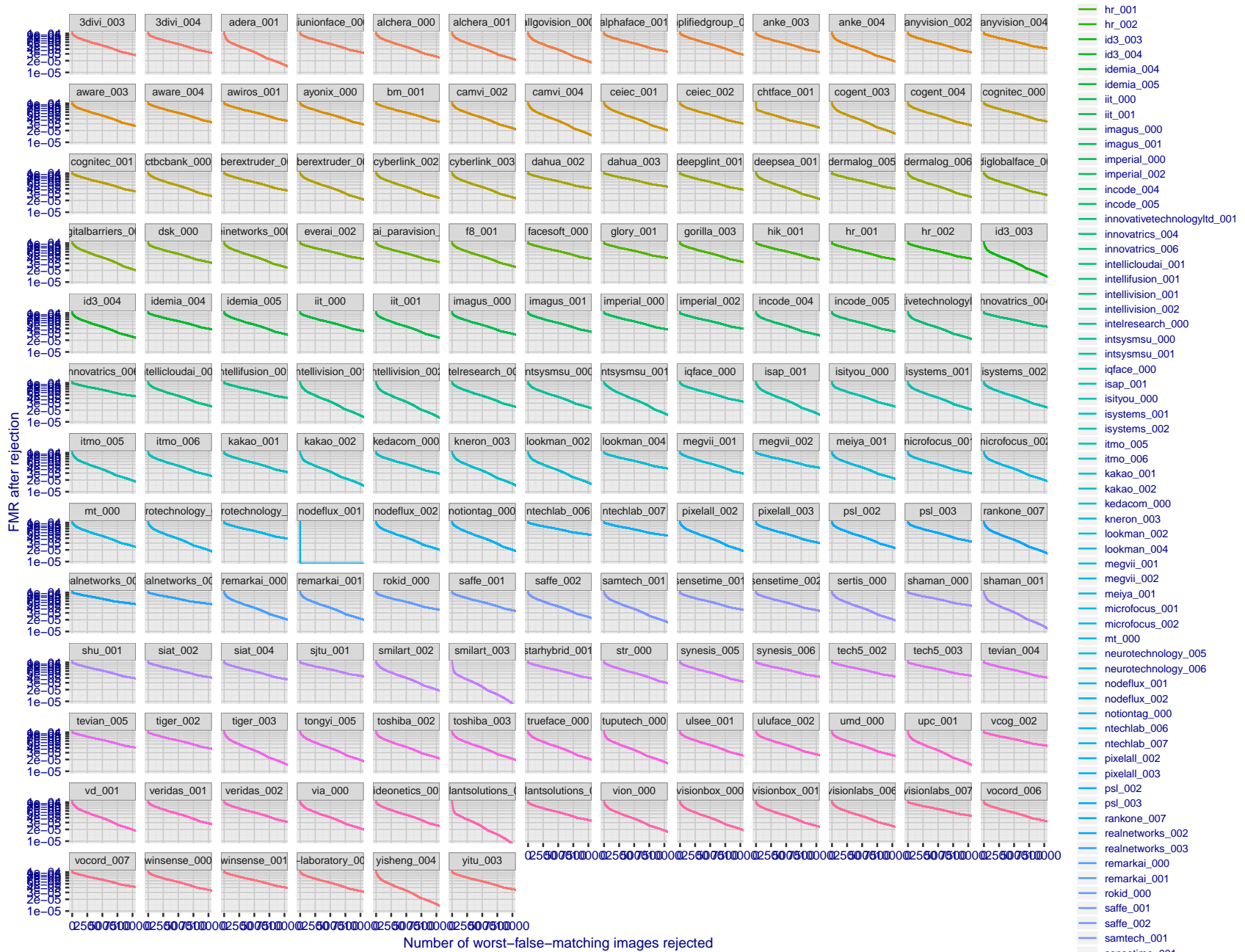


Figure 112: For the visa images, the false match calibration curves show FMR vs. threshold,  $T$ . The blue (lower) curves are for zero-effort impostors (i.e. comparing all images against all). The red (upper) curves are for persons of the same-sex, same-age, and same national-origin. This shows that FMR is underestimated (by a factor of 10 or more) by using a zero-effort impostor calculation to calibrate  $T$ . As shown later (sec. 3.6), FMR is higher for demographic-matched impostors.



FNMR(T) "False non-match rate"  
 FMR(T) "False match rate"

Figure 113: For the visa images, the curves show how false matches are concentrated in certain images. Specifically each line plots  $FMR(k)$  with  $k$  the number of images rejected in decreasing order of how many false matches that image was involved in.  $FMR(0) = 10^{-4}$ . In terms of the biometric zoo, the most "wolf-ish" images are rejected first i.e. those enrollment or verification images most often involved in false matches. A flatter response is considered superior. A steeply descending response indicates that certain kinds of images false match against others, e.g. if hypothetically images of men with particular mustaches would falsely match others.

## 3.5 Genuine distribution stability

### 3.5.1 Effect of birth place on the genuine distribution

**Background:** Both skin tone and bone structure vary geographically. Prior studies have reported variations in FNMR and FMR.

**Goal:** To measure false non-match rate (FNMR) variation with country of birth.

**Methods:** Thresholds are determined that give  $FMR = \{0.001, 0.0001\}$  over the entire impostor set. Then FNMR is measured over 1000 bootstrap replications of the genuine scores. Only those countries with at least 140 individuals are included in the analysis.

**Results:** Figure 127 shows FNMR by country of birth for the two thresholds.

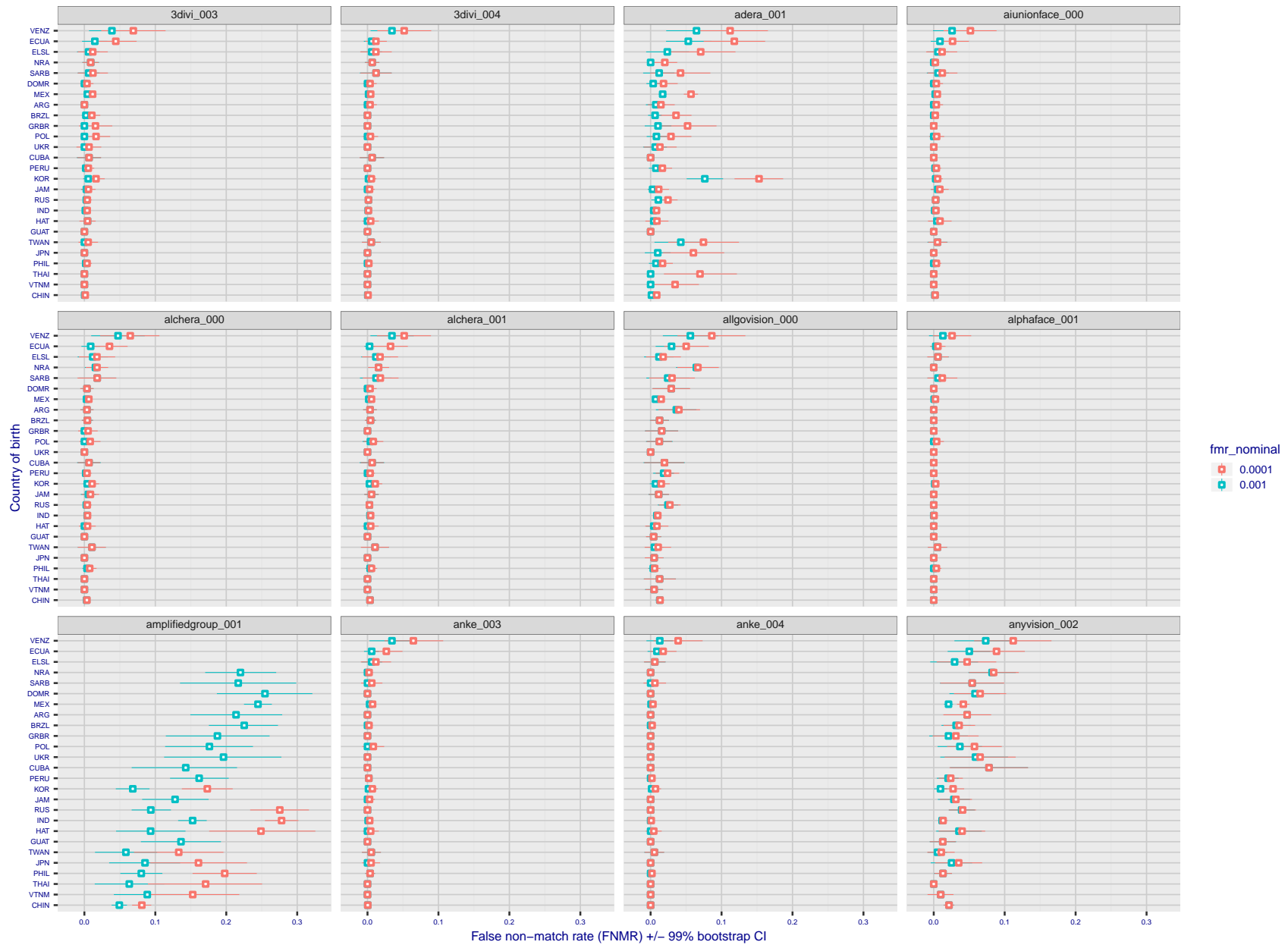


Figure 114: For the visa images, the dots show FNMR by country of birth for two globally set operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.1. The figures shows an order of magnitude variation in FNMR across country of birth; these effects are likely due quality variations, then demographics like age and race. The error rates in some cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.

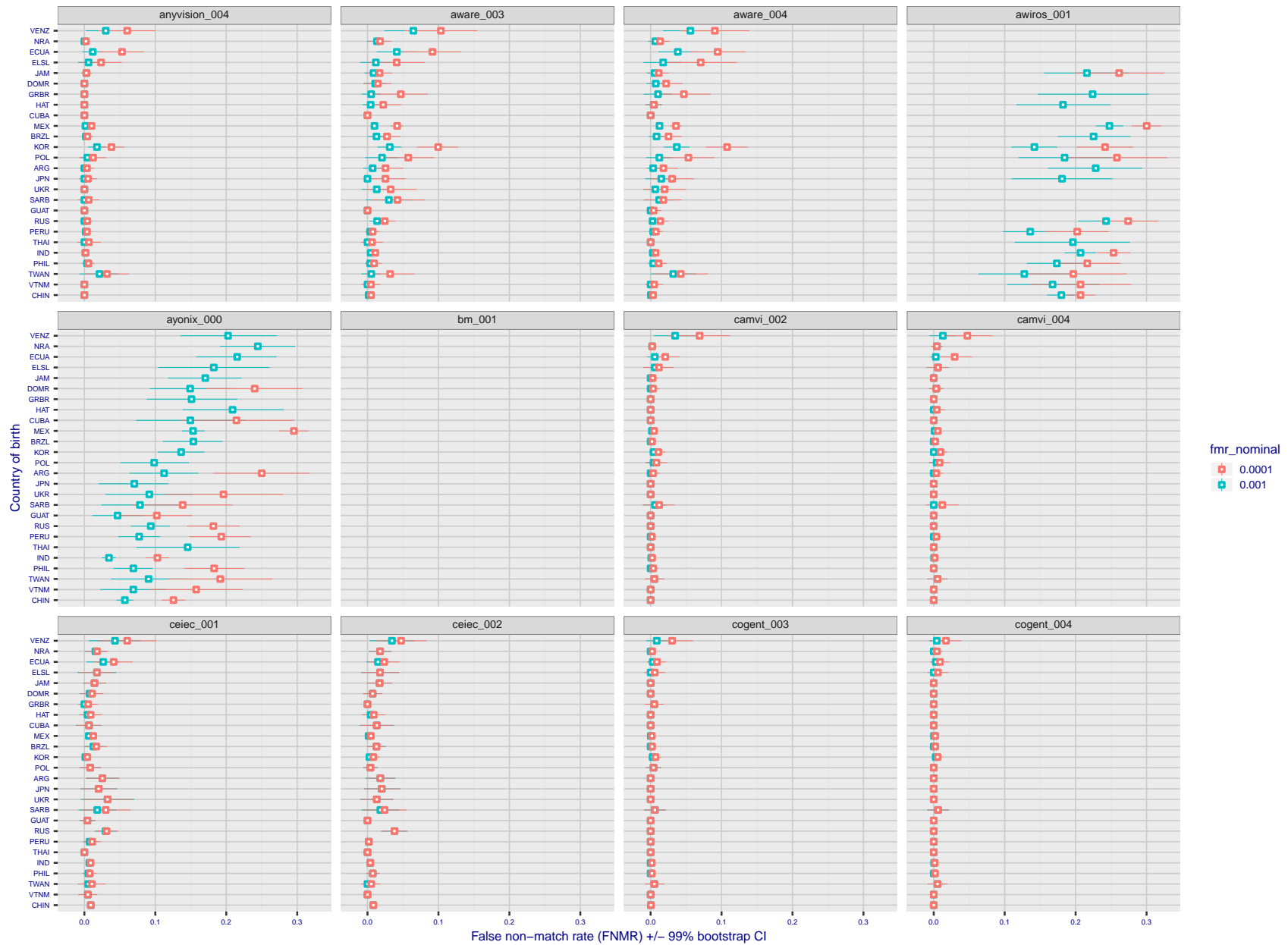


Figure 115: For the visa images, the dots show FNMR by country of birth for two globally set operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.1. The figures shows an order of magnitude variation in FNMR across country of birth; these effects are likely due quality variations, then demographics like age and race. The error rates in some cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.

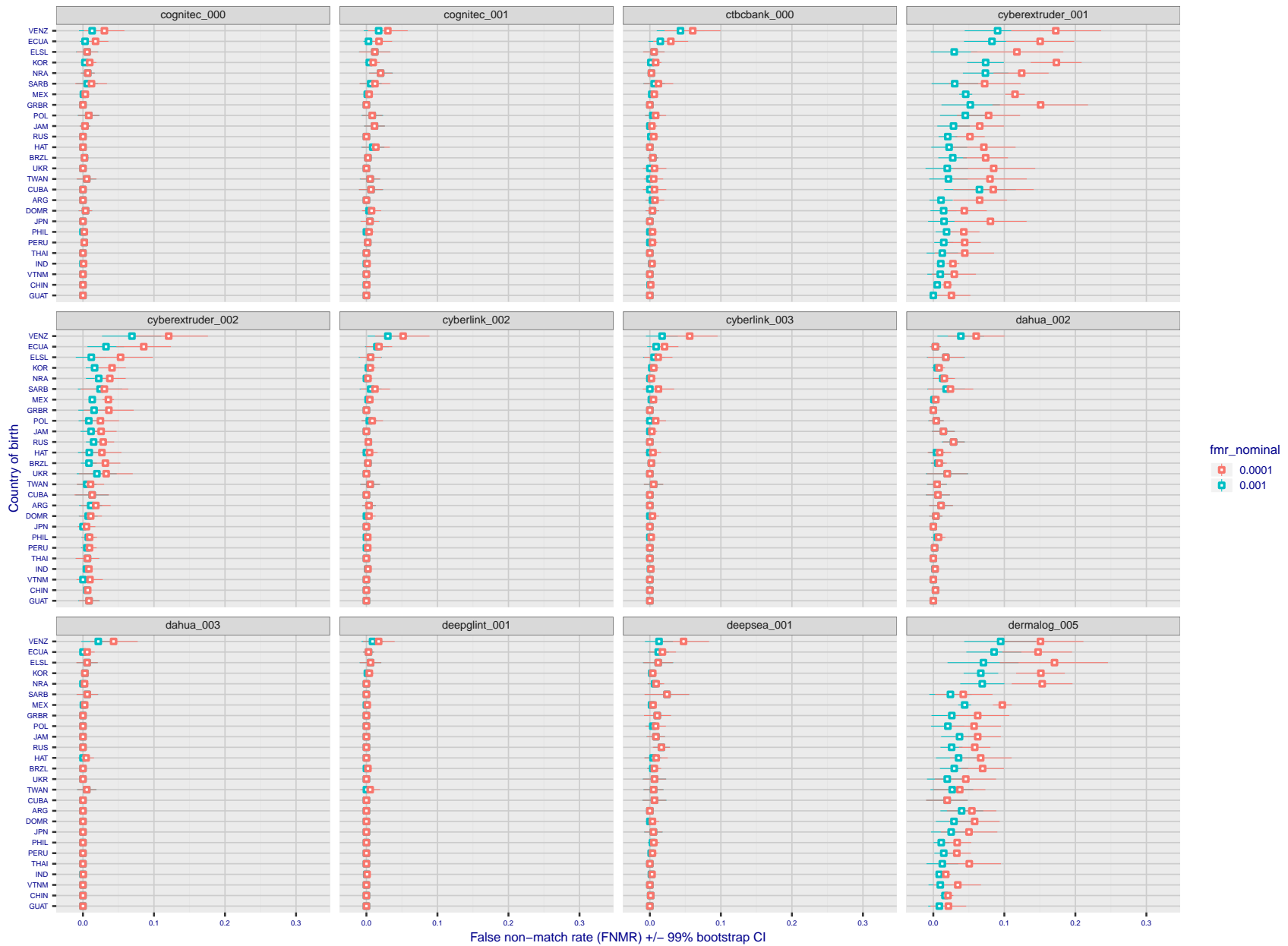


Figure 116: For the visa images, the dots show FNMR by country of birth for two globally set operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.1. The figures shows an order of magnitude variation in FNMR across country of birth; these effects are likely due quality variations, then demographics like age and race. The error rates in some cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.

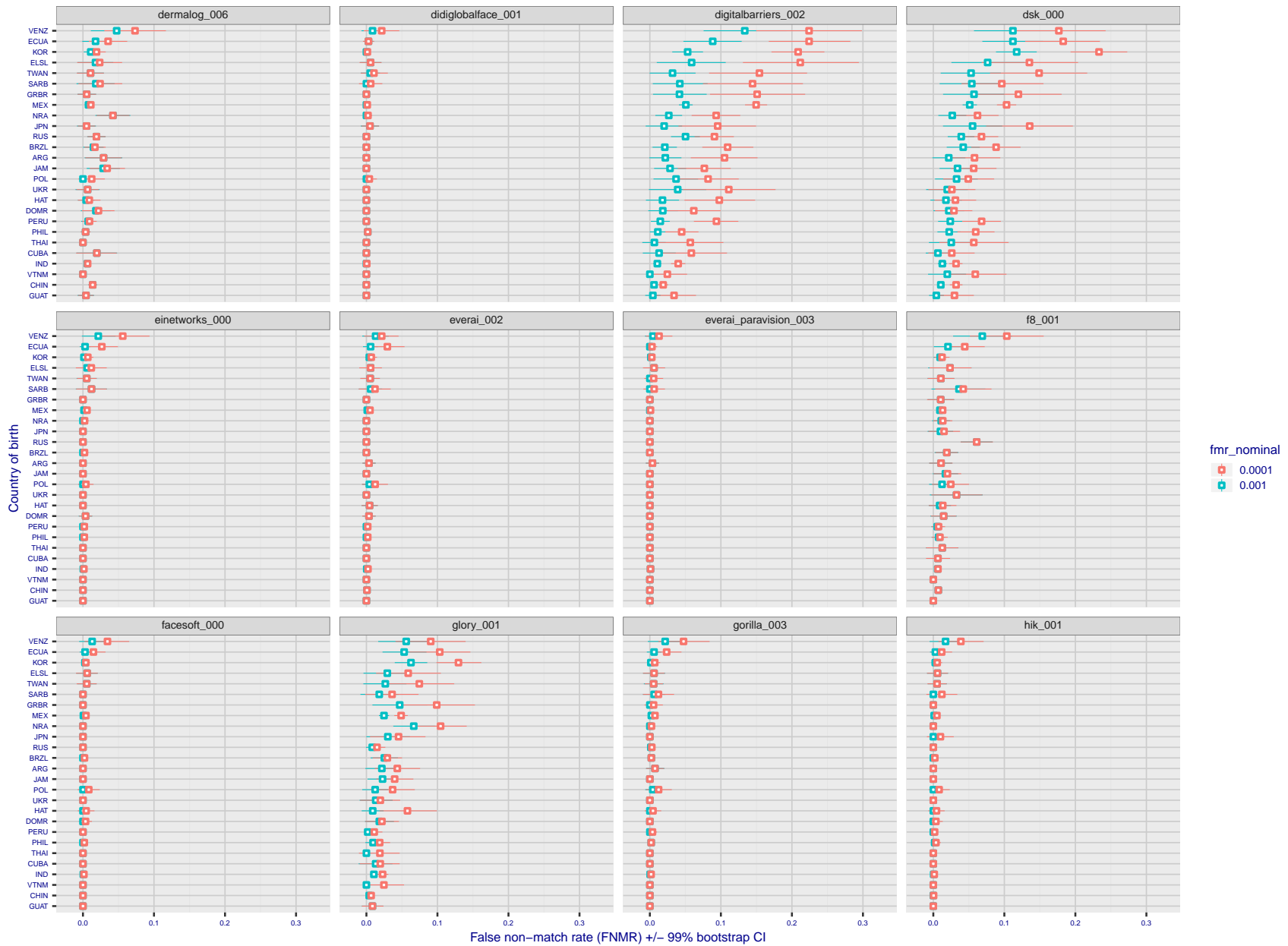
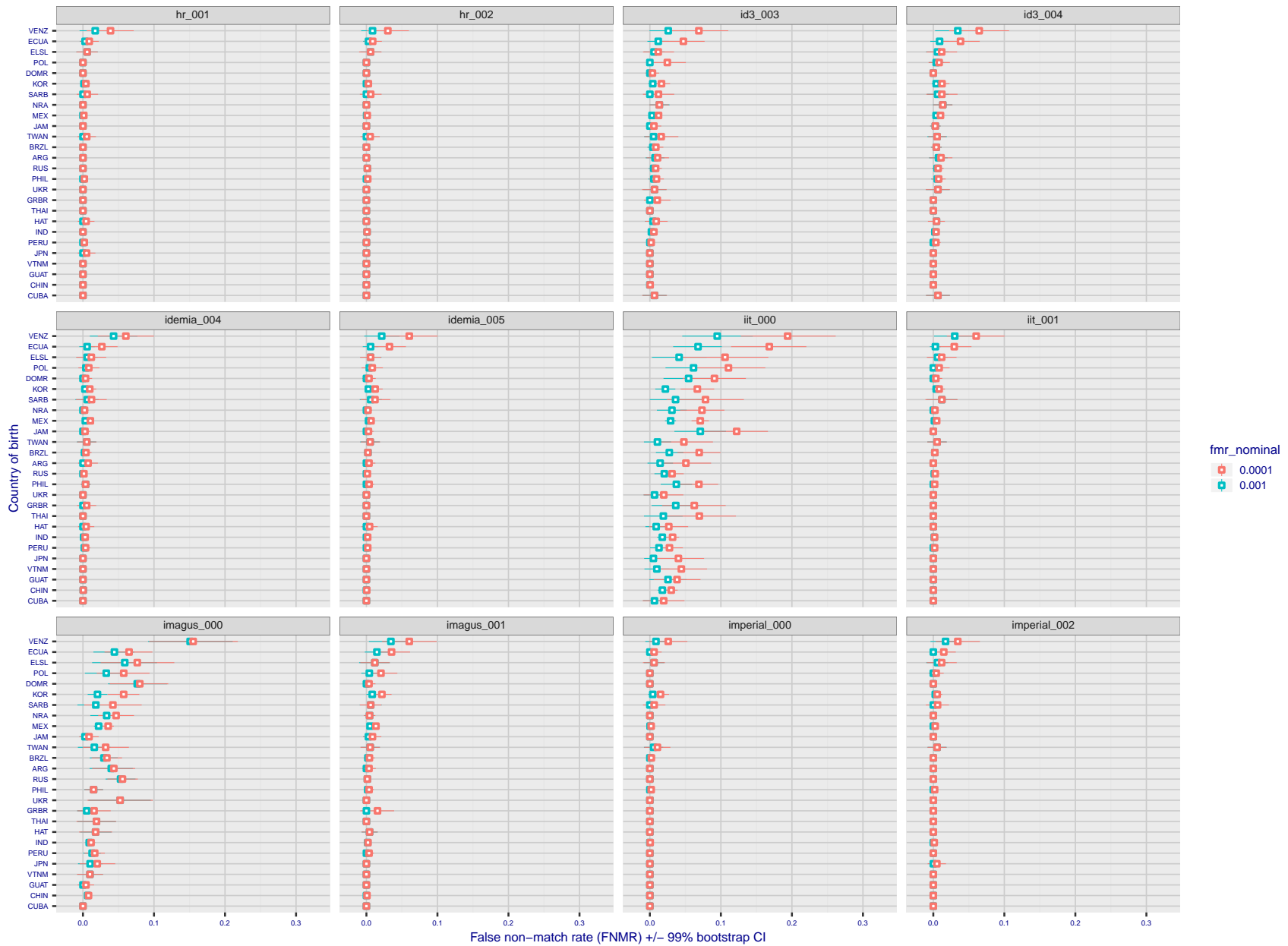


Figure 117: For the visa images, the dots show FNMR by country of birth for two globally set operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.1. The figures shows an order of magnitude variation in FNMR across country of birth; these effects are likely due quality variations, then demographics like age and race. The error rates in some cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.





FNMR(T)  
 FMR(T)  
 "False non-match rate"  
 "False match rate"

Figure 118: For the visa images, the dots show FNMR by country of birth for two globally set operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.1. The figures shows an order of magnitude variation in FNMR across country of birth; these effects are likely due quality variations, then demographics like age and race. The error rates in some cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.

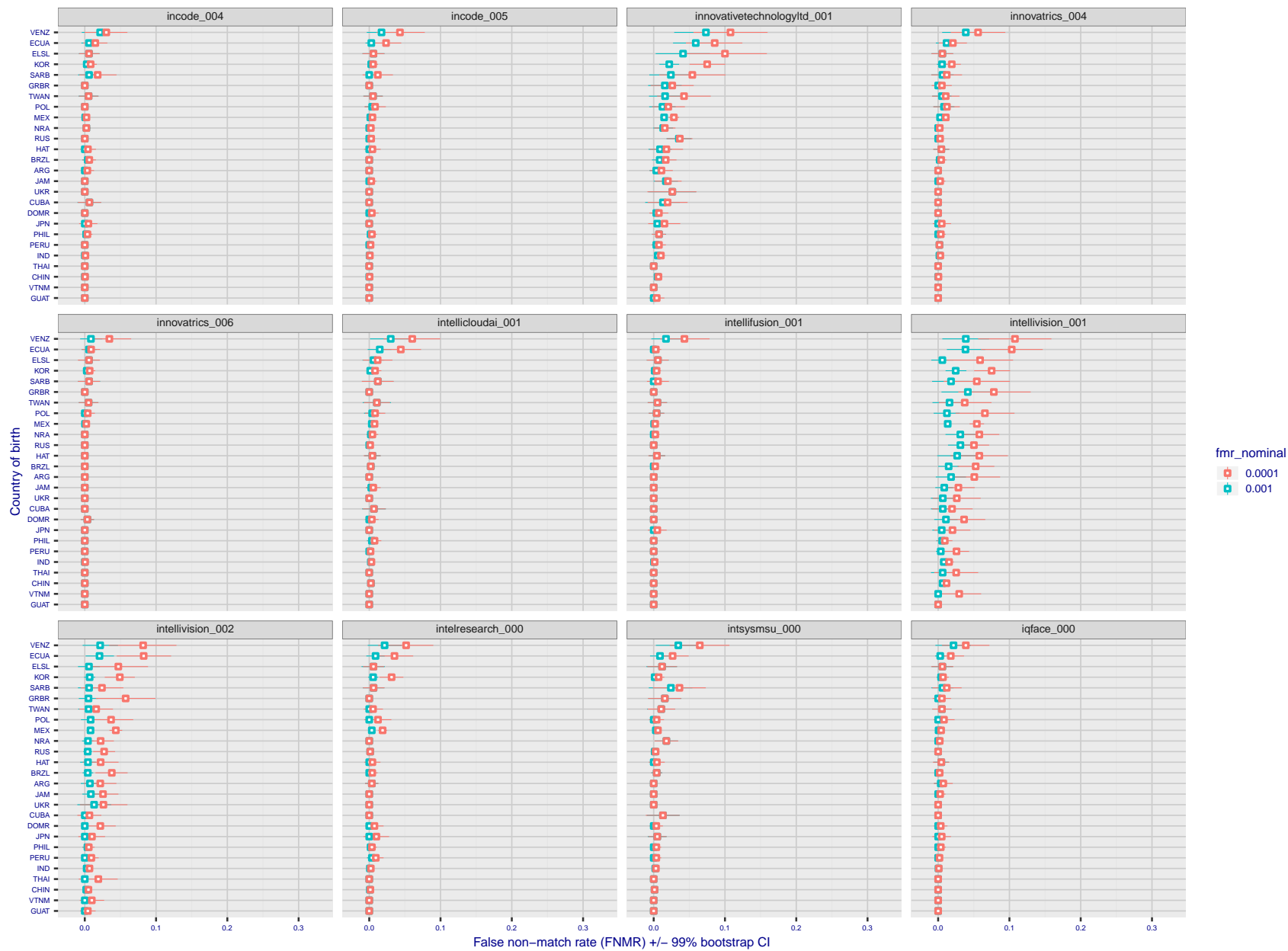
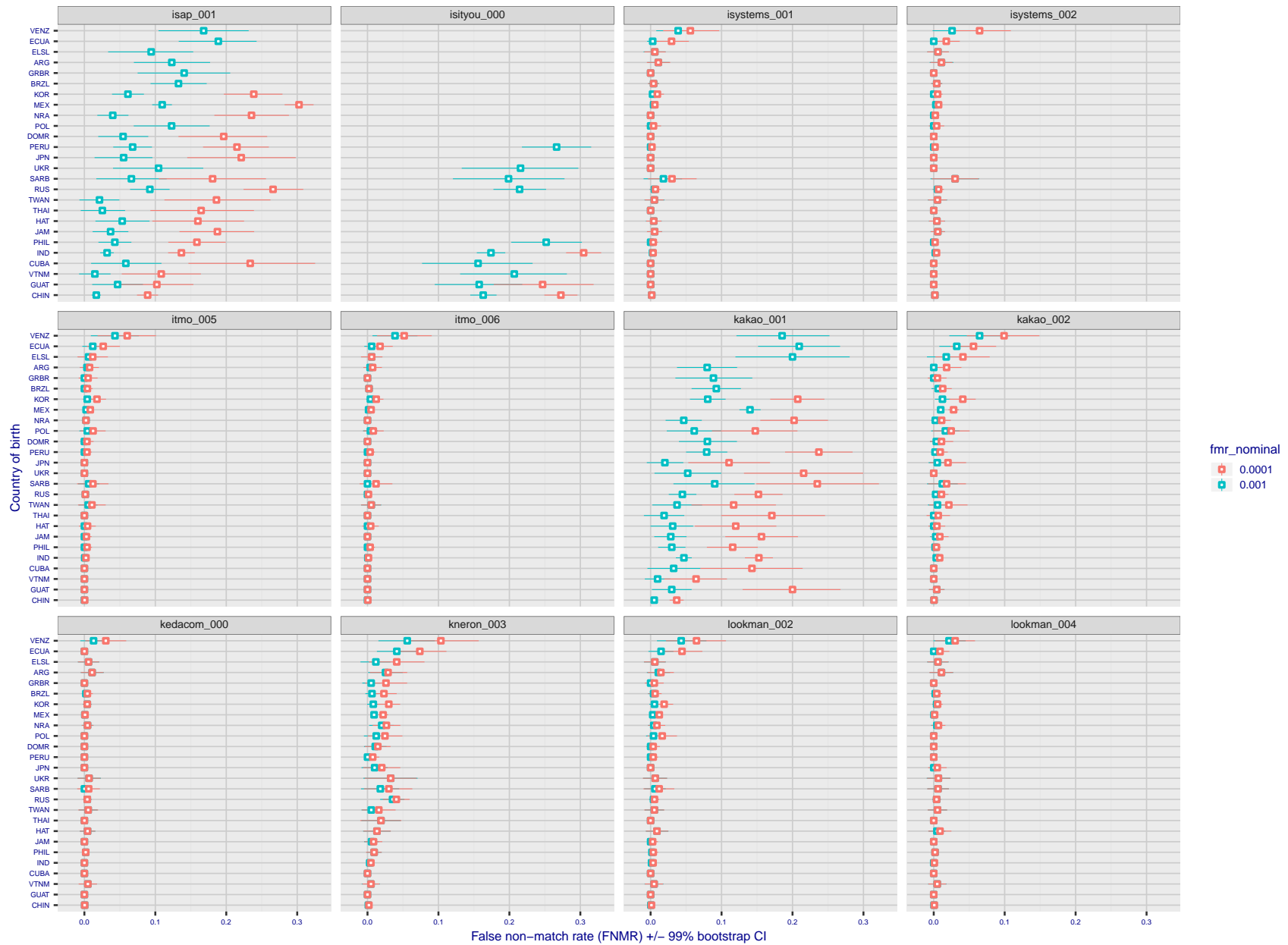
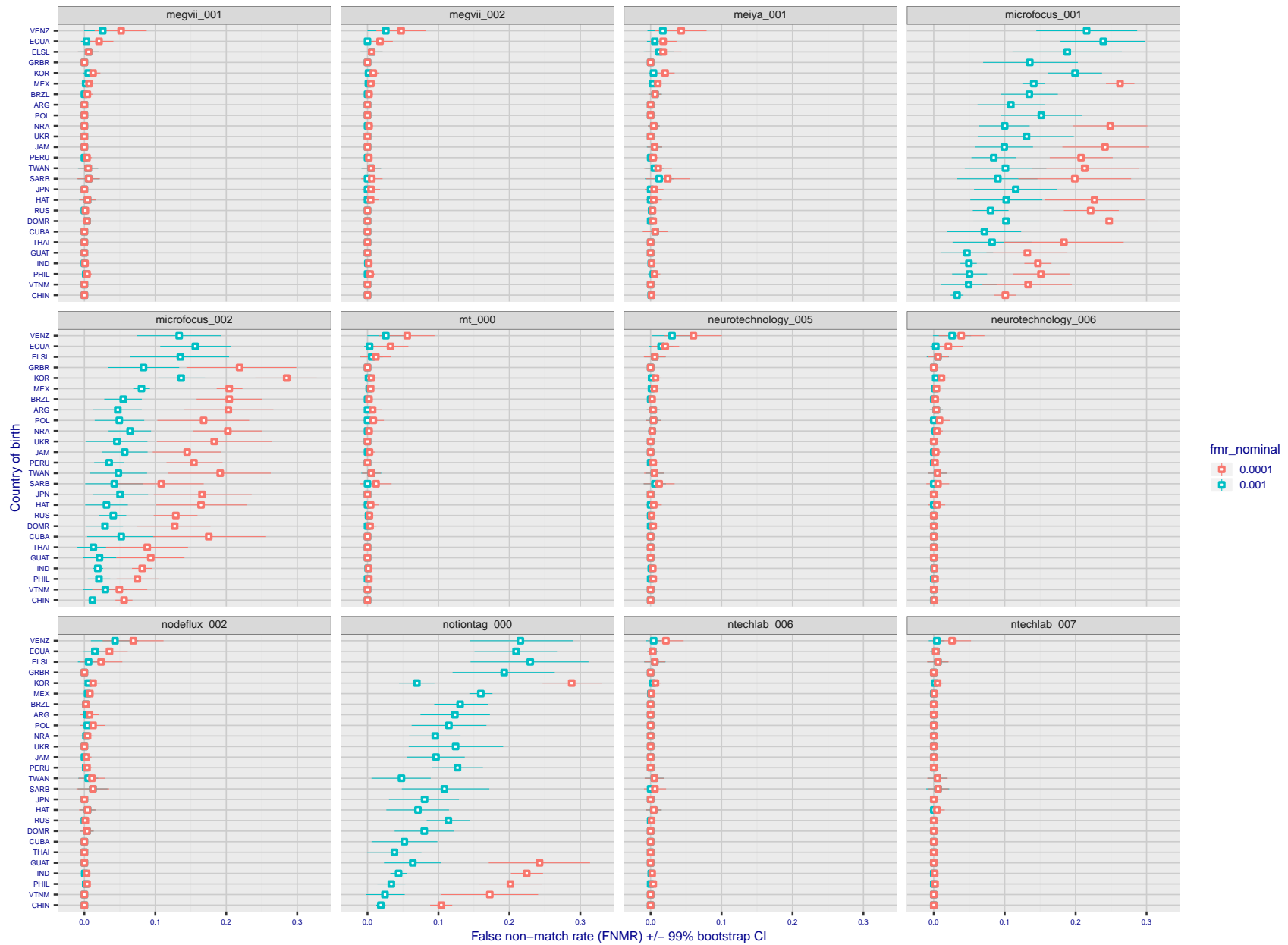


Figure 119: For the visa images, the dots show FNMR by country of birth for two globally set operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.1. The figures shows an order of magnitude variation in FNMR across country of birth; these effects are likely due quality variations, then demographics like age and race. The error rates in some cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.



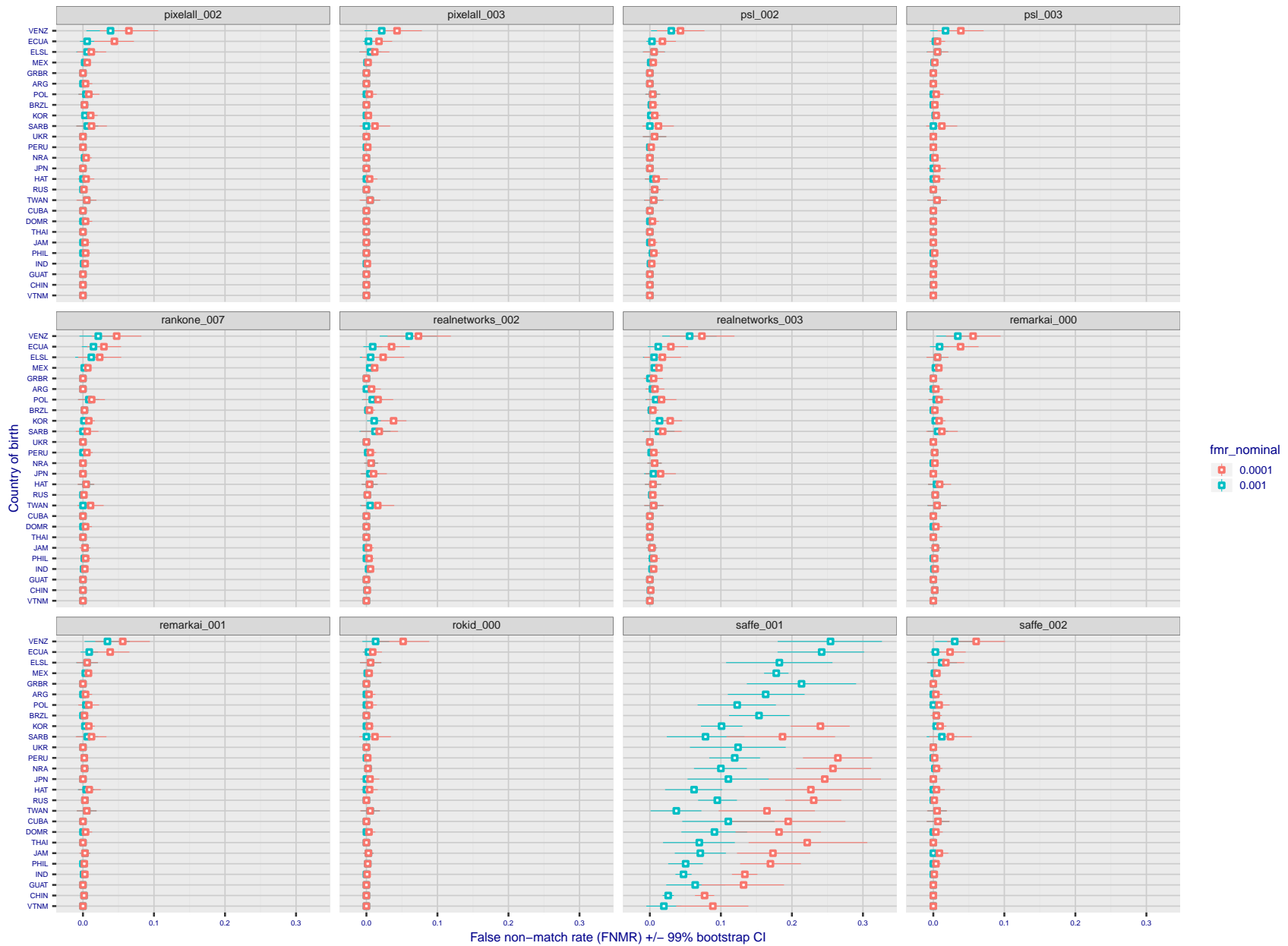
FNMR(T)  
 FMR(T)  
 "False non-match rate"  
 "False match rate"

Figure 120: For the visa images, the dots show FNMR by country of birth for two globally set operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.1. The figures shows an order of magnitude variation in FNMR across country of birth; these effects are likely due quality variations, then demographics like age and race. The error rates in some cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.



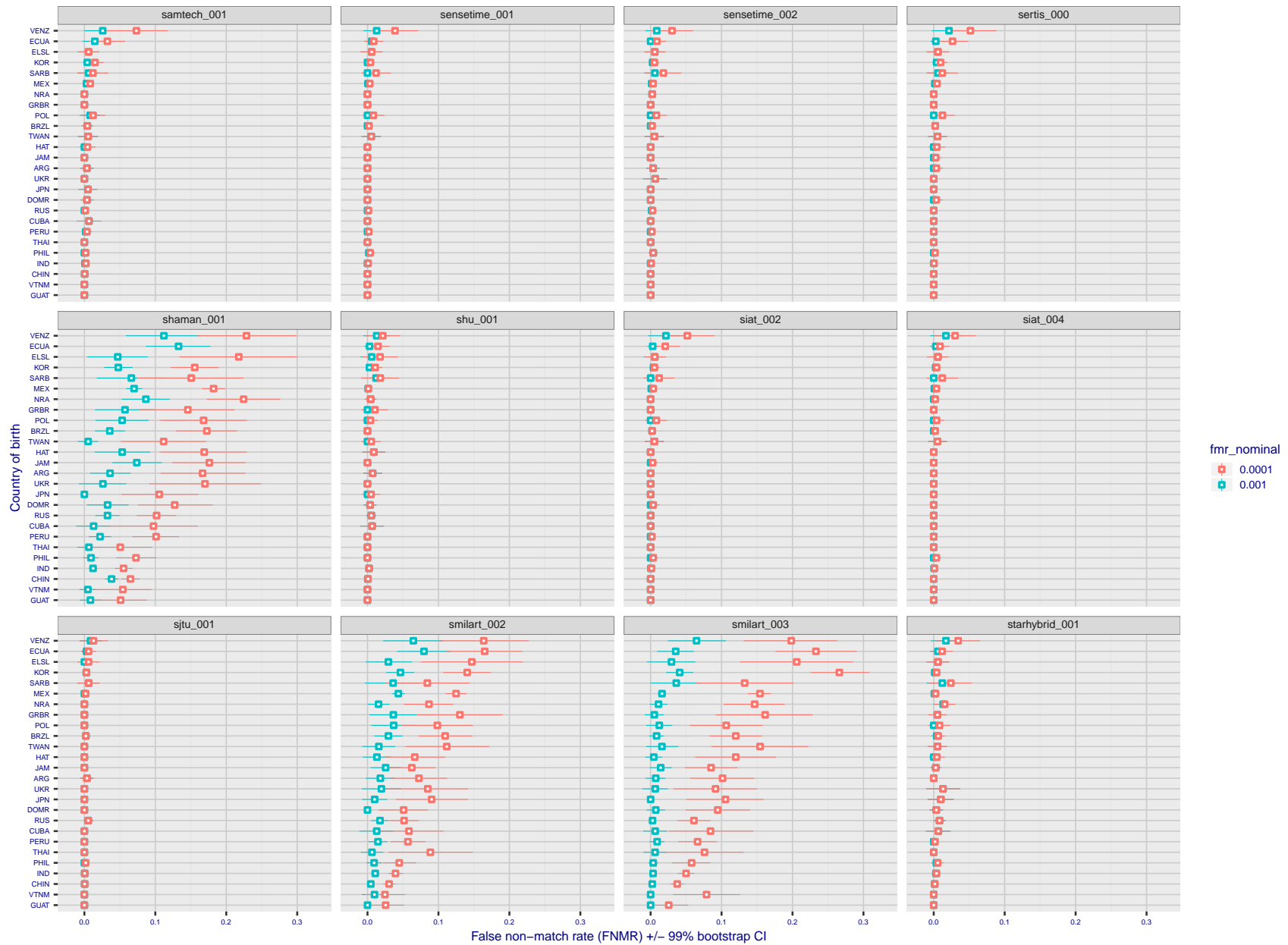
FNMR(T)  
 FMR(T)  
 "False non-match rate"  
 "False match rate"

Figure 121: For the visa images, the dots show FNMR by country of birth for two globally set operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.1. The figures shows an order of magnitude variation in FNMR across country of birth; these effects are likely due quality variations, then demographics like age and race. The error rates in some cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.



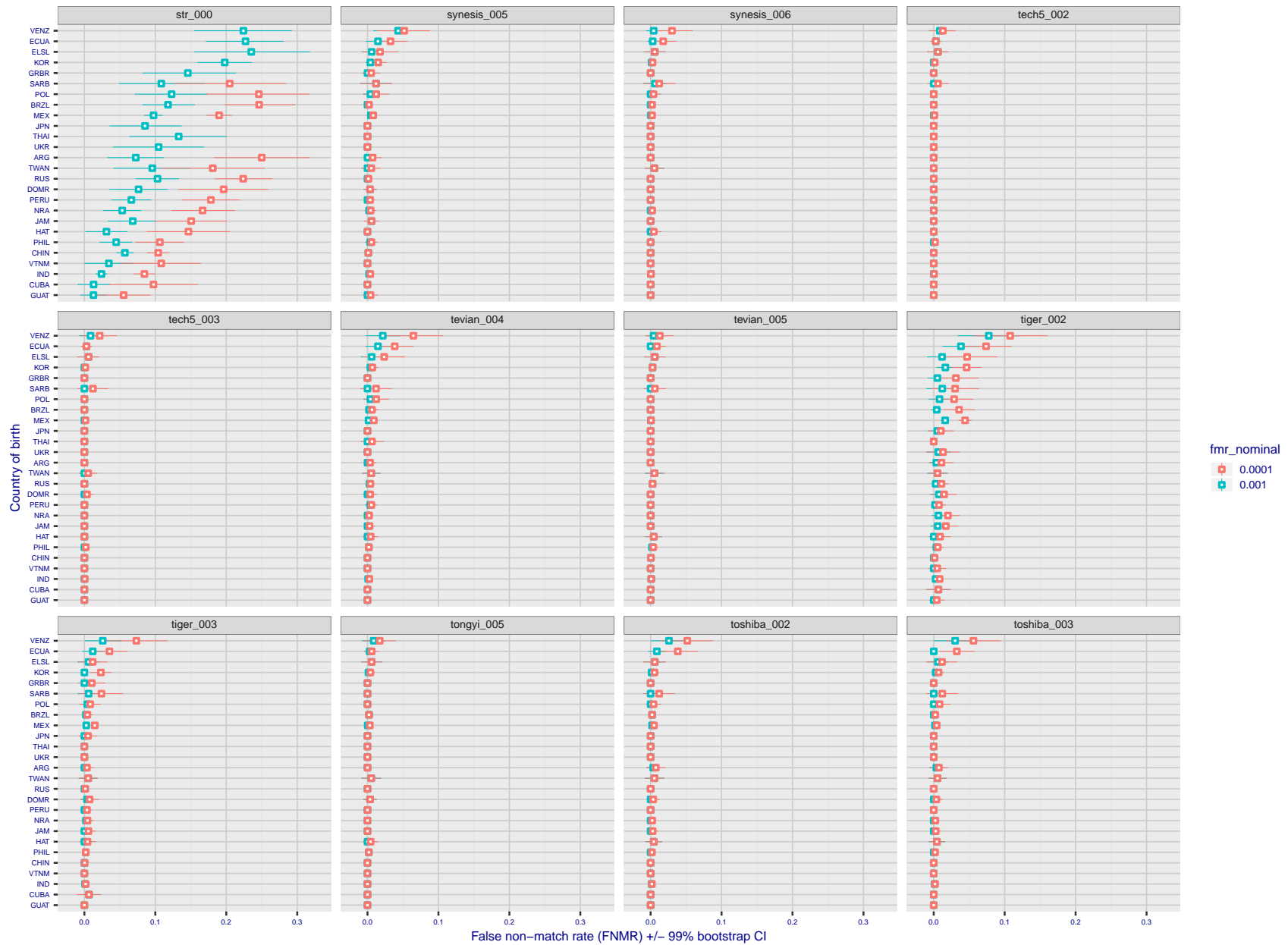
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 122: For the visa images, the dots show FNMR by country of birth for two globally set operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.1. The figures shows an order of magnitude variation in FNMR across country of birth; these effects are likely due quality variations, then demographics like age and race. The error rates in some cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.



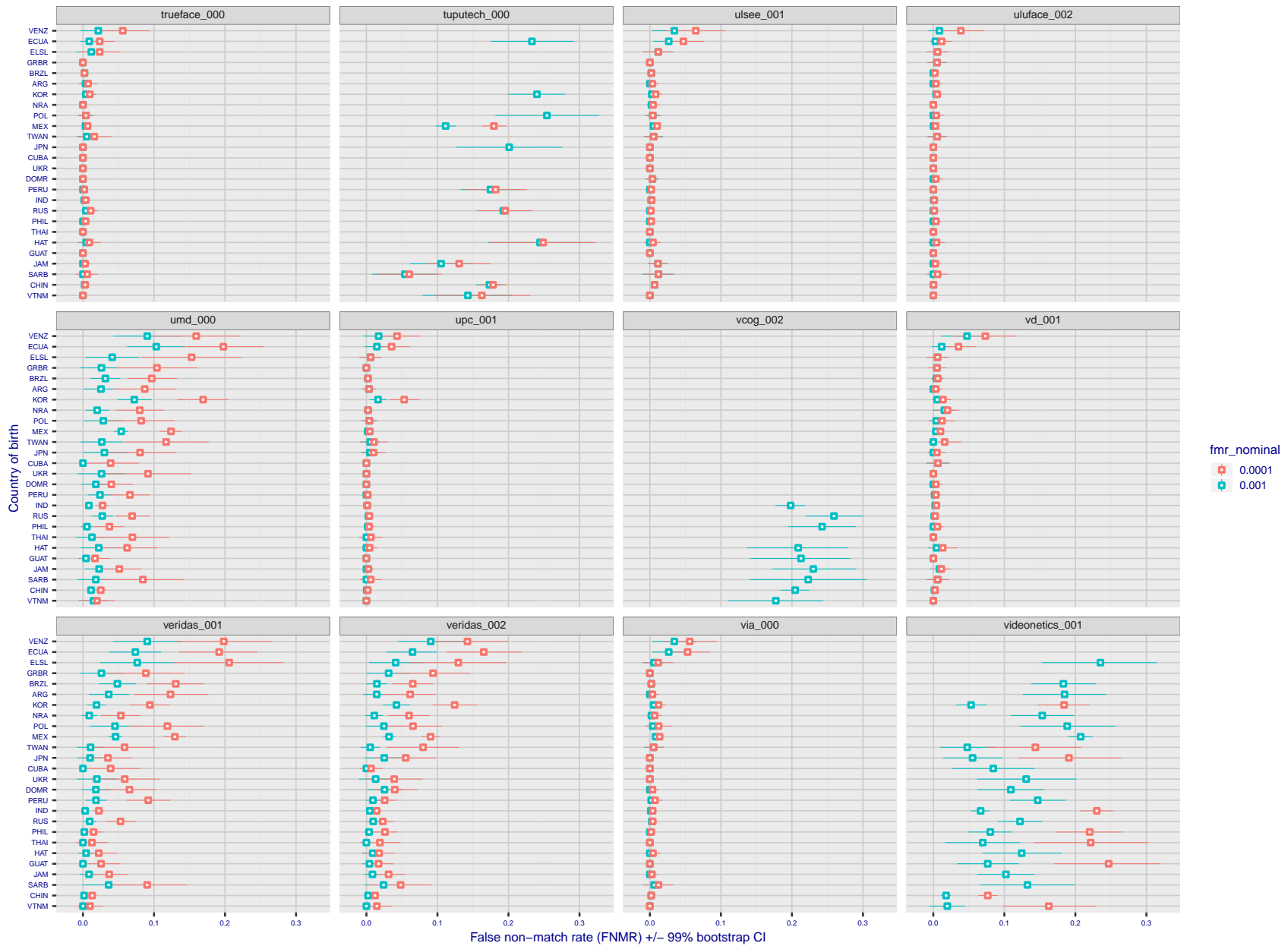
FNMR(T)  
 FMR(T)  
 "False non-match rate"  
 "False match rate"

Figure 123: For the visa images, the dots show FNMR by country of birth for two globally set operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.1. The figures shows an order of magnitude variation in FNMR across country of birth; these effects are likely due quality variations, then demographics like age and race. The error rates in some cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.



FNMR(T)  
 FMR(T)  
 "False non-match rate"  
 "False match rate"

Figure 124: For the visa images, the dots show FNMR by country of birth for two globally set operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.1. The figures shows an order of magnitude variation in FNMR across country of birth; these effects are likely due quality variations, then demographics like age and race. The error rates in some cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 125: For the visa images, the dots show FNMR by country of birth for two globally set operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.1. The figures shows an order of magnitude variation in FNMR across country of birth; these effects are likely due quality variations, then demographics like age and race. The error rates in some cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.





Figure 126: For the visa images, the dots show FNMR by country of birth for two globally set operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.1. The figures shows an order of magnitude variation in FNMR across country of birth; these effects are likely due quality variations, then demographics like age and race. The error rates in some cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.



Figure 127: For the visa images, the dots show FNMR by country of birth for two globally set operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.1. The figures shows an order of magnitude variation in FNMR across country of birth; these effects are likely due quality variations, then demographics like age and race. The error rates in some cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.

**Caveats:** The results may not relate to subject-specific properties. Instead they could reflect image-specific quality differences, which could occur due to collection protocol or software processing variations.

### 3.5.2 Effect of ageing

**Background:** Faces change appearance throughout life. This change gradually reduces similarity of a new image to an earlier image. Face recognition algorithms give reduced similarity scores and more frequent false rejections.

**Goal:** To quantify false non-match rates (FNMR) as a function of elapsed time in an adult population.

**Methods:** Using the mugshot images, a threshold is set to give  $FMR = 0.00001$  over the entire impostor set. Then FNMR is measured over 1000 bootstrap replications of the genuine scores.

**Results:** For the visa images, Figure 138 shows how false non-match rates for genuine users, as a function of age group.

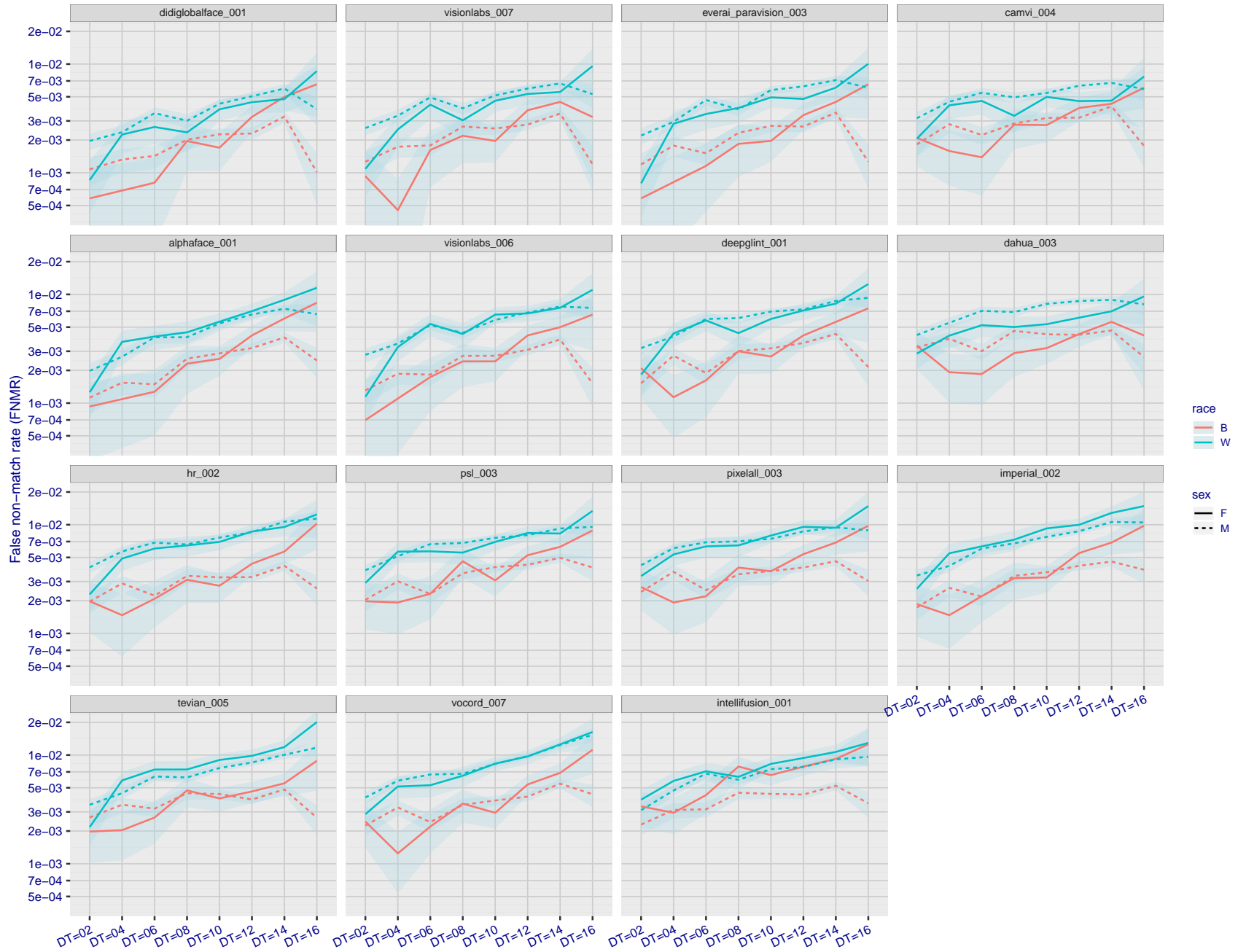


Figure 128: For the mugshot images, FNMR as a function of elapsed time between initial enrollment and second verification images. The panels appear most accurate first, and vertical scale changes on each page. The four traces correspond to images annotated with codes for black female, black male, white female, white male. The threshold is fixed for each algorithm to give FMR = 0.00001 over all ( $10^8$ ) impostor comparisons. For short time-lapses, the most accurate algorithms give very few errors (FNMR < 0.001) so that the uncertainty estimates are high.

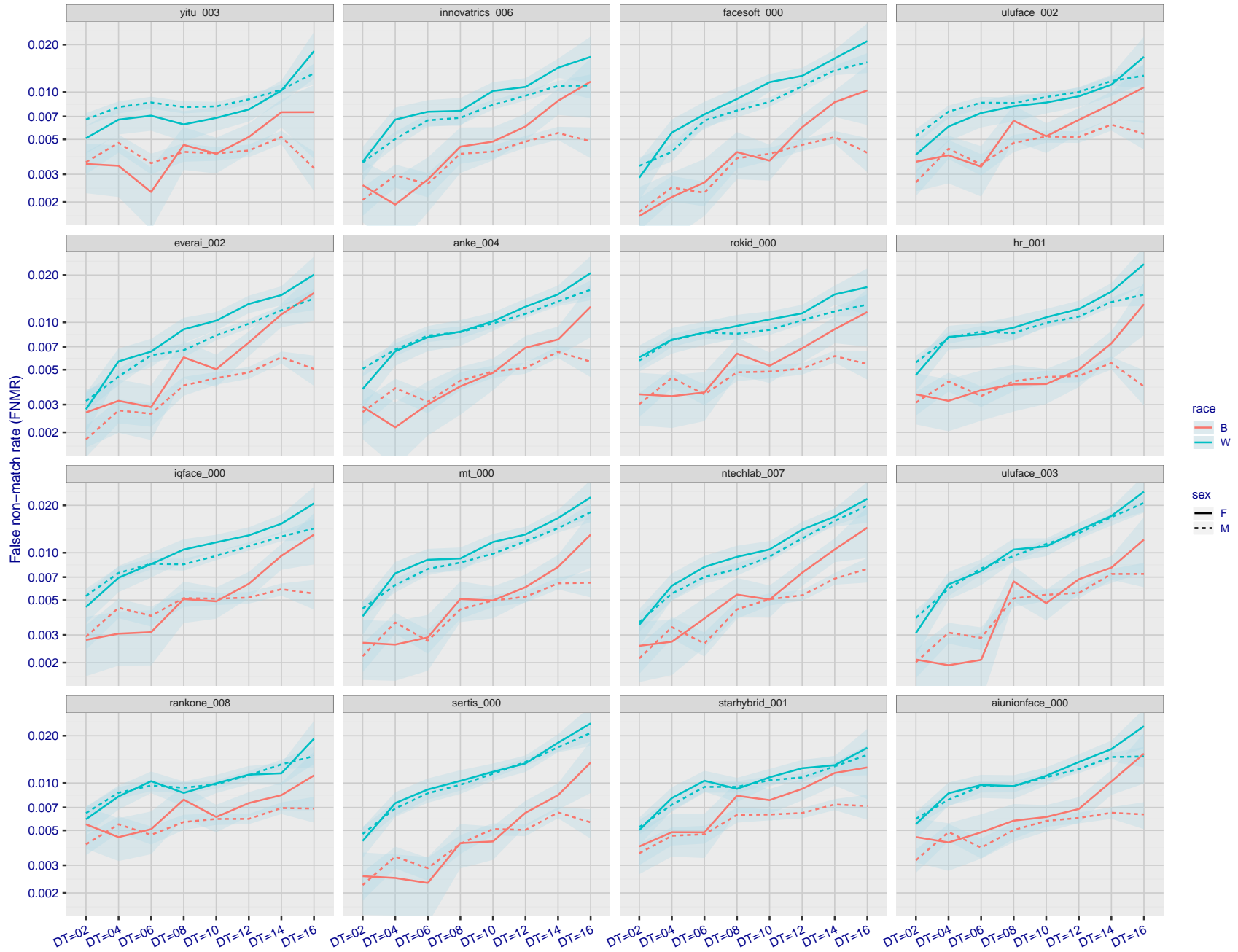


Figure 129: For the mugshot images, FNMR as a function of elapsed time between initial enrollment and second verification images. The panels appear most accurate first, and vertical scale changes on each page. The four traces correspond to images annotated with codes for black female, black male, white female, white male. The threshold is fixed for each algorithm to give FMR = 0.00001 over all ( $10^8$ ) impostor comparisons. For short time-lapses, the most accurate algorithms give very few errors (FNMR < 0.001) so that the uncertainty estimates are high.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

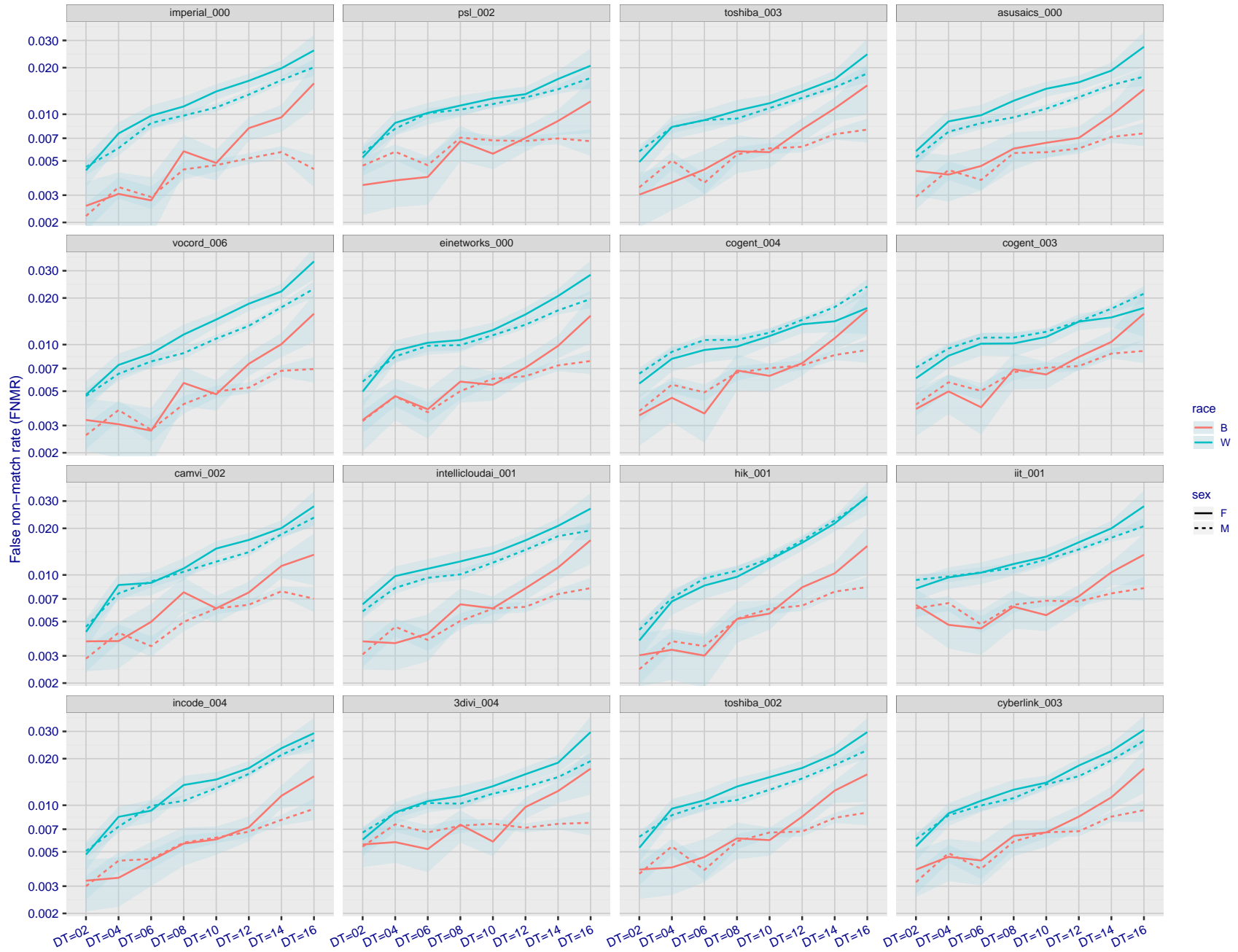


Figure 130: For the mugshot images, FNMR as a function of elapsed time between initial enrollment and second verification images. The panels appear most accurate first, and vertical scale changes on each page. The four traces correspond to images annotated with codes for black female, black male, white female, white male. The threshold is fixed for each algorithm to give FMR = 0.00001 over all ( $10^8$ ) impostor comparisons. For short time-lapses, the most accurate algorithms give very few errors (FNMR < 0.001) so that the uncertainty estimates are high.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

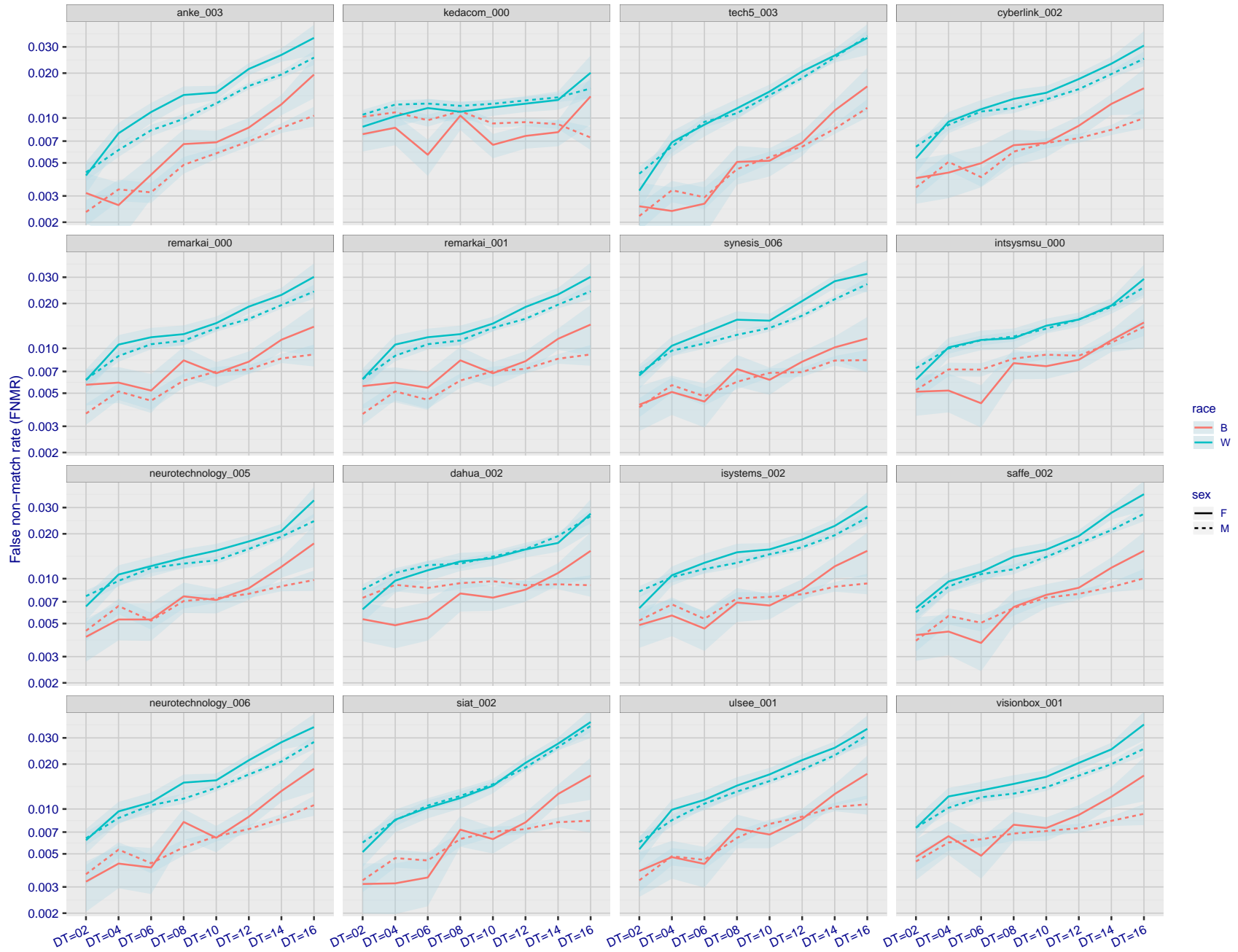


Figure 131: For the mugshot images, FNMR as a function of elapsed time between initial enrollment and second verification images. The panels appear most accurate first, and vertical scale changes on each page. The four traces correspond to images annotated with codes for black female, black male, white female, white male. The threshold is fixed for each algorithm to give FMR = 0.00001 over all ( $10^8$ ) impostor comparisons. For short time-lapses, the most accurate algorithms give very few errors (FNMR < 0.001) so that the uncertainty estimates are high.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

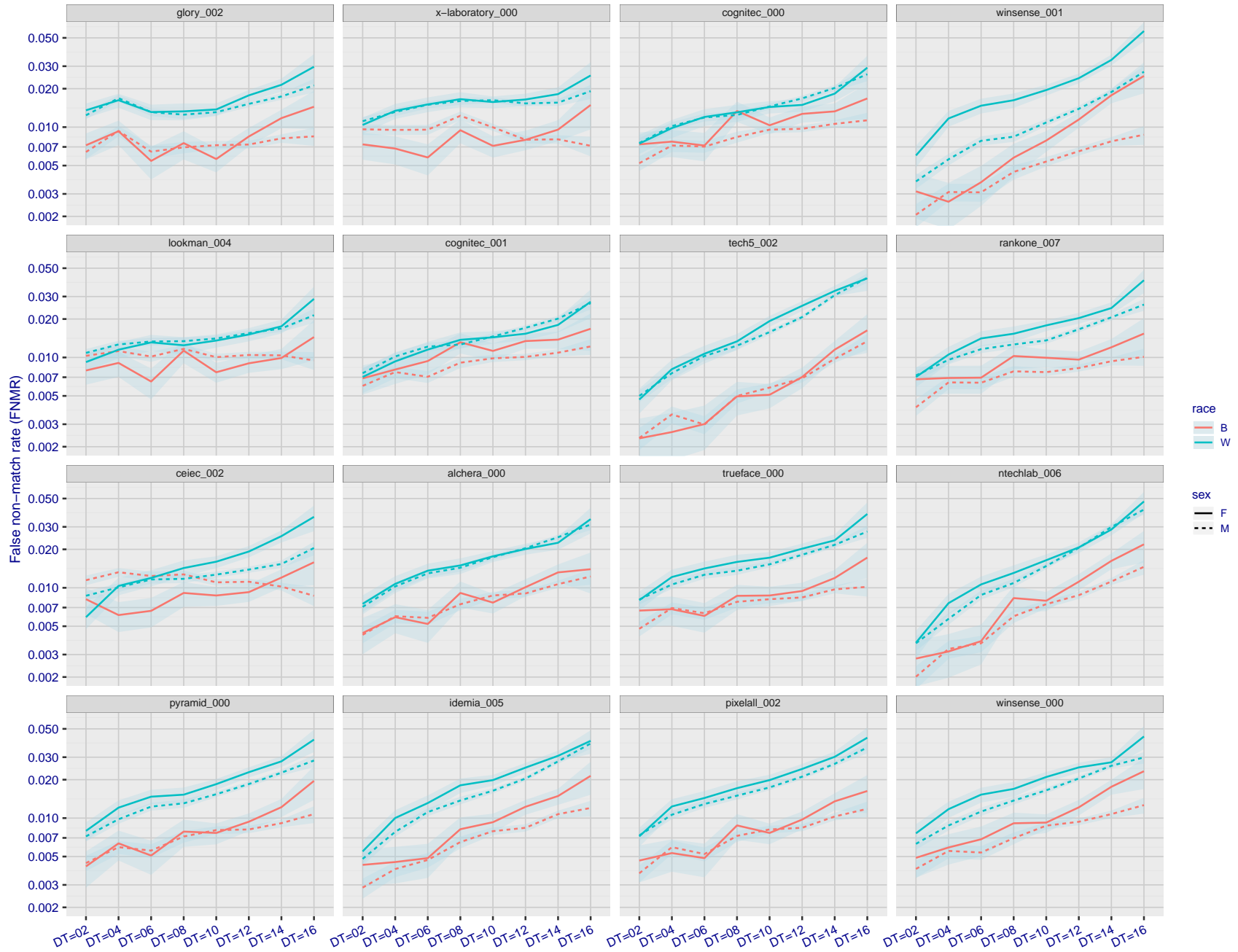


Figure 132: For the mugshot images, FNMR as a function of elapsed time between initial enrollment and second verification images. The panels appear most accurate first, and vertical scale changes on each page. The four traces correspond to images annotated with codes for black female, black male, white female, white male. The threshold is fixed for each algorithm to give FMR = 0.00001 over all ( $10^8$ ) impostor comparisons. For short time-lapses, the most accurate algorithms give very few errors (FNMR < 0.001) so that the uncertainty estimates are high.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"



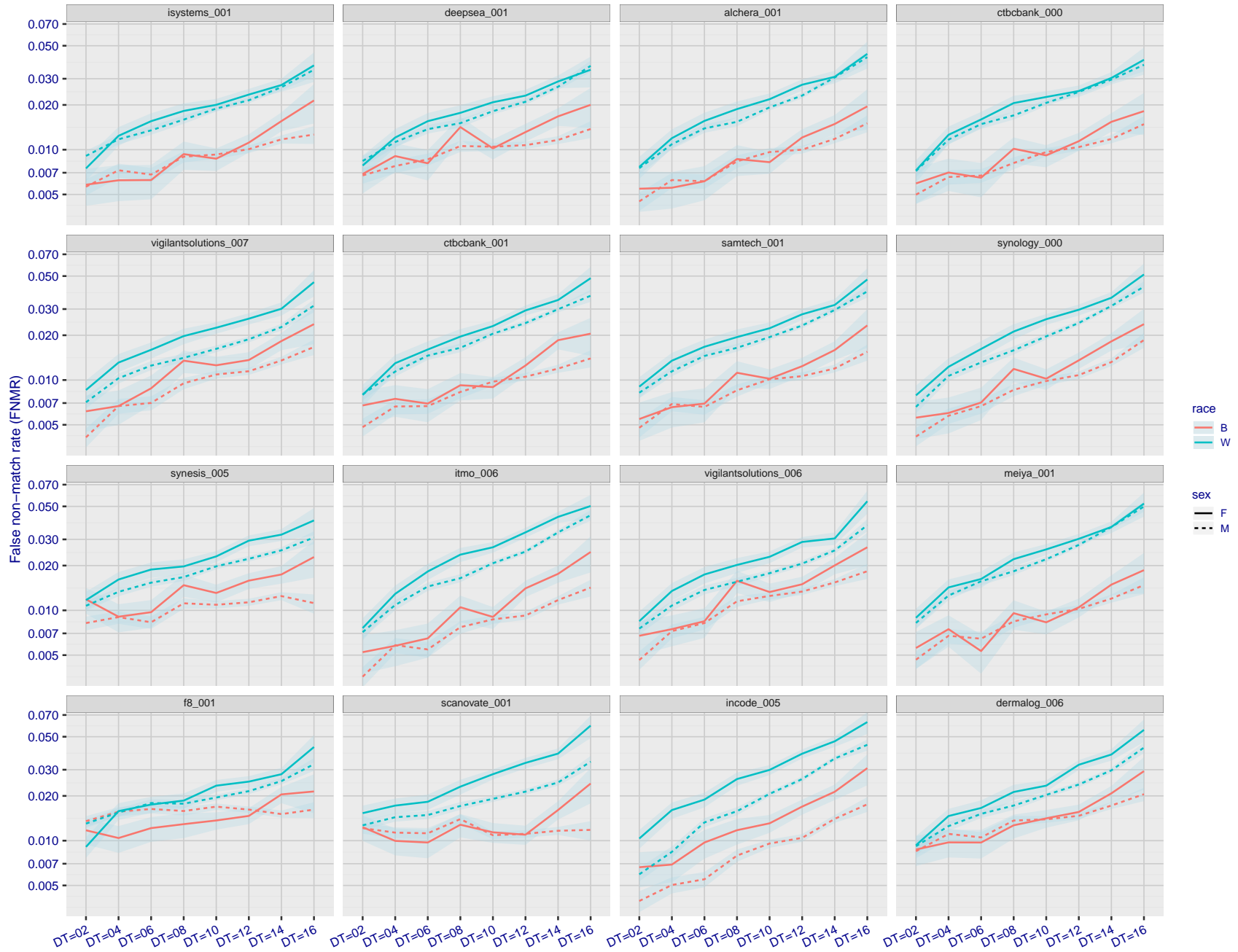


Figure 133: For the mugshot images, FNMR as a function of elapsed time between initial enrollment and second verification images. The panels appear most accurate first, and vertical scale changes on each page. The four traces correspond to images annotated with codes for black female, black male, white female, white male. The threshold is fixed for each algorithm to give FMR = 0.00001 over all ( $10^8$ ) impostor comparisons. For short time-lapses, the most accurate algorithms give very few errors (FNMR < 0.001) so that the uncertainty estimates are high.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

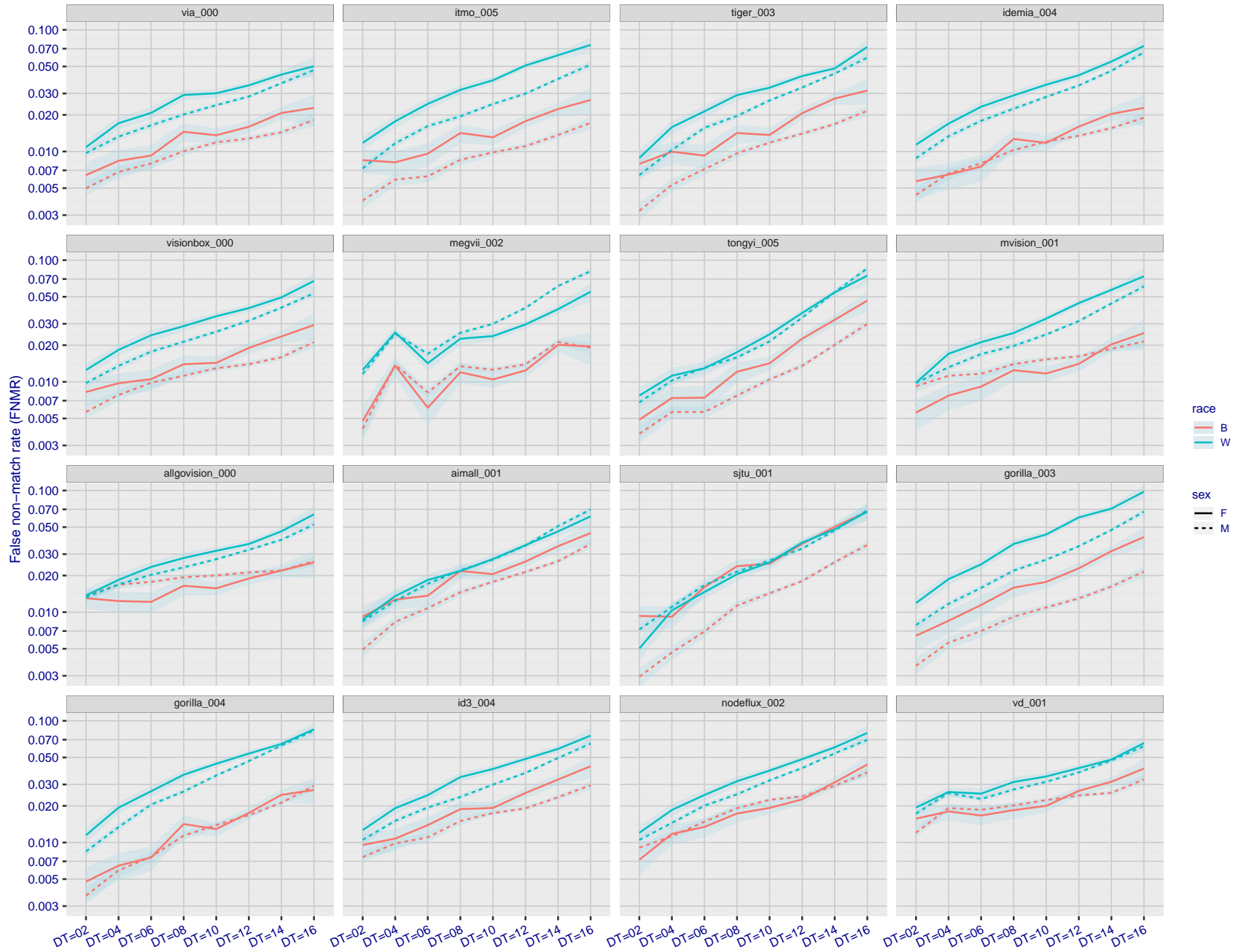


Figure 134: For the mugshot images, FNMR as a function of elapsed time between initial enrollment and second verification images. The panels appear most accurate first, and vertical scale changes on each page. The four traces correspond to images annotated with codes for black female, black male, white female, white male. The threshold is fixed for each algorithm to give FMR = 0.00001 over all ( $10^8$ ) impostor comparisons. For short time-lapses, the most accurate algorithms give very few errors (FNMR < 0.001) so that the uncertainty estimates are high.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

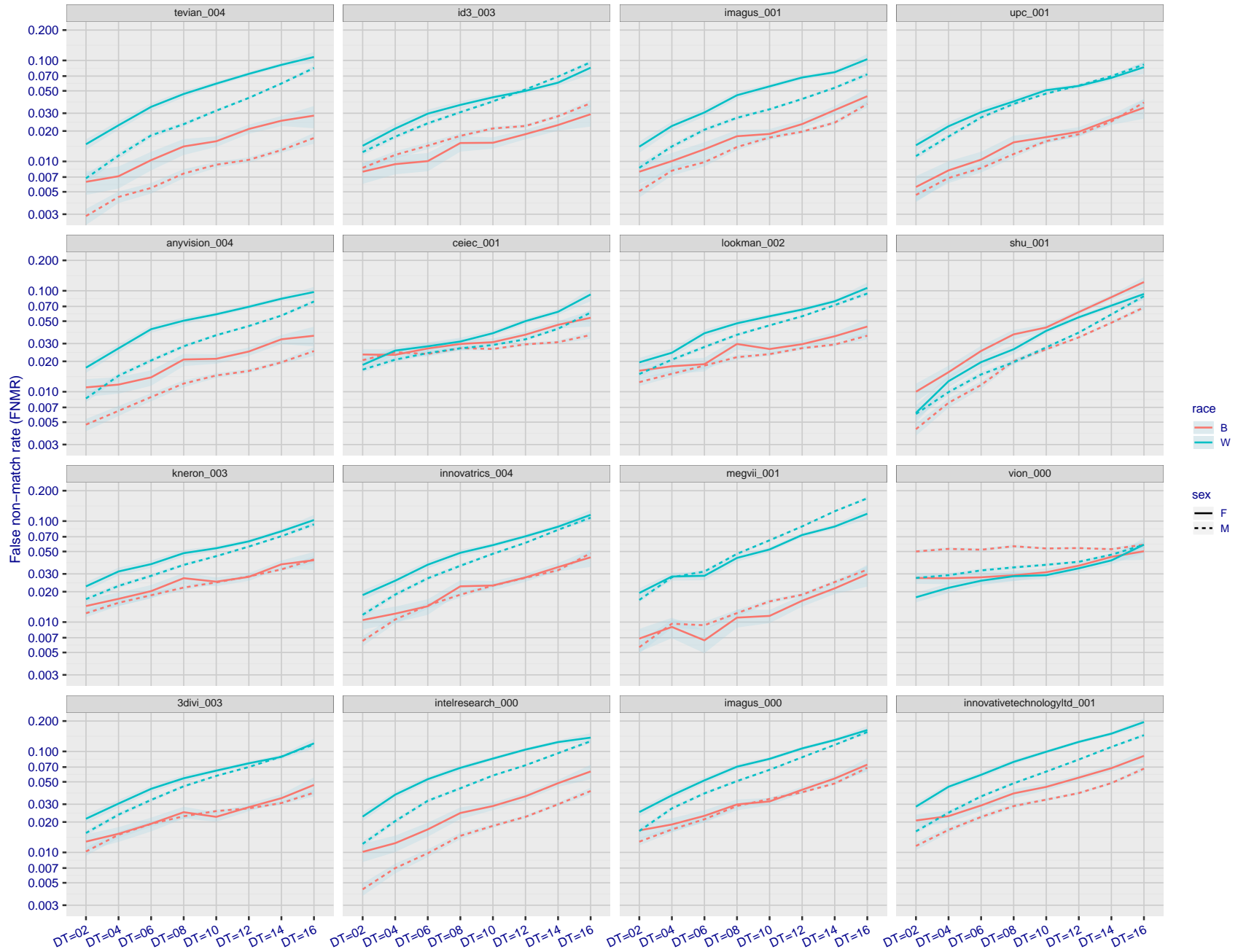
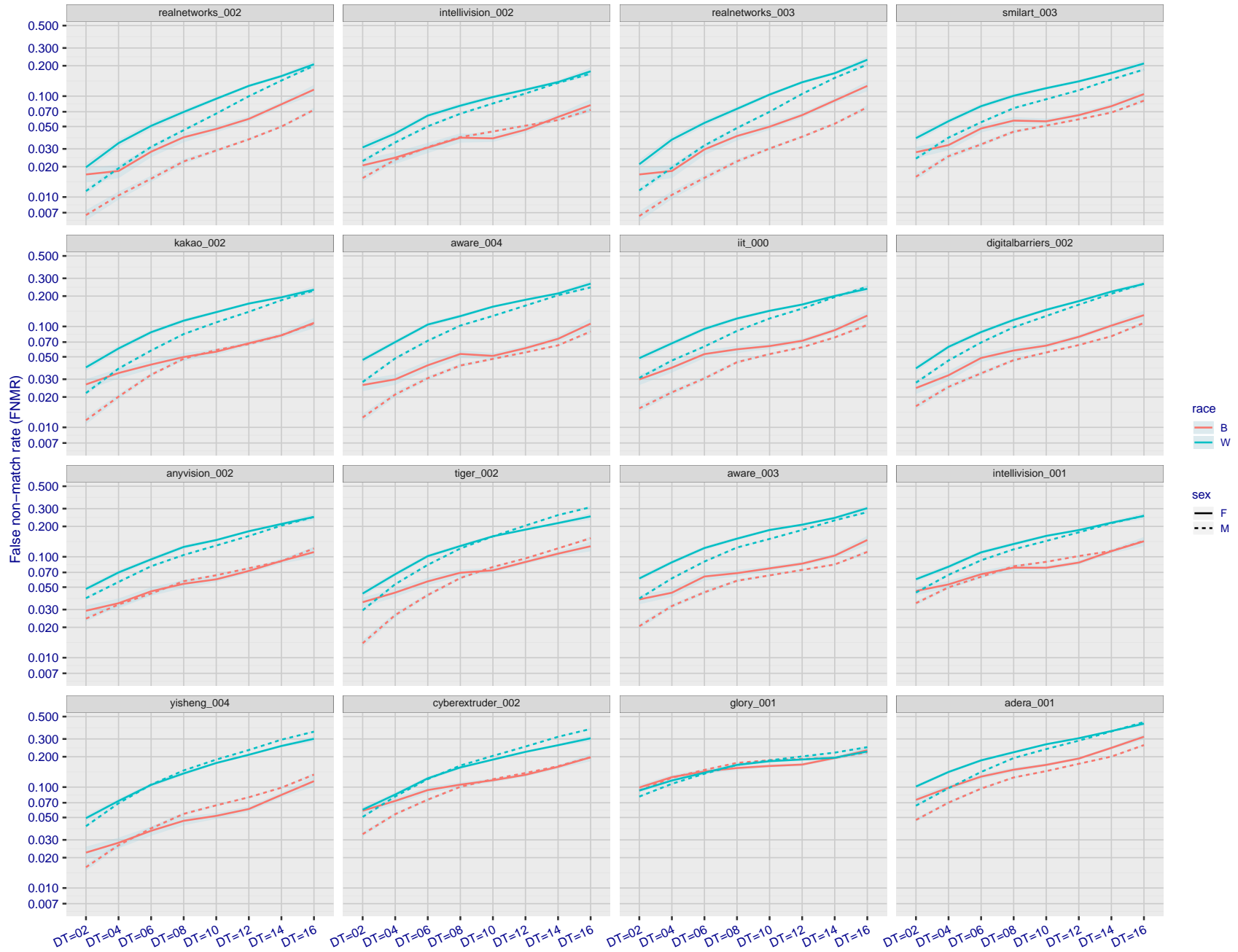


Figure 135: For the mugshot images, FNMR as a function of elapsed time between initial enrollment and second verification images. The panels appear most accurate first, and vertical scale changes on each page. The four traces correspond to images annotated with codes for black female, black male, white female, white male. The threshold is fixed for each algorithm to give FMR = 0.00001 over all ( $10^8$ ) impostor comparisons. For short time-lapses, the most accurate algorithms give very few errors (FNMR < 0.001) so that the uncertainty estimates are high.



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 136: For the mugshot images, FNMR as a function of elapsed time between initial enrollment and second verification images. The panels appear most accurate first, and vertical scale changes on each page. The four traces correspond to images annotated with codes for black female, black male, white female, white male. The threshold is fixed for each algorithm to give FMR = 0.00001 over all ( $10^8$ ) impostor comparisons. For short time-lapses, the most accurate algorithms give very few errors (FNMR < 0.001) so that the uncertainty estimates are high.

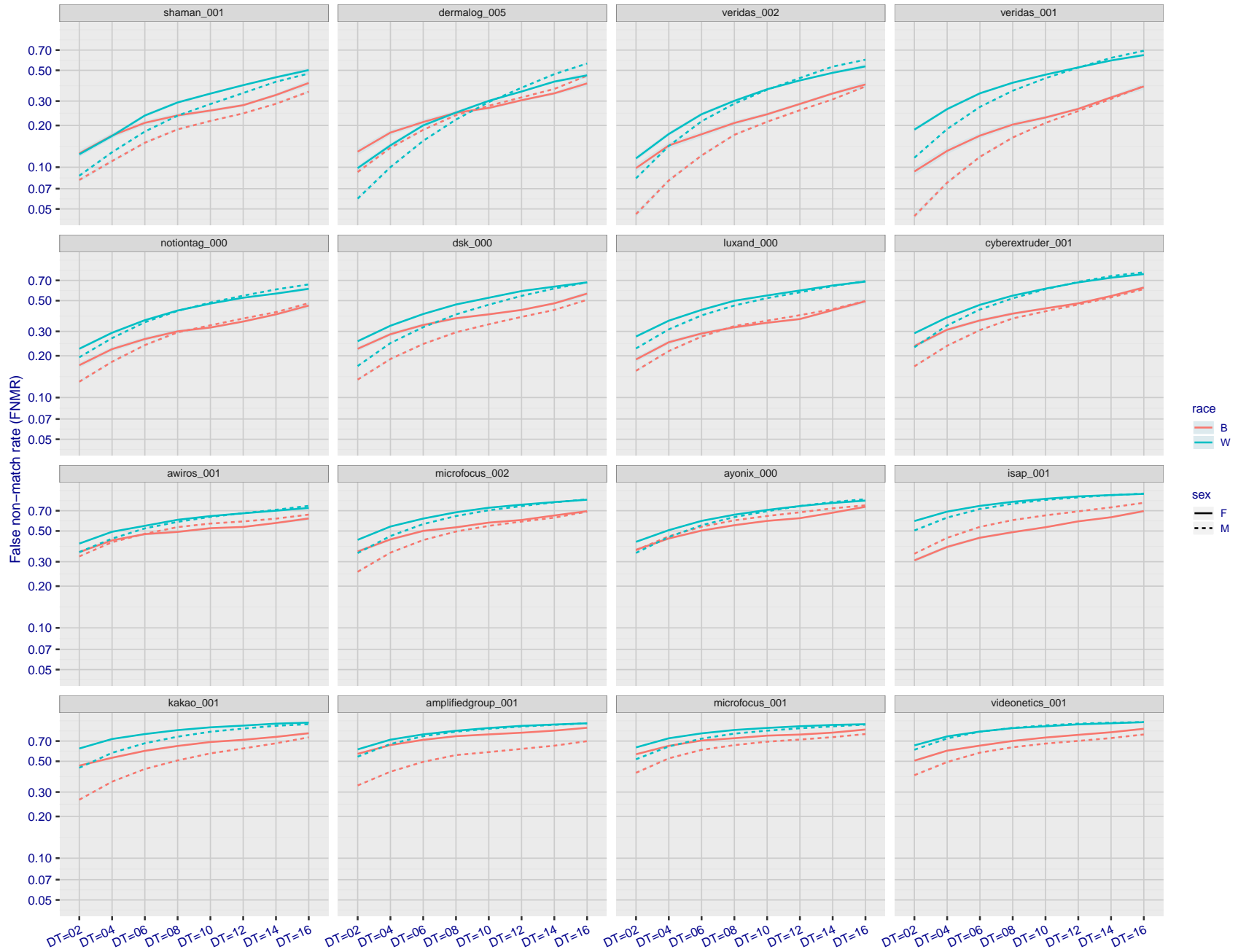


Figure 137: For the mugshot images, FNMR as a function of elapsed time between initial enrollment and second verification images. The panels appear most accurate first, and vertical scale changes on each page. The four traces correspond to images annotated with codes for black female, black male, white female, white male. The threshold is fixed for each algorithm to give FMR = 0.00001 over all ( $10^8$ ) impostor comparisons. For short time-lapses, the most accurate algorithms give very few errors (FNMR < 0.001) so that the uncertainty estimates are high.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

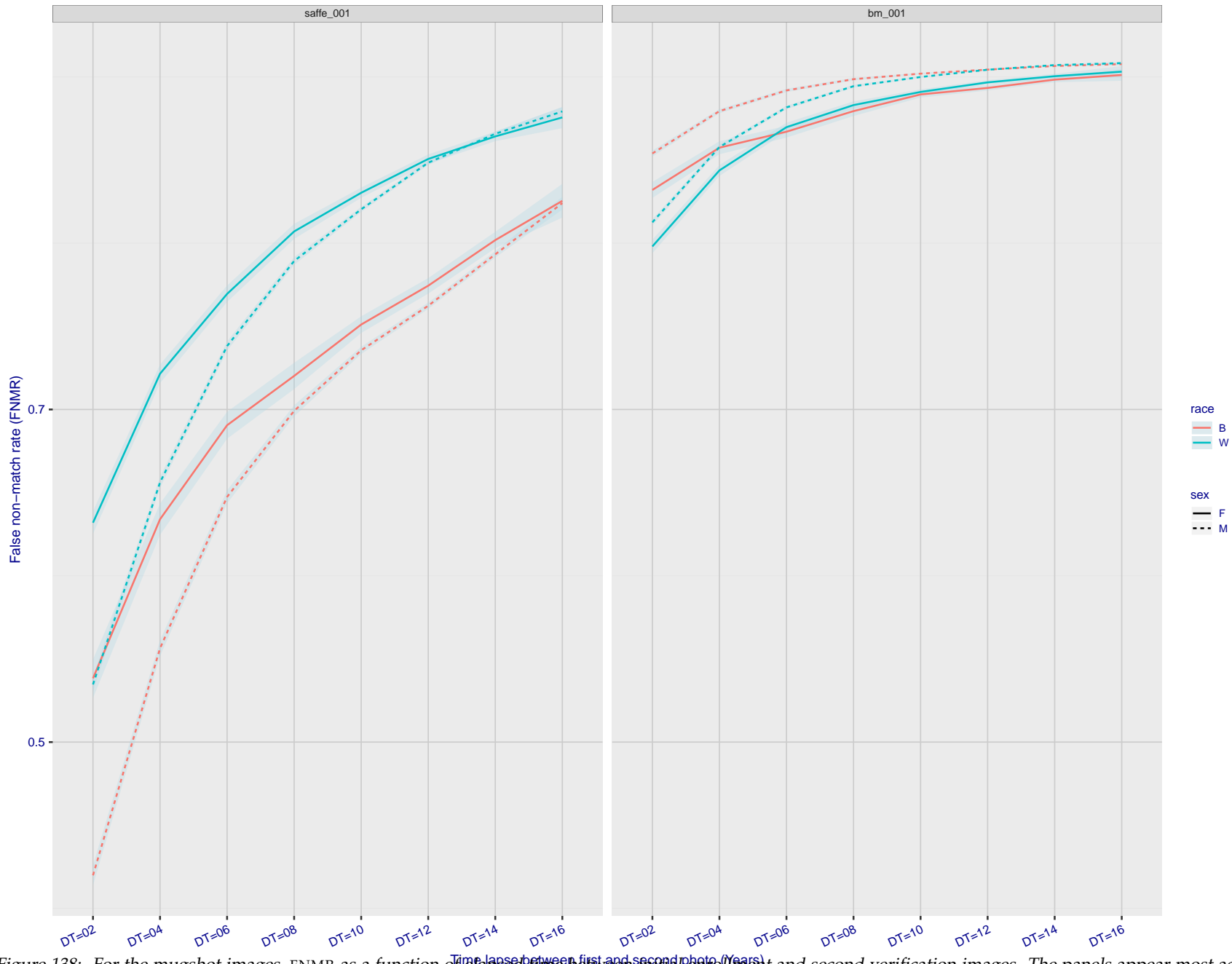


Figure 138: For the mugshot images, FNMR as a function of elapsed time between initial enrollment and second verification images. The panels appear most accurate first, and vertical scale changes on each page. The four traces correspond to images annotated with codes for black female, black male, white female, white male. The threshold is fixed for each algorithm to give FMR = 0.00001 over all ( $10^8$ ) impostor comparisons. For short time-lapses, the most accurate algorithms give very few errors (FNMR < 0.001) so that the uncertainty estimates are high.

### 3.5.3 Effect of age on genuine subjects

**Background:** Faces change appearance throughout life. Face recognition algorithms have previously been reported to give better accuracy on older individuals (See NIST IR 8009).

**Goal:** To quantify false non-match rates (FNMR) as a function of age, without an ageing component.

**Methods:** Using the visa images, which span fewer than five years, thresholds are determined that give FMR = 0.001 and 0.0001 over the entire impostor set. Then FNMR is measured over 1000 bootstrap replications of the genuine scores.

**Results:** For the visa images, Figure 152 shows how false non-match rates for genuine users, as a function of age group. The notable aspects are:

- ▷ Younger subjects give considerably higher FNMR. This is likely due to rapid growth and change in facial appearance.
- ▷ FNMR trends down throughout life. The last bin, AGE > 72, contains fewer than 140 mated pairs, and may be affected by small sample size.



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 139: For the visa images, the dots show FNMR by age group for two operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.2. Given a pair of face images taken at different times, we assign the comparison to the bin that is the arithmetic average of the subject's ages. This plot shows only the effect of age, not ageing. The number of comparisons in each bin is generally in the thousands, however the first and last bins are computed over 149 and 124 respectively. The error rates in some (adult) cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.



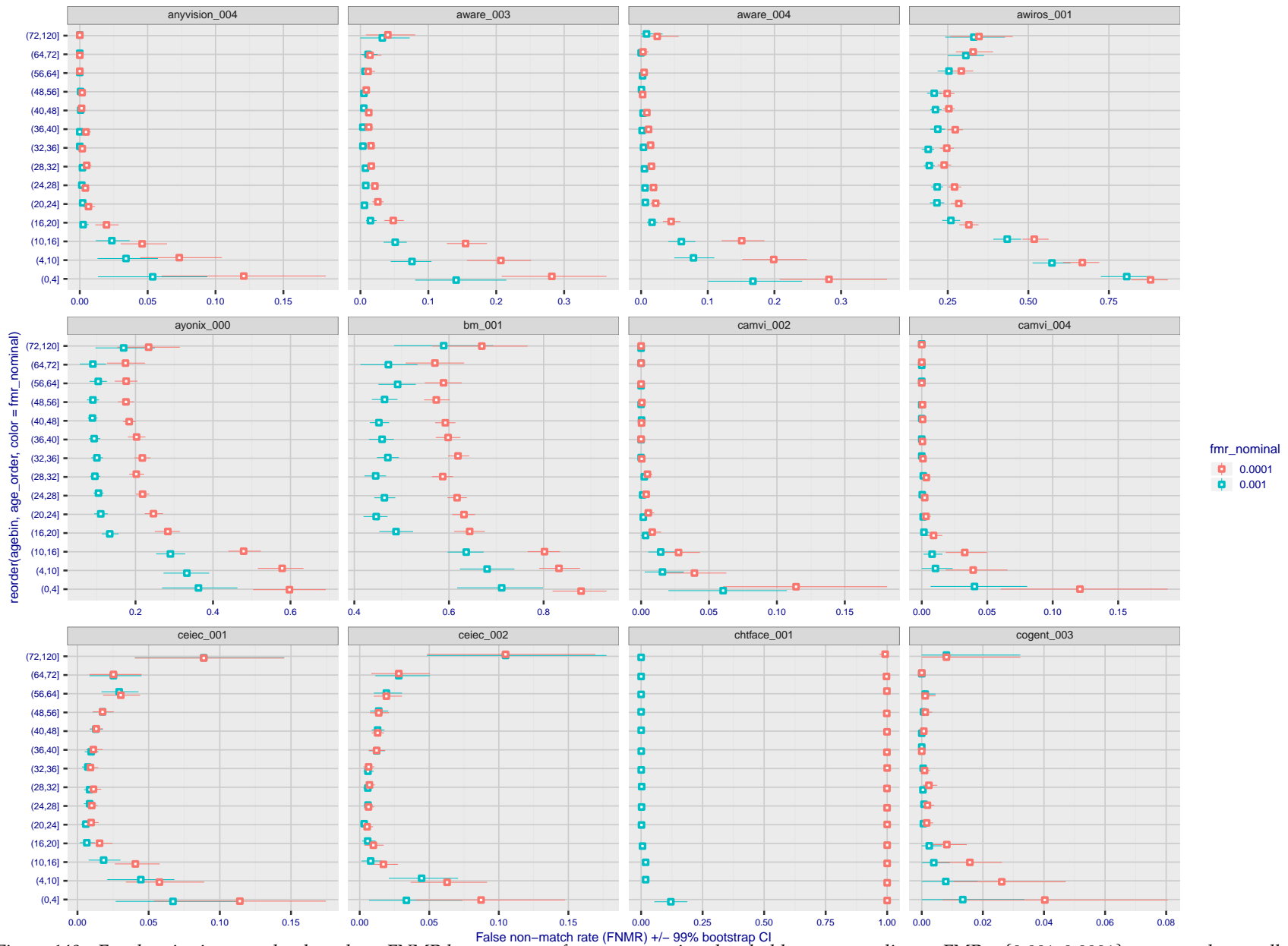
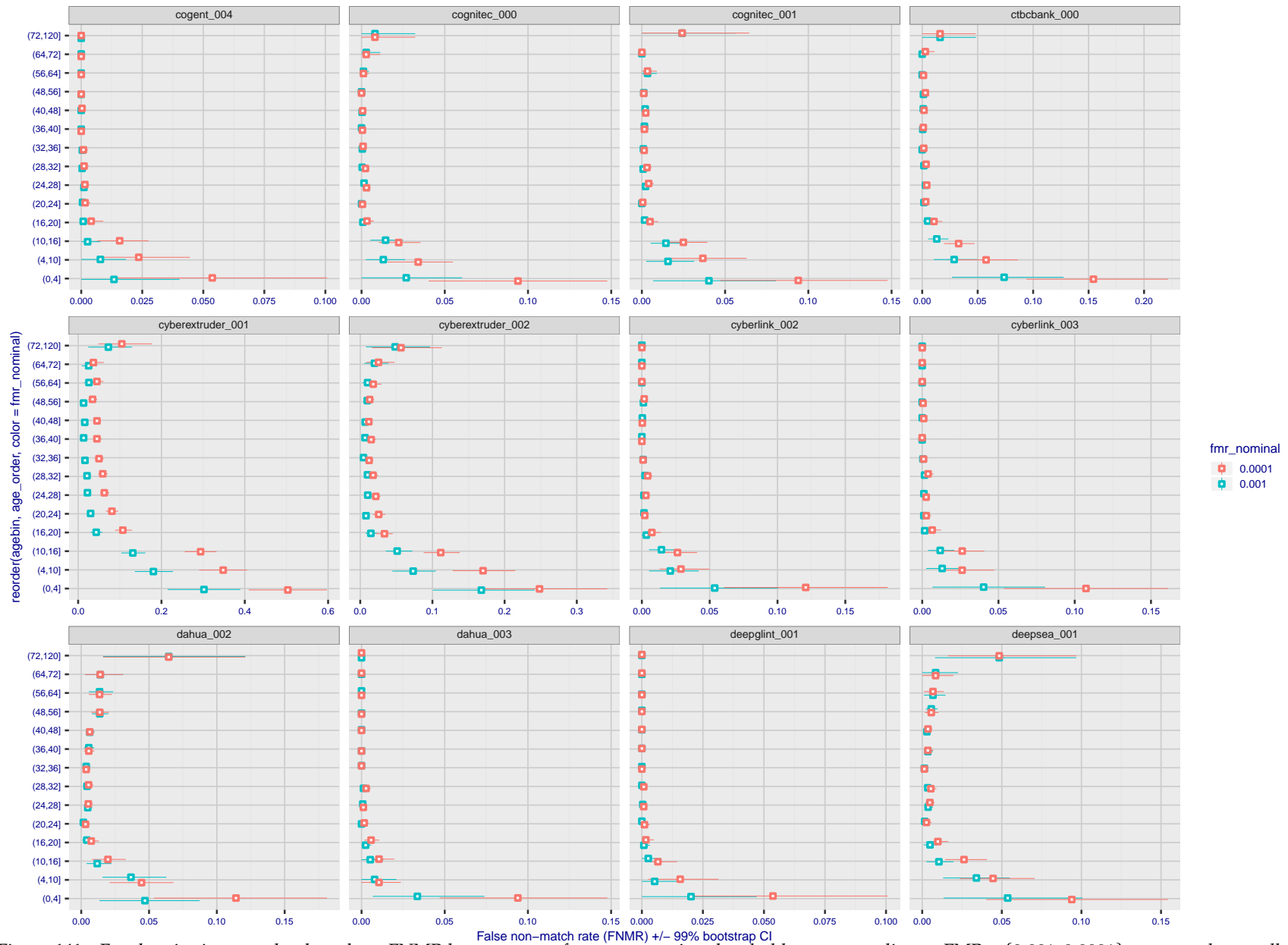


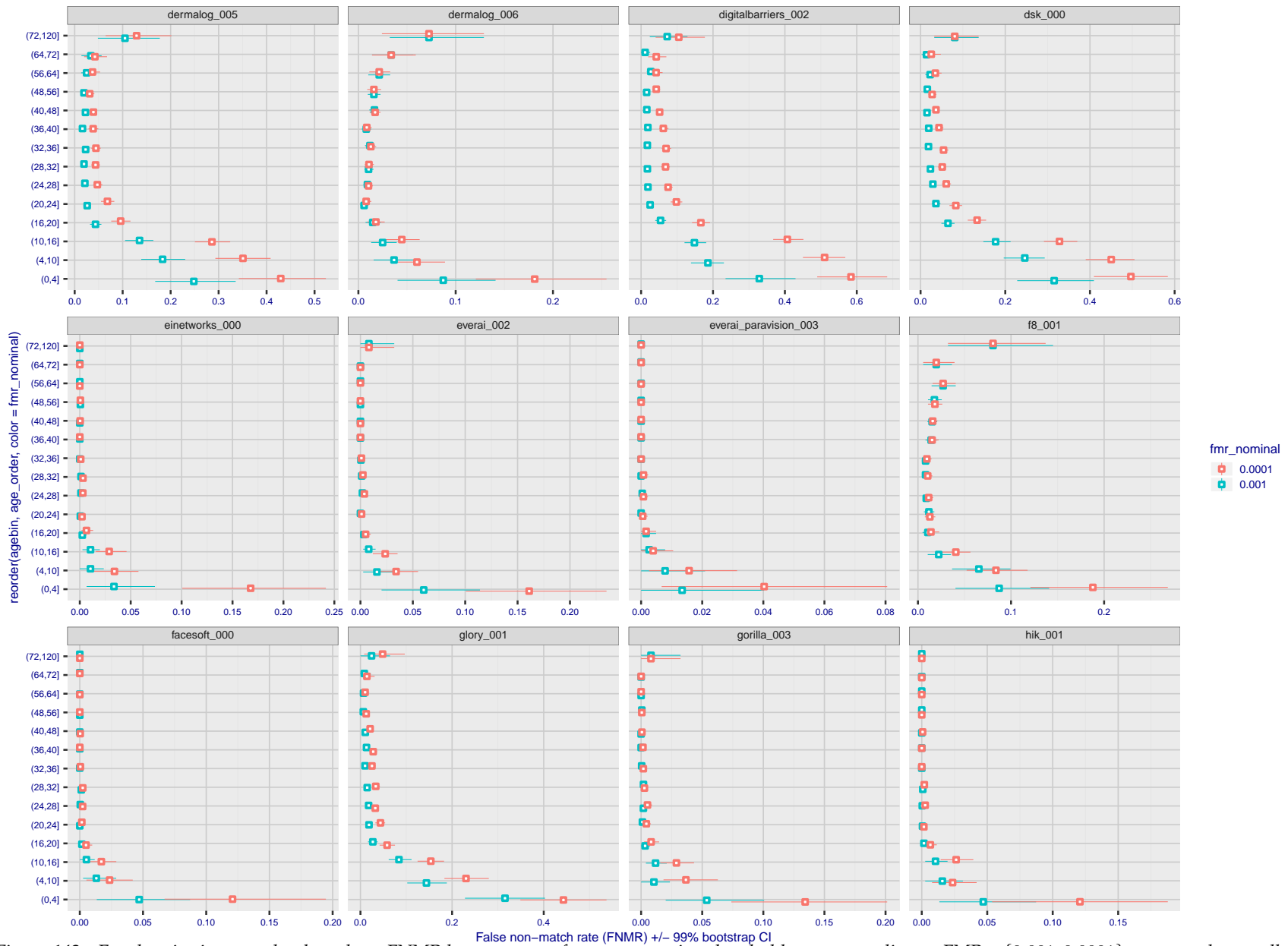
Figure 140: For the visa images, the dots show FNMR by age group for two operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.2. Given a pair of face images taken at different times, we assign the comparison to the bin that is the arithmetic average of the subject's ages. This plot shows only the effect of age, not ageing. The number of comparisons in each bin is generally in the thousands, however the first and last bins are computed over 149 and 124 respectively. The error rates in some (adult) cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"



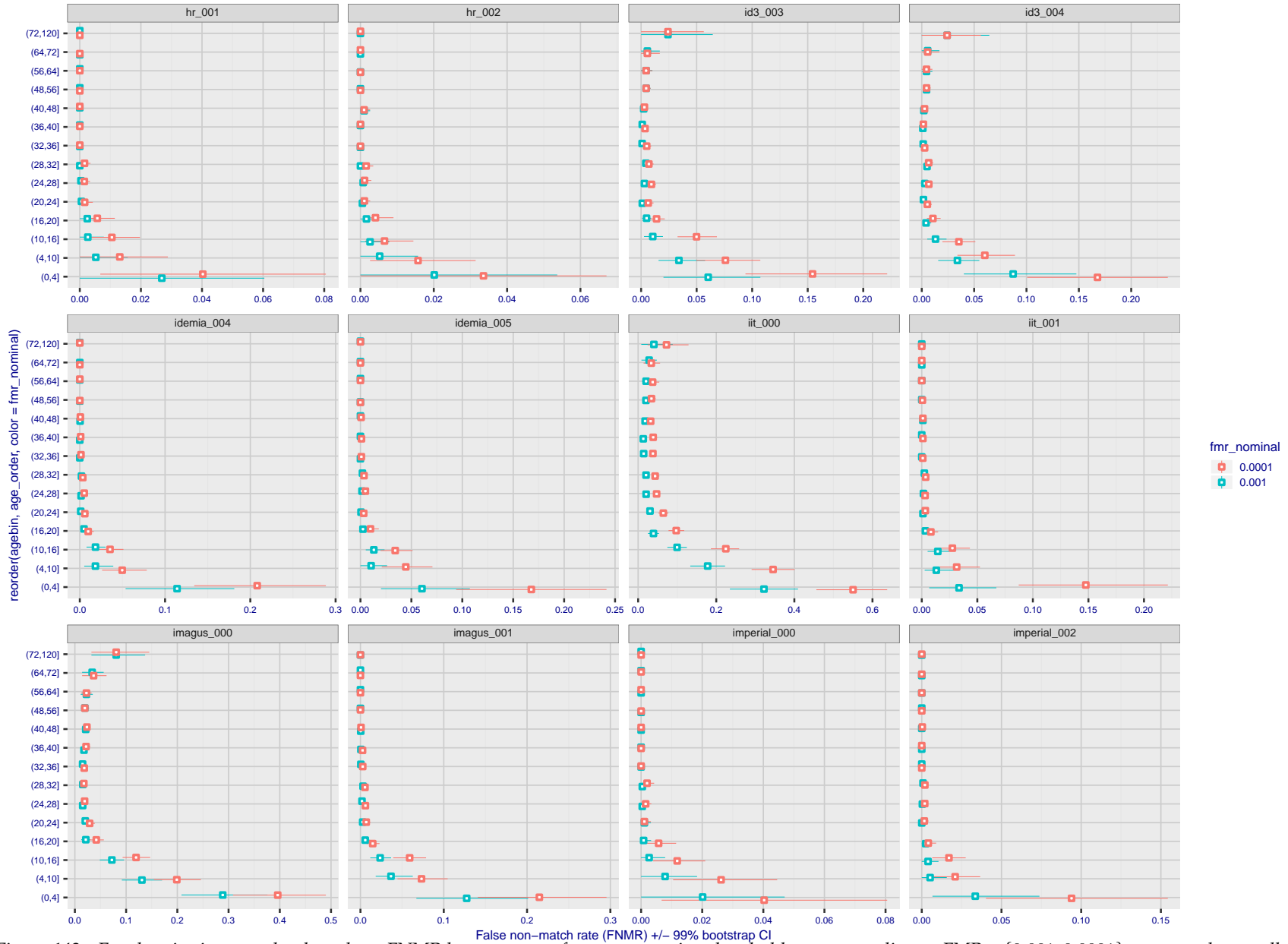
FNMR(T)  
 FMR(T)  
 "False non-match rate"  
 "False match rate"

Figure 141: For the visa images, the dots show FNMR by age group for two operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.2. Given a pair of face images taken at different times, we assign the comparison to the bin that is the arithmetic average of the subject's ages. This plot shows only the effect of age, not ageing. The number of comparisons in each bin is generally in the thousands, however the first and last bins are computed over 149 and 124 respectively. The error rates in some (adult) cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.



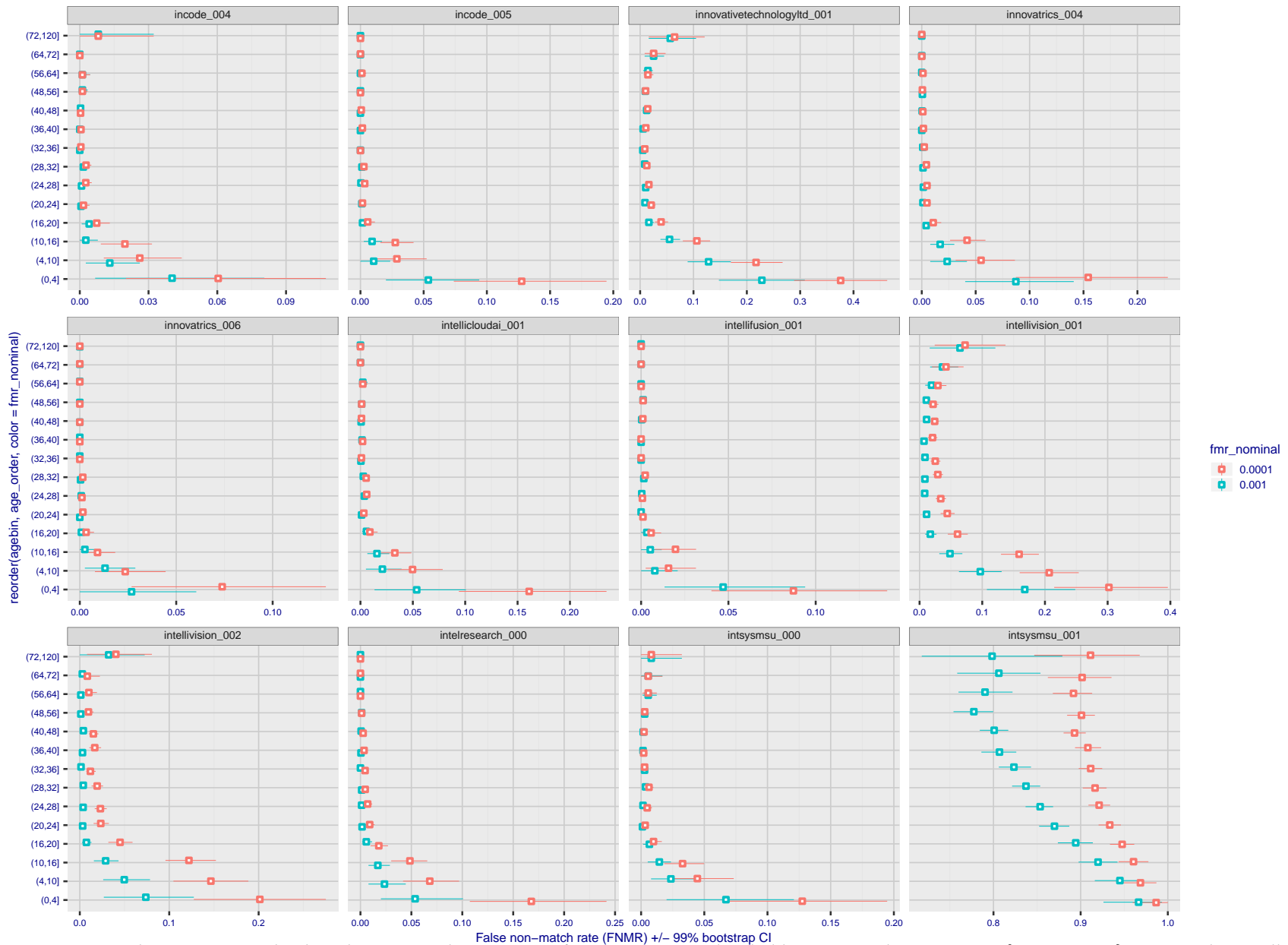
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 142: For the visa images, the dots show FNMR by age group for two operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.2. Given a pair of face images taken at different times, we assign the comparison to the bin that is the arithmetic average of the subject's ages. This plot shows only the effect of age, not ageing. The number of comparisons in each bin is generally in the thousands, however the first and last bins are computed over 149 and 124 respectively. The error rates in some (adult) cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.



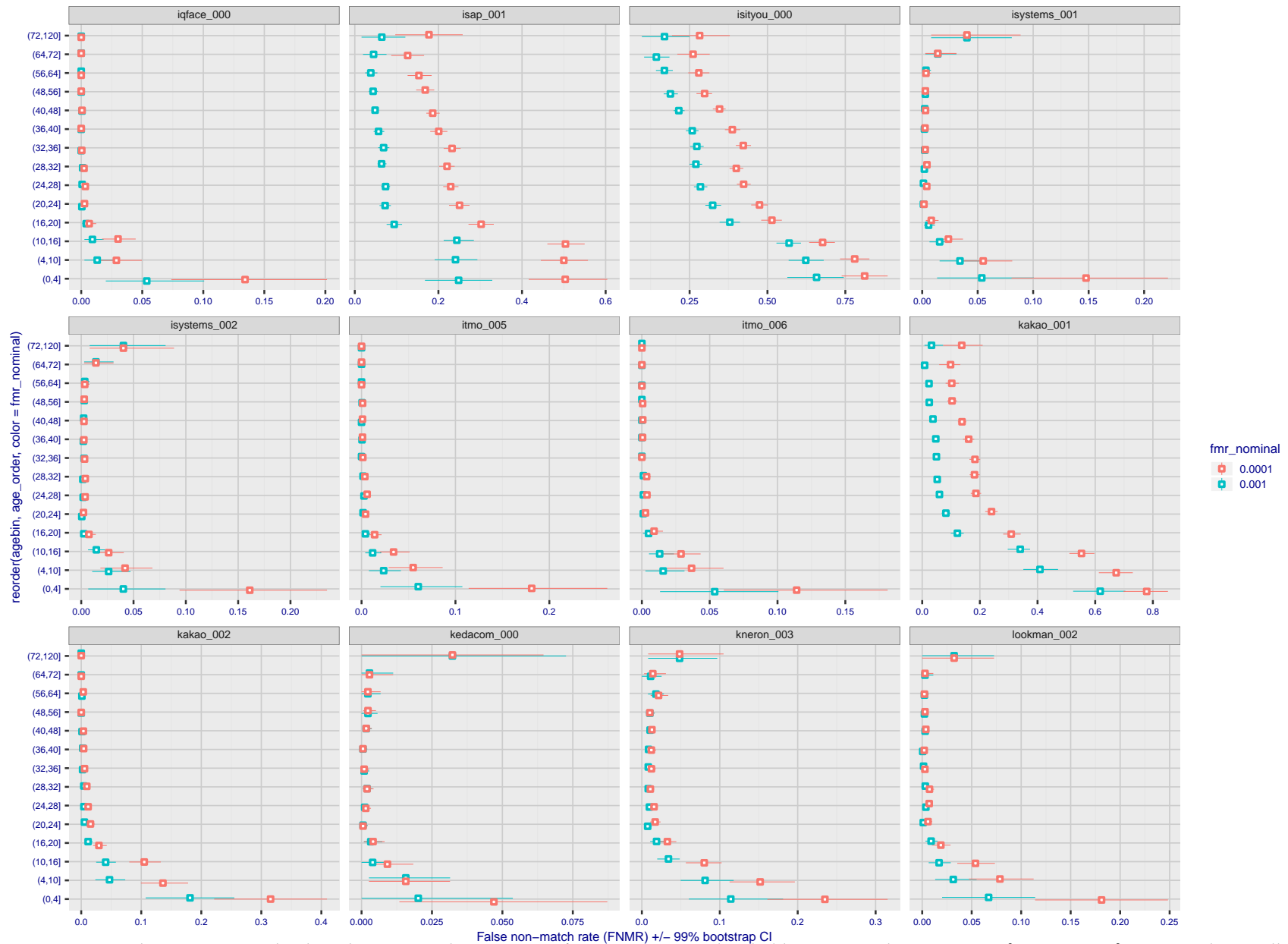
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 143: For the visa images, the dots show FNMR by age group for two operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.2. Given a pair of face images taken at different times, we assign the comparison to the bin that is the arithmetic average of the subject's ages. This plot shows only the effect of age, not ageing. The number of comparisons in each bin is generally in the thousands, however the first and last bins are computed over 149 and 124 respectively. The error rates in some (adult) cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.



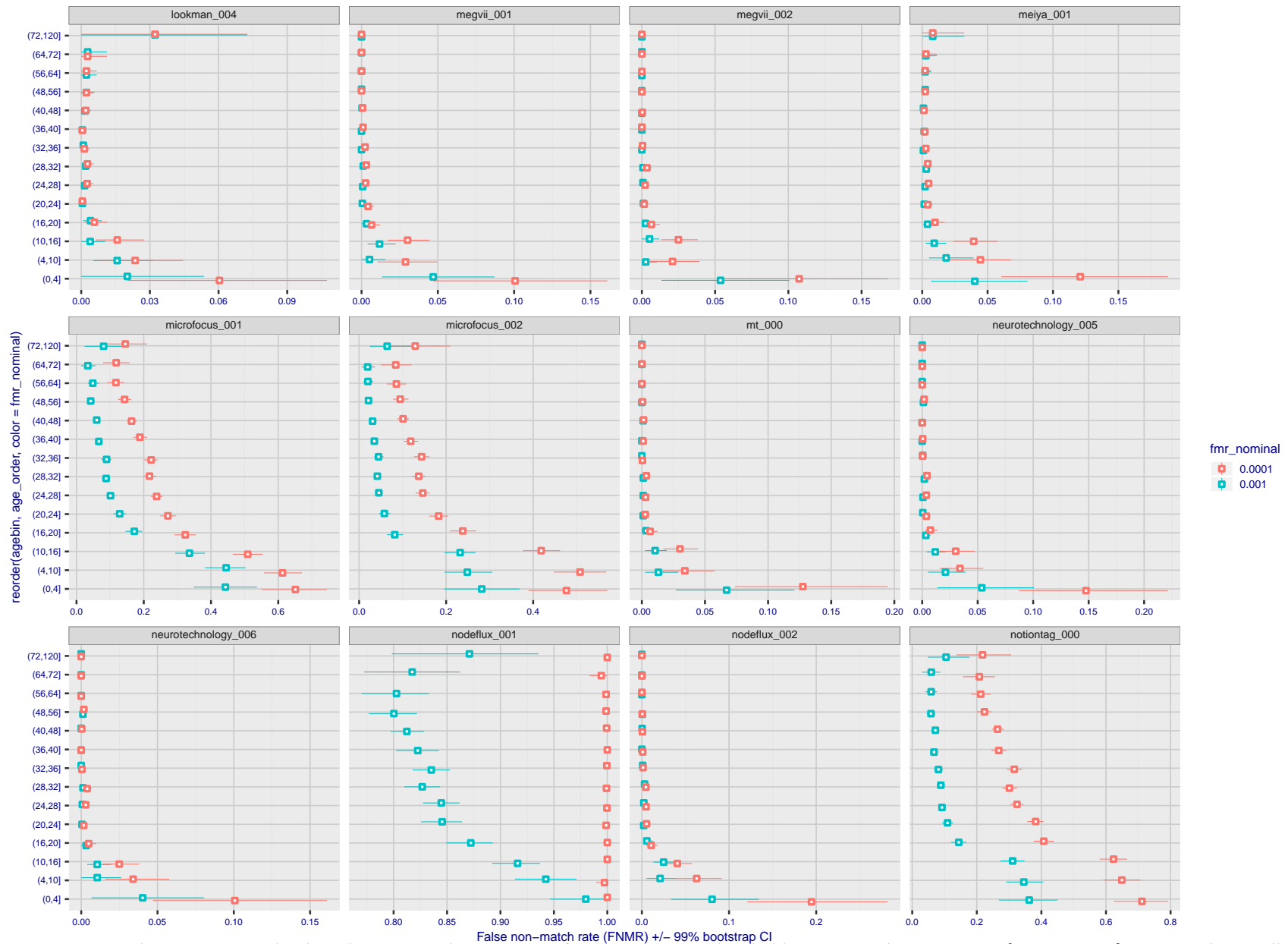
FNMR(T)  
 FMR(T)  
 "False non-match rate"  
 "False match rate"

Figure 144: For the visa images, the dots show FNMR by age group for two operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.2. Given a pair of face images taken at different times, we assign the comparison to the bin that is the arithmetic average of the subject's ages. This plot shows only the effect of age, not ageing. The number of comparisons in each bin is generally in the thousands, however the first and last bins are computed over 149 and 124 respectively. The error rates in some (adult) cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.



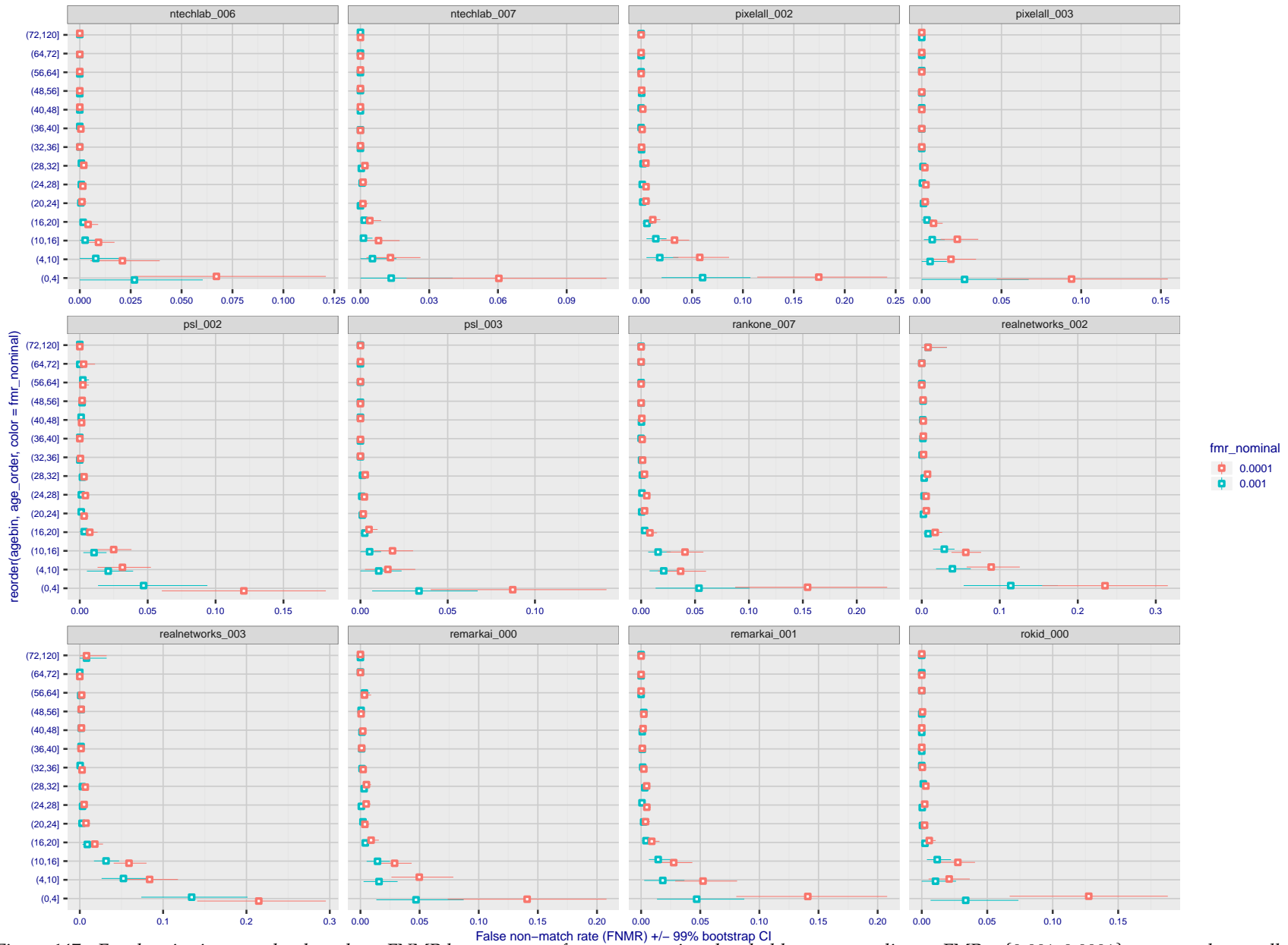
FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 145: For the visa images, the dots show FNMR by age group for two operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.2. Given a pair of face images taken at different times, we assign the comparison to the bin that is the arithmetic average of the subject's ages. This plot shows only the effect of age, not ageing. The number of comparisons in each bin is generally in the thousands, however the first and last bins are computed over 149 and 124 respectively. The error rates in some (adult) cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 146: For the visa images, the dots show FNMR by age group for two operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.2. Given a pair of face images taken at different times, we assign the comparison to the bin that is the arithmetic average of the subject's ages. This plot shows only the effect of age, not ageing. The number of comparisons in each bin is generally in the thousands, however the first and last bins are computed over 149 and 124 respectively. The error rates in some (adult) cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

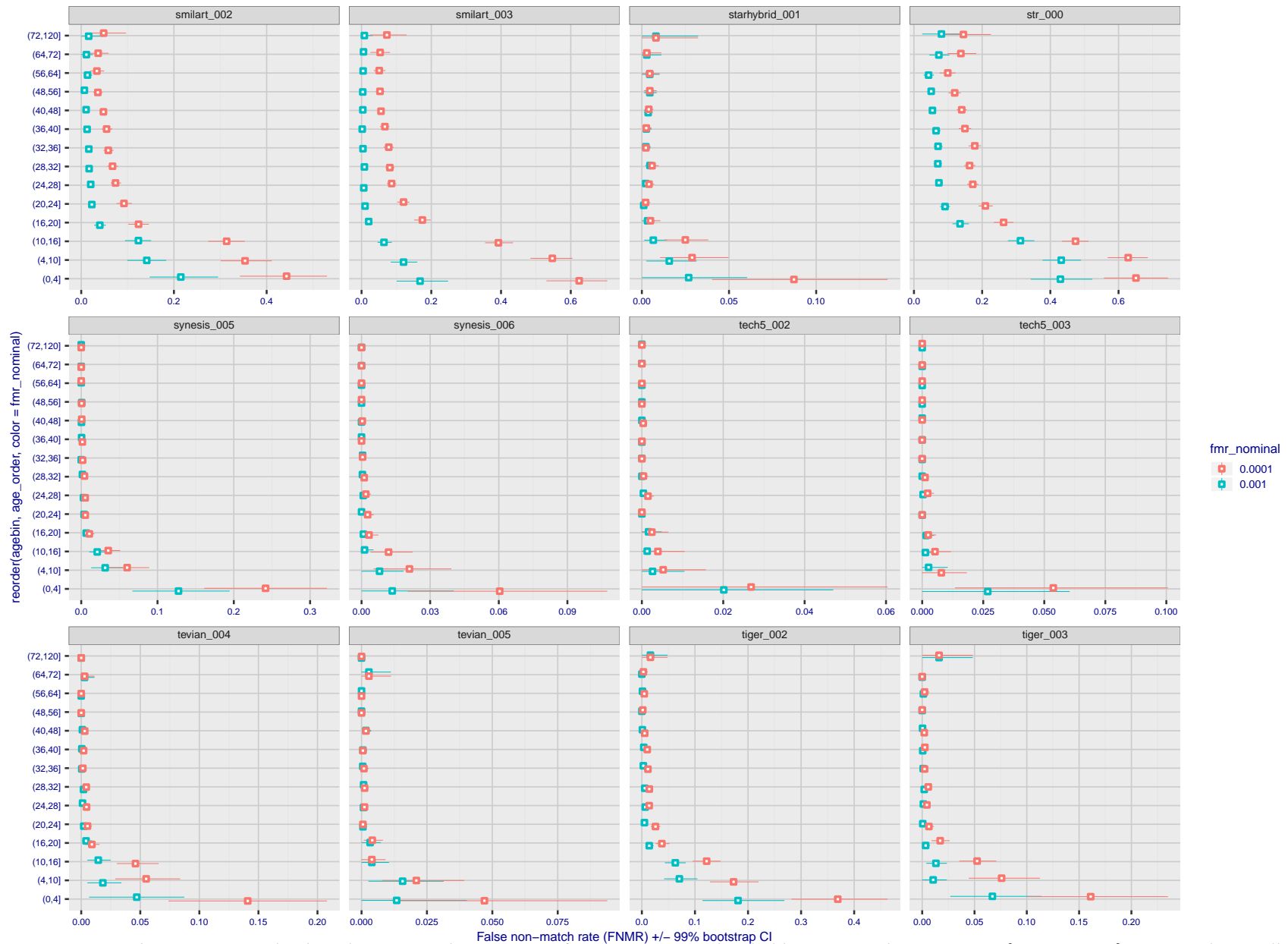
Figure 147: For the visa images, the dots show FNMR by age group for two operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.2. Given a pair of face images taken at different times, we assign the comparison to the bin that is the arithmetic average of the subject's ages. This plot shows only the effect of age, not ageing. The number of comparisons in each bin is generally in the thousands, however the first and last bins are computed over 149 and 124 respectively. The error rates in some (adult) cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.





FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 148: For the visa images, the dots show FNMR by age group for two operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.2. Given a pair of face images taken at different times, we assign the comparison to the bin that is the arithmetic average of the subject's ages. This plot shows only the effect of age, not ageing. The number of comparisons in each bin is generally in the thousands, however the first and last bins are computed over 149 and 124 respectively. The error rates in some (adult) cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 149: For the visa images, the dots show FNMR by age group for two operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.2. Given a pair of face images taken at different times, we assign the comparison to the bin that is the arithmetic average of the subject's ages. This plot shows only the effect of age, not ageing. The number of comparisons in each bin is generally in the thousands, however the first and last bins are computed over 149 and 124 respectively. The error rates in some (adult) cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.

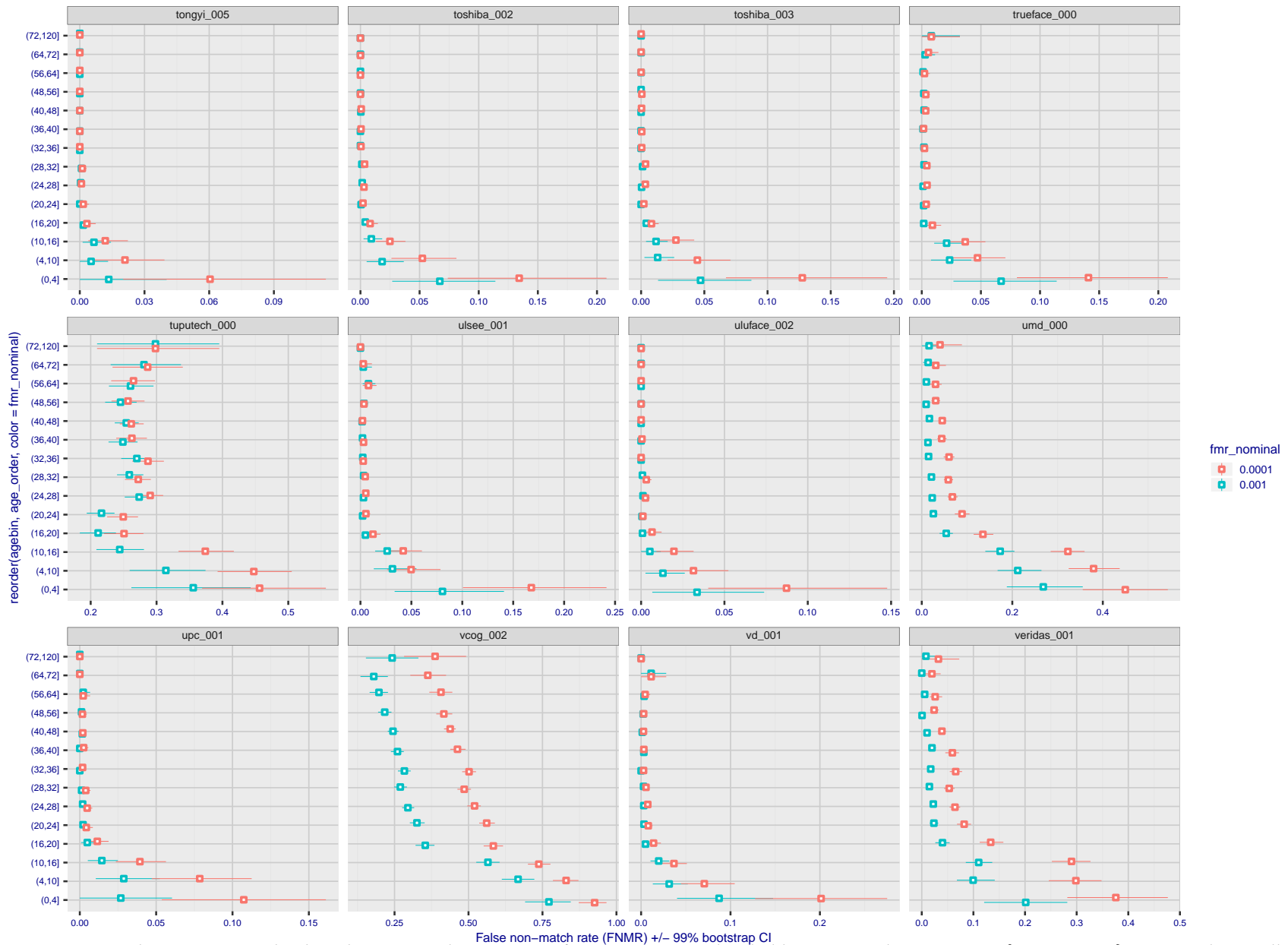


Figure 150: For the visa images, the dots show FNMR by age group for two operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.2. Given a pair of face images taken at different times, we assign the comparison to the bin that is the arithmetic average of the subject's ages. This plot shows only the effect of age, not ageing. The number of comparisons in each bin is generally in the thousands, however the first and last bins are computed over 149 and 124 respectively. The error rates in some (adult) cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.

FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

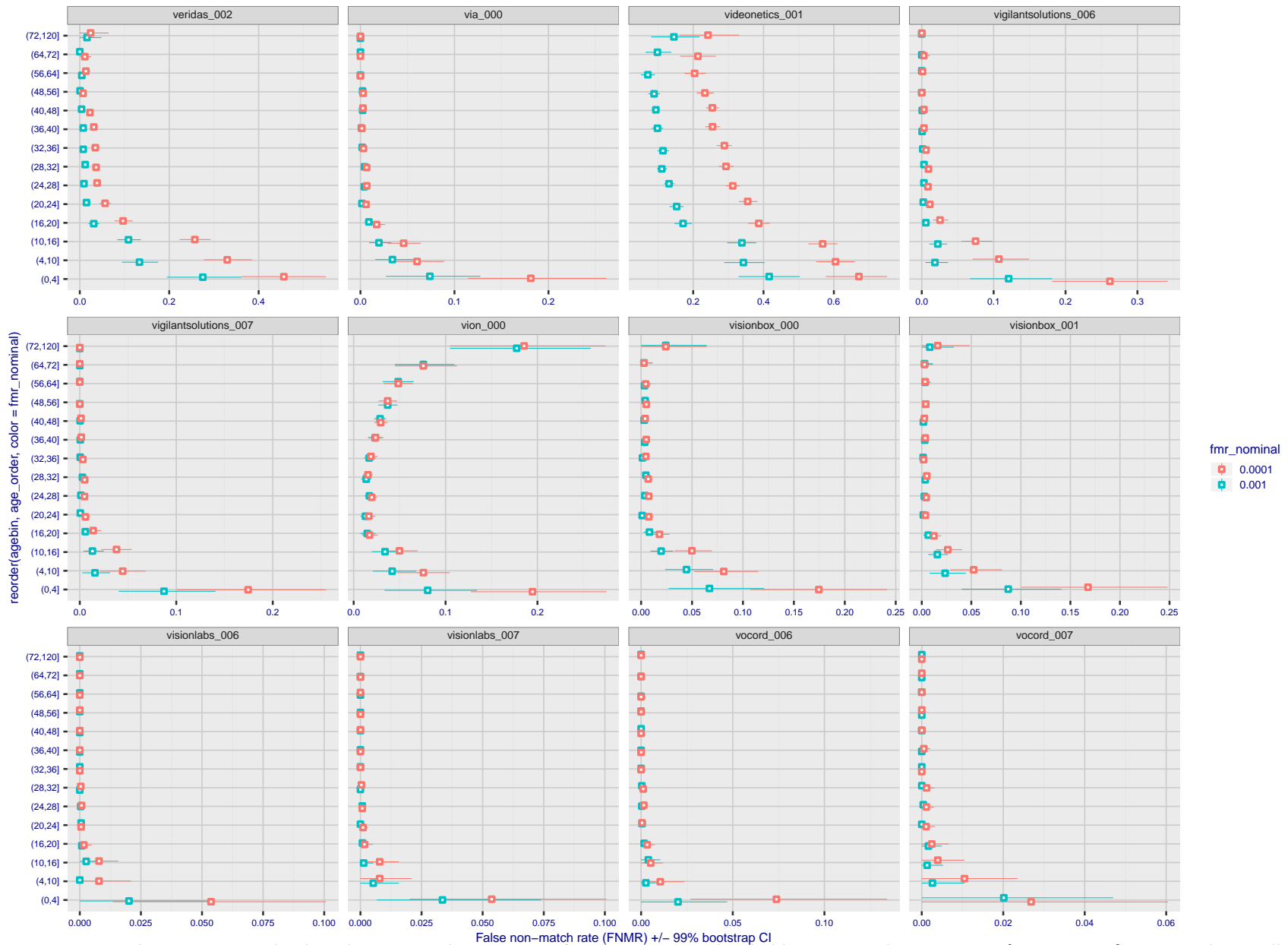


Figure 151: For the visa images, the dots show FNMR by age group for two operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.2. Given a pair of face images taken at different times, we assign the comparison to the bin that is the arithmetic average of the subject's ages. This plot shows only the effect of age, not ageing. The number of comparisons in each bin is generally in the thousands, however the first and last bins are computed over 149 and 124 respectively. The error rates in some (adult) cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.



FNMR(T)  
FMR(T)  
"False non-match rate"  
"False match rate"

Figure 152: For the visa images, the dots show FNMR by age group for two operating thresholds corresponding to  $FMR = \{0.001, 0.0001\}$  computed over all on the order of  $10^{10}$  impostor scores. The FMR in each bin will vary also - see subsequent impostor heatmaps in sec. 3.6.2. Given a pair of face images taken at different times, we assign the comparison to the bin that is the arithmetic average of the subject's ages. This plot shows only the effect of age, not ageing. The number of comparisons in each bin is generally in the thousands, however the first and last bins are computed over 149 and 124 respectively. The error rates in some (adult) cases are zero, and in others the DET is flat so the error rates at the two thresholds are identical. The lines span 1% and 99% of bootstrap replicated FNMR estimates.

**Caveats:** None.

## 3.6 Impostor distribution stability

### 3.6.1 Effect of birth place on the impostor distribution

**Background:** Facial appearance varies geographically, both in terms of skin tone, cranio-facial structure and size. This section addresses whether false match rates vary intra- and inter-regionally.

**Goals:**

- ▷ To show the effect of birth region of the impostor and enrollee on false match rates.
- ▷ To determine whether some algorithms give better impostor distribution stability.

**Methods:**

- ▷ For the visa images, NIST defined 10 regions: Sub-Saharan Africa, South Asia, Polynesia, North Africa, Middle East, Europe, East Asia, Central and South America, Central Asia, and the Caribbean.
- ▷ For the visa images, NIST mapped each country of birth to a region. There is some arbitrariness to this. For example, Egypt could reasonably be assigned to the Middle East instead of North Africa. An alternative methodology could, for example, assign the Philippines to *both* Polynesia and East Asia.
- ▷ FMR is computed for cases where all face images of impostors born in region  $r_2$  are compared with enrolled face images of persons born in region  $r_1$ .

$$\text{FMR}(r_1, r_2, T) = \frac{\sum_{i=1}^{N_{r_1, r_2}} H(s_i - T)}{N_{r_1, r_2}} \quad (5)$$

where the same threshold,  $T$ , is used in all cells, and  $H$  is the unit step function. The threshold is set to give  $\text{FMR}(T) = 0.001$  over the entire set of visa image impostor comparisons.

- ▷ This analysis is then repeated by country-pair, but only for those country pairs where both have at least 1000 images available. The countries<sup>1</sup> appear in the axes of graphs that follow.
- ▷ The mean number of impostor scores in any cross-region bin is 33 million. The smallest number of impostor scores in any bin is 135000, for Central Asia - North Africa. While these counts are large enough to support reasonable significance, the number of individual faces is much smaller, on the order of  $N^{0.5}$ .
- ▷ The numbers of impostor scores in any cross-country bin is shown in Figure 486.

**Results:** Subsequent figures show heatmaps that use color to represent the base-10 logarithm of the false match rate. Red colors indicate high (bad) false match rates. Dark colors indicate benign false match rates. There are two series of graphs corresponding to aggregated geographical regions, and to countries. The notable observations are:

- ▷ The on-diagonal elements correspond to within-region impostors. FMR is generally above the nominal value of  $\text{FMR} = 0.001$ . Particularly there is usually higher FMR in, Sub-Saharan Africa, South Asia, and the Caribbean. Europe and Central Asia, on the other hand, usually give FMR closer to the nominal value.
- ▷ The off-diagonal elements correspond to across-region impostors. The highest FMR is produced between the Caribbean and Sub-Saharan Africa.
- ▷ Algorithms vary.

<sup>1</sup>These are Argentina, Australia, Brazil, Chile, China, Costa Rica, Cuba, Czech Republic, Dominican Republic, Ecuador, Egypt, El Salvador, Germany, Ghana, Great Britain, Greece, Guatemala, Haiti, Hong Kong, Honduras, Indonesia, India, Israel, Jamaica, Japan, Kenya, Korea, Lebanon, Mexico, Malaysia, Nepal, Nigeria, Peru, Philippines, Pakistan, Poland, Romania, Russia, South Africa, Saudi Arabia, Thailand, Trinidad, Turkey, Taiwan, Ukraine, Venezuela, and Vietnam.





- ▷ We computed the same quantities for a global FMR = 0.0001. The effects are similar.

**Caveats:**

- ▷ The effects of variable impostor rates on one-to-many identification systems may well differ from what's implied by these one-to-one verification results. Two reasons for this are a) the enrollment galleries are usually imbalanced across countries of birth, age and sex; b) one-to-many identification algorithms often implement techniques aimed at stabilizing the impostor distribution. Further research is necessary.
- ▷ In principle, the effects seen in this subsection could be due to differences in the image capture process. We consider this unlikely since the effects are maintained across geography - e.g. Caribbean vs. Africa, or Japan vs. China.

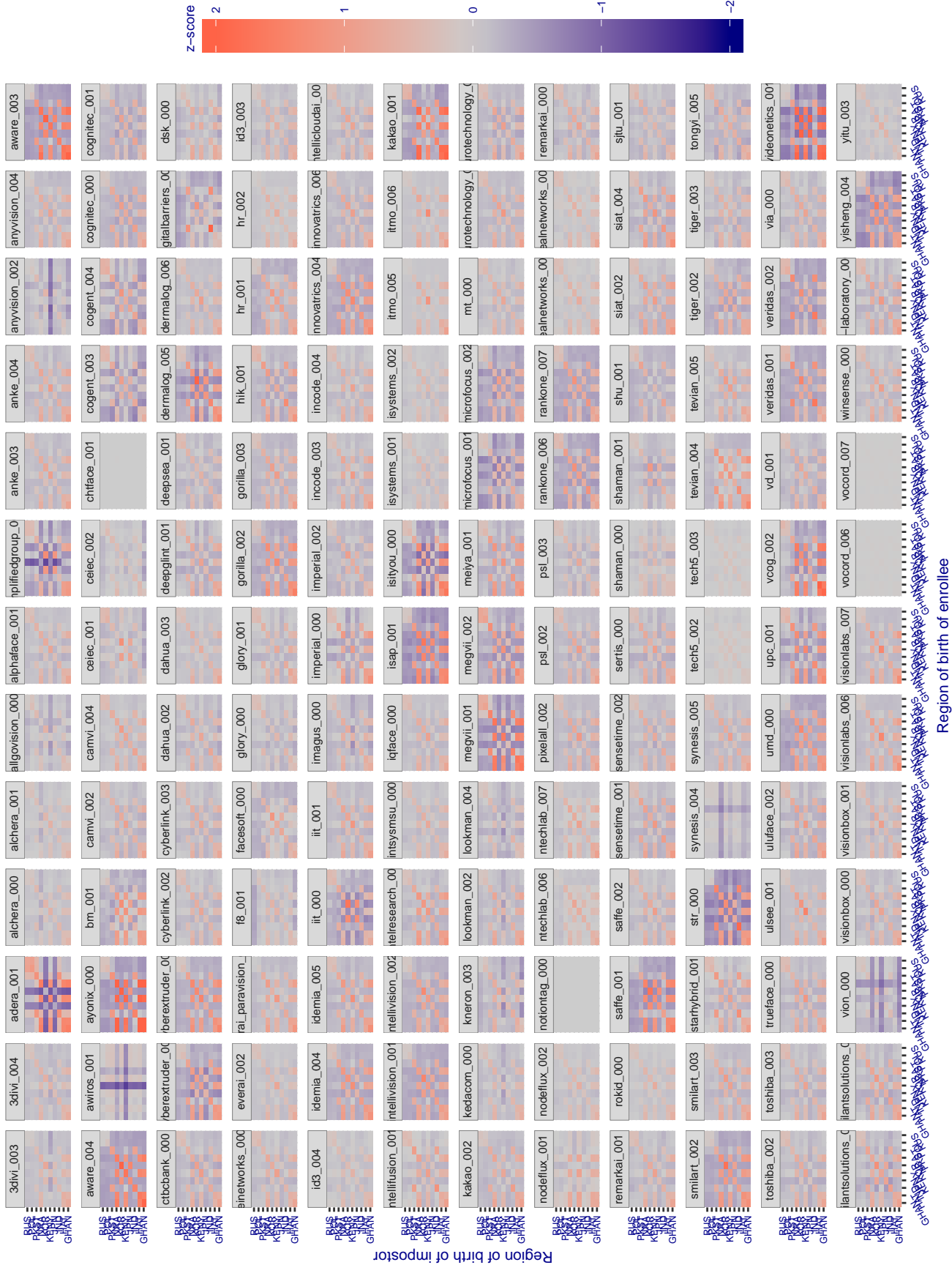


Figure 154: For visa images, the heatmap shows how the mean of the impostor distribution for the country pair (a,b) is shifted relative to the mean of the global impostor distribution, expressed as a number of standard deviations of the global impostor distribution. This statistic is designed to show shifts in the entire impostor distribution, not just tail effects that manifest as the anomalously high (or low) false match rates that appear in the subsequent figures. The countries are chosen to show that skin tone alone does not explain impostor distribution shifts. The reduced shift in Asian populations with the Yitu and TongYiTrans algorithms, is accompanied by positive shifts in the European populations. This reversal relative to most other algorithms, may derive from use of nationally weighted training sets. The Visionlabs algorithm appears most insensitive to country effects. The figure is computed from same-sex and same-age impostor pairs.

Cross region FMR at threshold  $T = 2.740$  for algorithm 3divi\_003, giving  $FMR(T) = 0.0001$  globally.

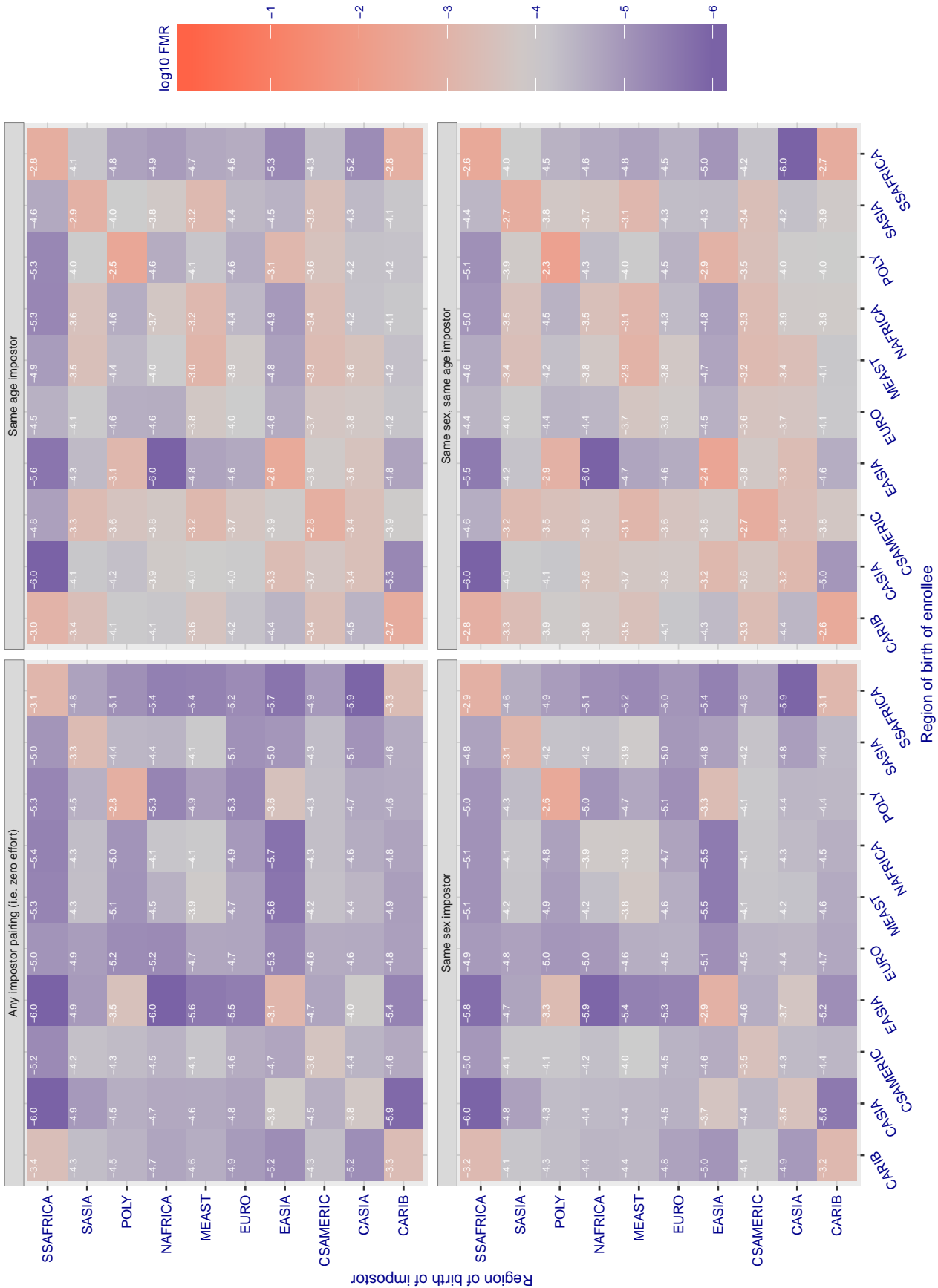


Figure 155: For algorithm 3divi-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 2.857$  for algorithm 3divi\_004, giving  $FMR(T) = 0.0001$  globally.

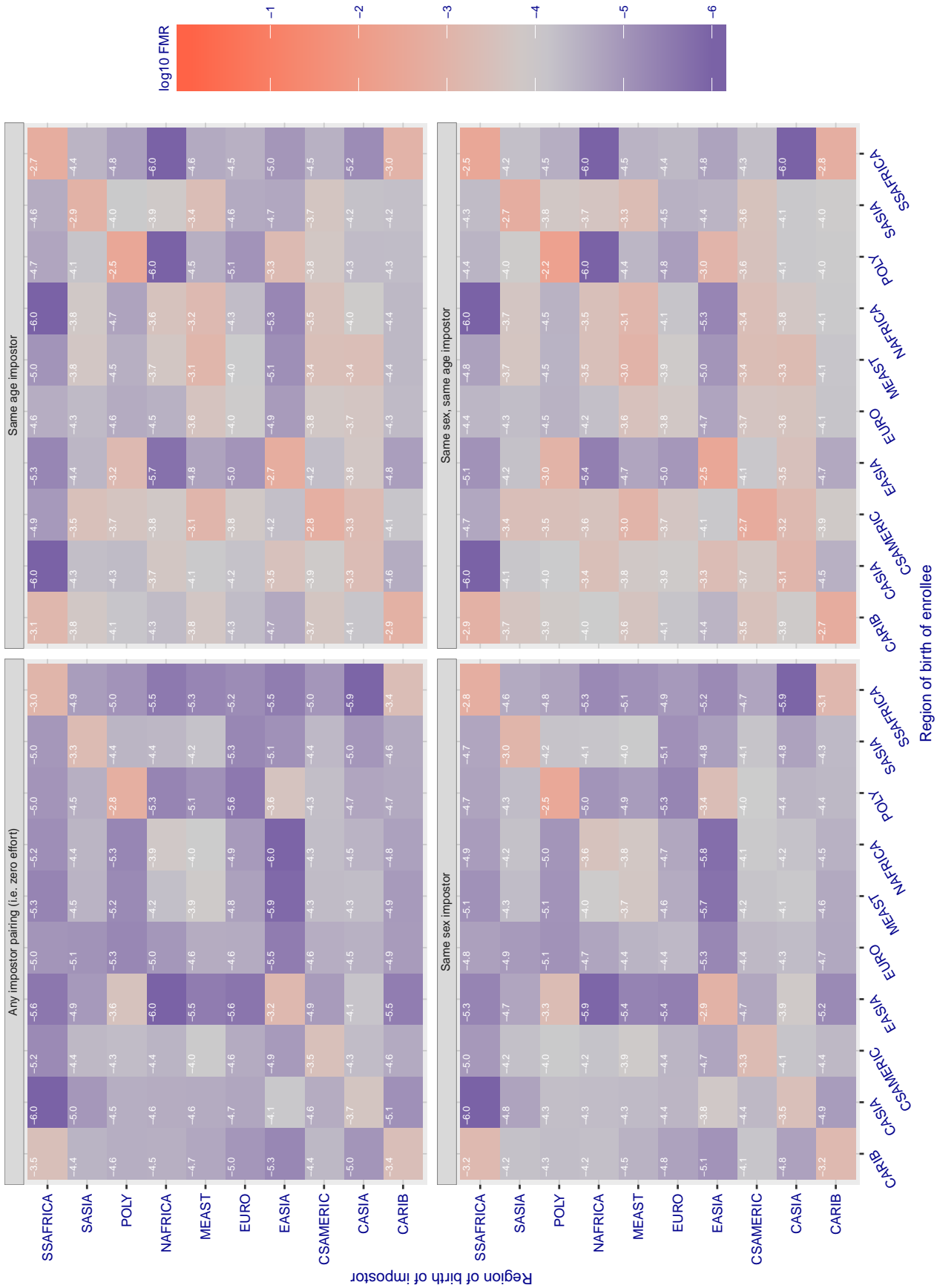


Figure 156: For algorithm 3divi-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.713$  for algorithm adera\_001, giving  $FMR(T) = 0.0001$  globally.

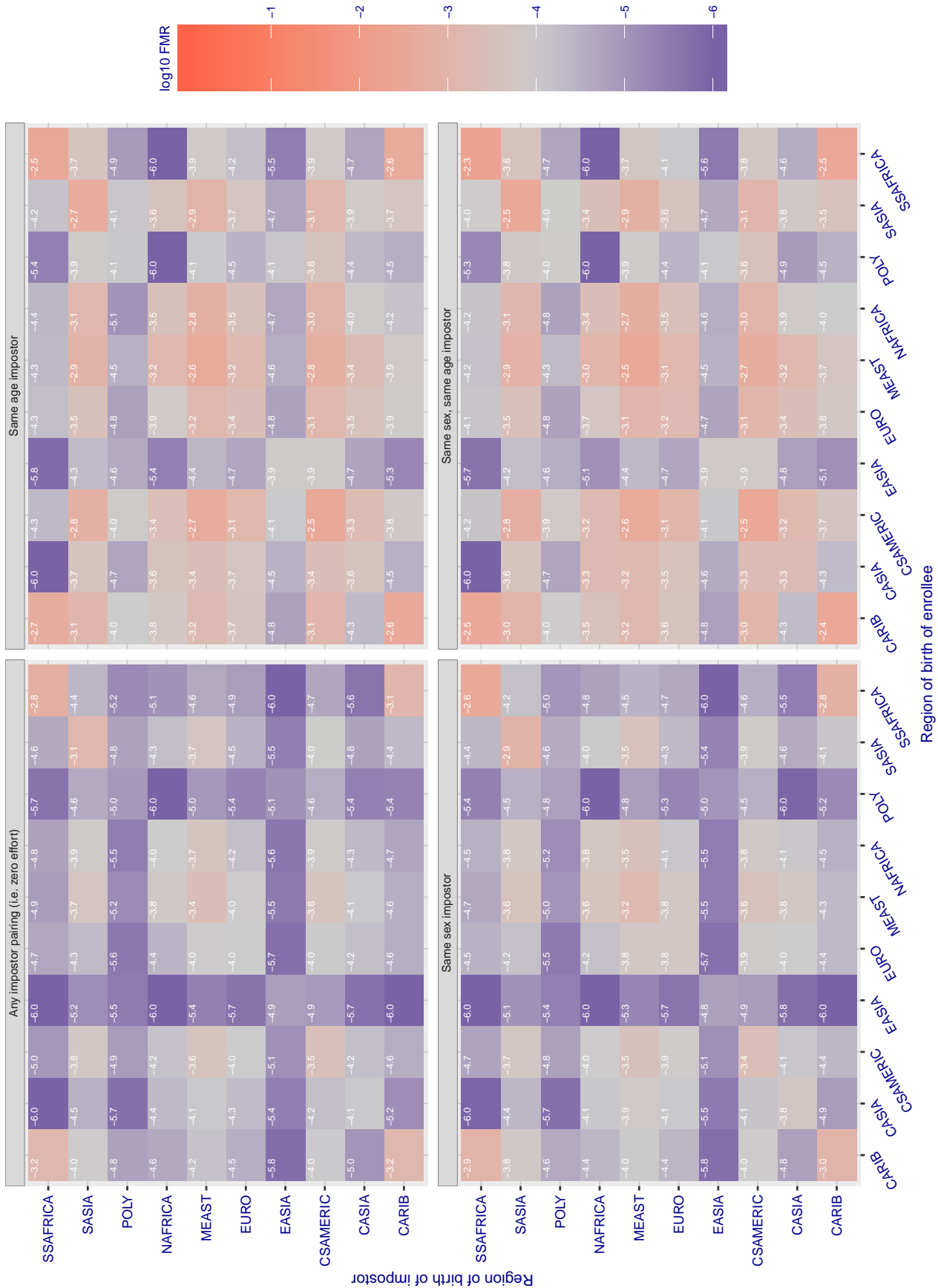


Figure 157: For algorithm adera-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.592$  for algorithm aim1\_001, giving  $FMR(T) = 0.0001$  globally.

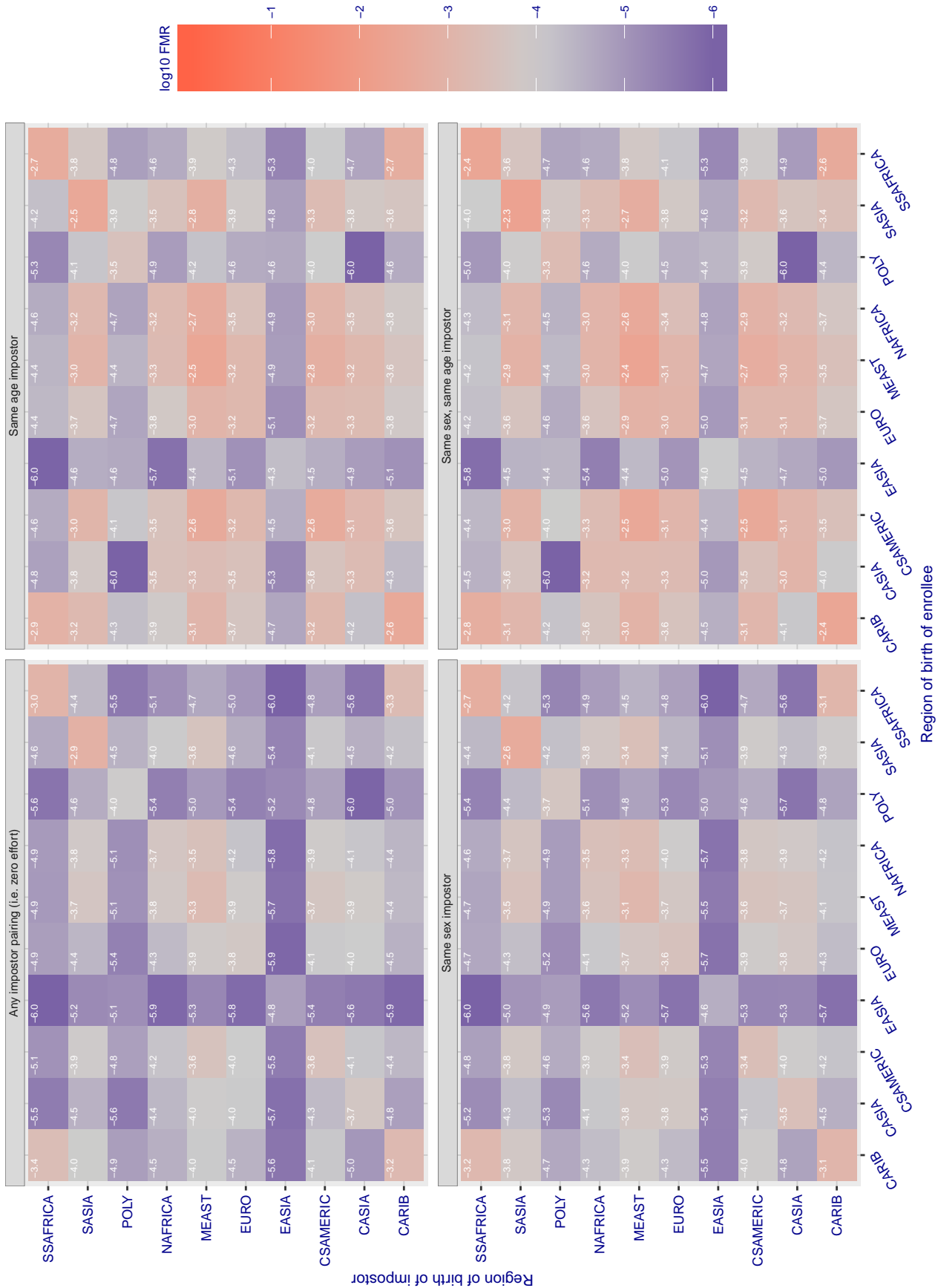


Figure 158: For algorithm aim1-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.699$  for algorithm aiunionface\_000, giving  $FMR(T) = 0.0001$  globally.

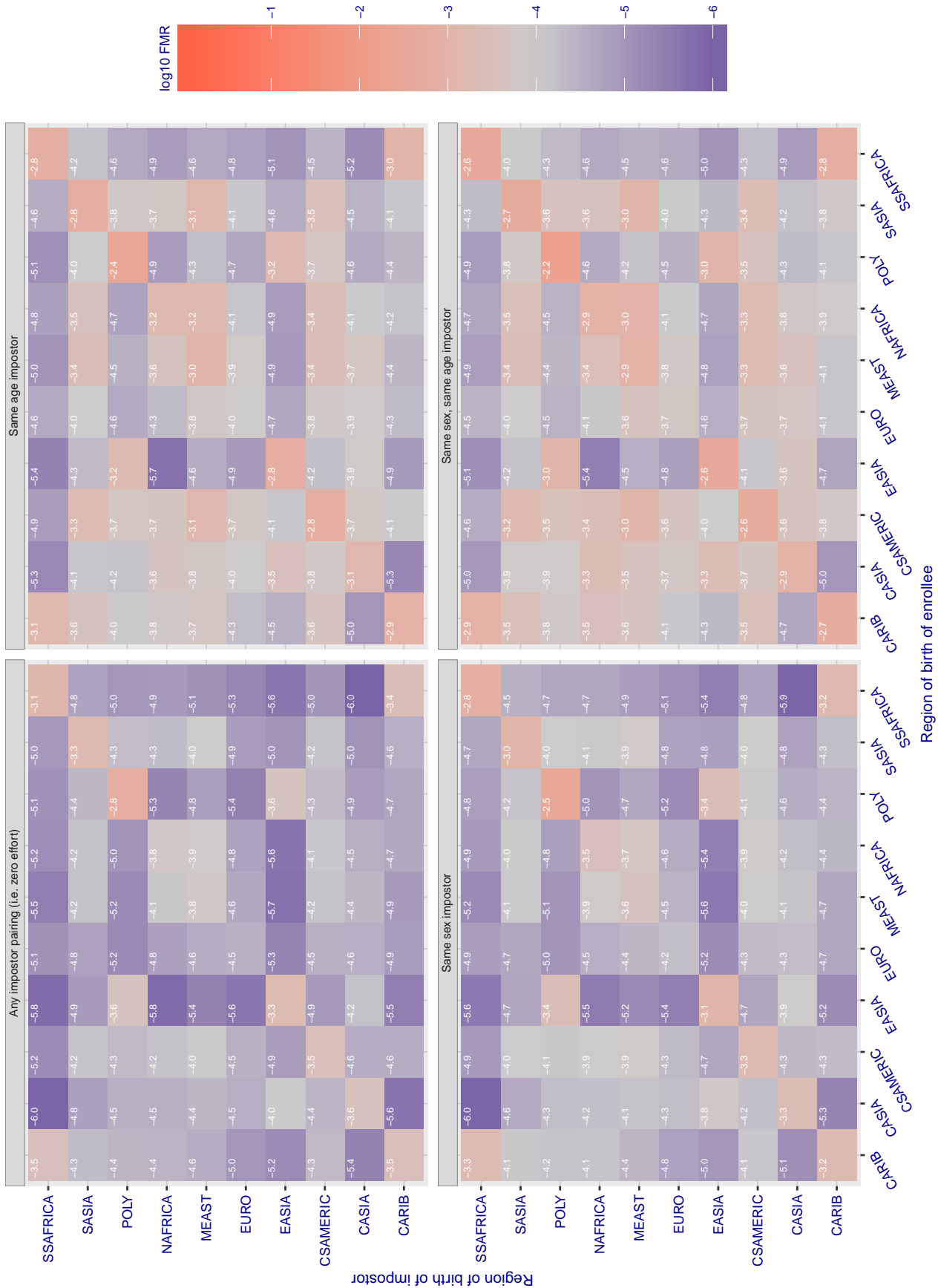


Figure 159: For algorithm aiunionface-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 0.702$  for algorithm alchera\_000, giving  $FMR(T) = 0.0001$  globally.

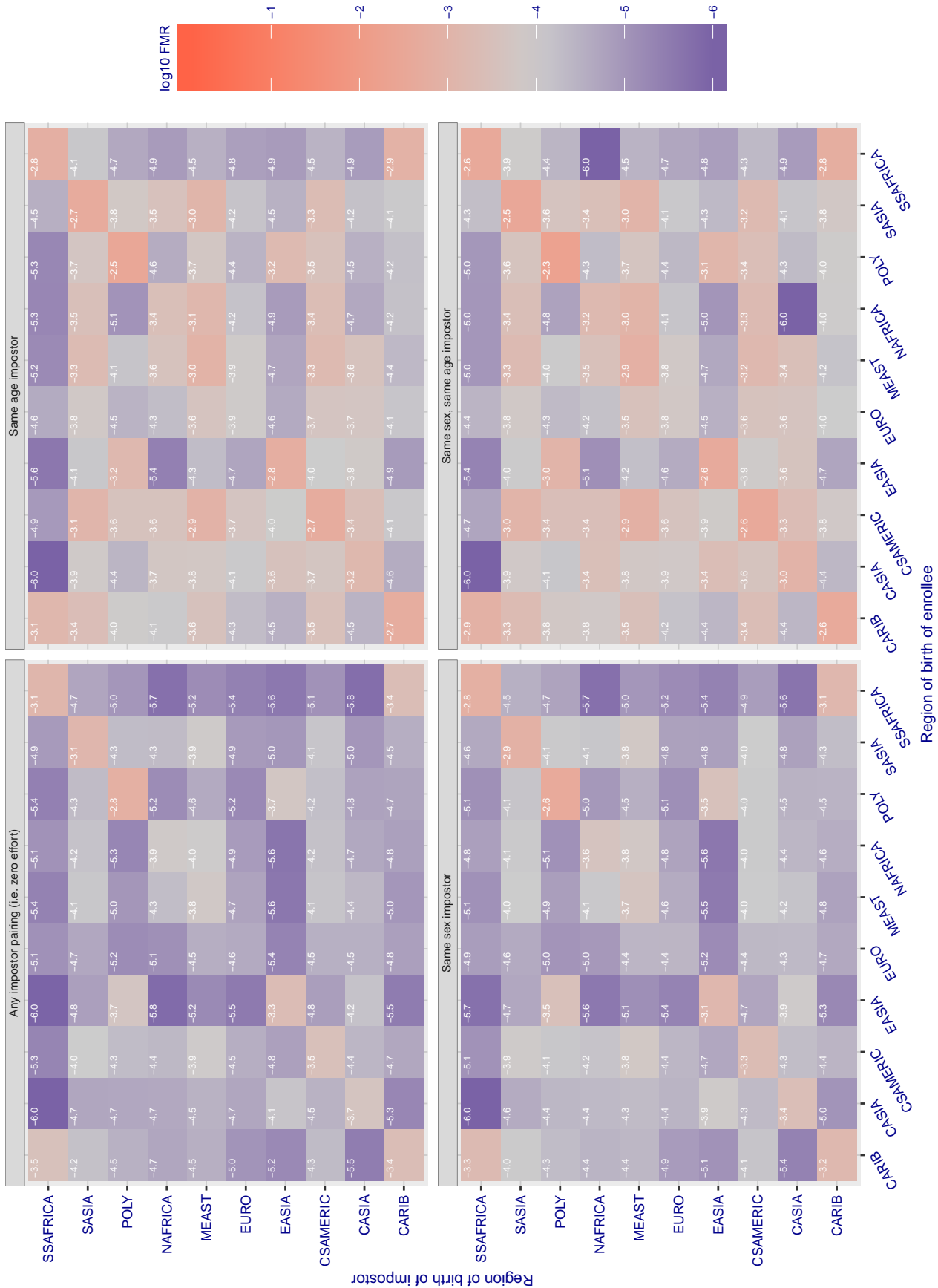


Figure 160: For algorithm alchera-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 0.713$  for algorithm alchera\_001, giving  $FMR(T) = 0.0001$  globally.

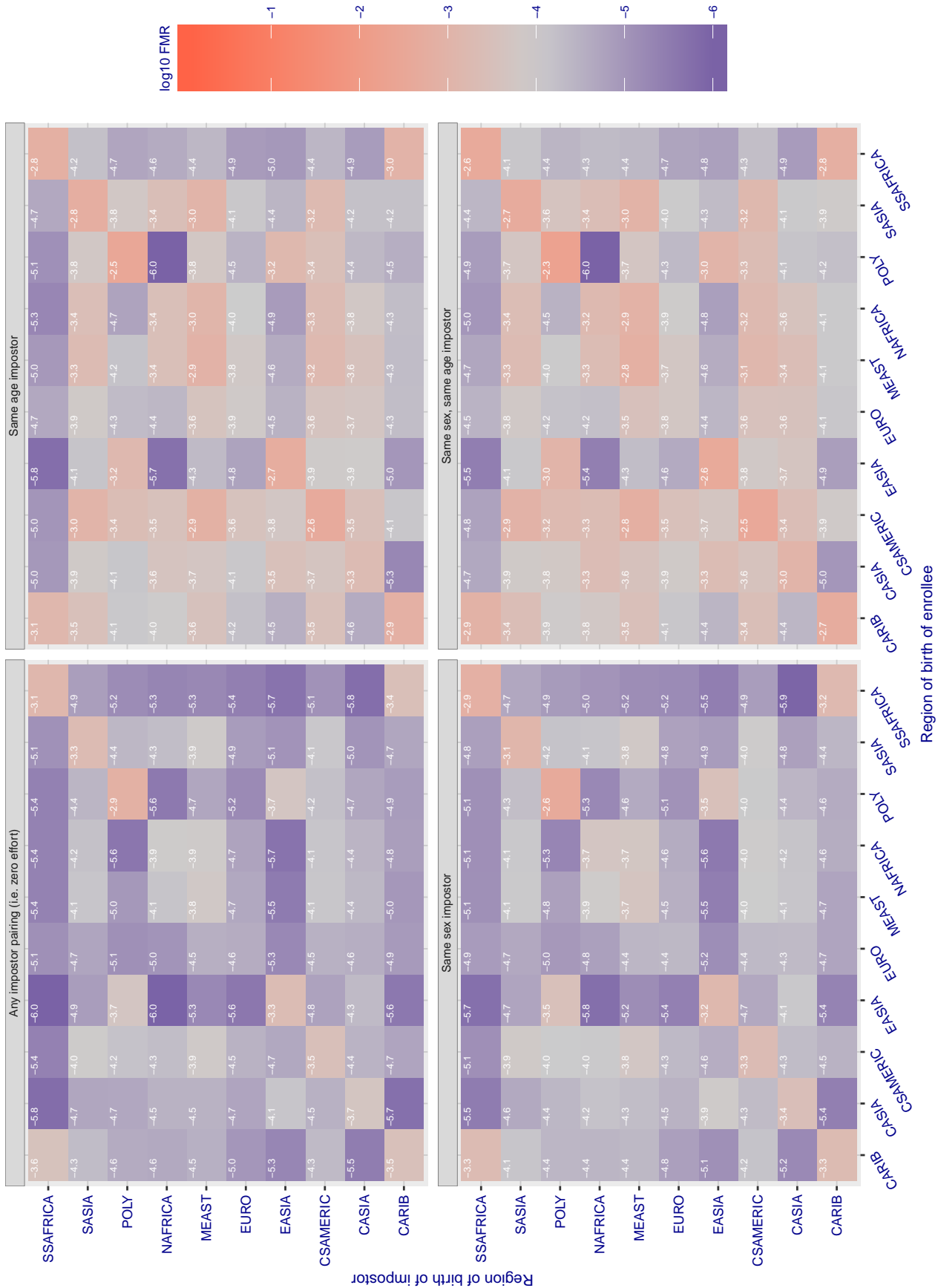


Figure 161: For algorithm alchera-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.433$  for algorithm allgvision\_000, giving  $FMR(T) = 0.0001$  globally.

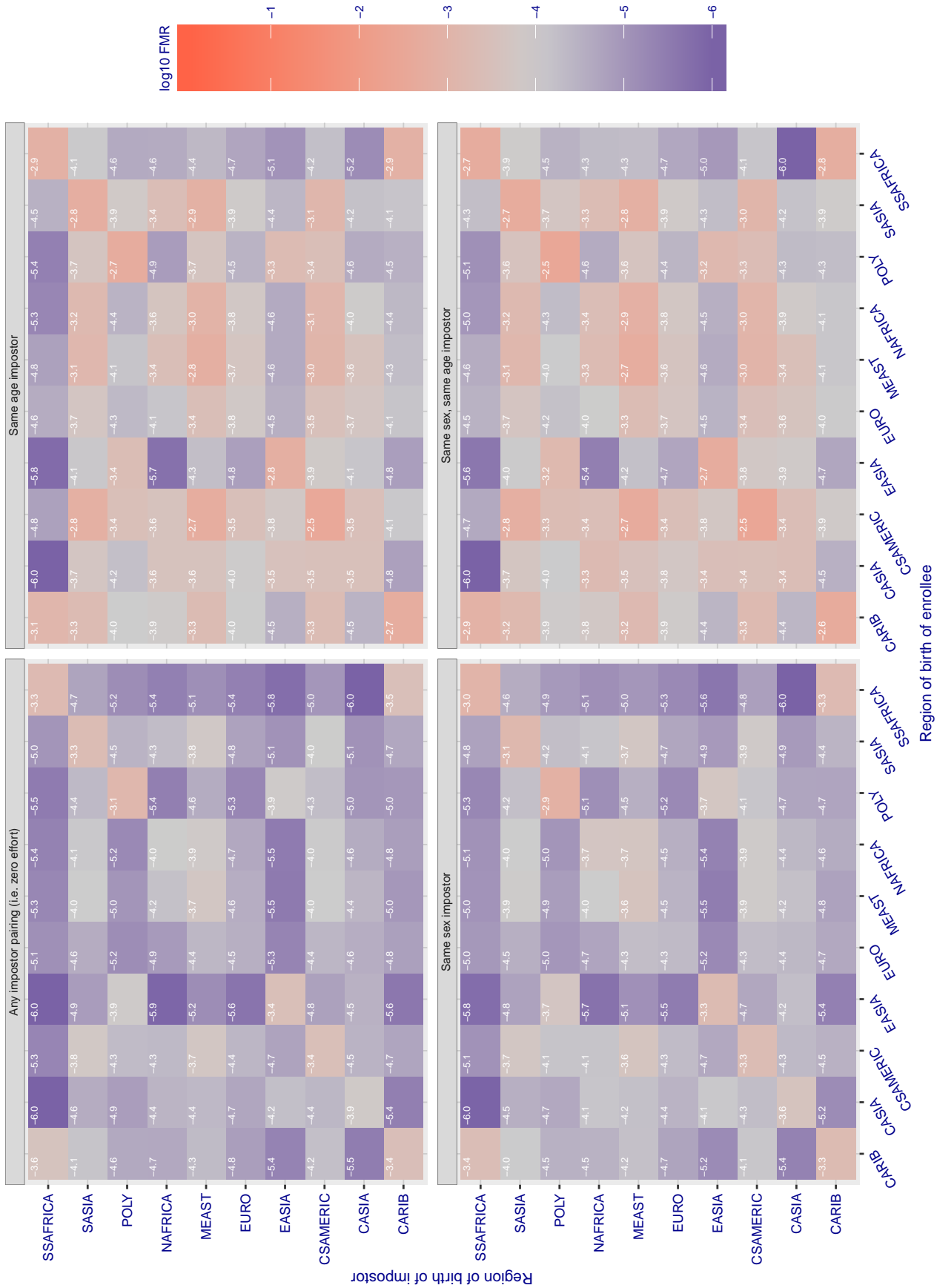


Figure 162: For algorithm allgvision-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 0.396 for algorithm alphaface\_001, giving FMR(T) = 0.0001 globally.

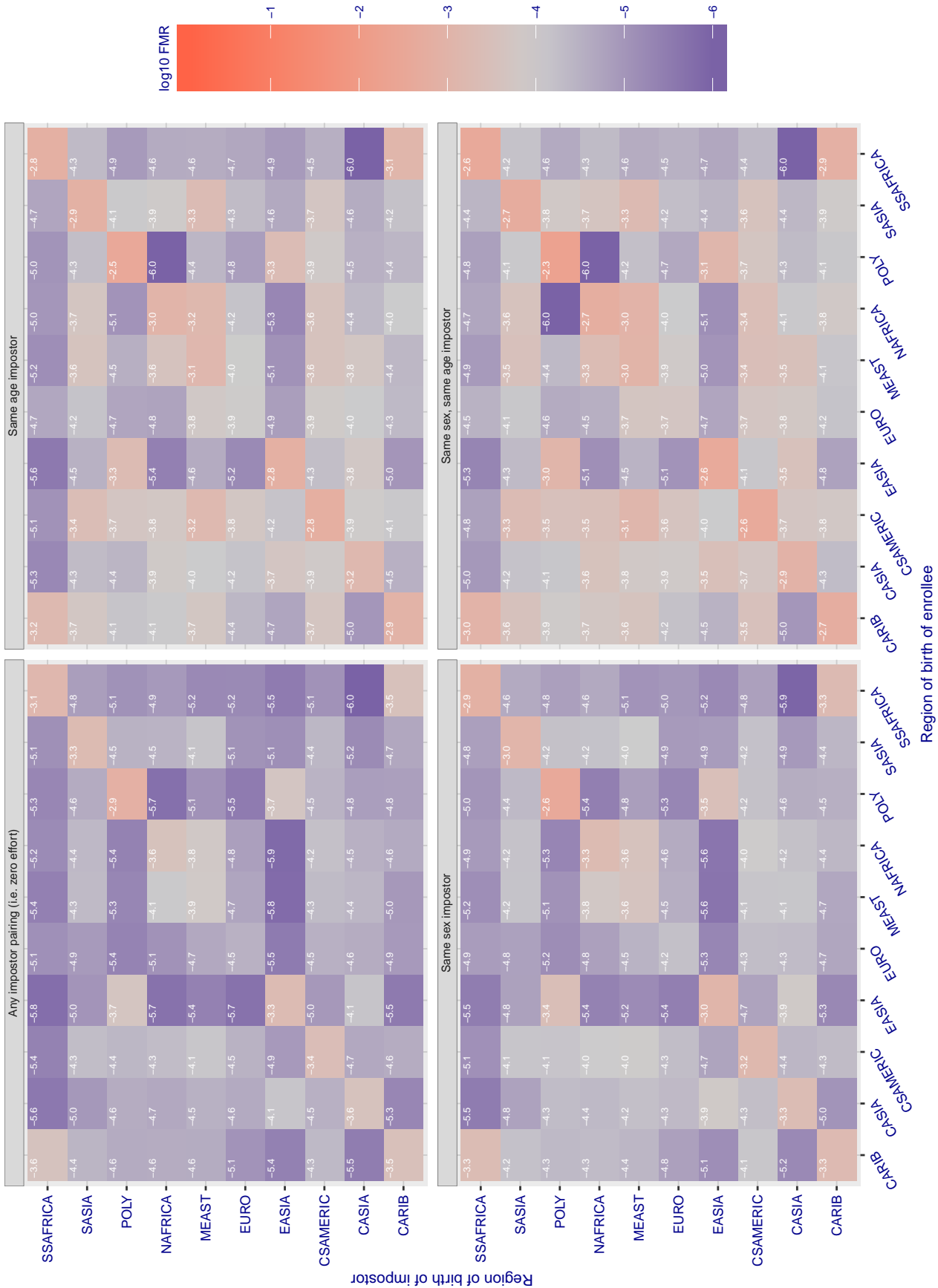


Figure 163: For algorithm alphaface-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 3.640 for algorithm amplifiedgroup\_001, giving FMR(T) = 0.0001 globally.

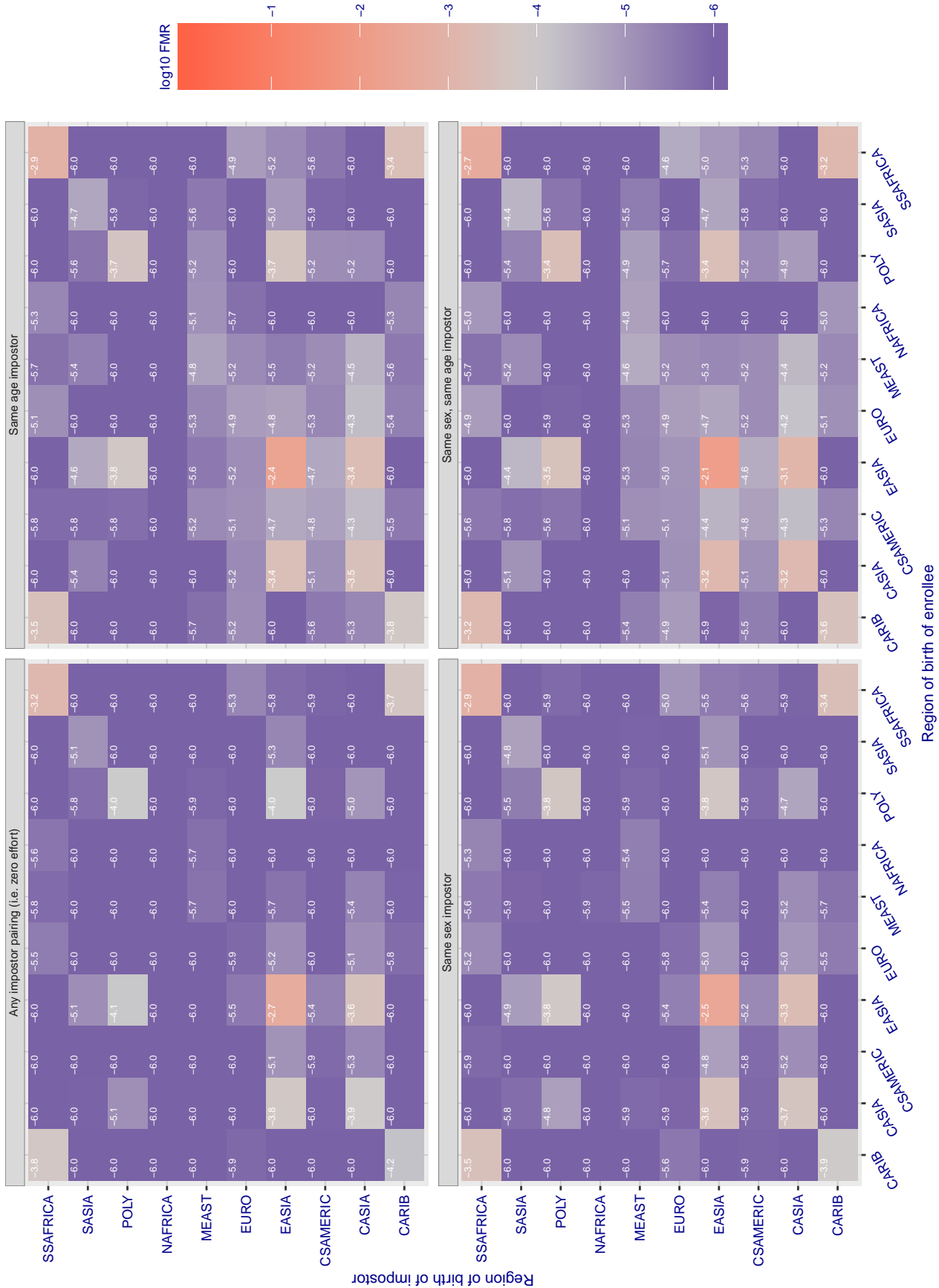


Figure 164: For algorithm amplifiedgroup-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of 10<sup>10</sup> impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 0.397$  for algorithm anke\_004, giving  $FMR(T) = 0.0001$  globally.

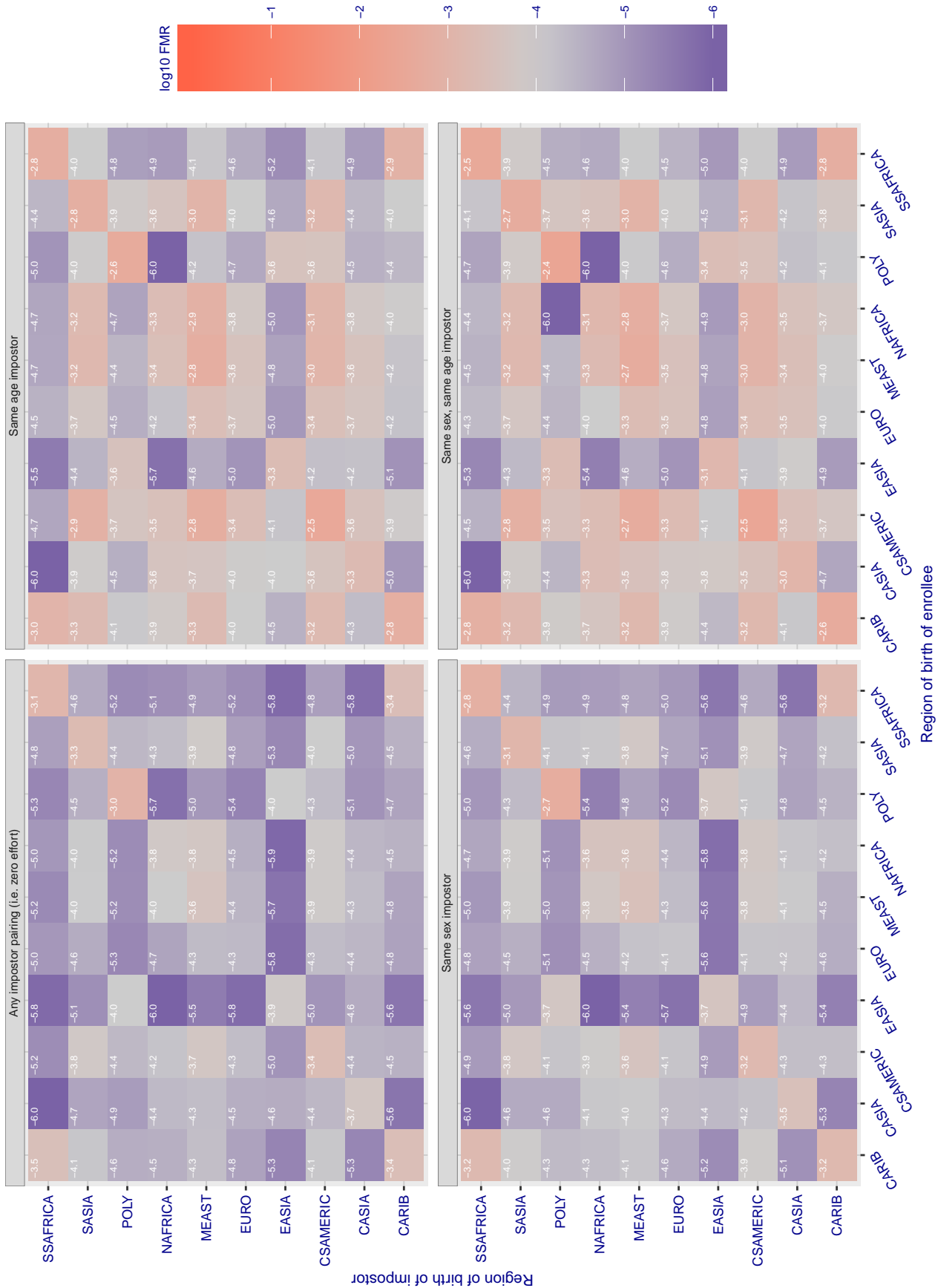


Figure 166: For algorithm anke-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 1.526$  for algorithm anyvision\_002, giving  $FMR(T) = 0.0001$  globally.

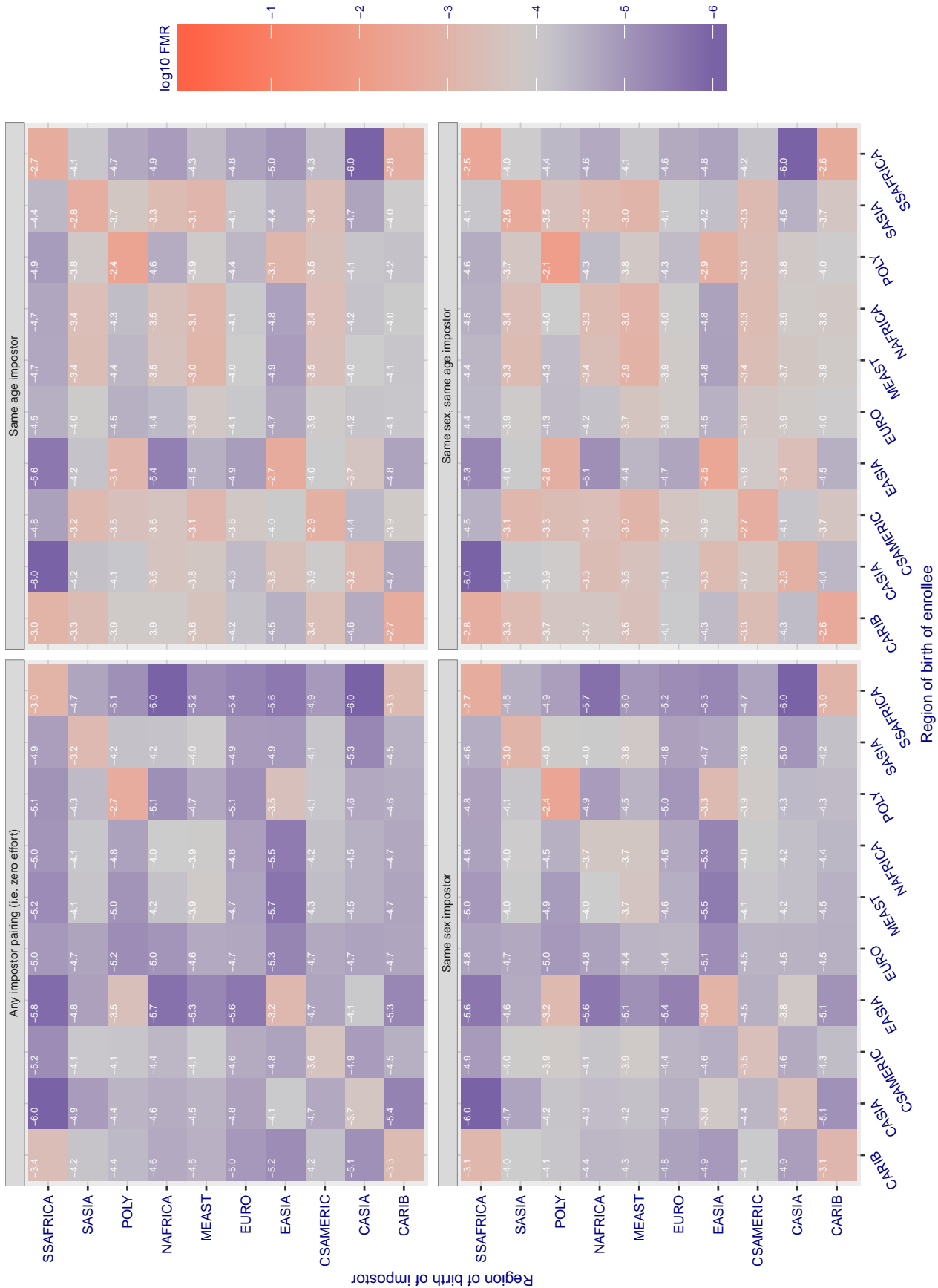


Figure 167: For algorithm anyvision-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 1.375$  for algorithm anyvision\_004, giving  $FMR(T) = 0.0001$  globally.

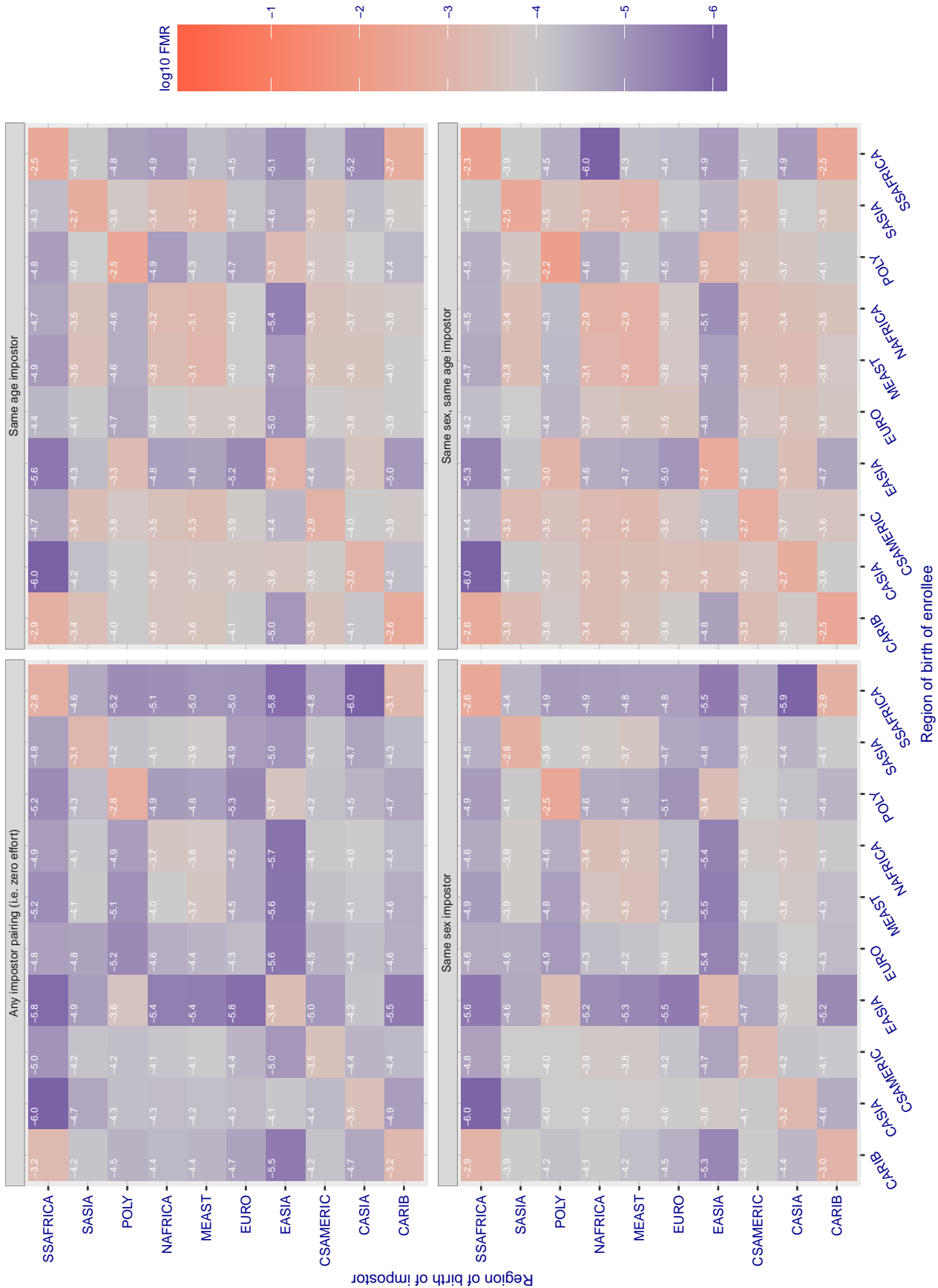


Figure 168: For algorithm anyvision-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



**Cross region FMR at threshold  $T = 1.388$  for algorithm asusaics\_000, giving  $FMR(T) = 0.0001$  globally.**

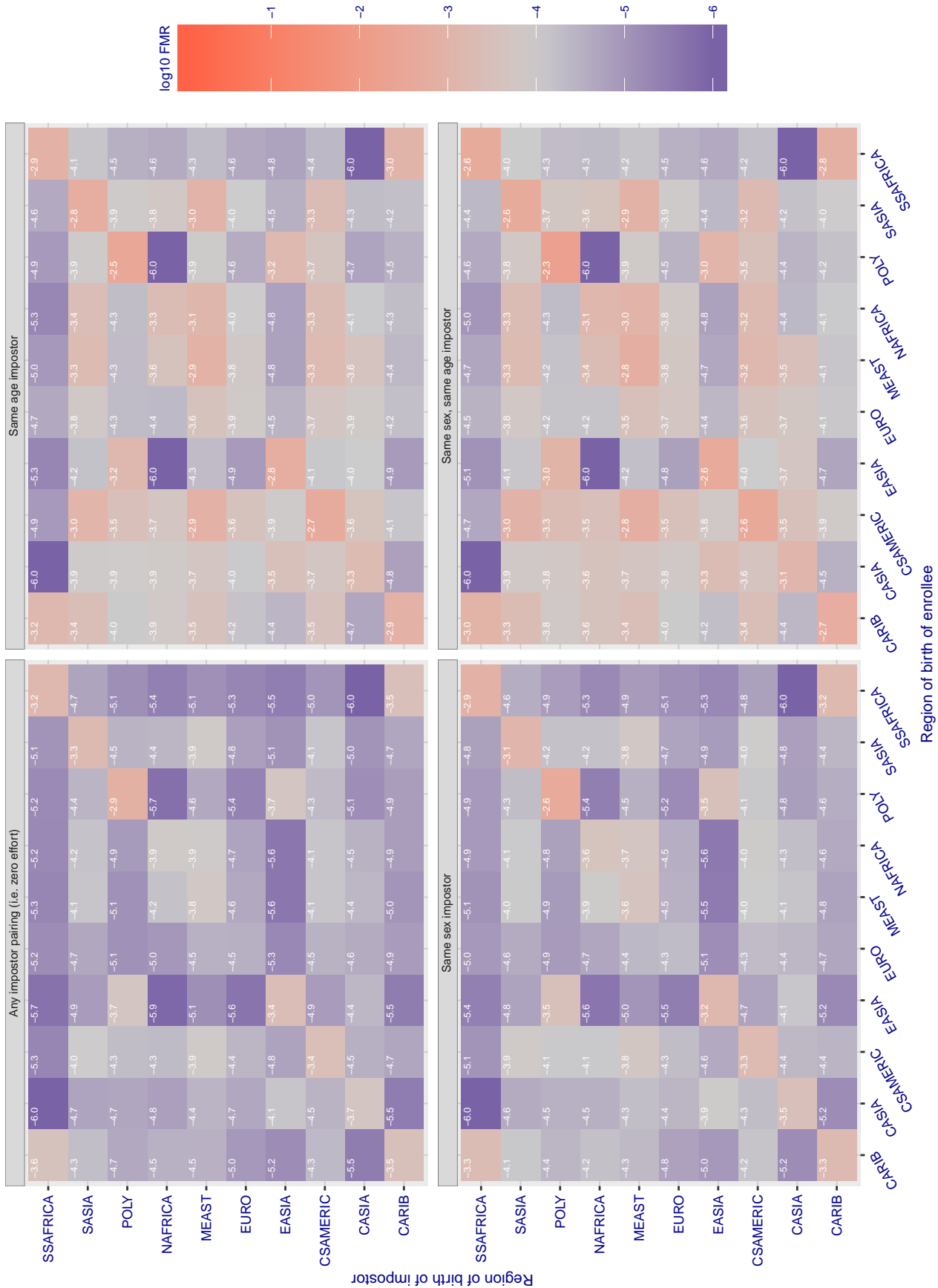


Figure 169: For algorithm asusaics-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 3.868$  for algorithm aware\_003, giving  $FMR(T) = 0.0001$  globally.

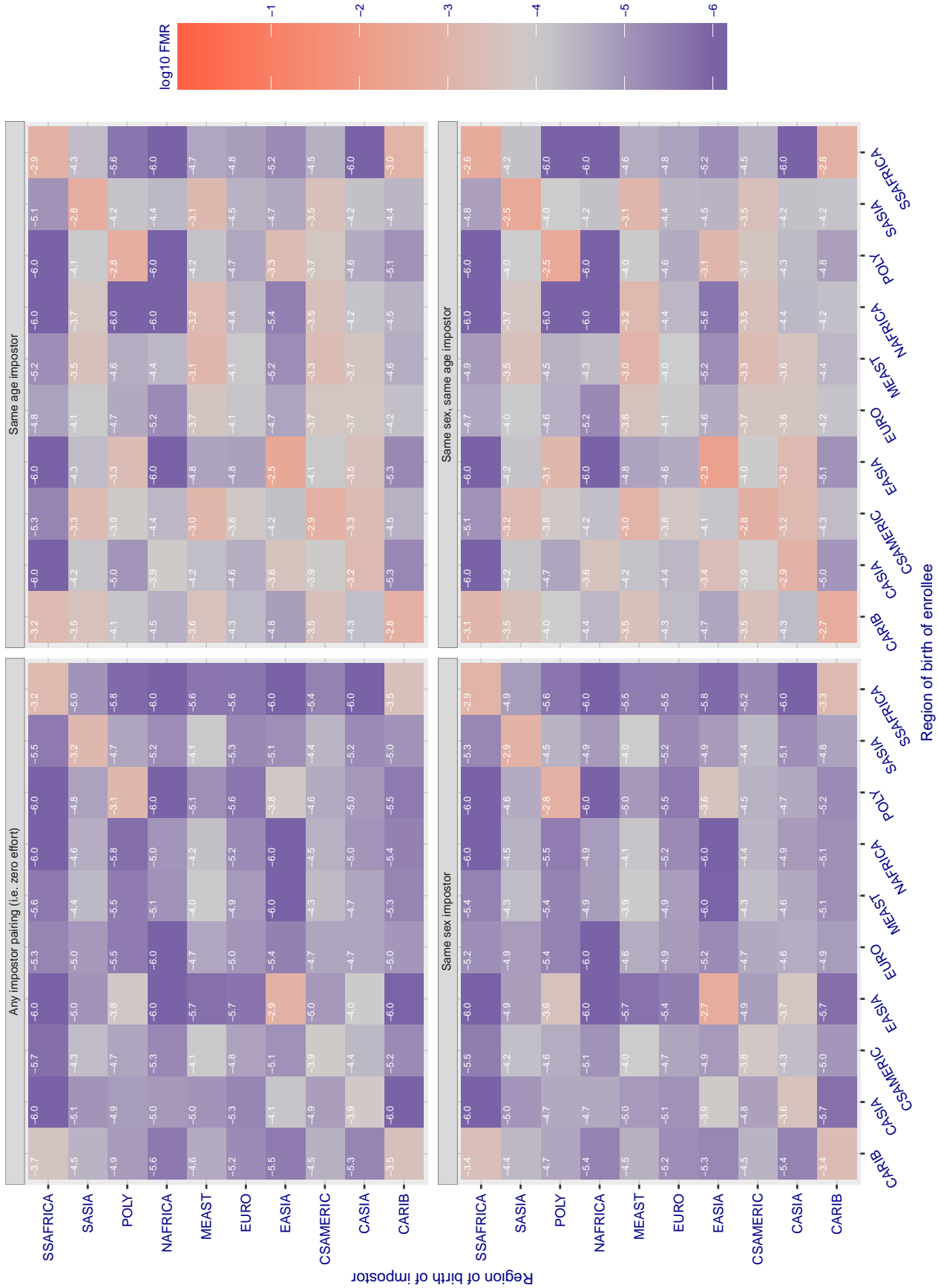


Figure 170: For algorithm aware-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 5.084$  for algorithm aware\_004, giving  $FMR(T) = 0.0001$  globally.

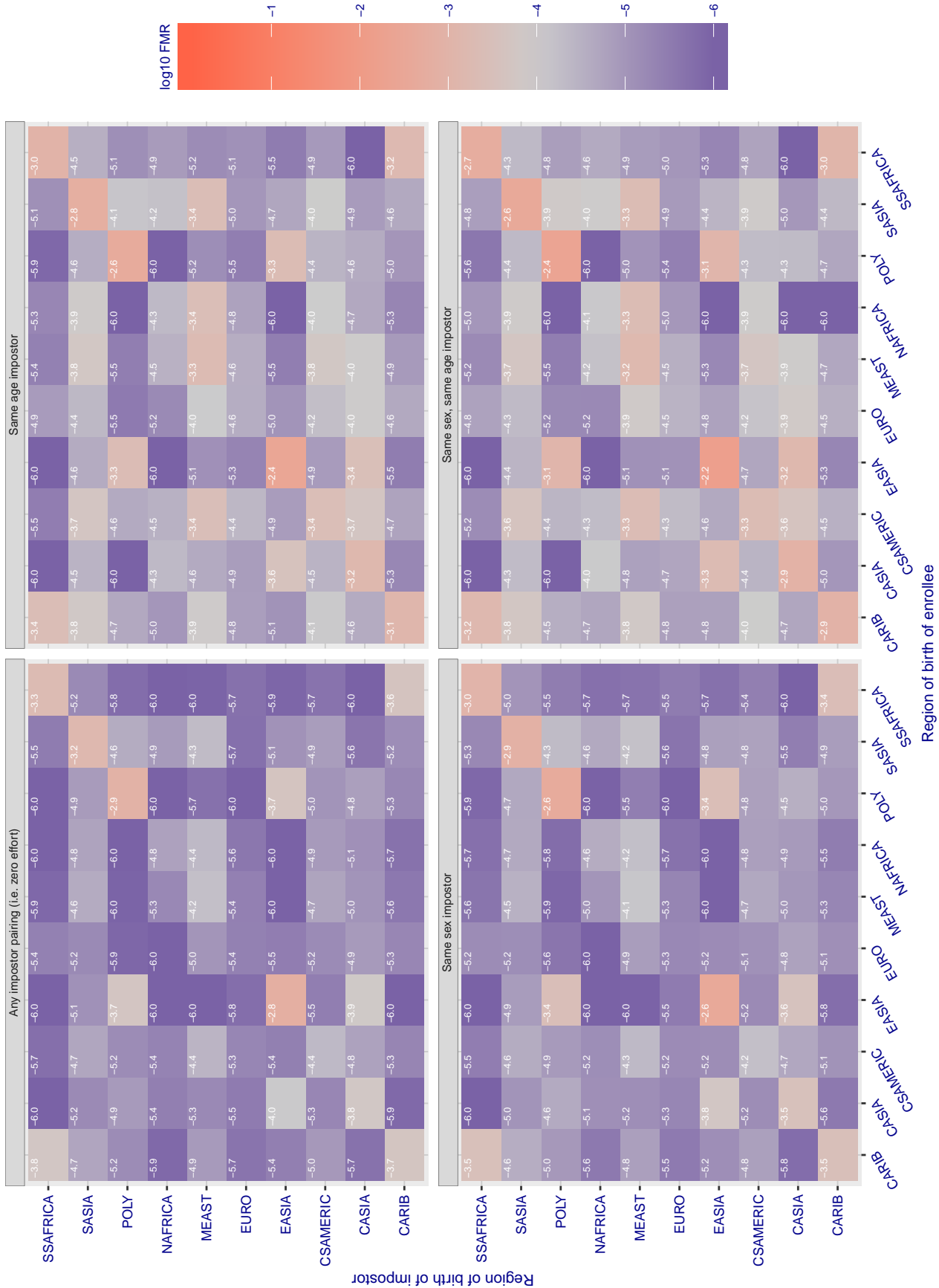


Figure 171: For algorithm aware-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.799$  for algorithm awiros\_001, giving  $FMR(T) = 0.0001$  globally.

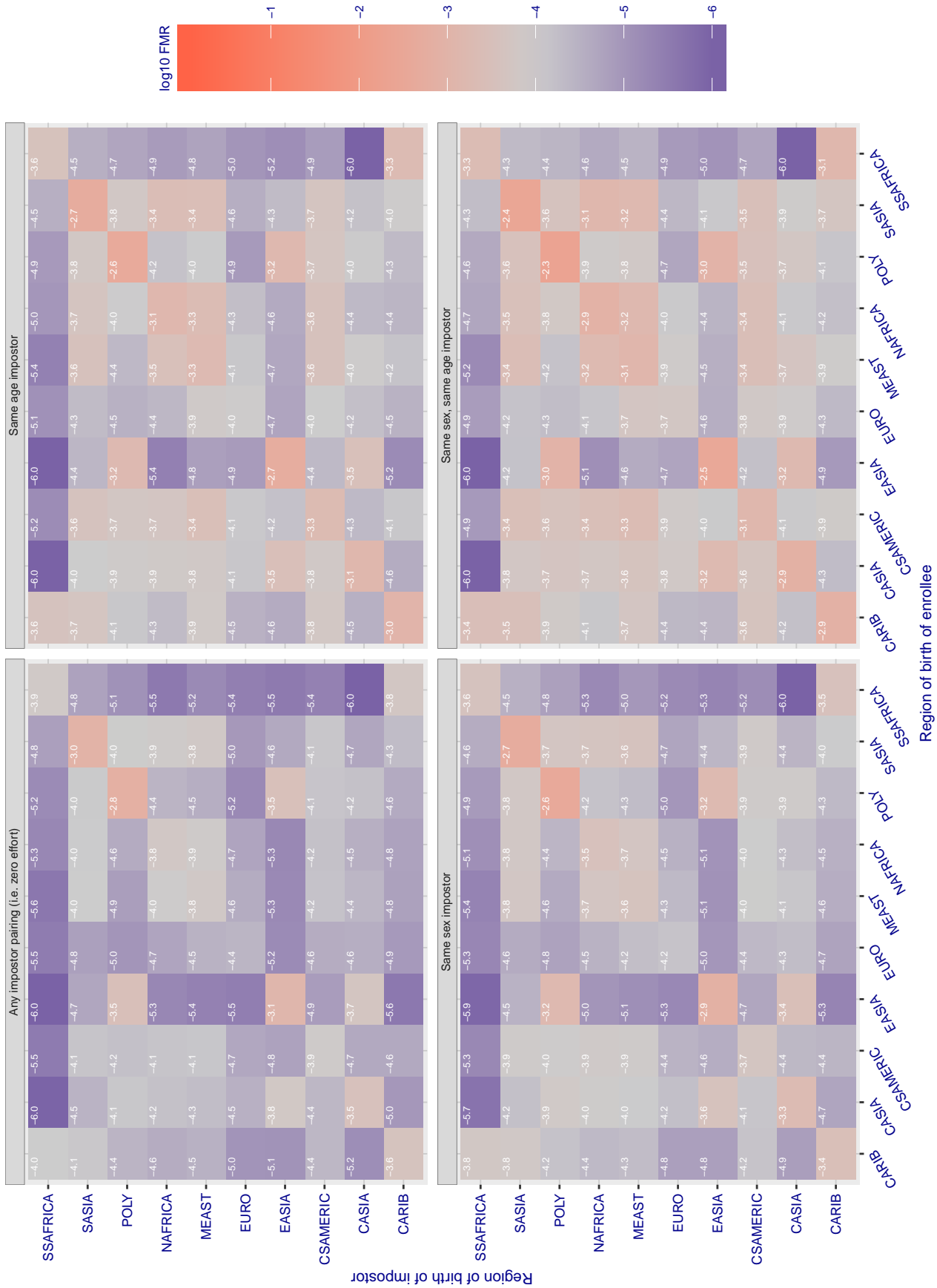


Figure 172: For algorithm awiros-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 0.919 for algorithm ayonix\_000, giving FMR(T) = 0.0001 globally.

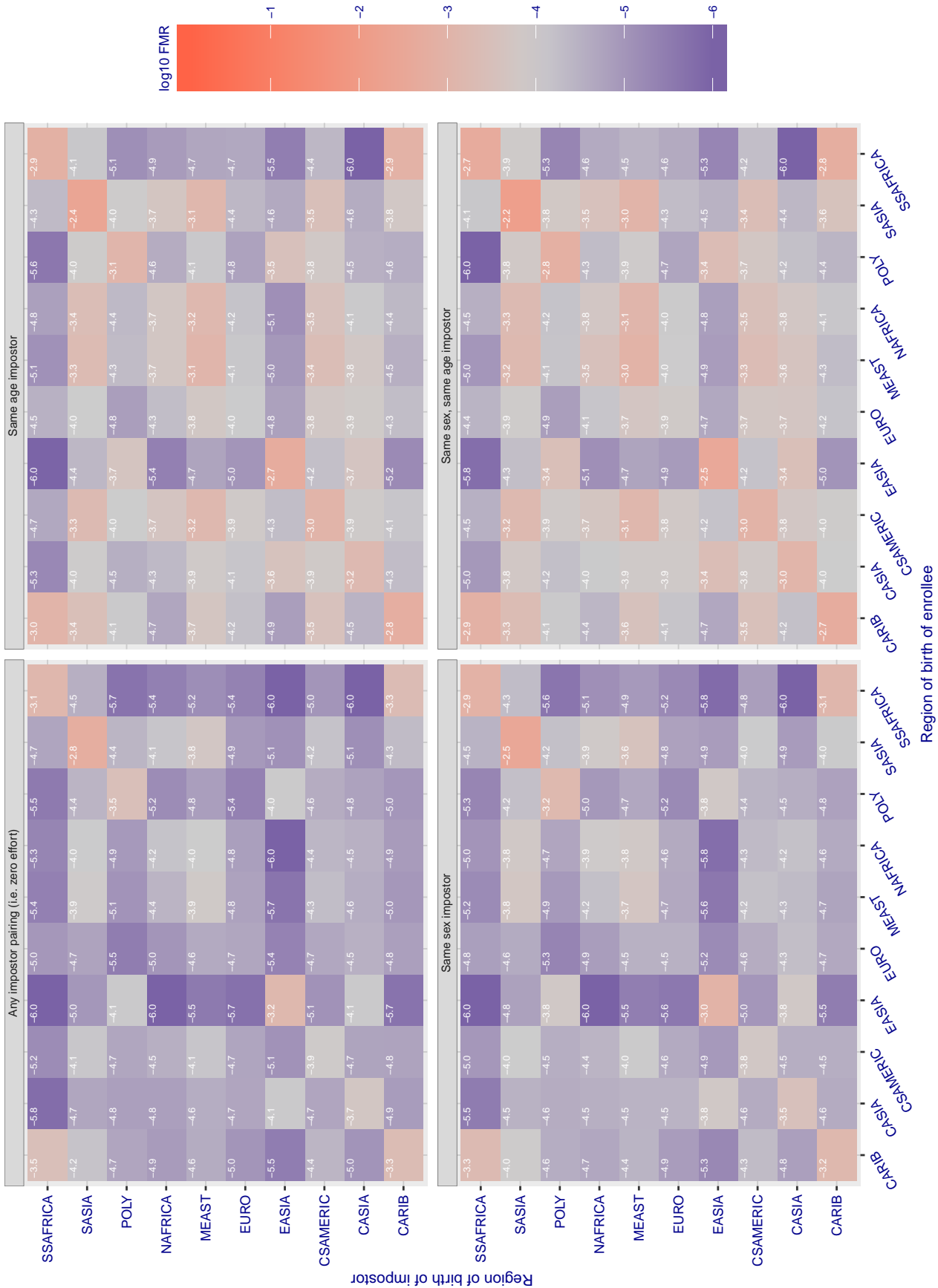


Figure 173: For algorithm ayonix-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.731$  for algorithm bm\_001, giving  $FMR(T) = 0.0001$  globally.

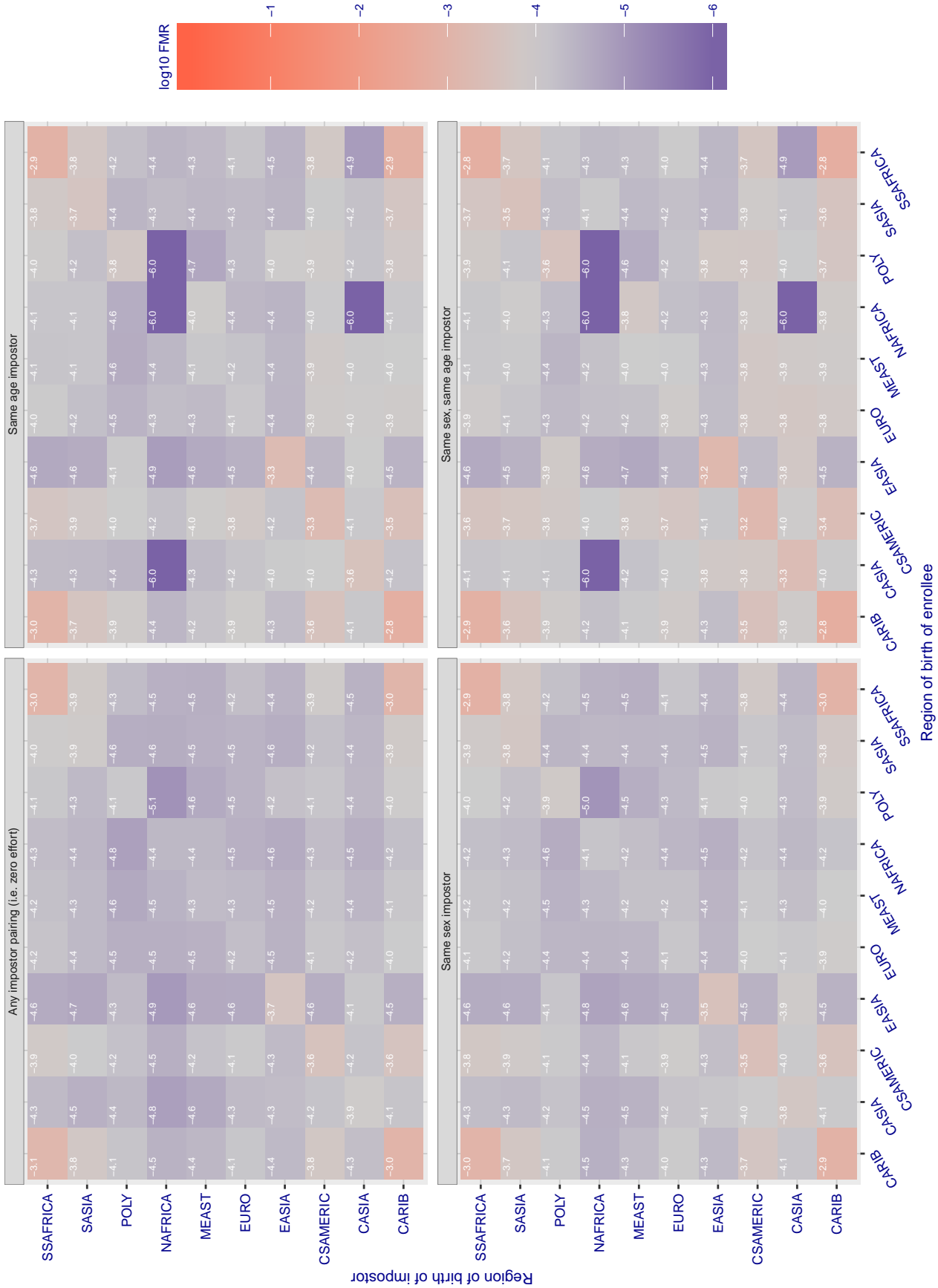


Figure 174: For algorithm bm-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 0.388$  for algorithm camvi\_002, giving  $FMR(T) = 0.0001$  globally.

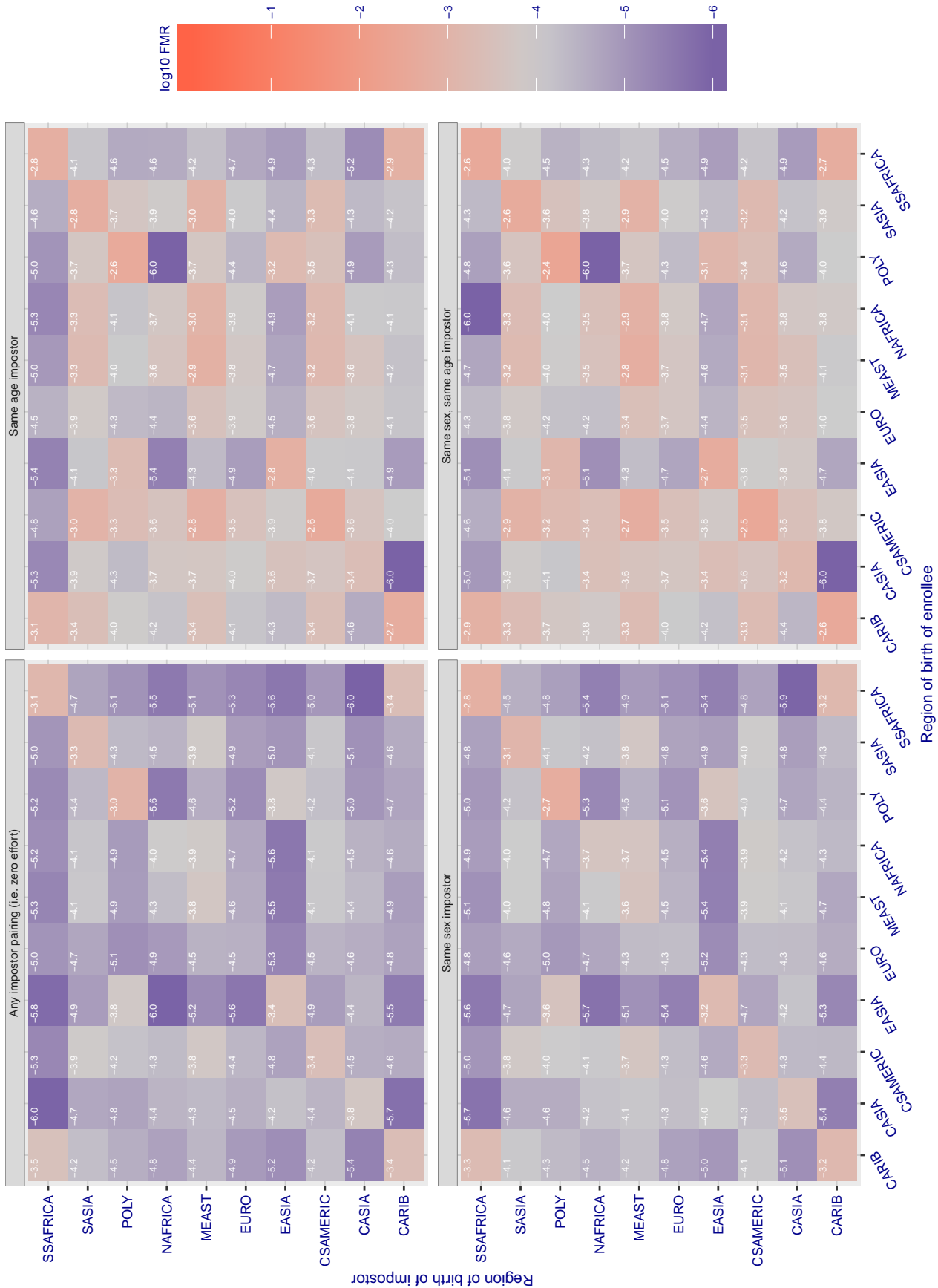


Figure 175: For algorithm camvi-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.377$  for algorithm camvi\_004, giving  $FMR(T) = 0.0001$  globally.

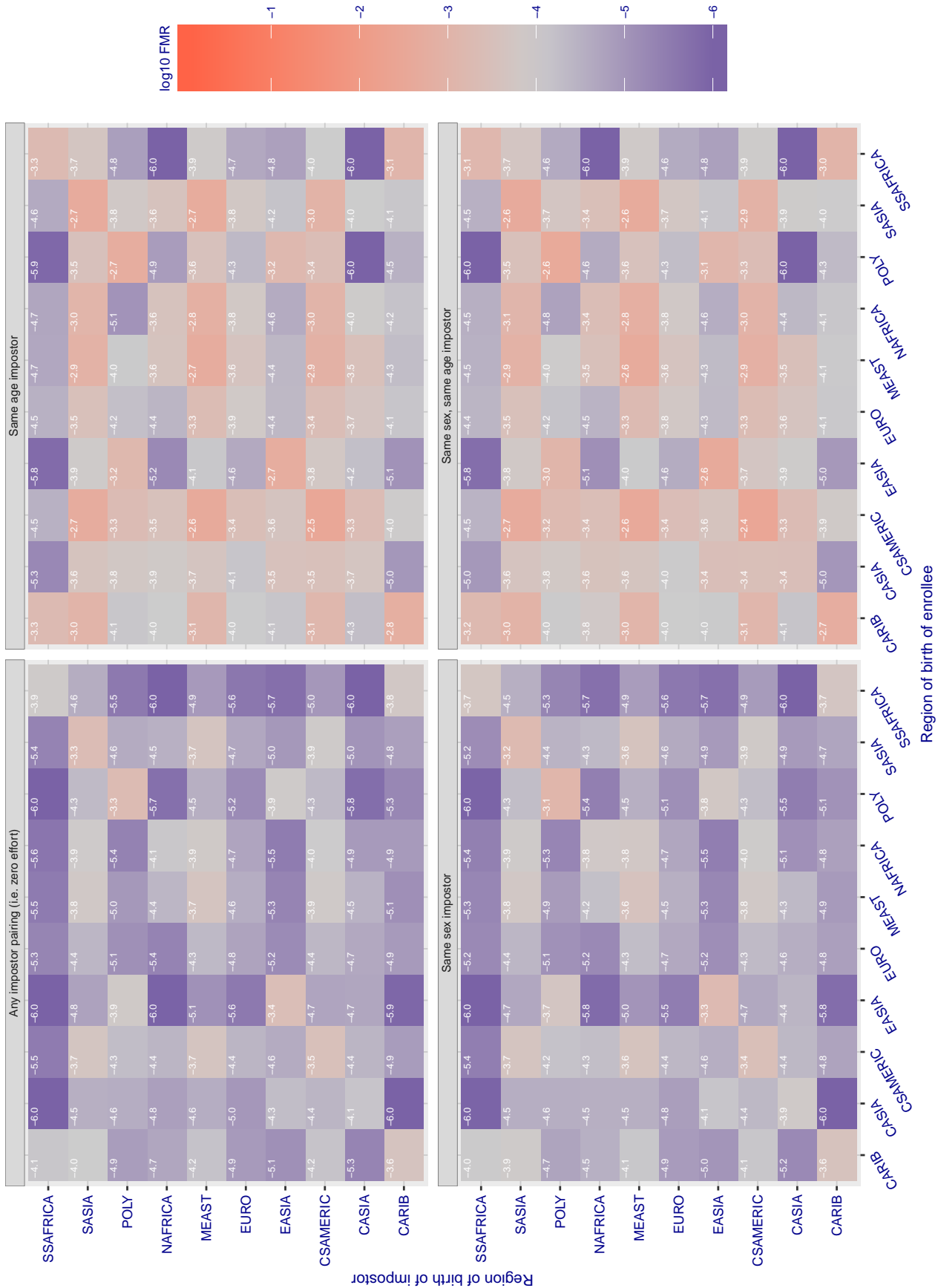


Figure 176: For algorithm camvi-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 0.436$  for algorithm ceiec\_001, giving  $FMR(T) = 0.0001$  globally.

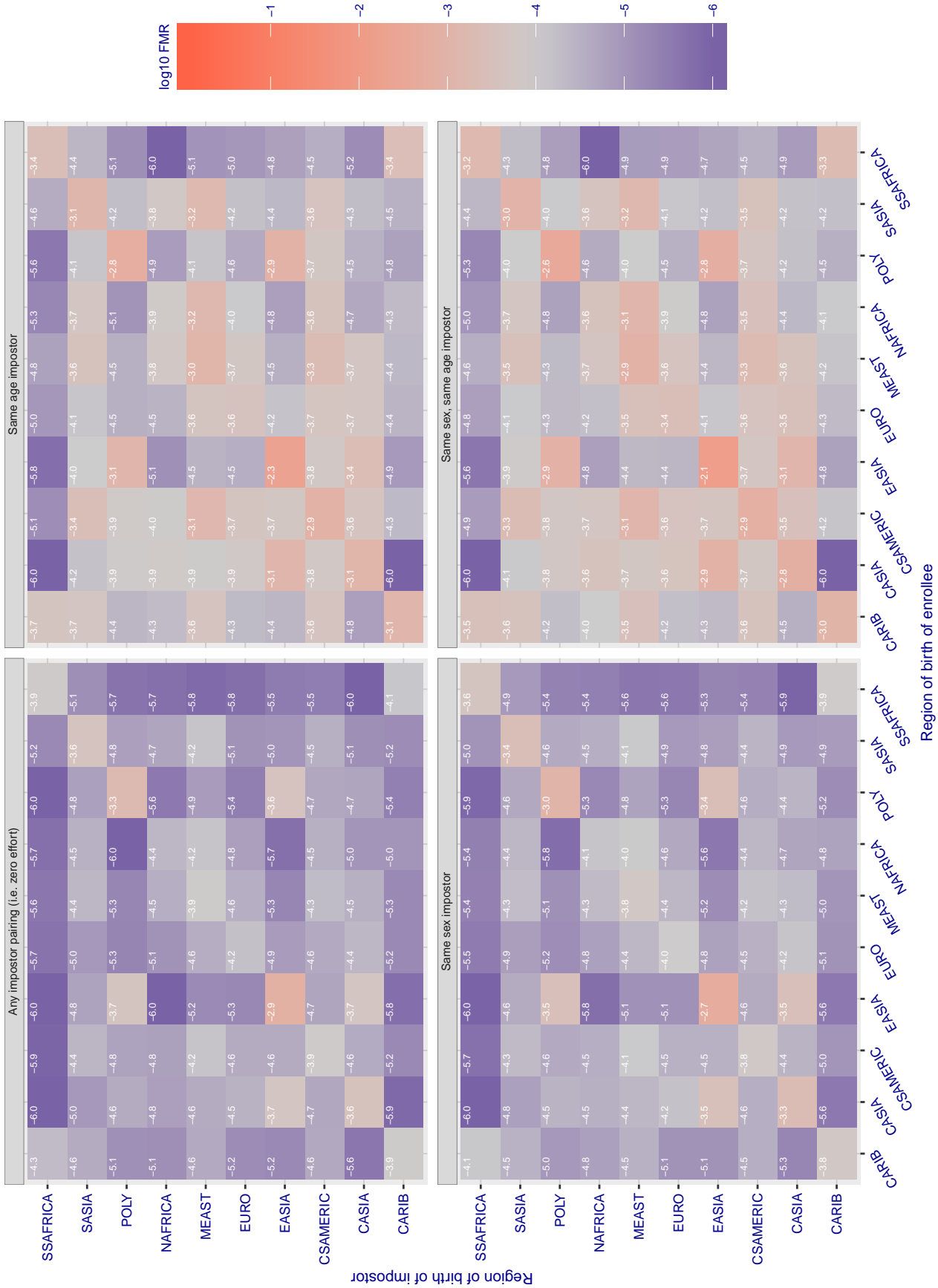


Figure 177: For algorithm ceiec-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.325$  for algorithm ceiec\_002, giving  $FMR(T) = 0.0001$  globally.

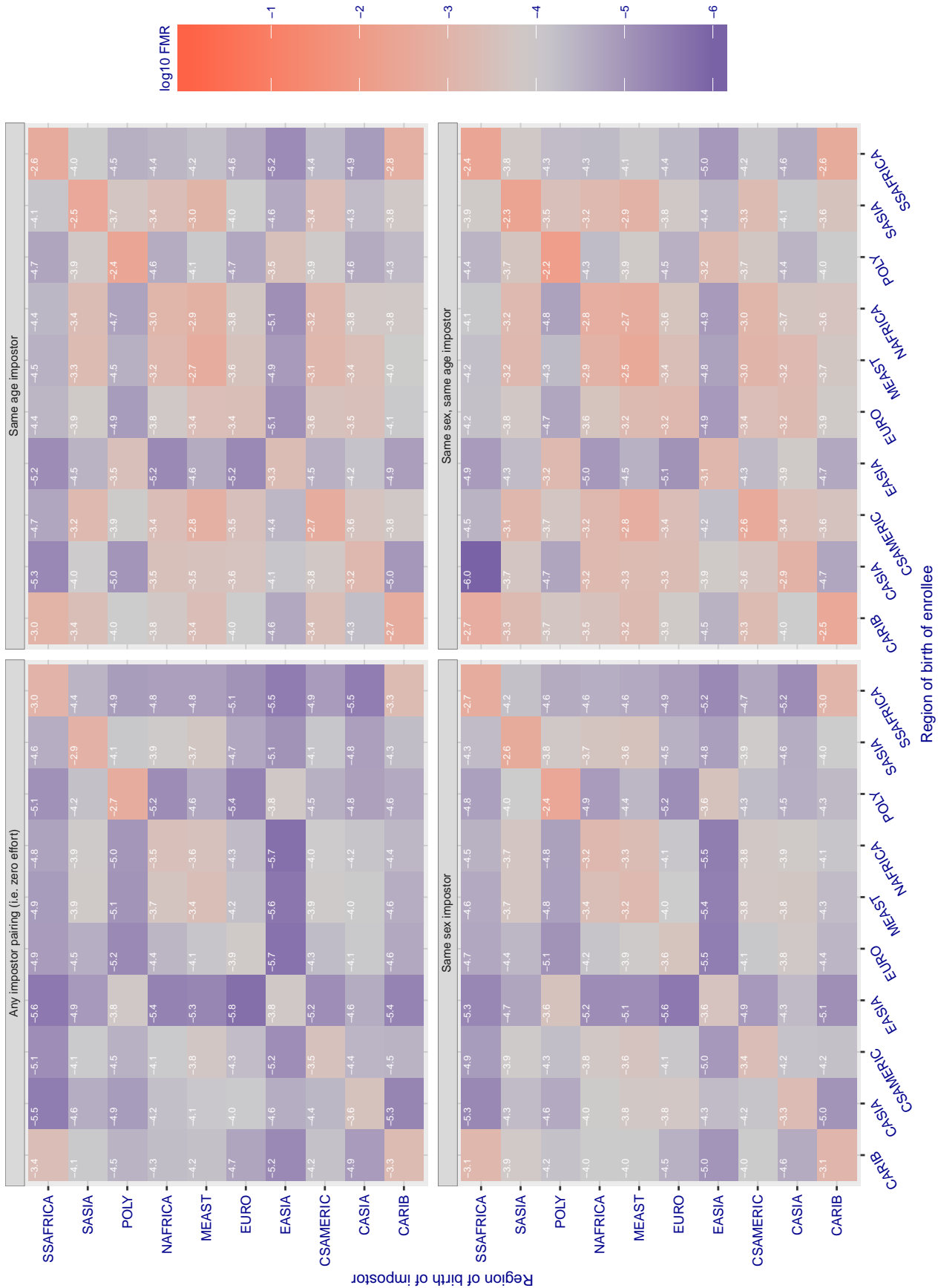


Figure 178: For algorithm ceiec-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 106.748 for algorithm chtface\_001, giving FMR(T) = 0.0001 globally.

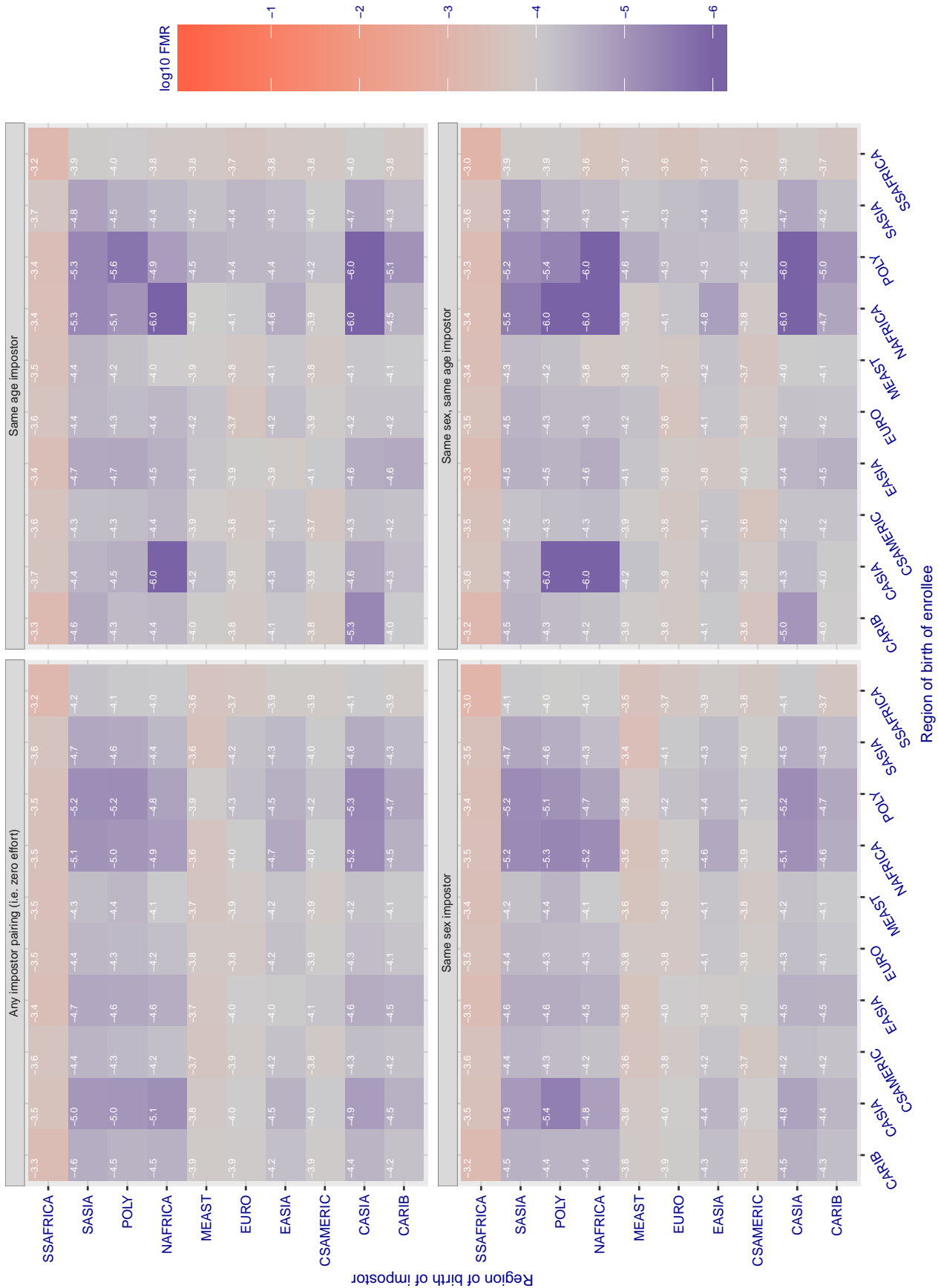


Figure 179: For algorithm chtface-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 2972.000 for algorithm cogent\_003, giving FMR(T) = 0.0001 globally.

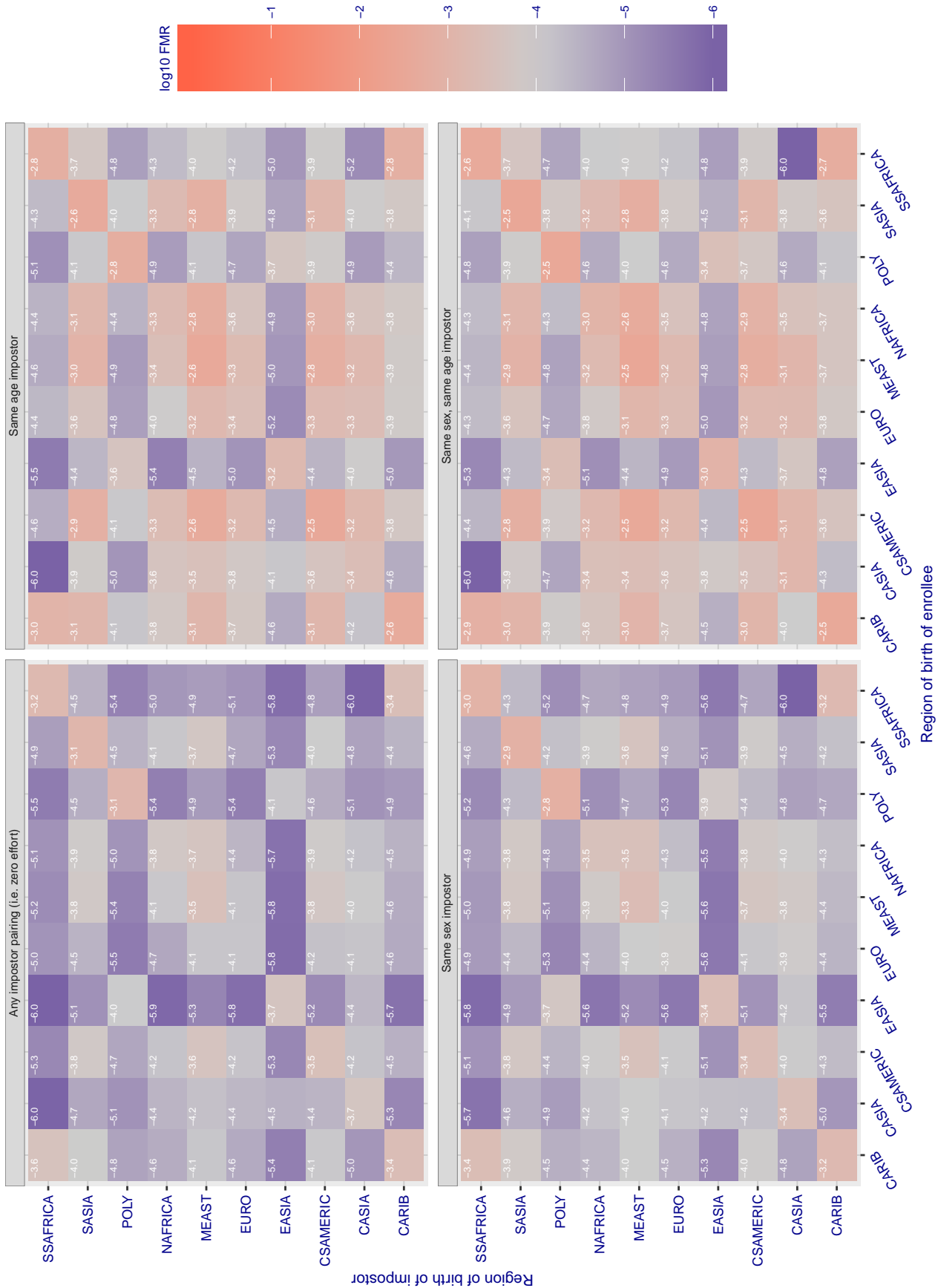


Figure 180: For algorithm cogent-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 3156.000 for algorithm cogent\_004, giving FMR(T) = 0.0001 globally.

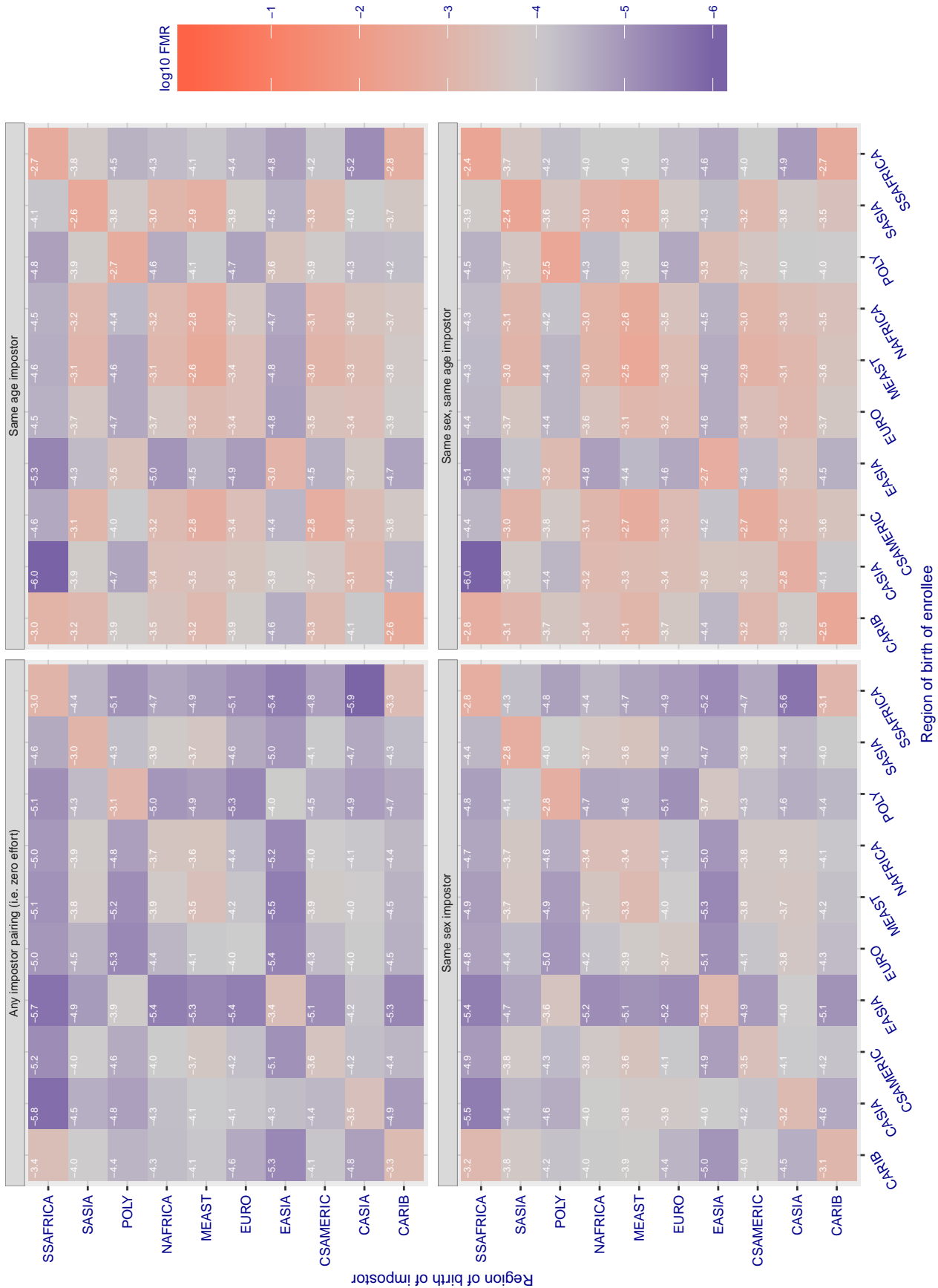


Figure 181: For algorithm cogent-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of 10<sup>10</sup> impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

**Cross region FMR at threshold  $T = 0.565$  for algorithm `cognitec_000`, giving  $FMR(T) = 0.0001$  globally.**

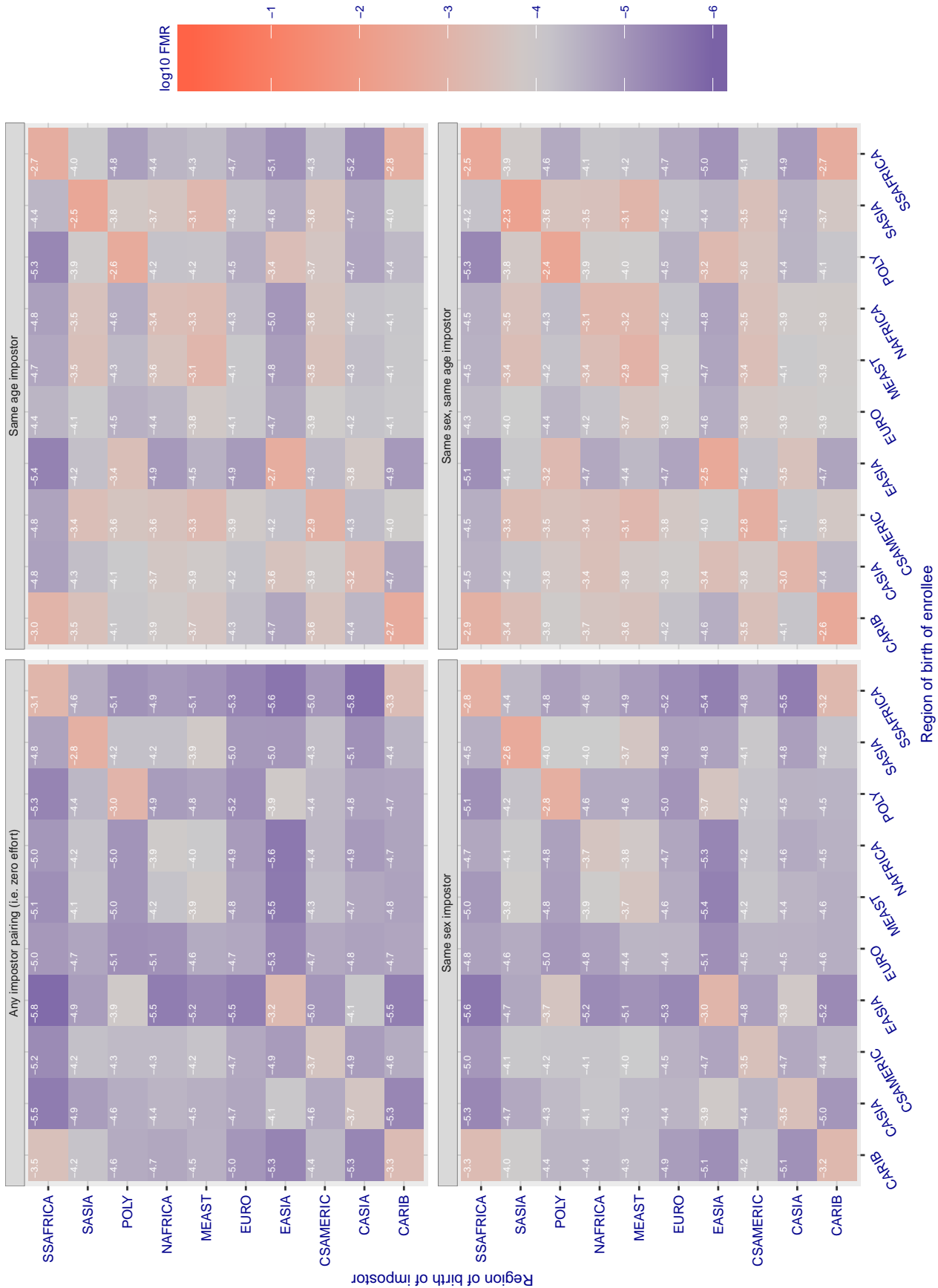


Figure 182: For algorithm `cognitec-000` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



**Cross region FMR at threshold T = 0.565 for algorithm cognitec\_001, giving FMR(T) = 0.0001 globally.**

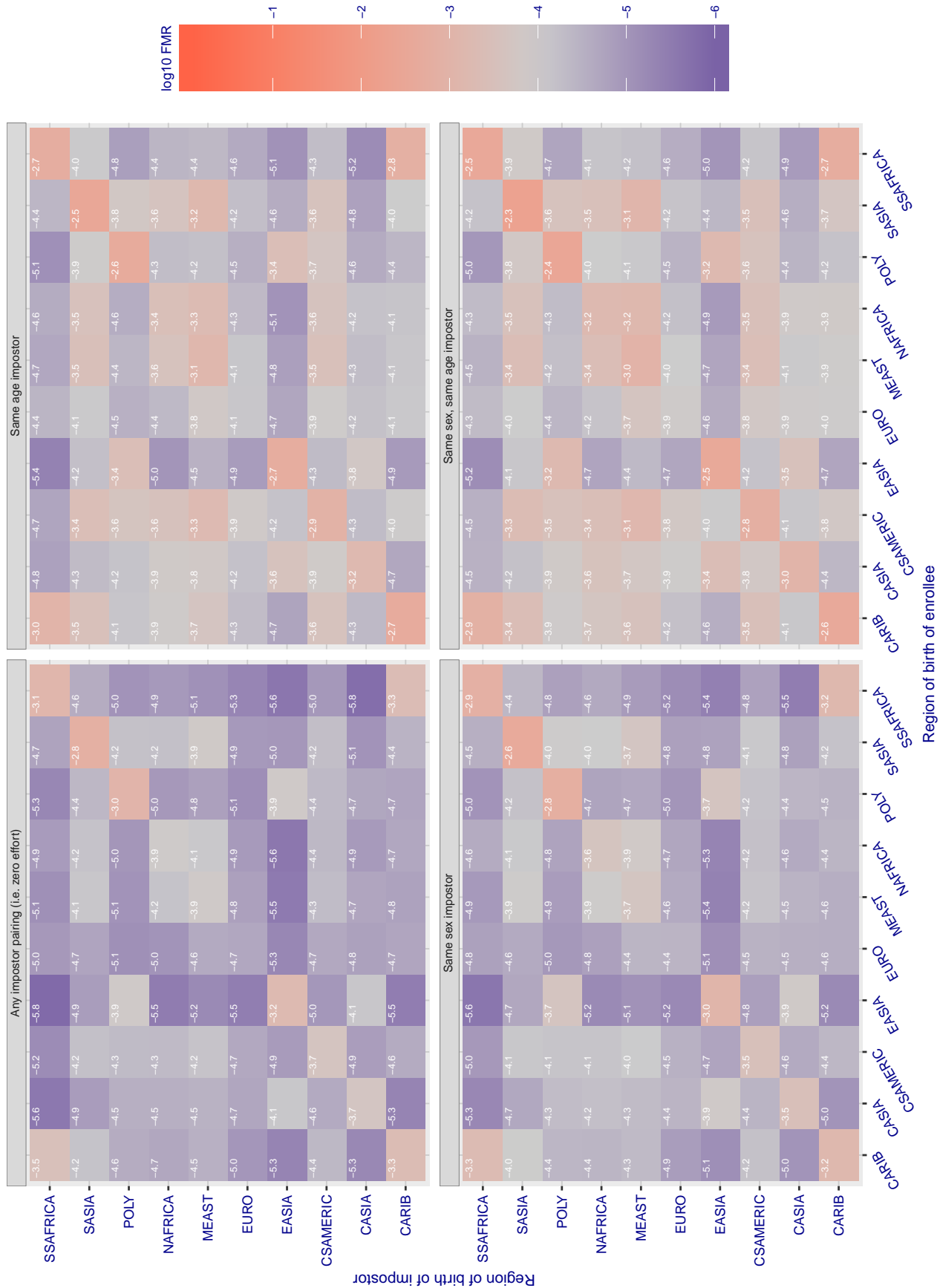


Figure 183: For algorithm cognitec-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 3.730$  for algorithm `ctcbank_000`, giving  $FMR(T) = 0.0001$  globally.

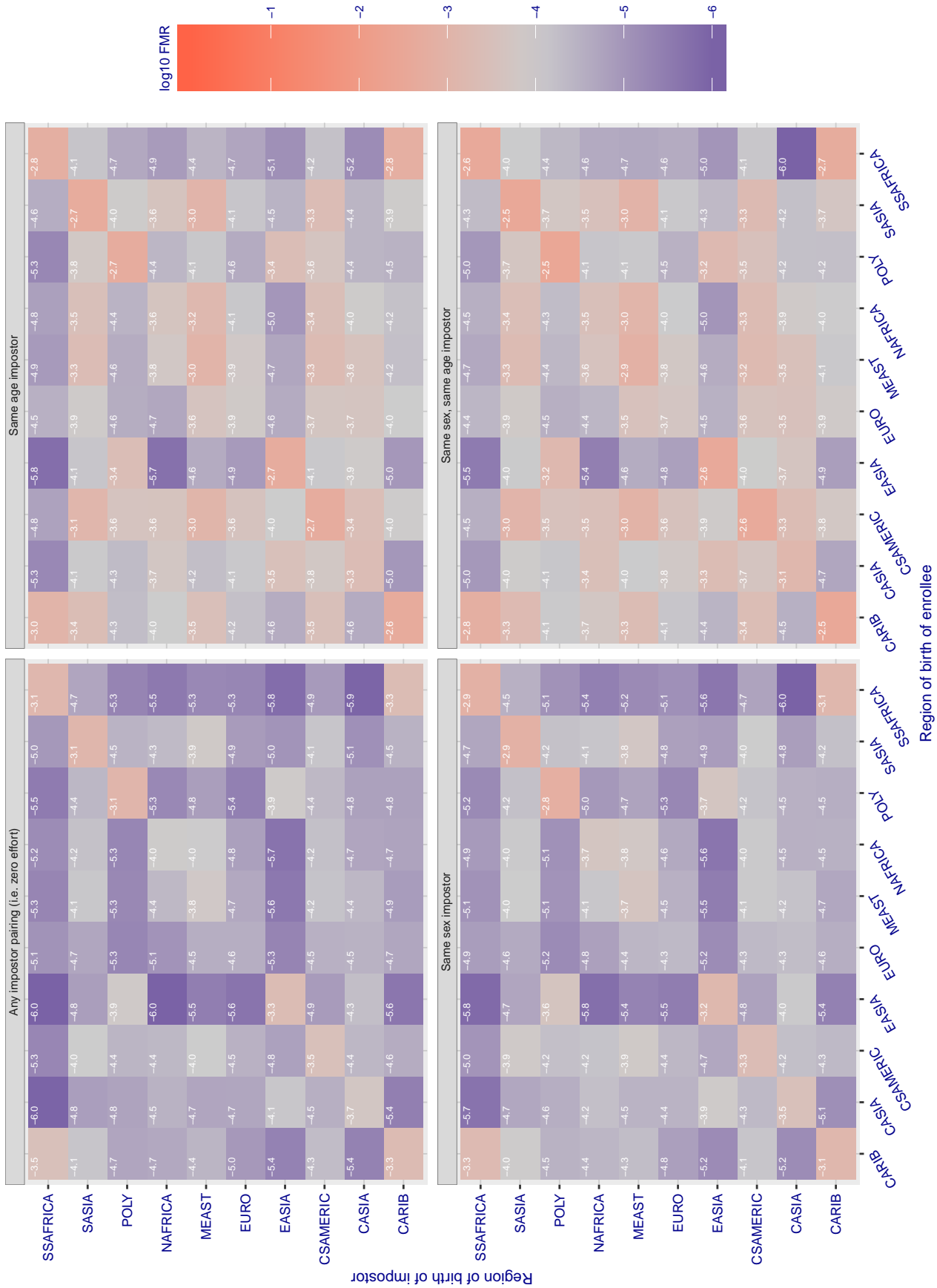


Figure 184: For algorithm `ctcbank-000` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 3.772$  for algorithm `ctcbank_001`, giving  $FMR(T) = 0.0001$  globally.

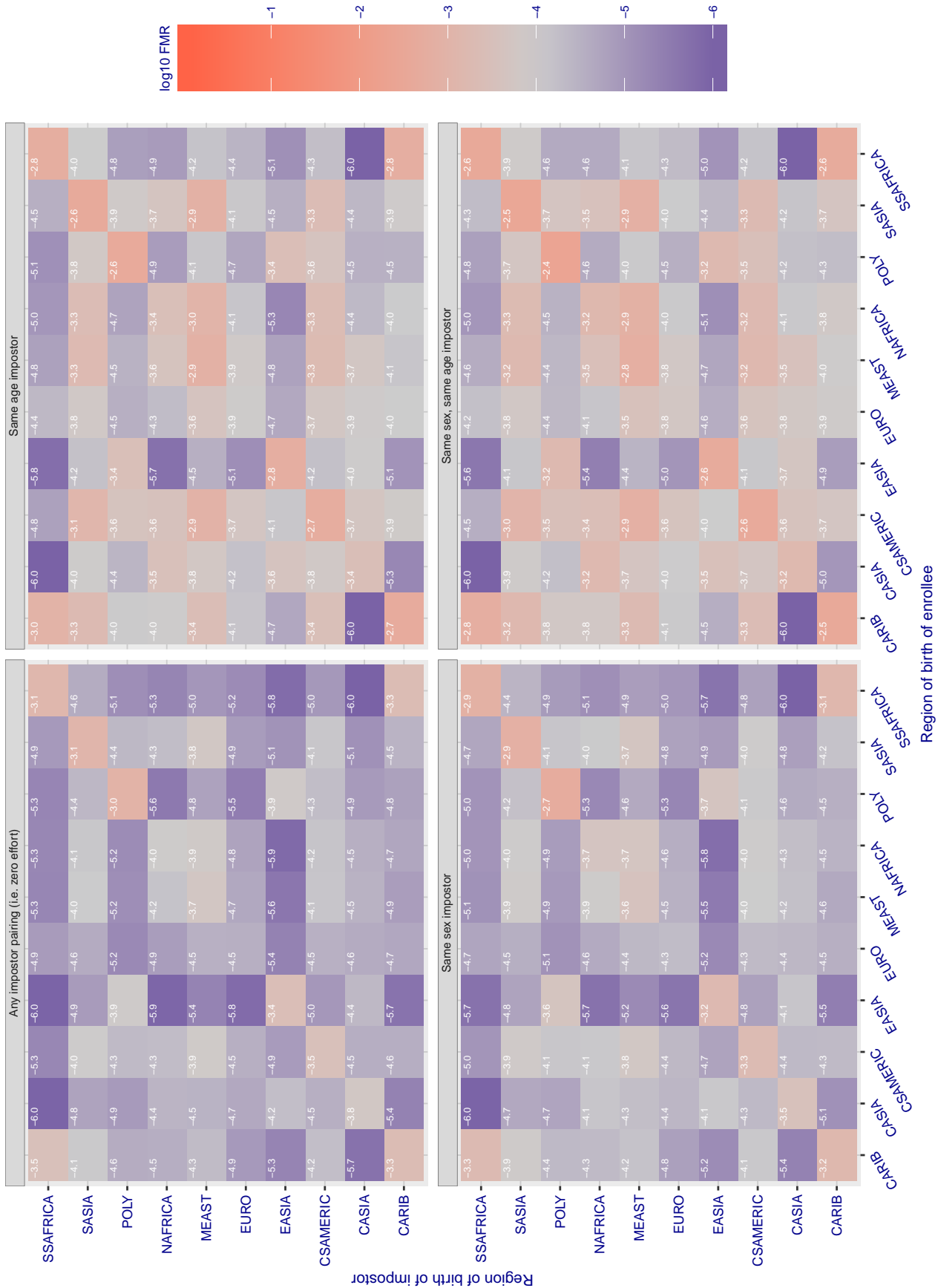


Figure 185: For algorithm `ctcbank-001` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.762$  for algorithm cyberextruder\_001, giving  $FMR(T) = 0.0001$  globally.

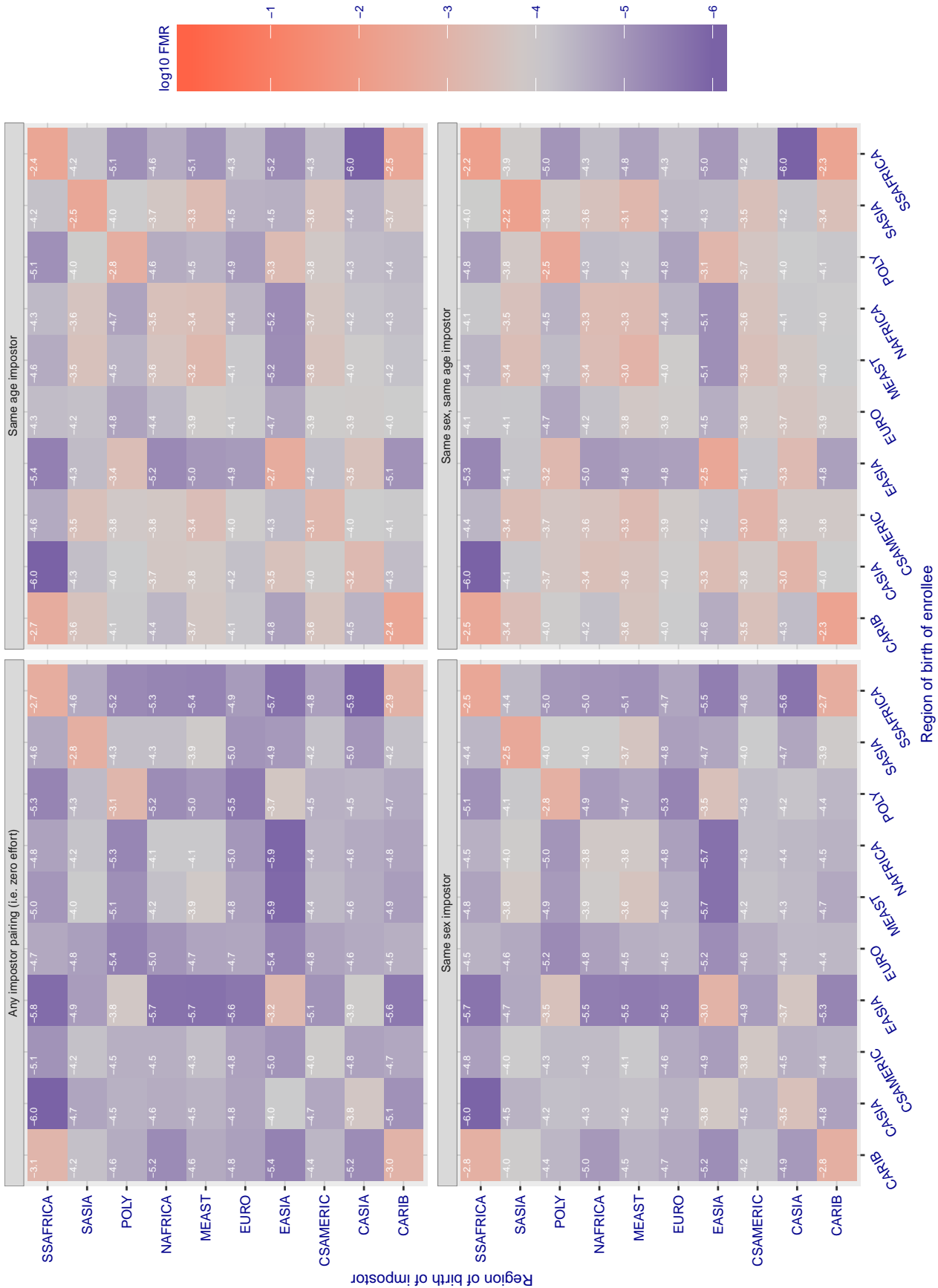


Figure 186: For algorithm cyberextruder-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 0.500 for algorithm cyberextruder\_002, giving FMR(T) = 0.0001 globally.

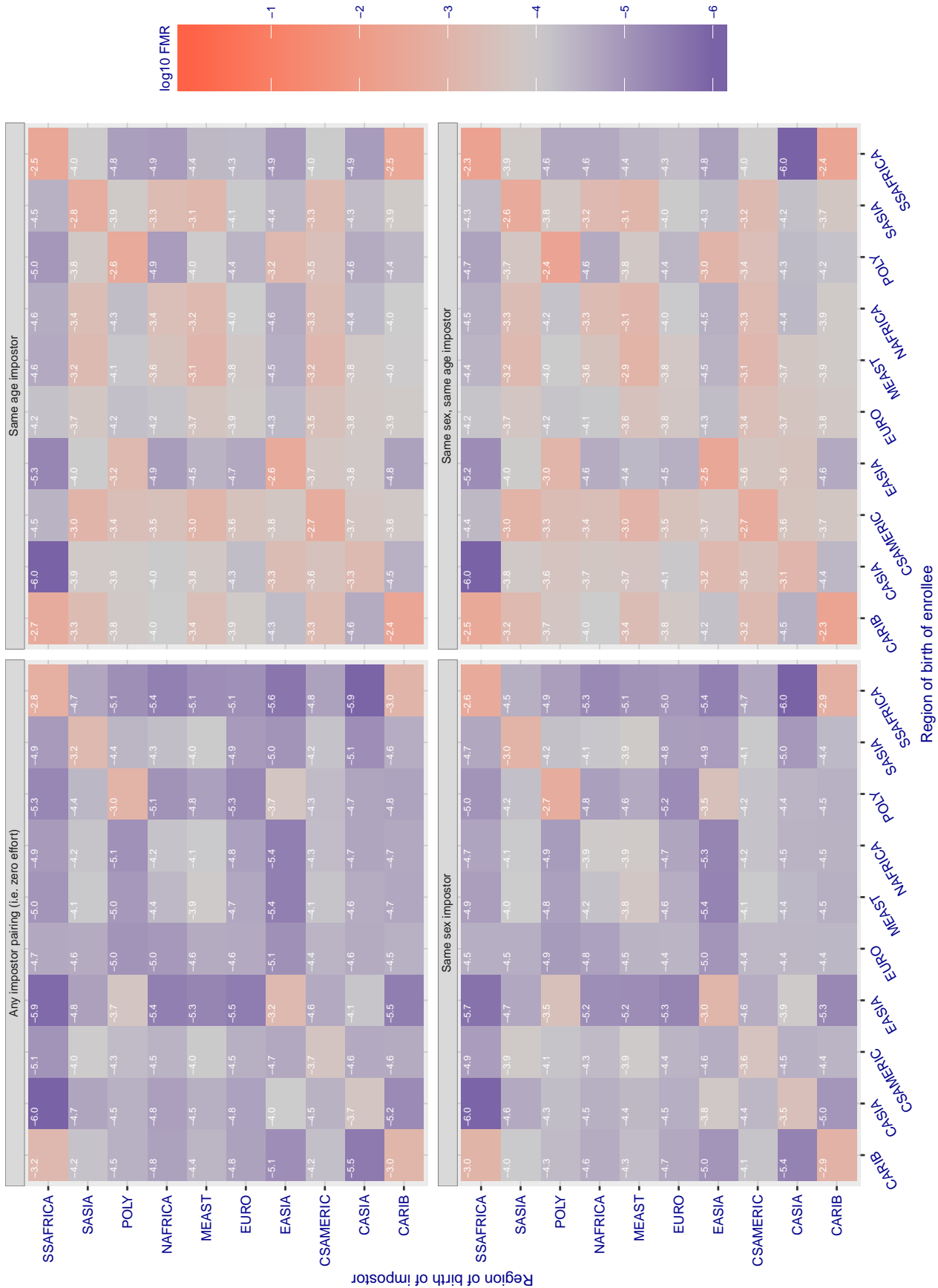


Figure 187: For algorithm cyberextruder-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of 10<sup>10</sup> impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

**Cross region FMR at threshold  $T = 1.409$  for algorithm cyberlink\_002, giving  $FMR(T) = 0.0001$  globally.**

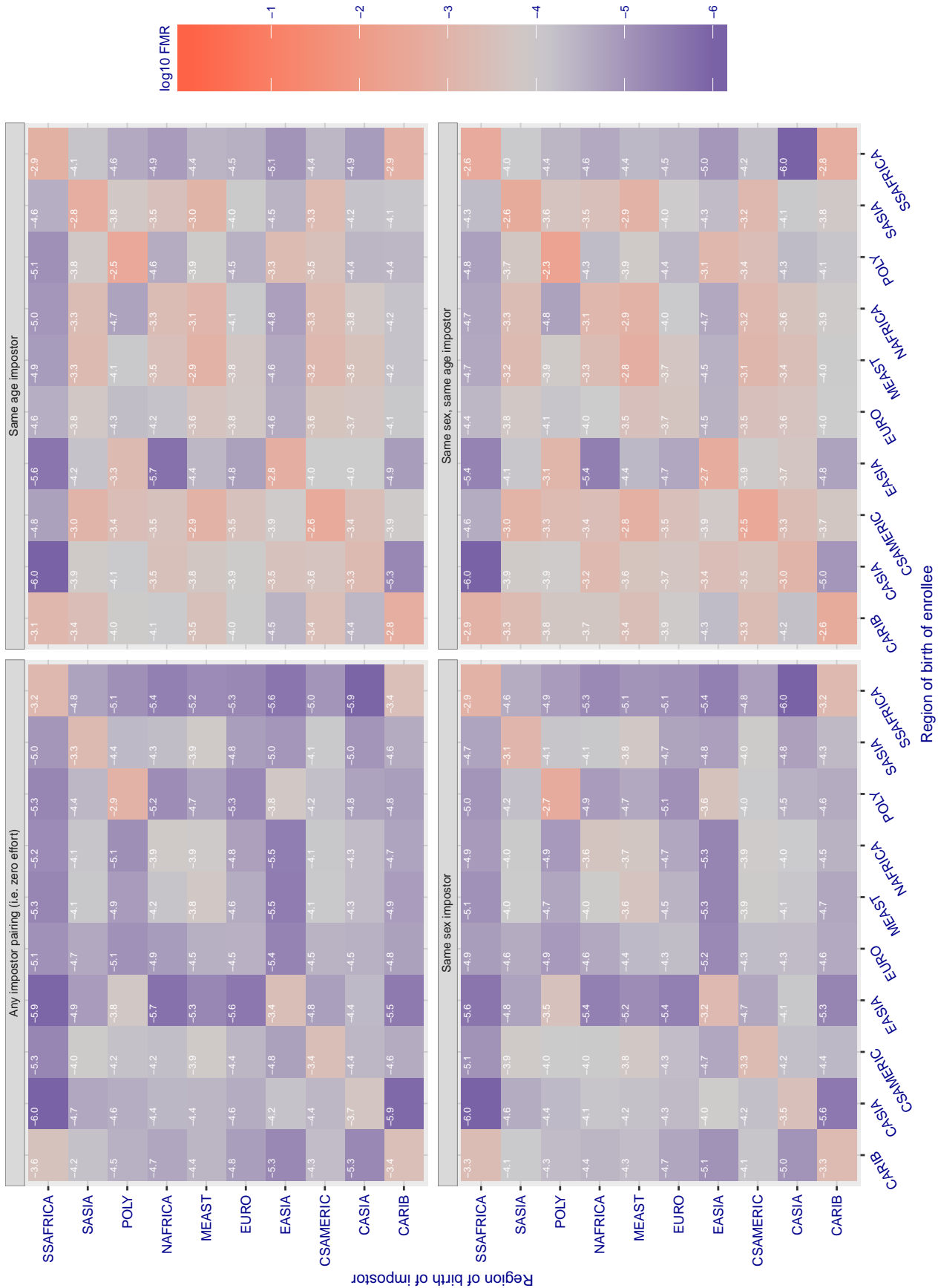


Figure 188: For algorithm cyberlink-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 1.409$  for algorithm cyberlink\_003, giving  $FMR(T) = 0.0001$  globally.

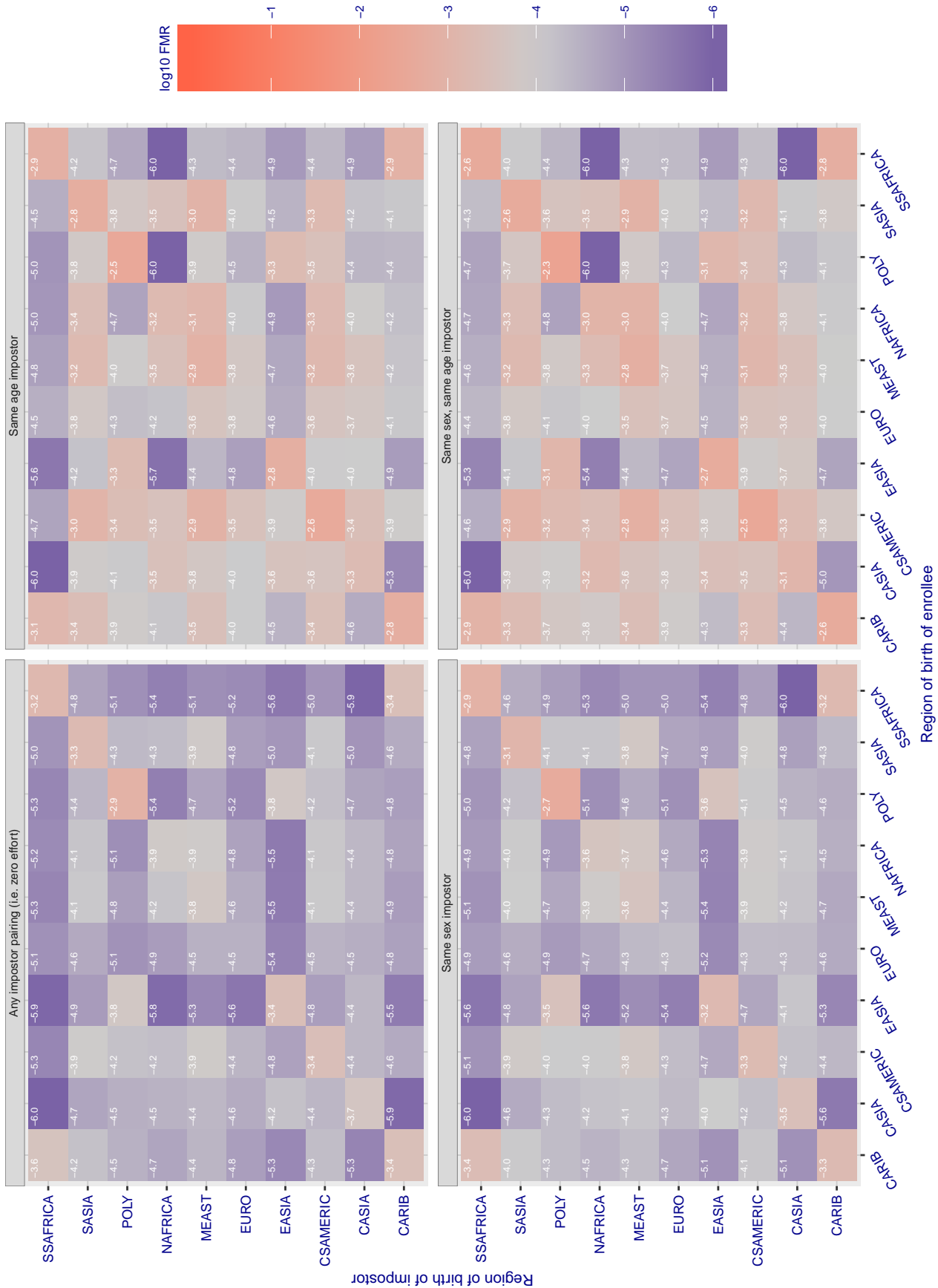


Figure 189: For algorithm cyberlink-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 6696.000 for algorithm dahua\_002, giving FMR(T) = 0.0001 globally.

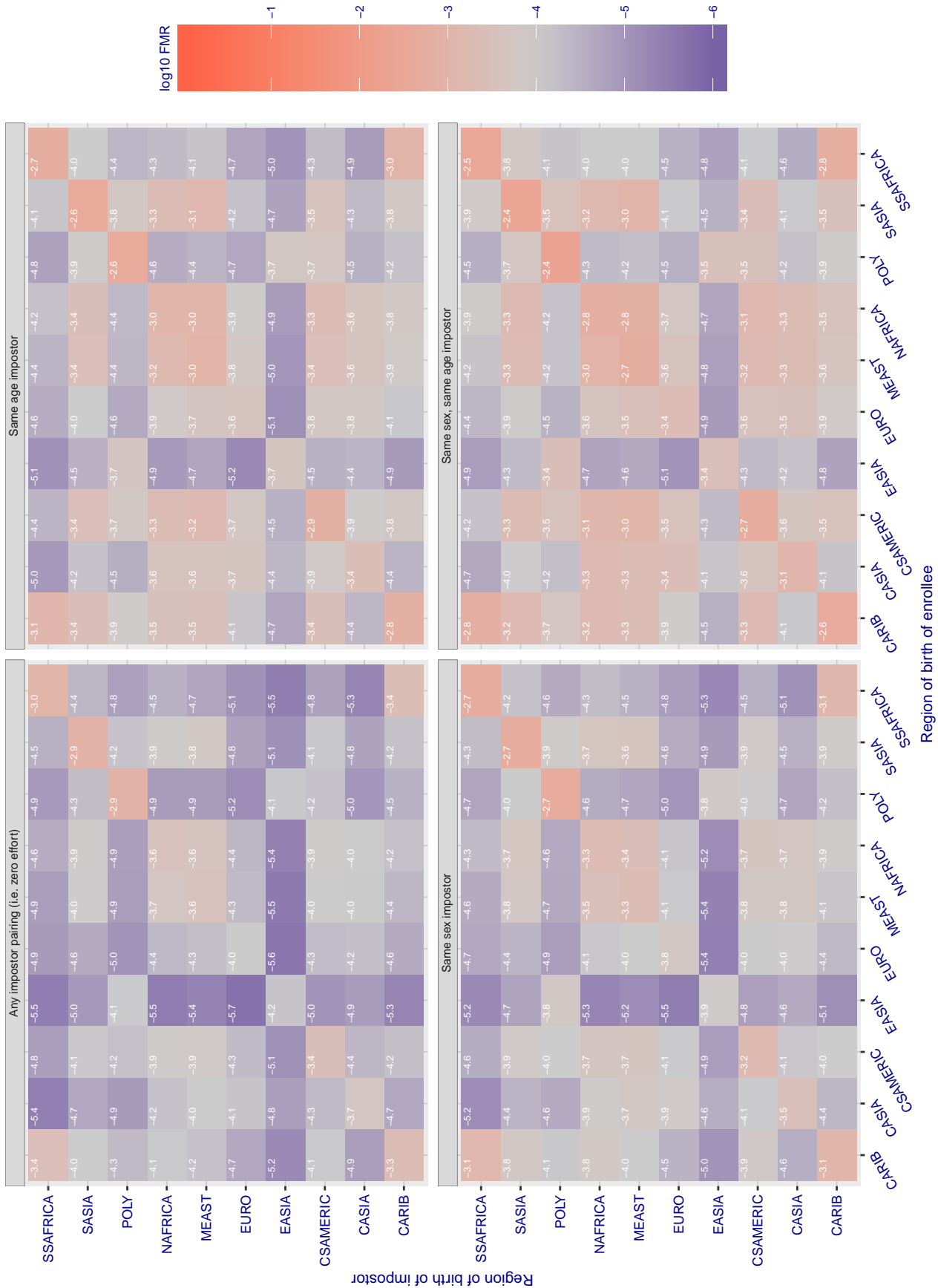


Figure 190: For algorithm dahua-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold T = 6034.000 for algorithm dahua\_003, giving FMR(T) = 0.0001 globally.

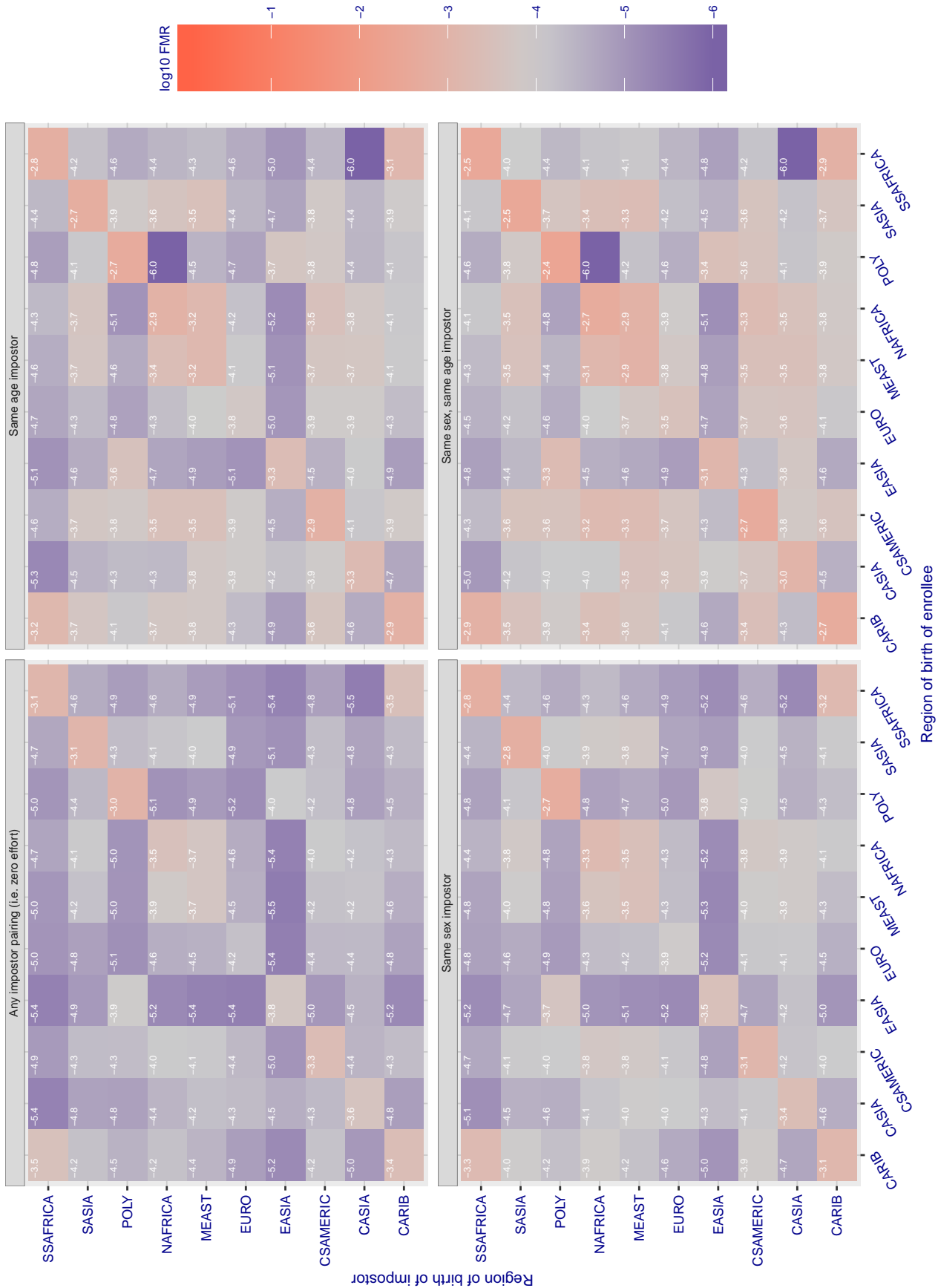


Figure 191: For algorithm dahua-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 1.359$  for algorithm deepglint\_001, giving  $FMR(T) = 0.0001$  globally.

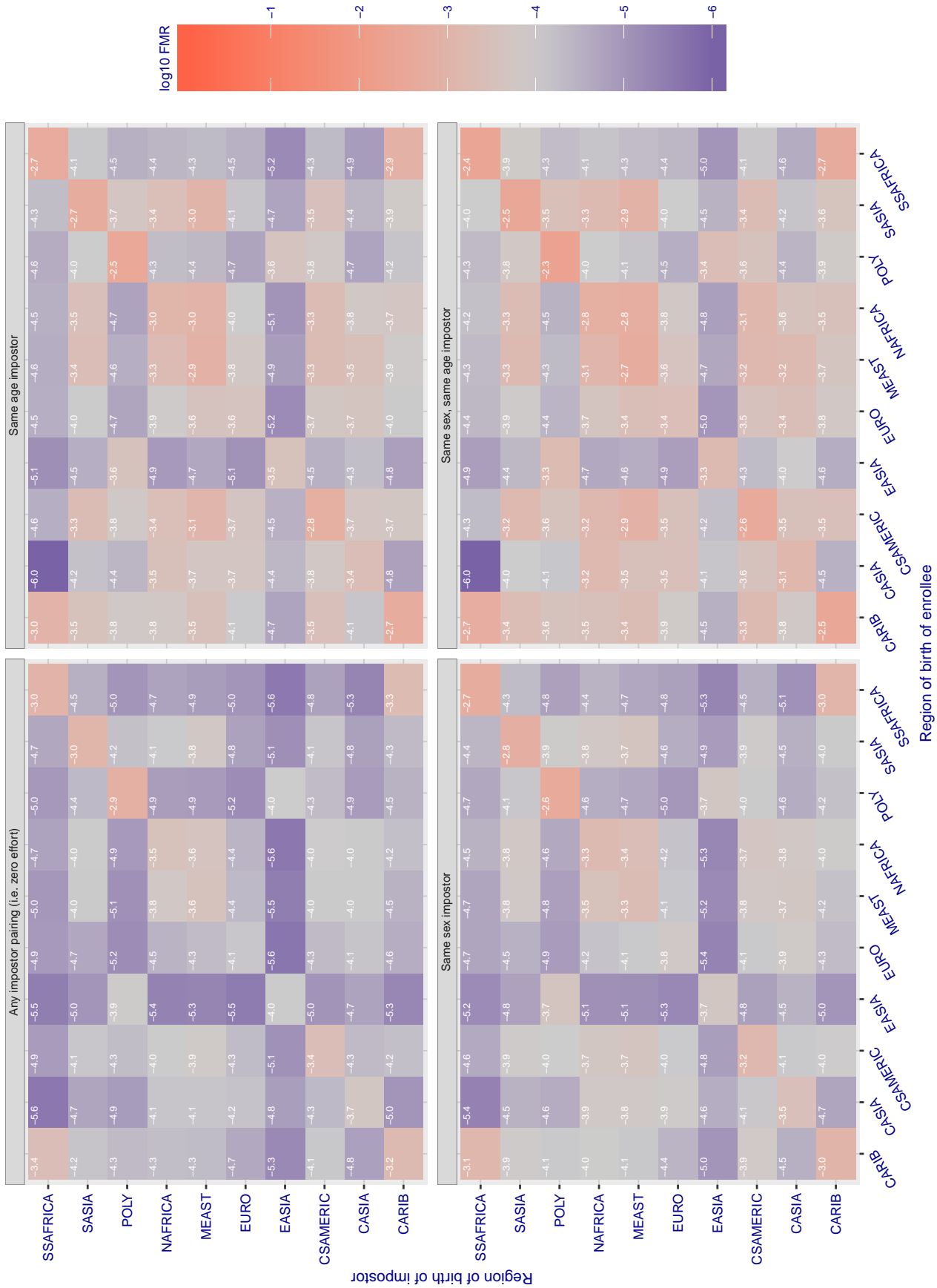


Figure 192: For algorithm deepglint-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 1.371$  for algorithm deepsea\_001, giving  $FMR(T) = 0.0001$  globally.

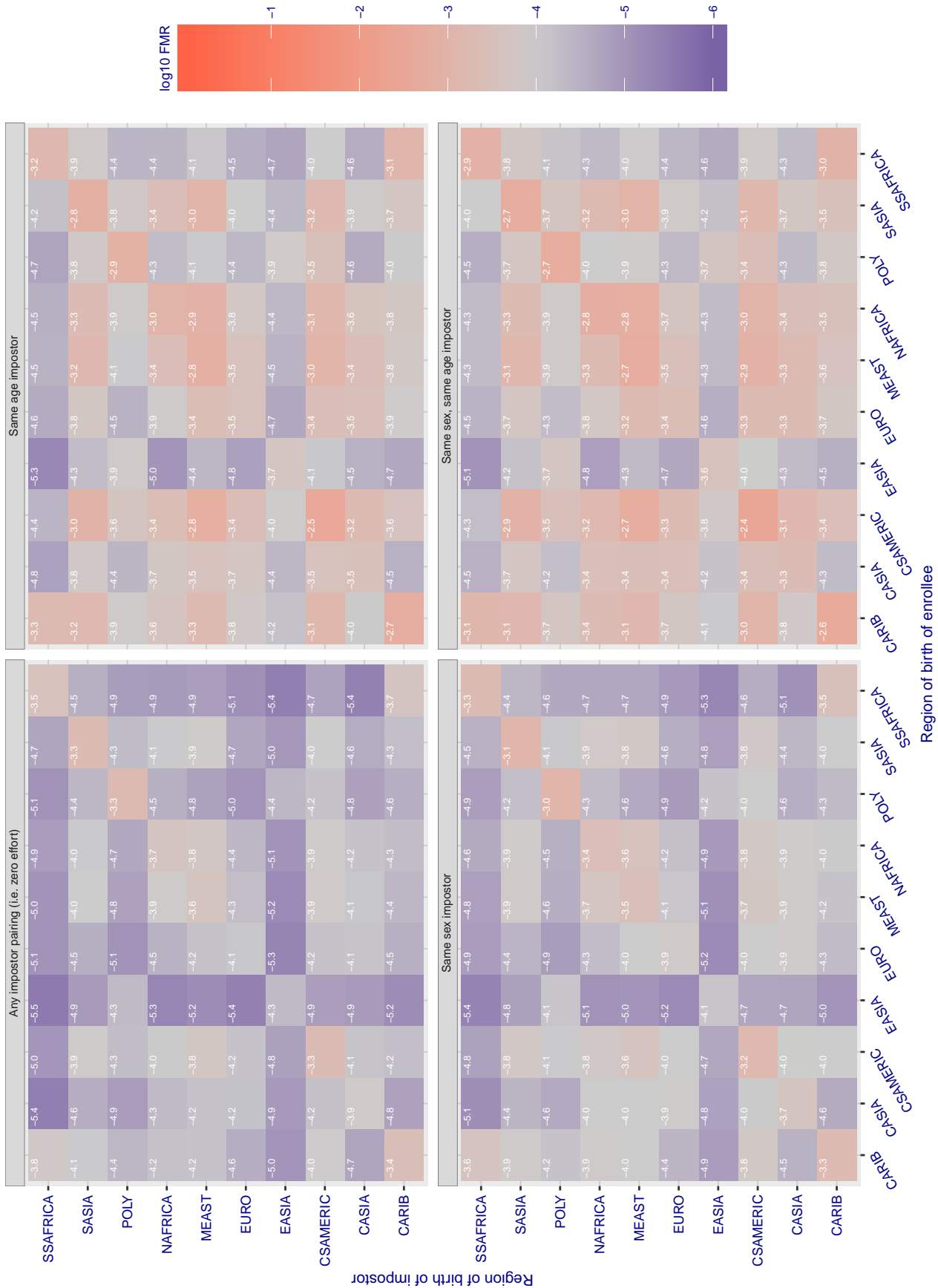


Figure 193: For algorithm deepsea-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 79.344 for algorithm dermalog\_005, giving FMR(T) = 0.0001 globally.

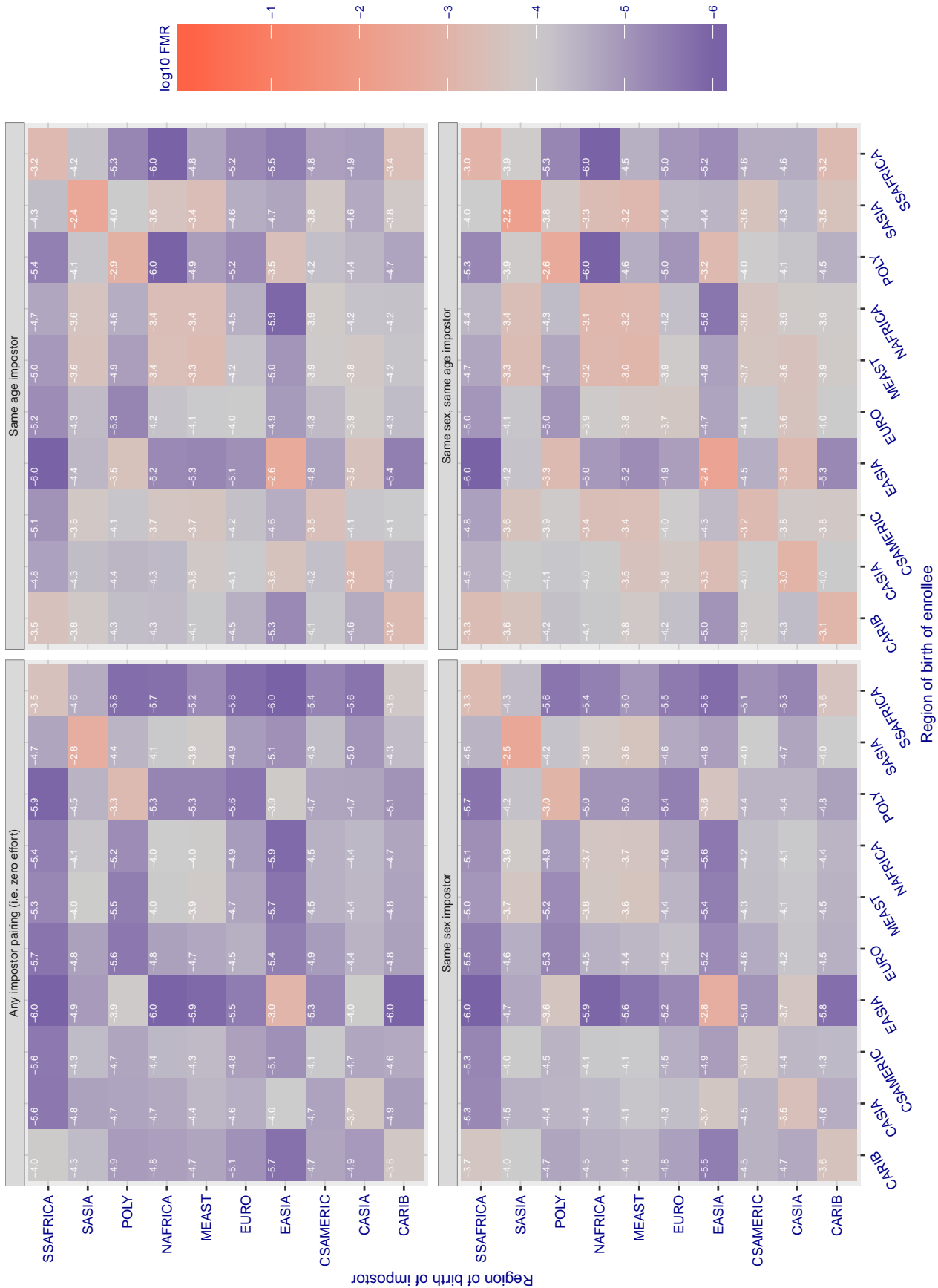


Figure 194: For algorithm dermalog-005 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of 10<sup>10</sup> impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

**Cross region FMR at threshold T = 79.670 for algorithm dermalog\_006, giving FMR(T) = 0.0001 globally.**

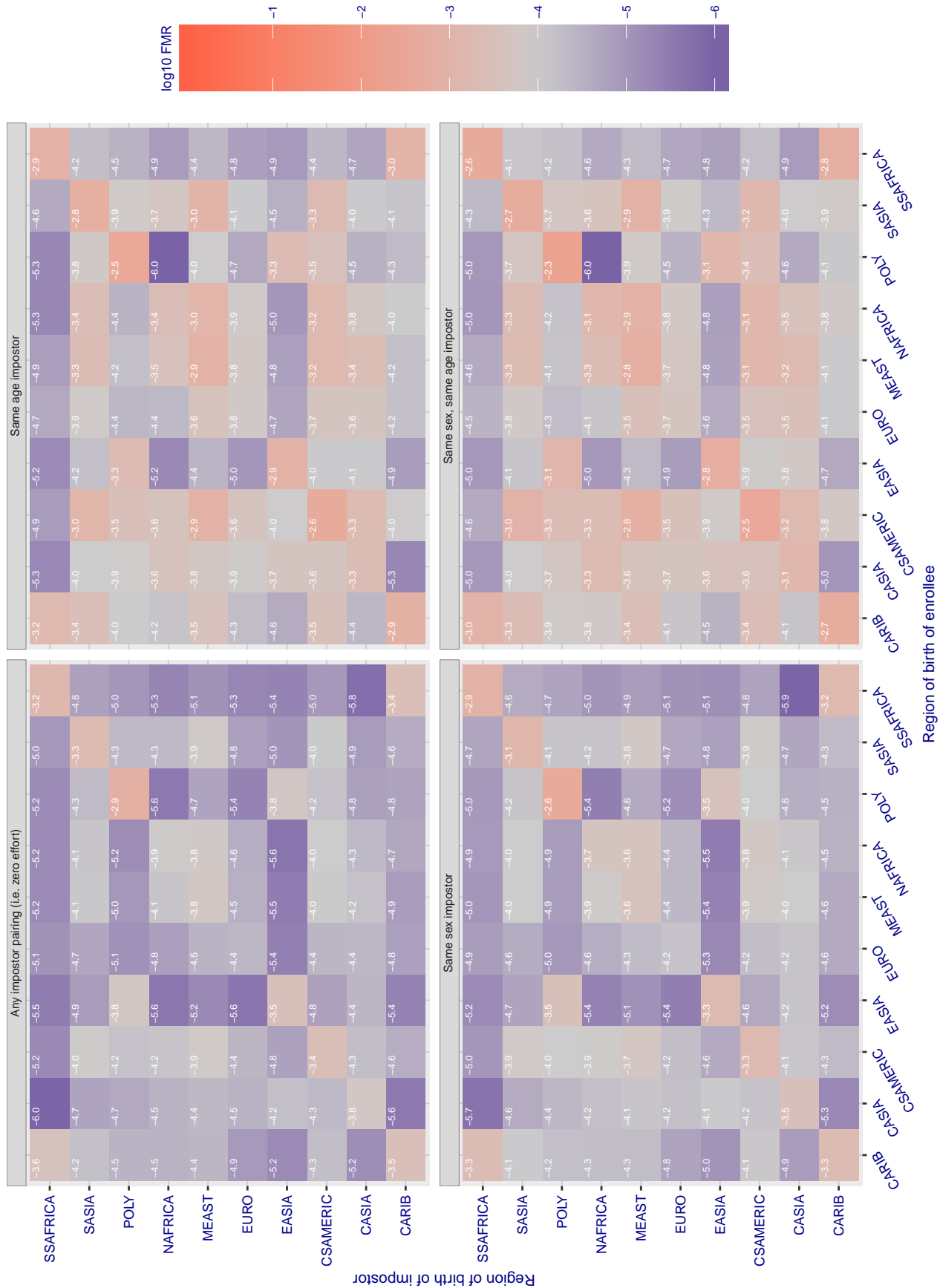


Figure 195: For algorithm dermalog-006 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

**Cross region FMR at threshold  $T = 0.331$  for algorithm didiglobalface\_001, giving  $FMR(T) = 0.0001$  globally.**

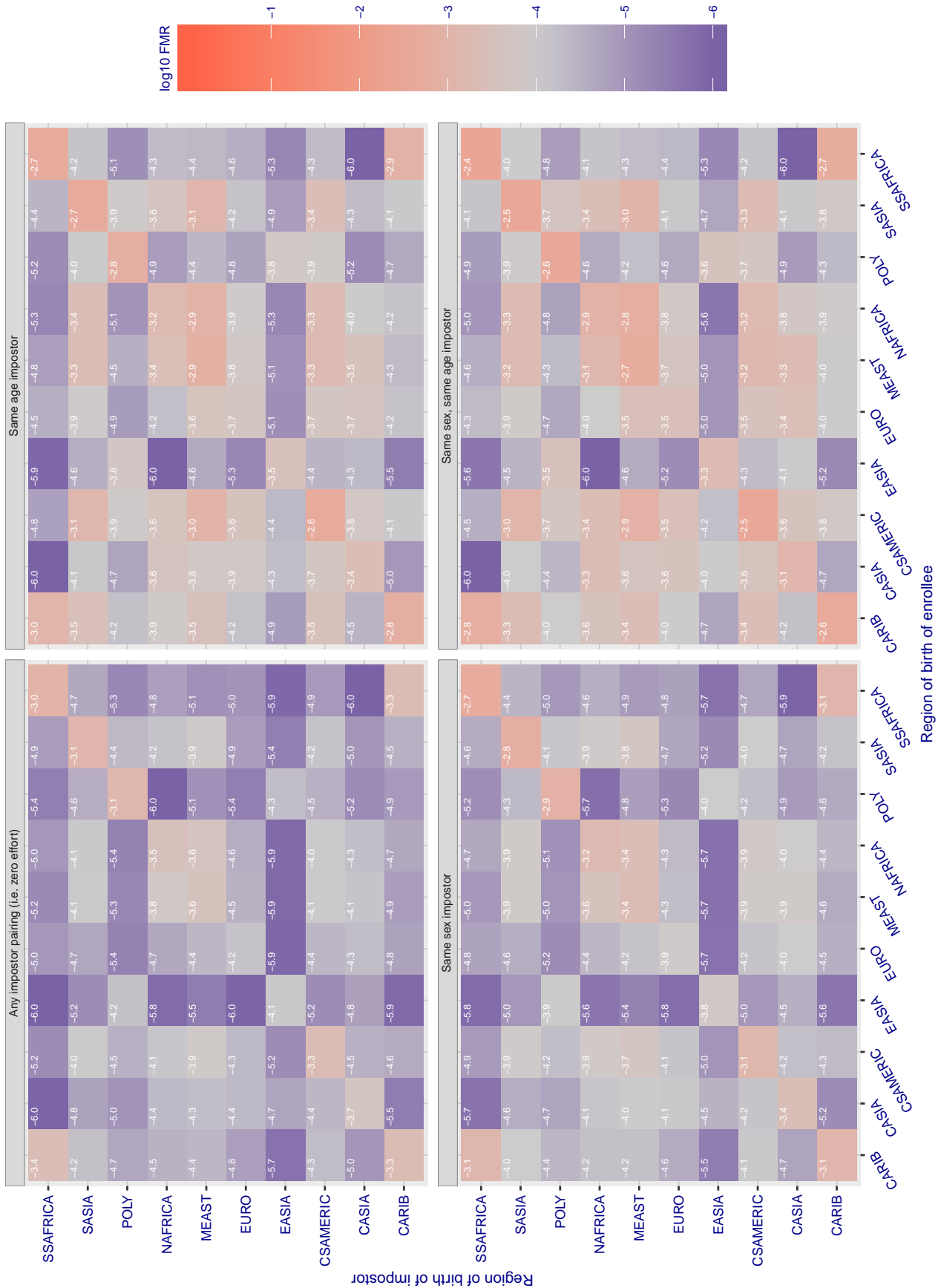


Figure 196: For algorithm didiglobalface-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

**Cross region FMR at threshold  $T = 0.675$  for algorithm digitalbarriers\_002, giving  $FMR(T) = 0.0001$  globally.**

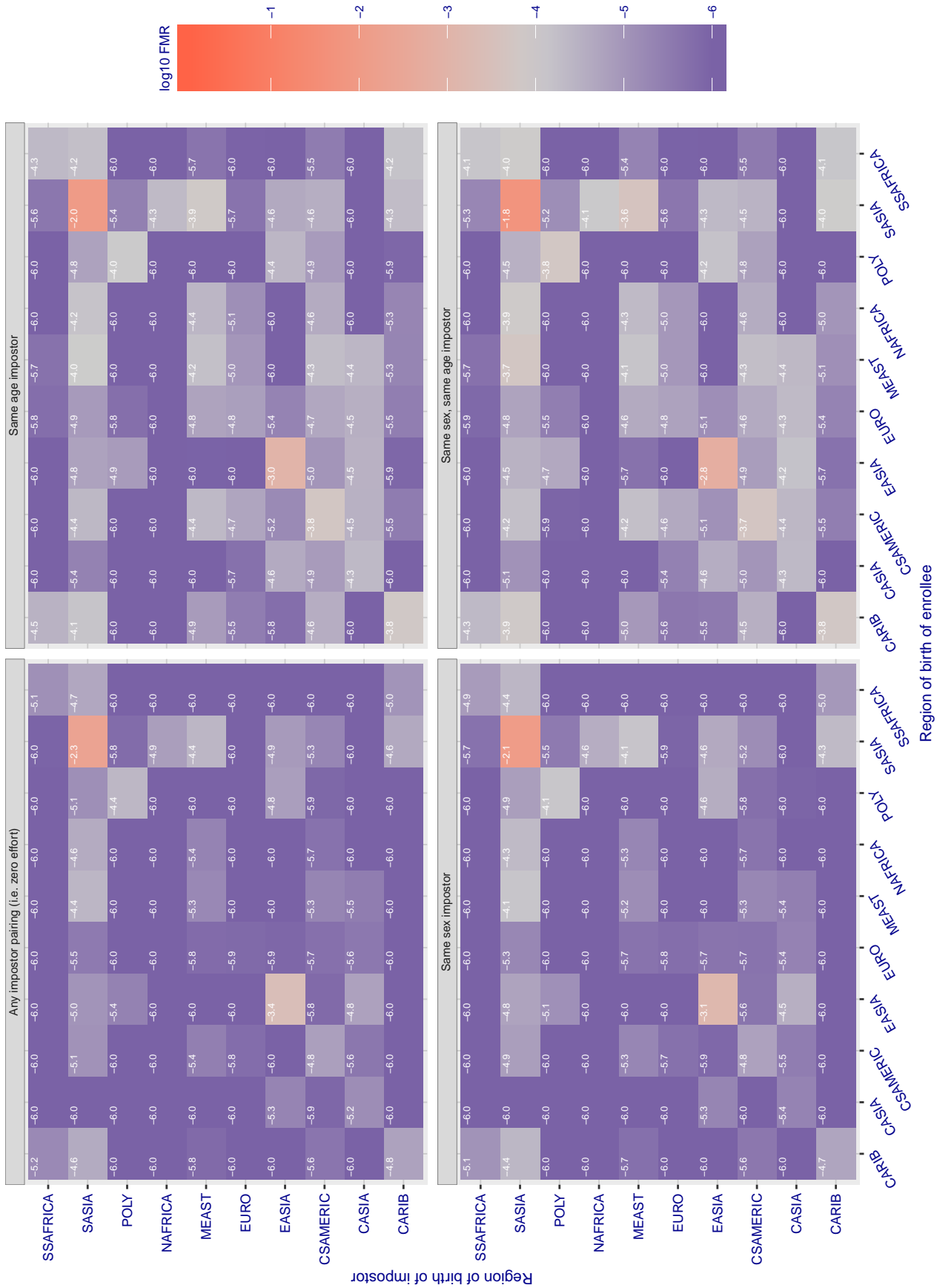


Figure 197: For algorithm digitalbarriers-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 1.061$  for algorithm  $\text{dsk}_{000}$ , giving  $\text{FMR}(T) = 0.0001$  globally.

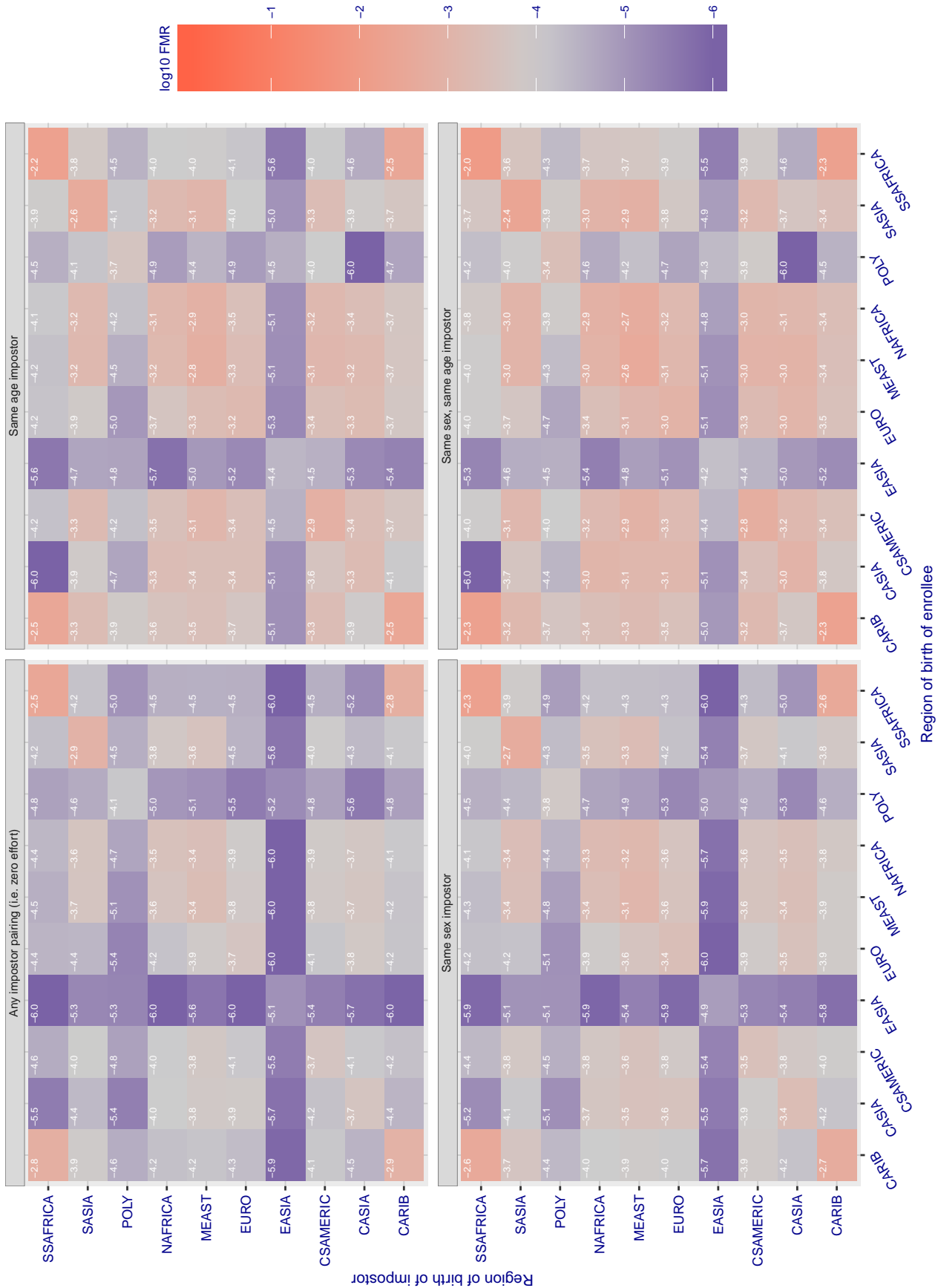


Figure 198: For algorithm  $\text{dsk}_{000}$  operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold T = 53.280 for algorithm einetworks\_000, giving FMR(T) = 0.0001 globally.

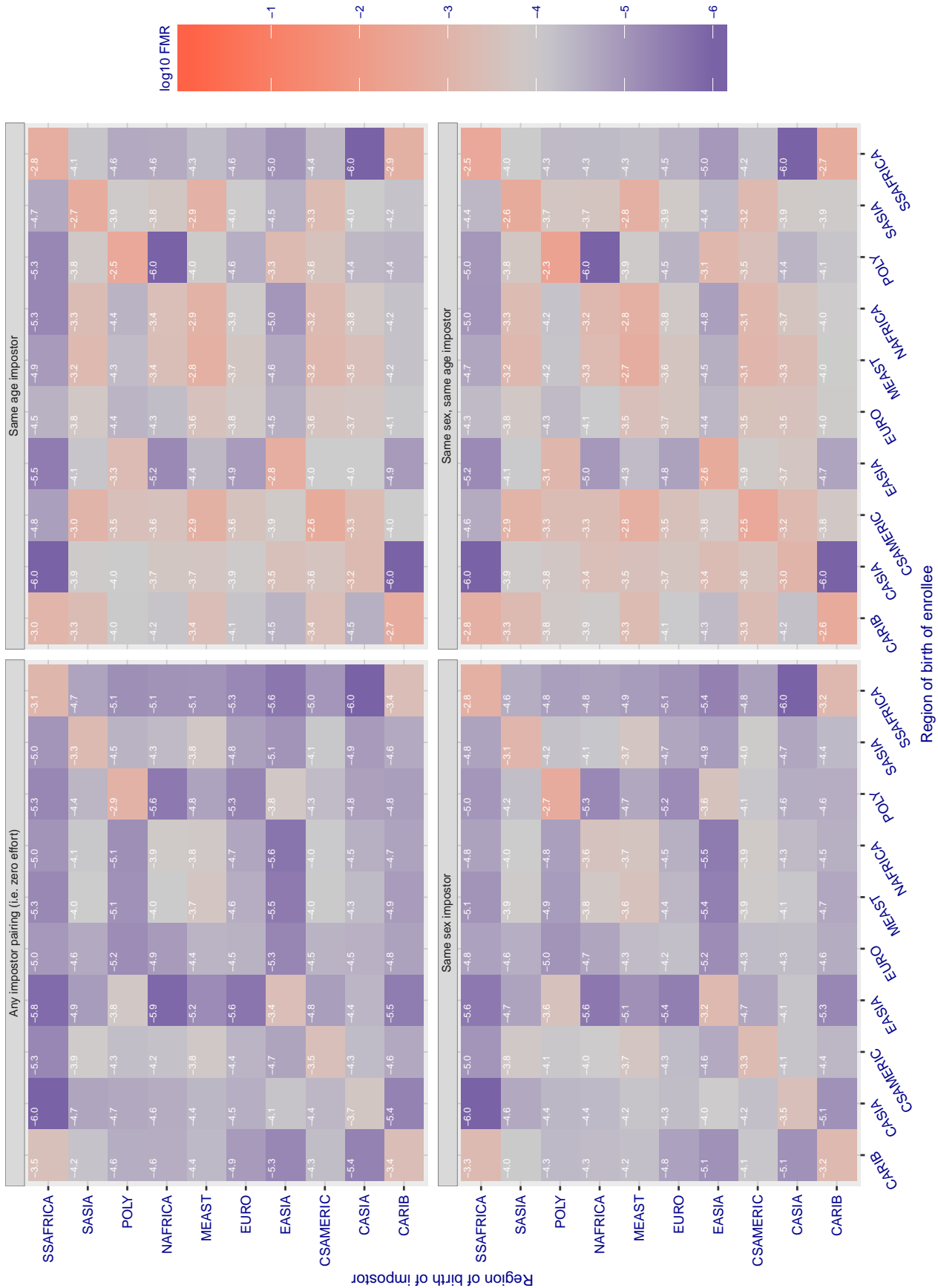


Figure 199: For algorithm einetworks-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 2.589$  for algorithm everai\_002, giving  $FMR(T) = 0.0001$  globally.

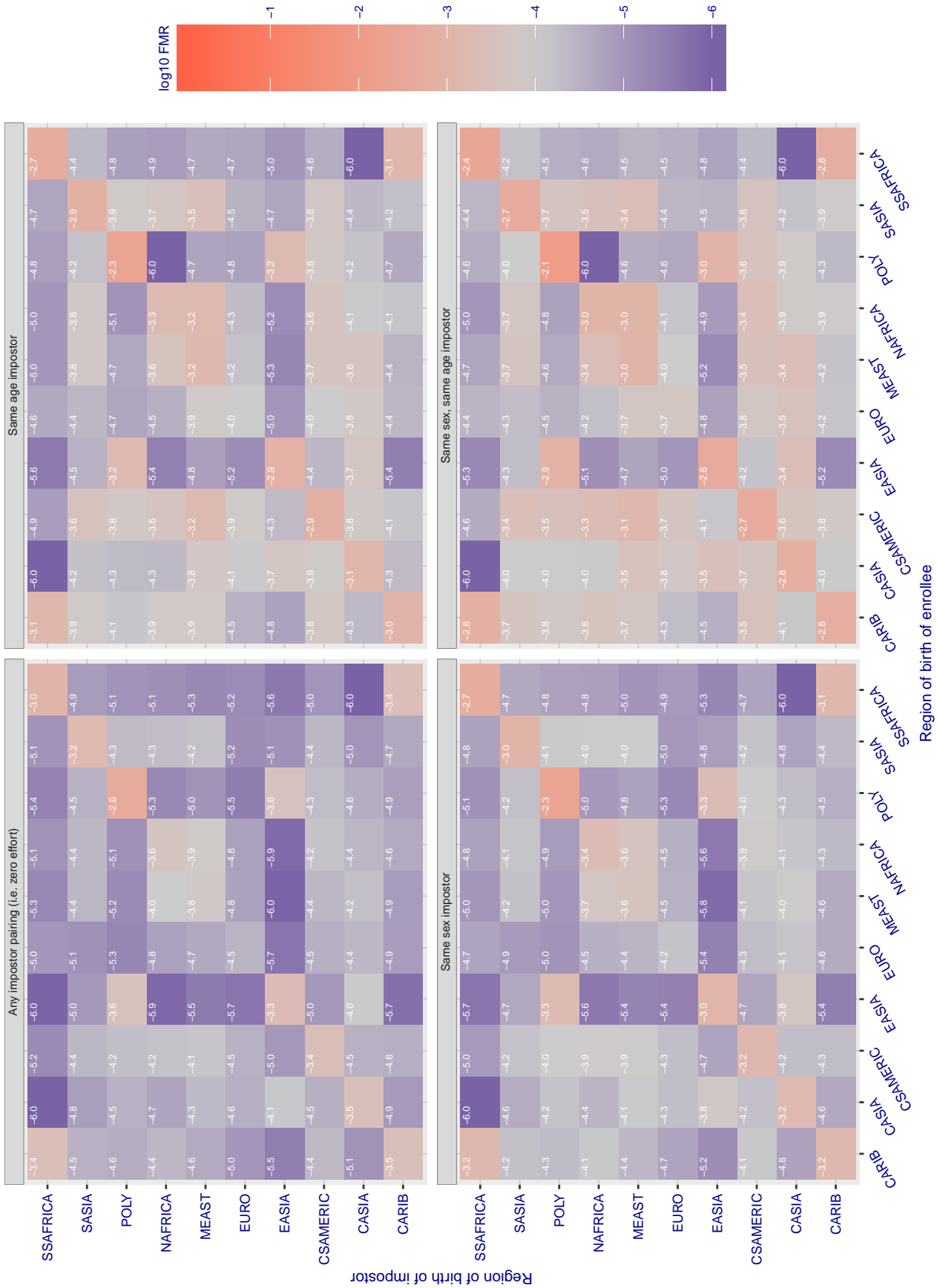


Figure 200: For algorithm everai-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 0.400$  for algorithm f8\_001, giving  $FMR(T) = 0.0001$  globally.

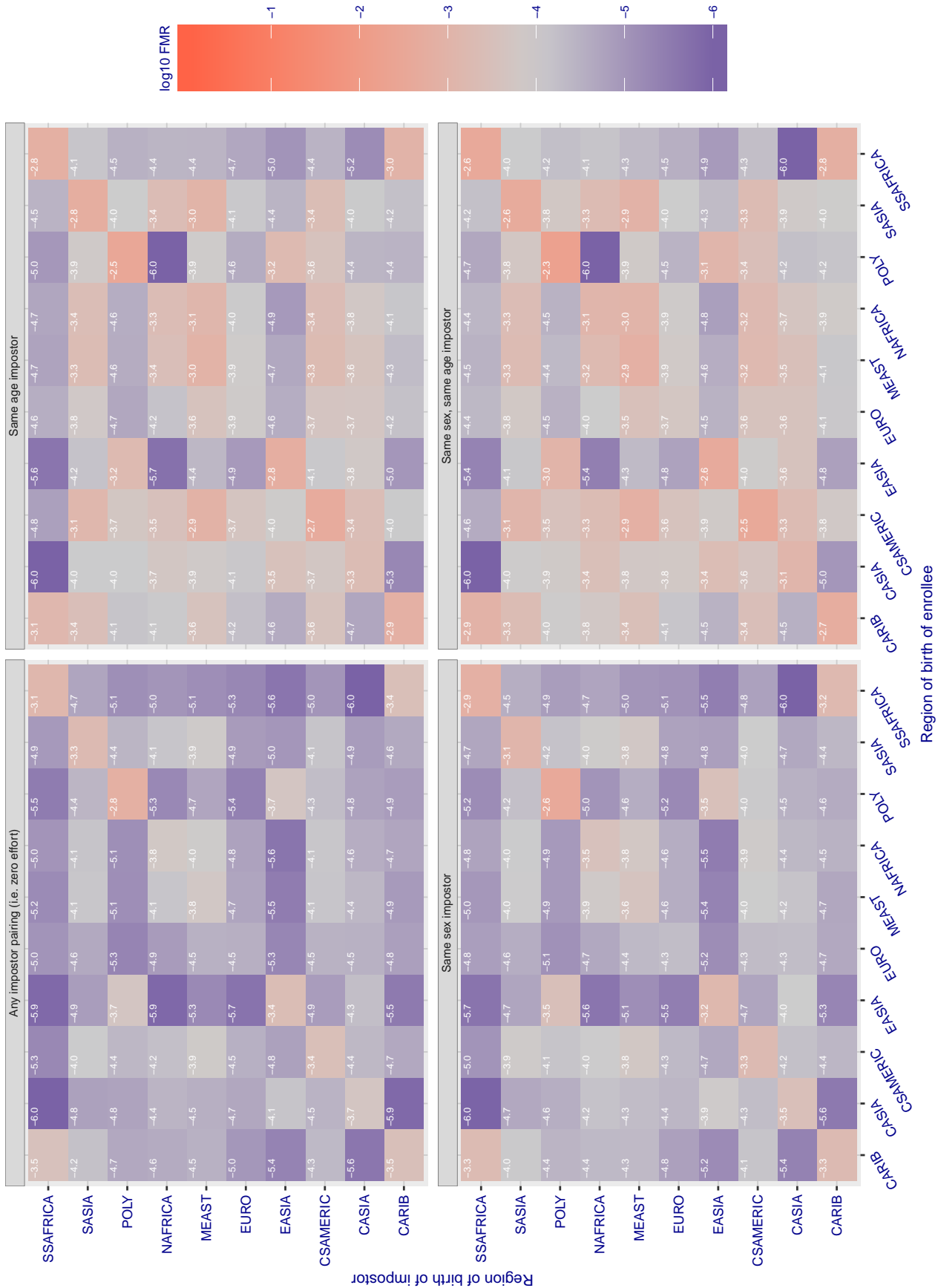


Figure 201: For algorithm f8-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 1.375$  for algorithm facesoft\_000, giving  $FMR(T) = 0.0001$  globally.

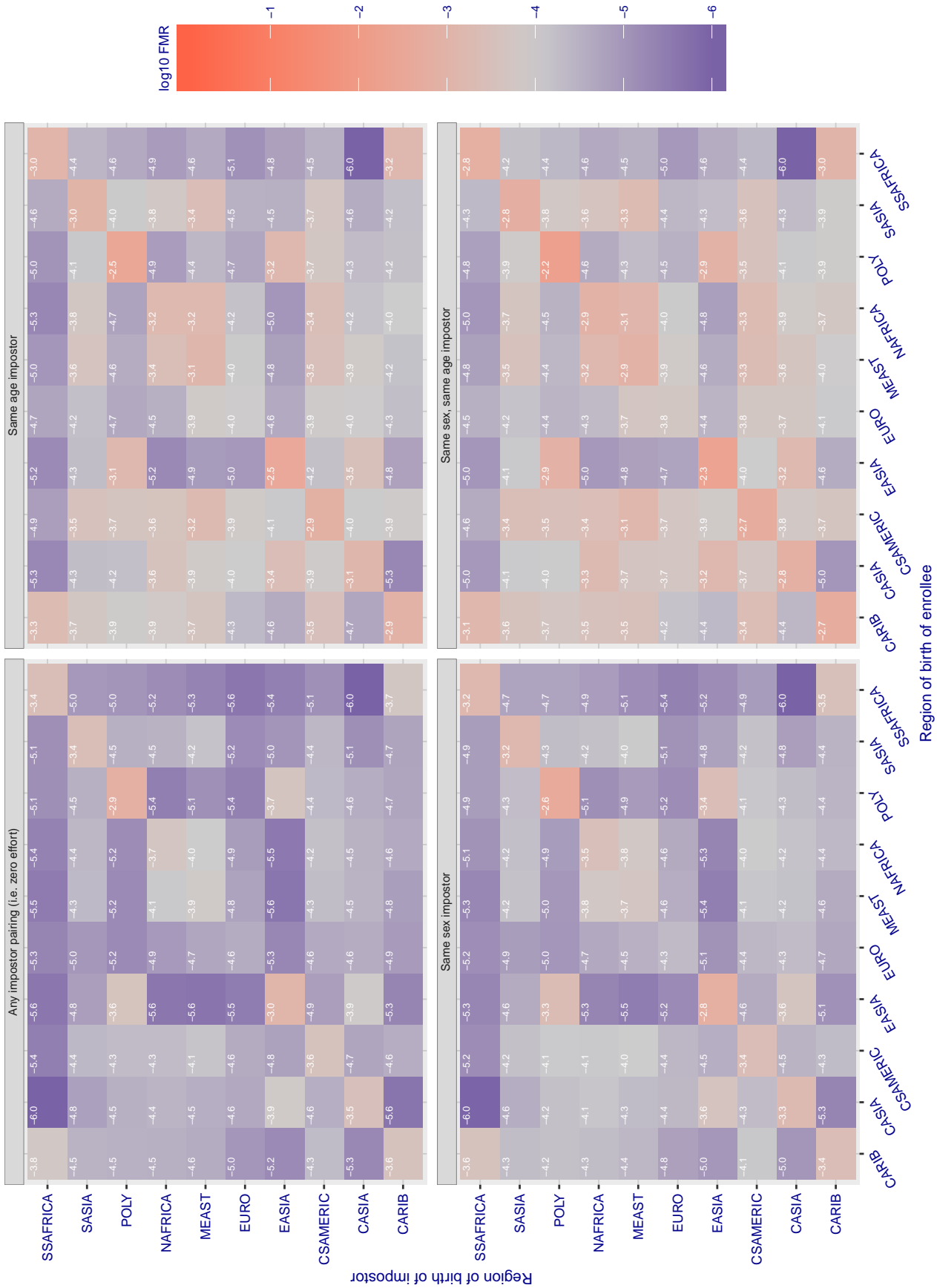


Figure 202: For algorithm facesoft-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 0.618 for algorithm glory\_001, giving FMR(T) = 0.0001 globally.

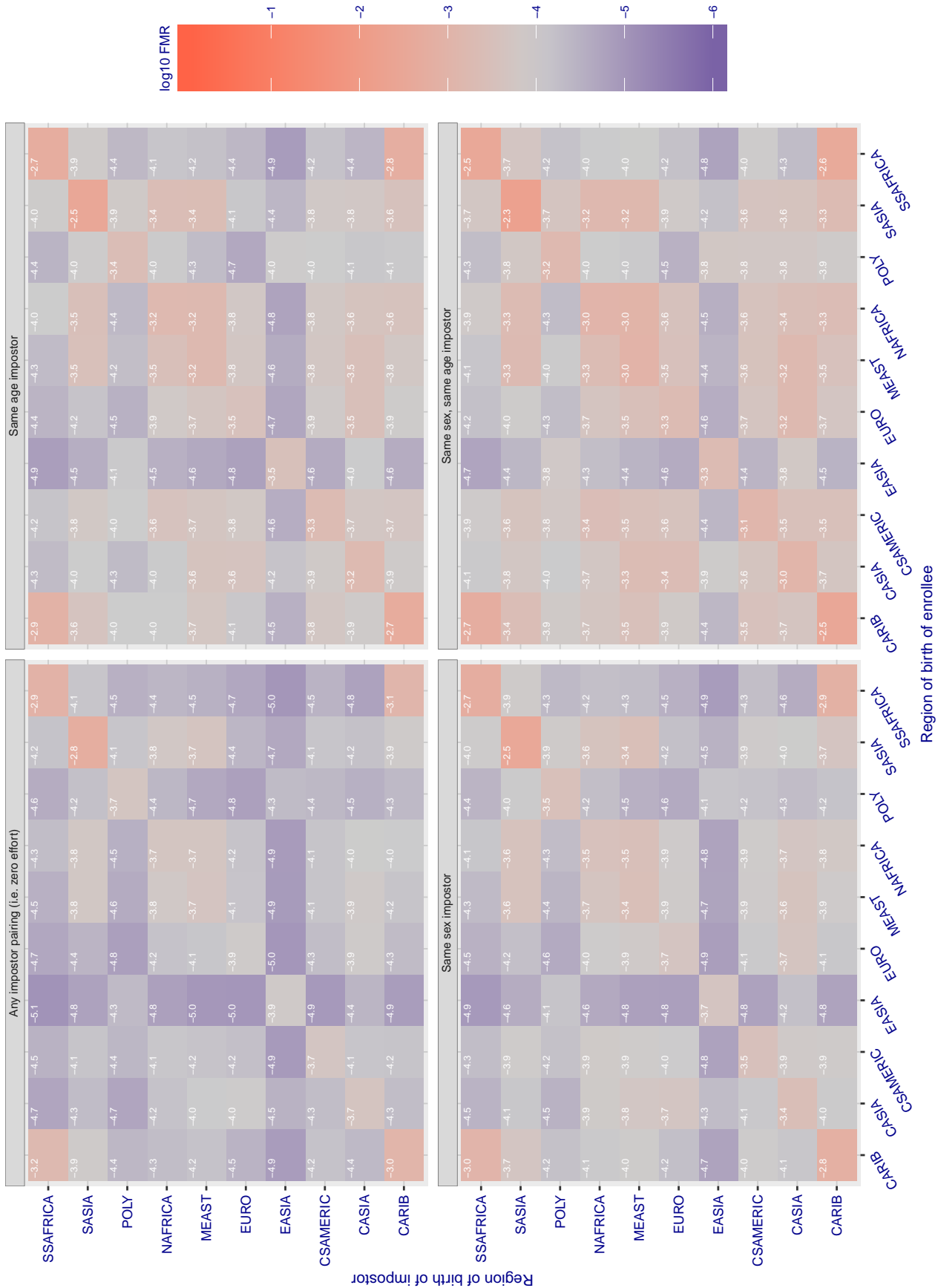


Figure 203: For algorithm glory-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.598$  for algorithm glory\_002, giving  $FMR(T) = 0.0001$  globally.

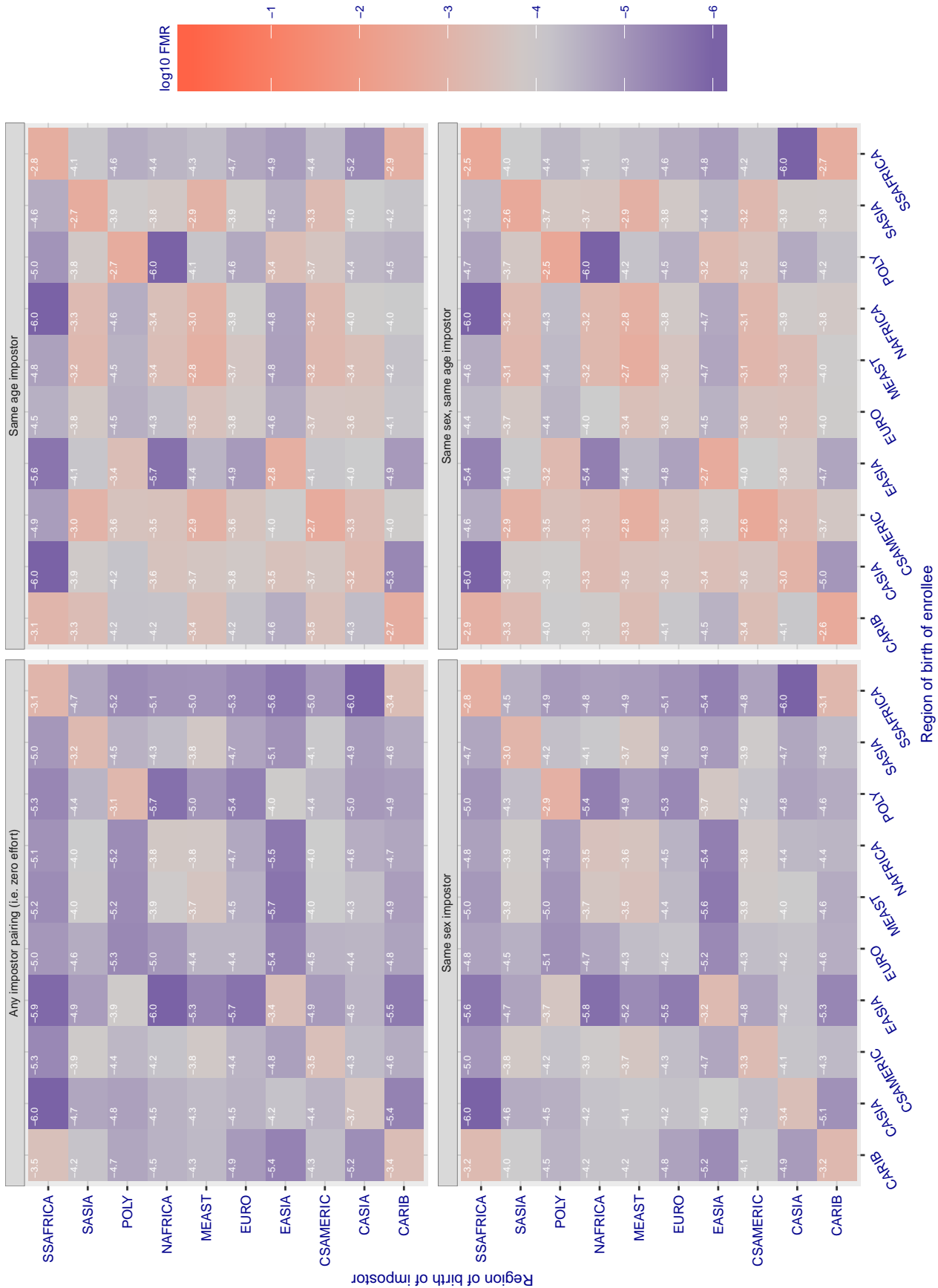


Figure 204: For algorithm glory-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.454$  for algorithm gorilla\_003, giving  $FMR(T) = 0.0001$  globally.

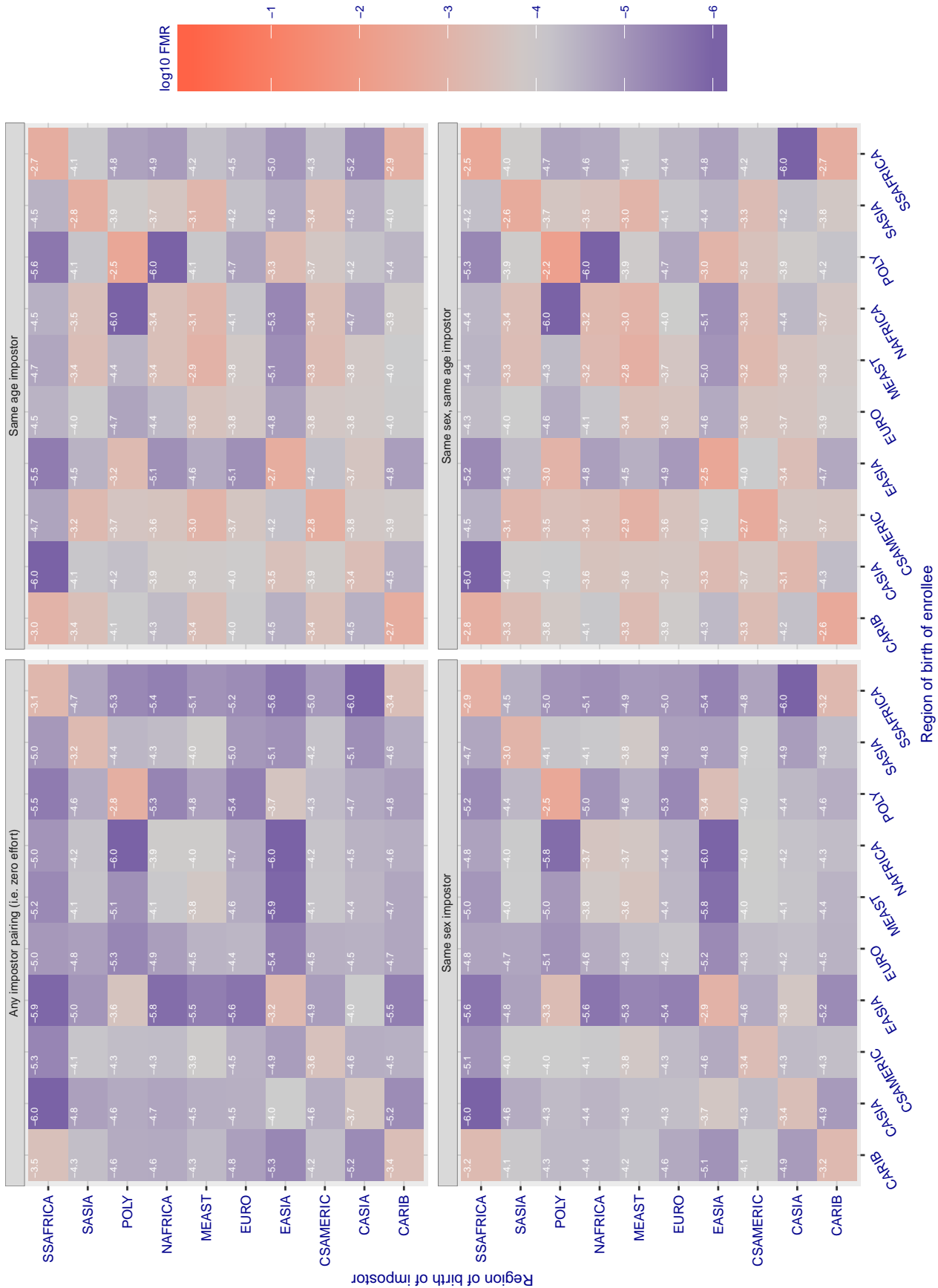


Figure 205: For algorithm gorilla-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.507$  for algorithm gorilla\_004, giving  $FMR(T) = 0.0001$  globally.

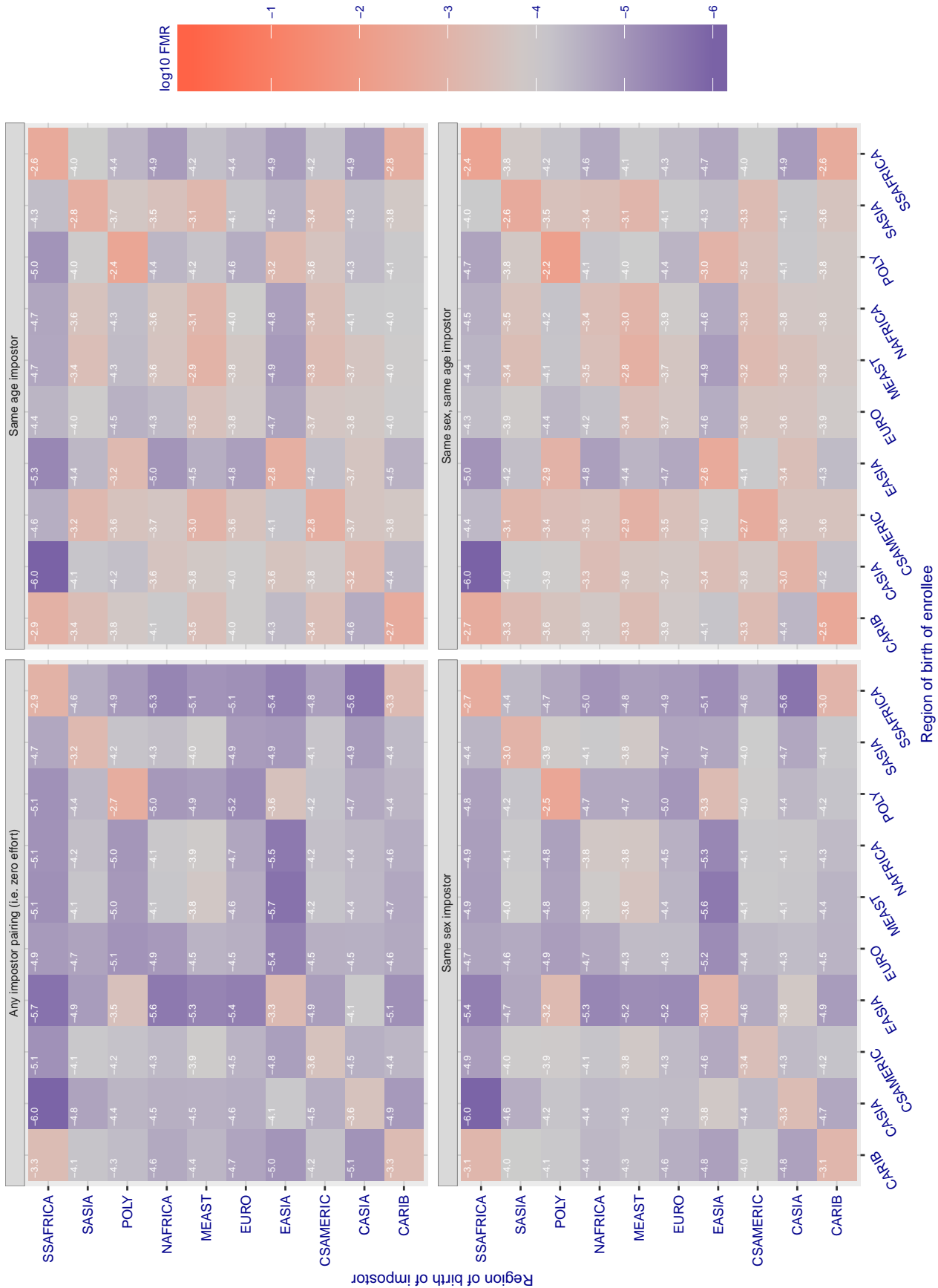


Figure 206: For algorithm gorilla-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold T = 66.565 for algorithm hik\_001, giving FMR(T) = 0.0001 globally.

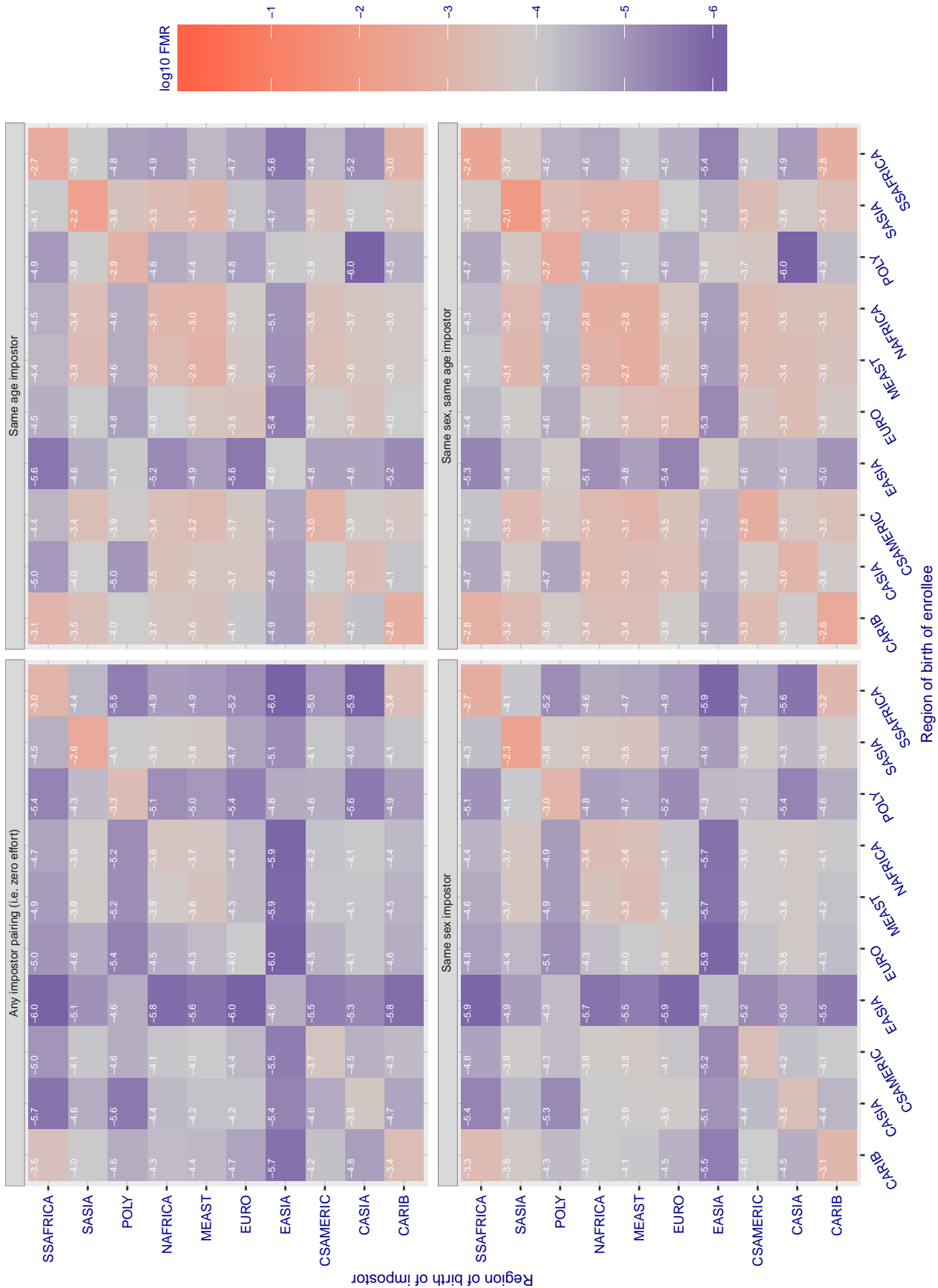


Figure 207: For algorithm hik-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.823$  for algorithm hr\_001, giving  $FMR(T) = 0.0001$  globally.

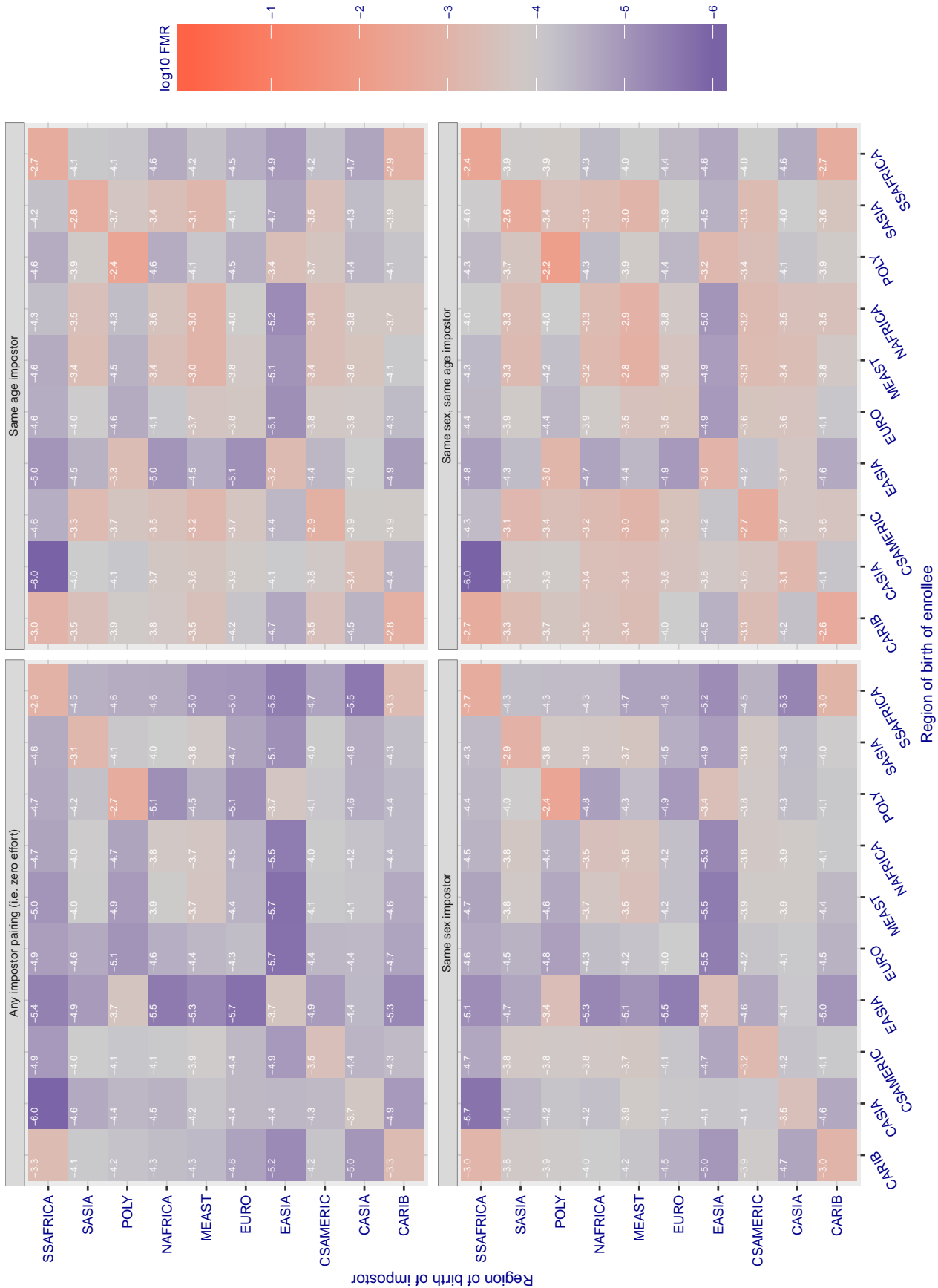


Figure 208: For algorithm hr-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 0.285$  for algorithm hr\_002, giving  $FMR(T) = 0.0001$  globally.

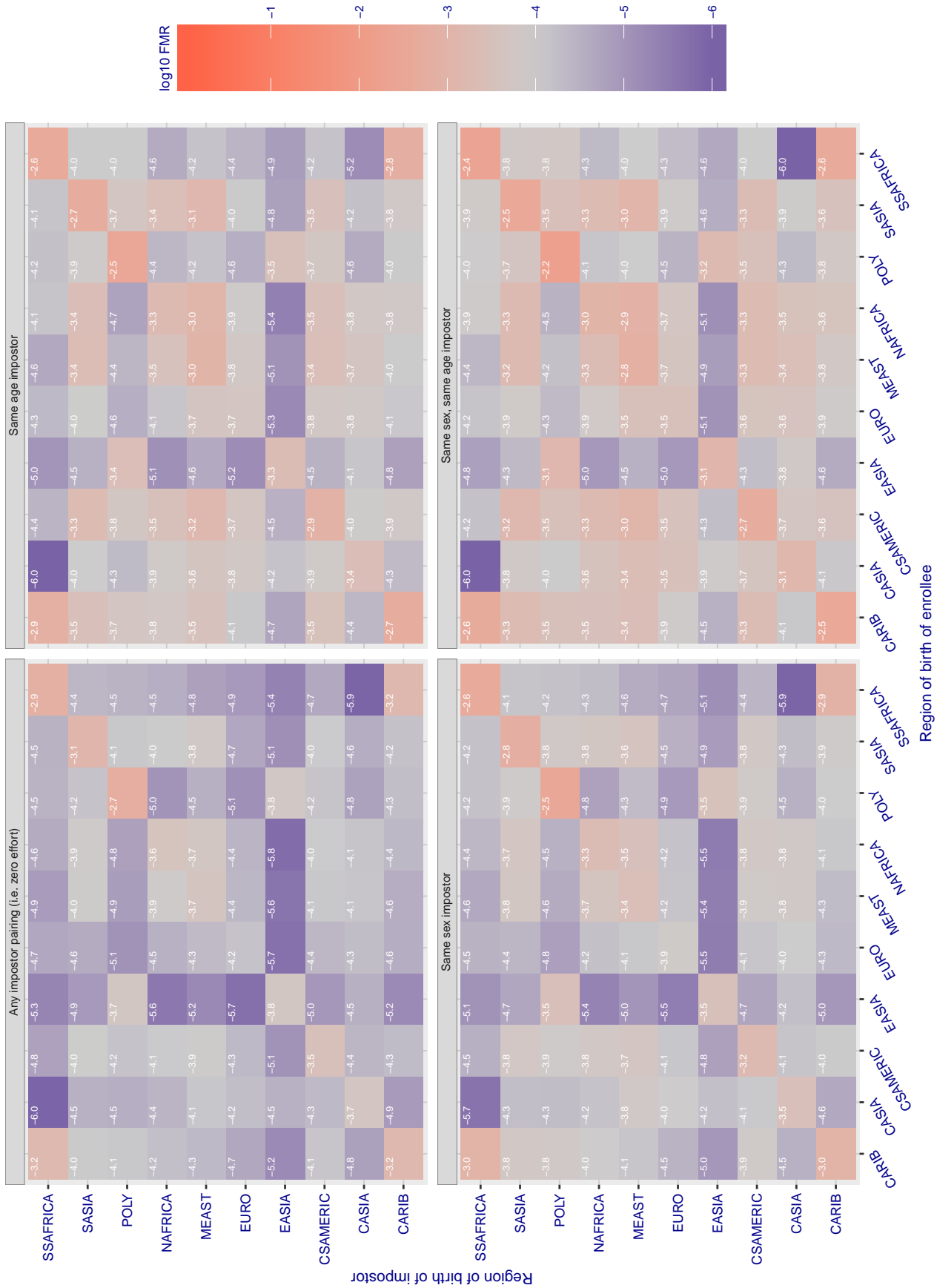


Figure 209: For algorithm hr-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 37645.000$  for algorithm `id3_003`, giving  $FMR(T) = 0.0001$  globally.

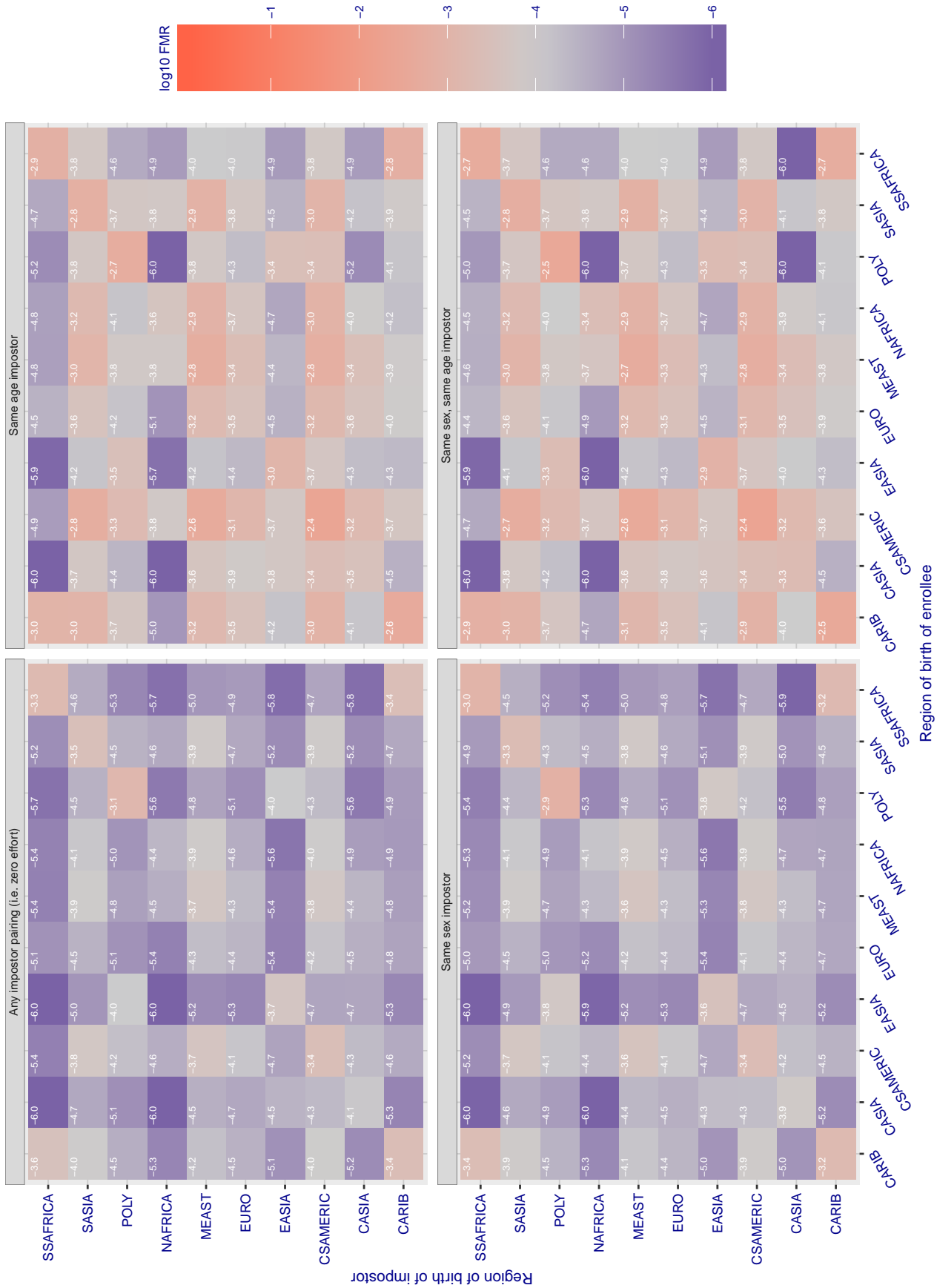


Figure 210: For algorithm `id3-003` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 37001.000 for algorithm id3\_004, giving FMR(T) = 0.0001 globally.

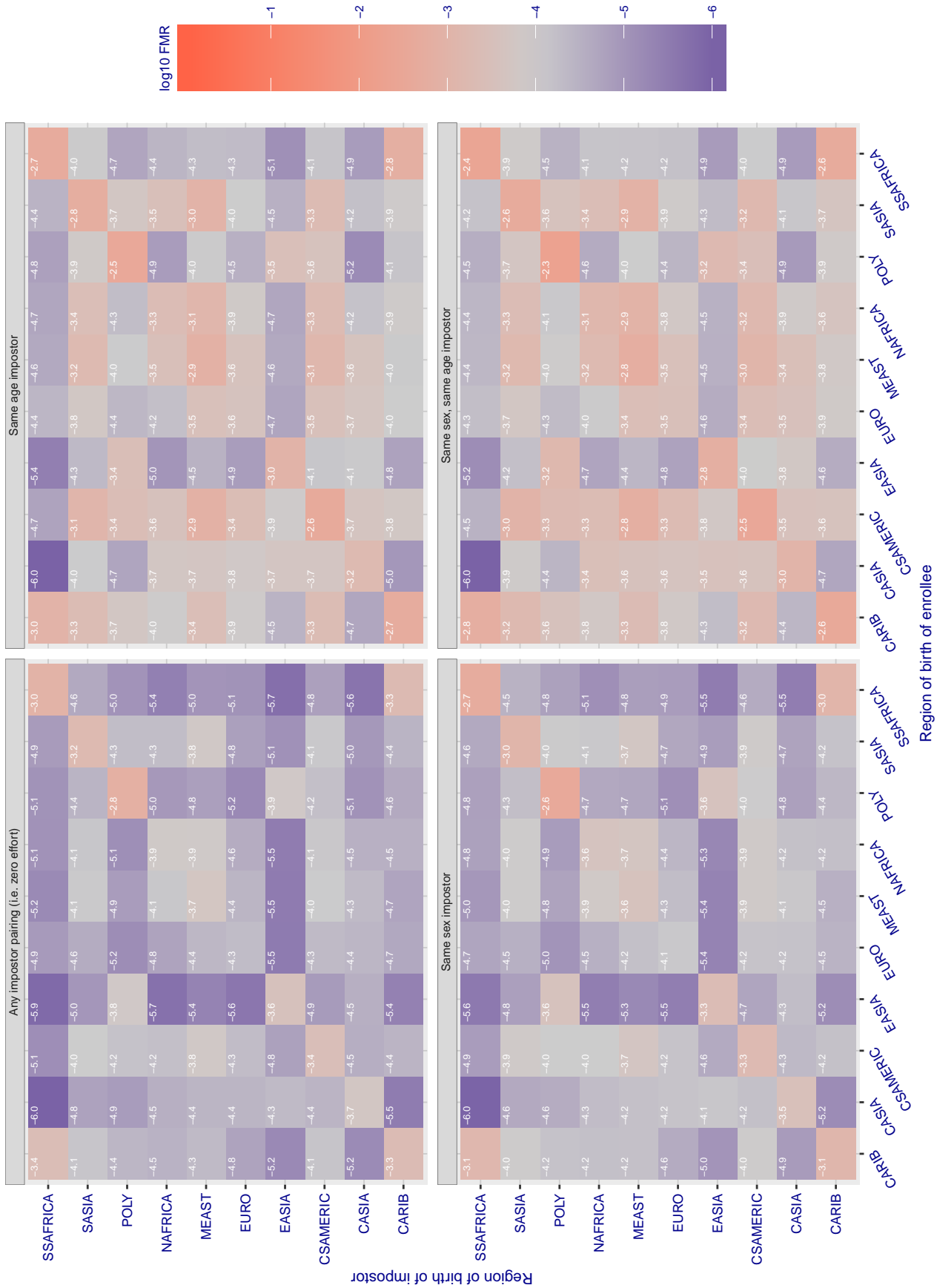


Figure 211: For algorithm id3-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 3925.463 for algorithm idemia\_004, giving FMR(T) = 0.0001 globally.

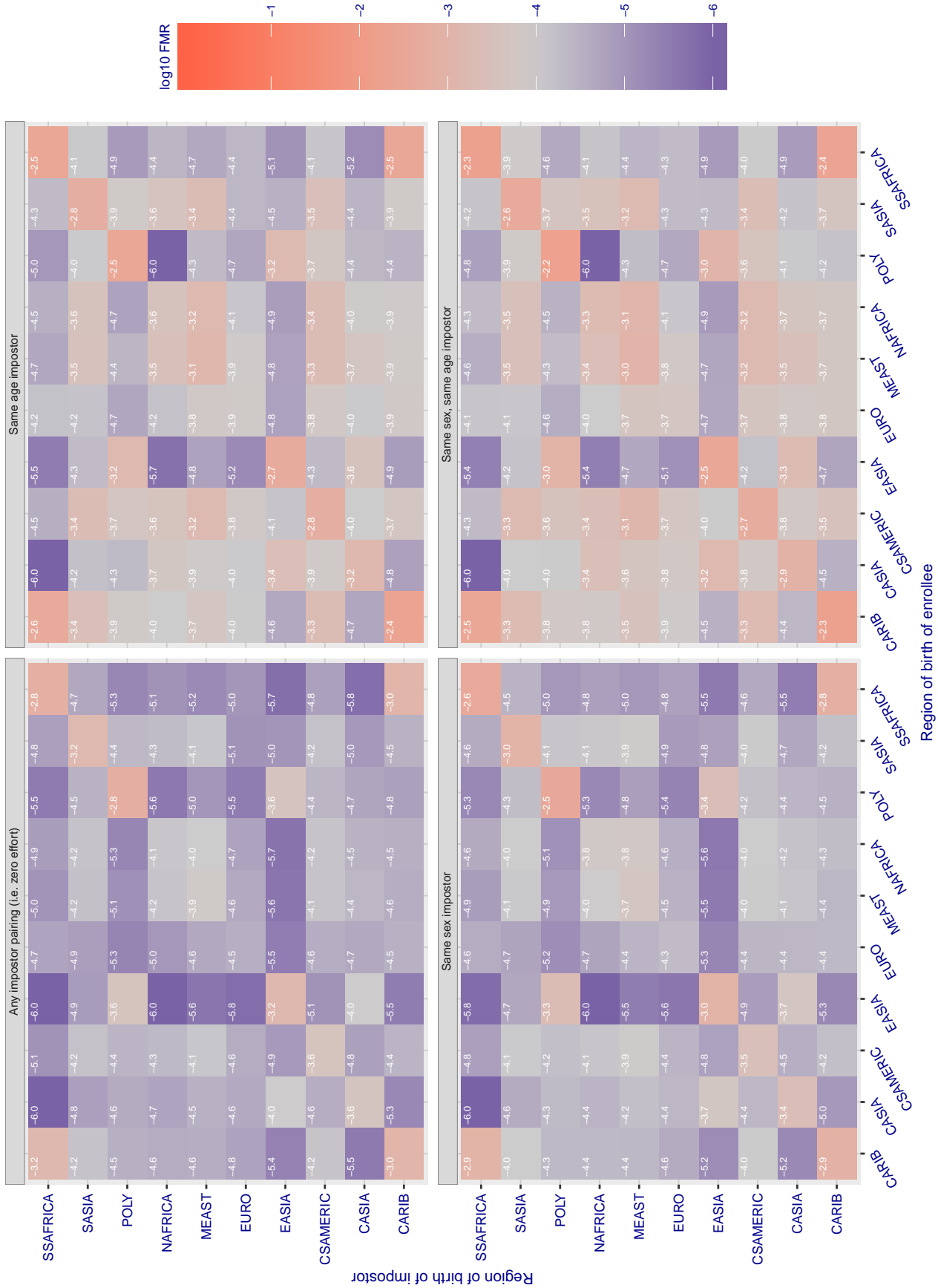


Figure 212: For algorithm idemia-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of 10<sup>10</sup> impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 3764.961 for algorithm idemia\_005, giving FMR(T) = 0.0001 globally.

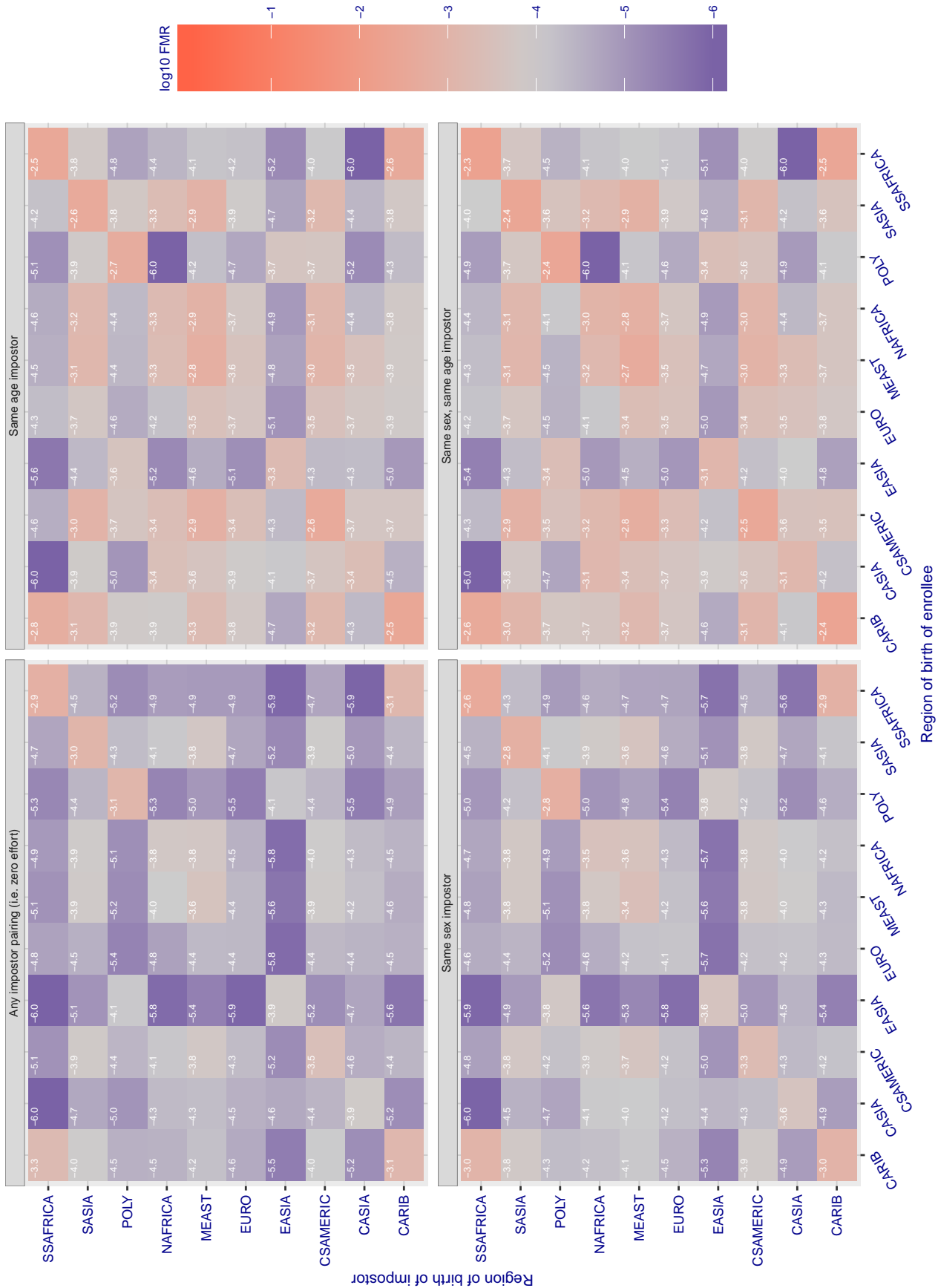


Figure 213: For algorithm idemia-005 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.760$  for algorithm  $it_{000}$ , giving  $FMR(T) = 0.0001$  globally.

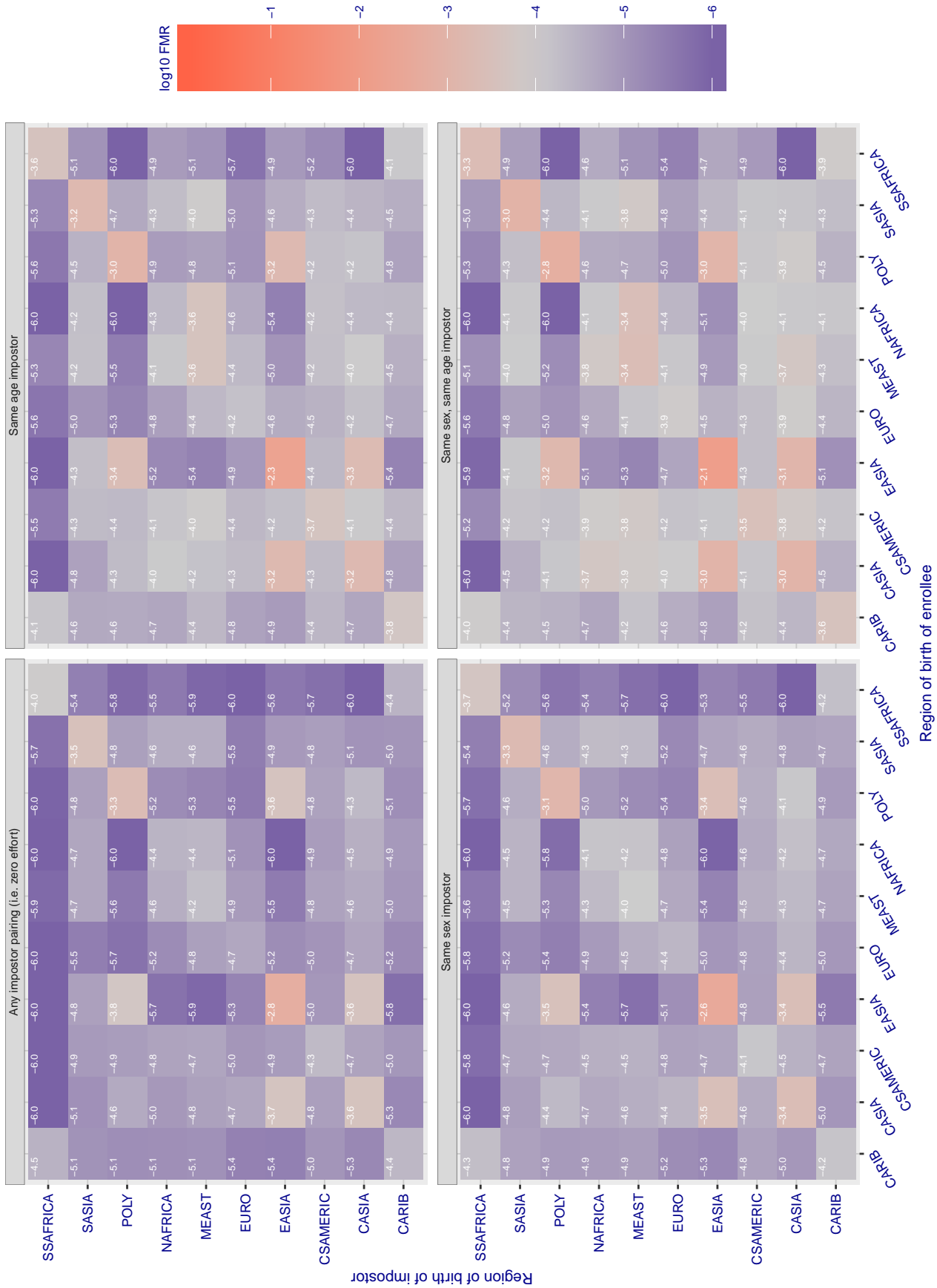


Figure 214: For algorithm  $it_{000}$  operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 0.691$  for algorithm `it_001`, giving  $FMR(T) = 0.0001$  globally.

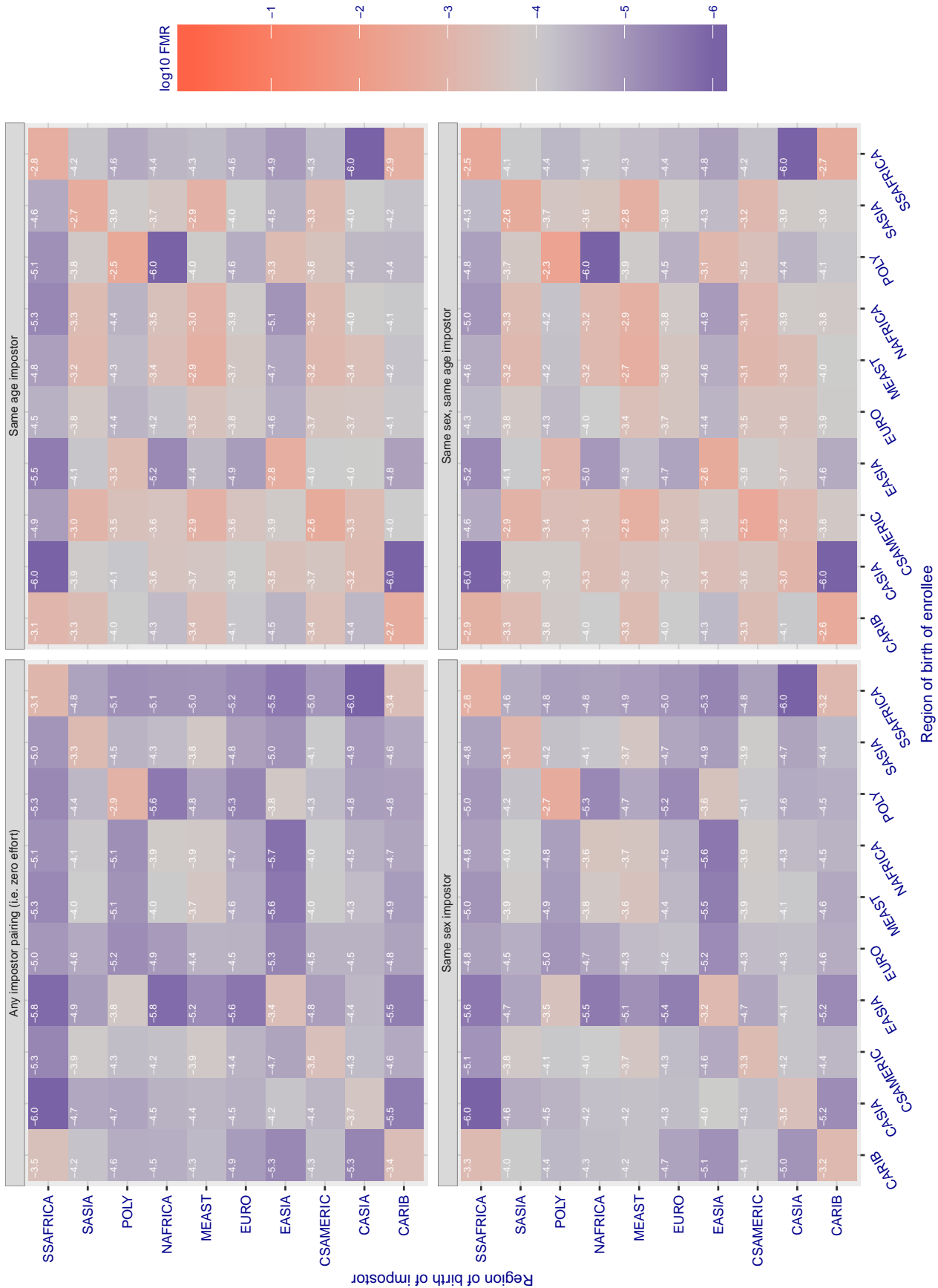


Figure 215: For algorithm `it-001` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 0.926 for algorithm imagus\_000, giving FMR(T) = 0.0001 globally.

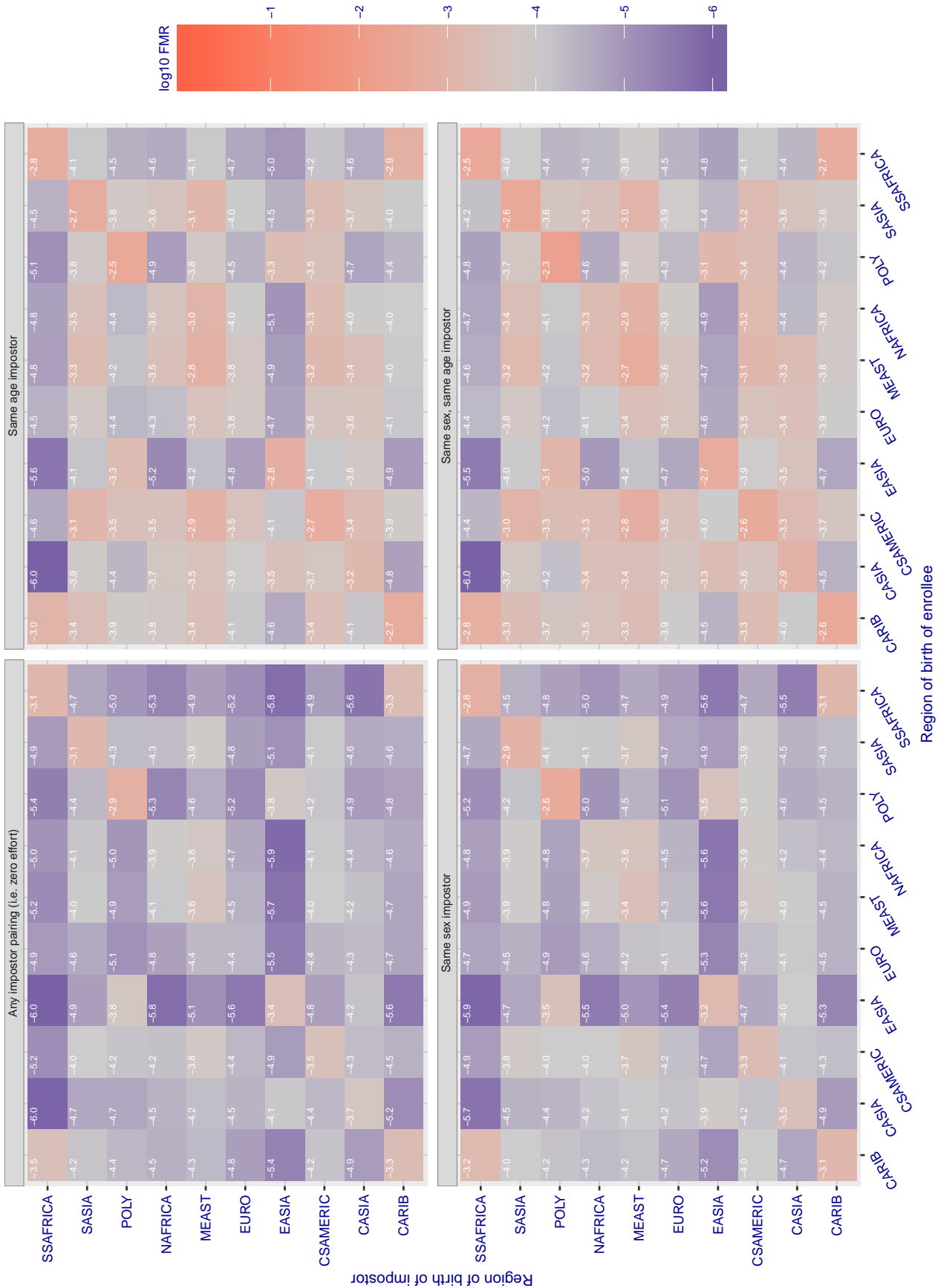


Figure 216: For algorithm imagus-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold T = 0.402 for algorithm imagus\_001, giving FMR(T) = 0.0001 globally.

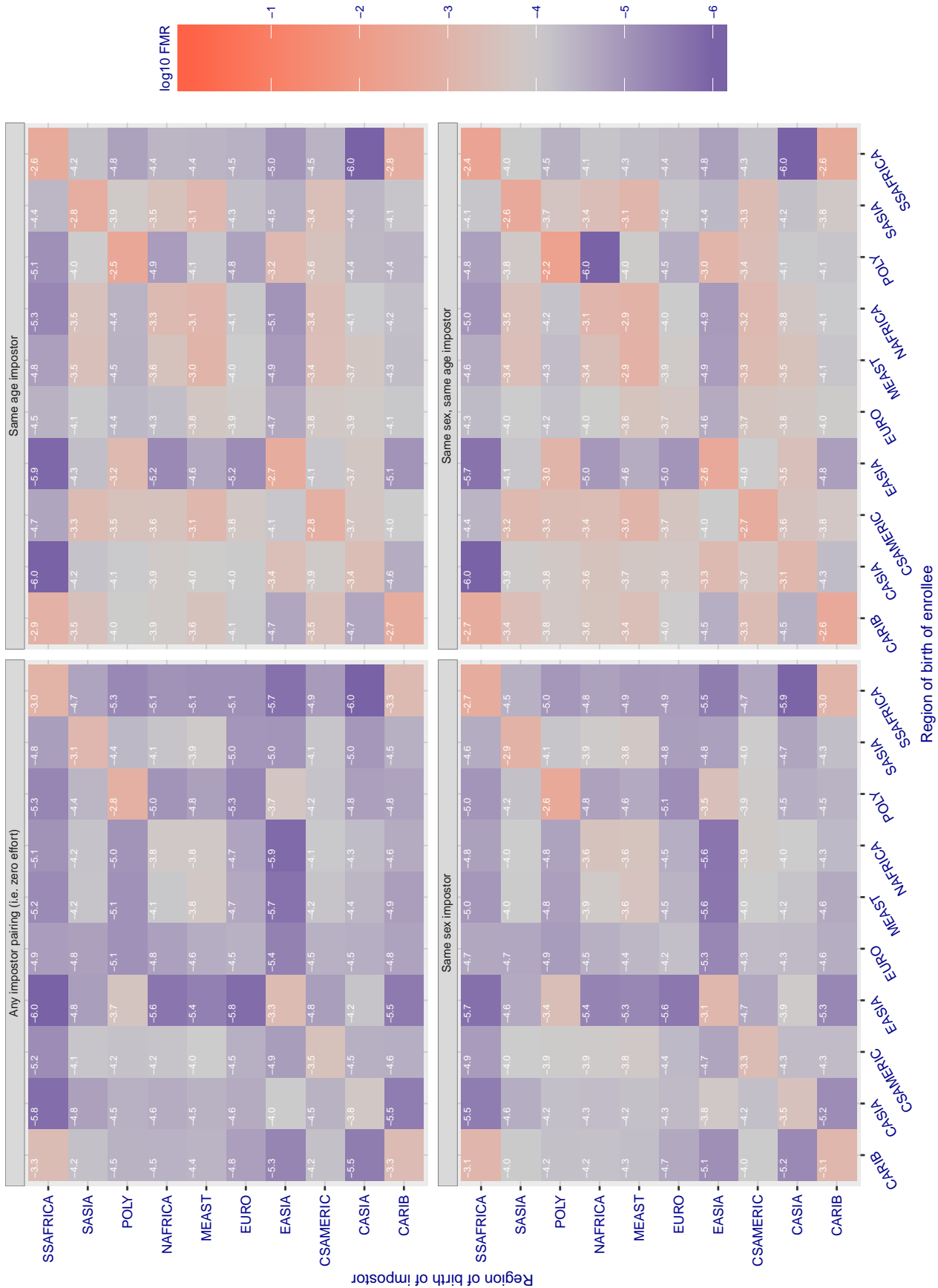


Figure 217: For algorithm imagus-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 1.375$  for algorithm imperial\_000, giving  $FMR(T) = 0.0001$  globally.

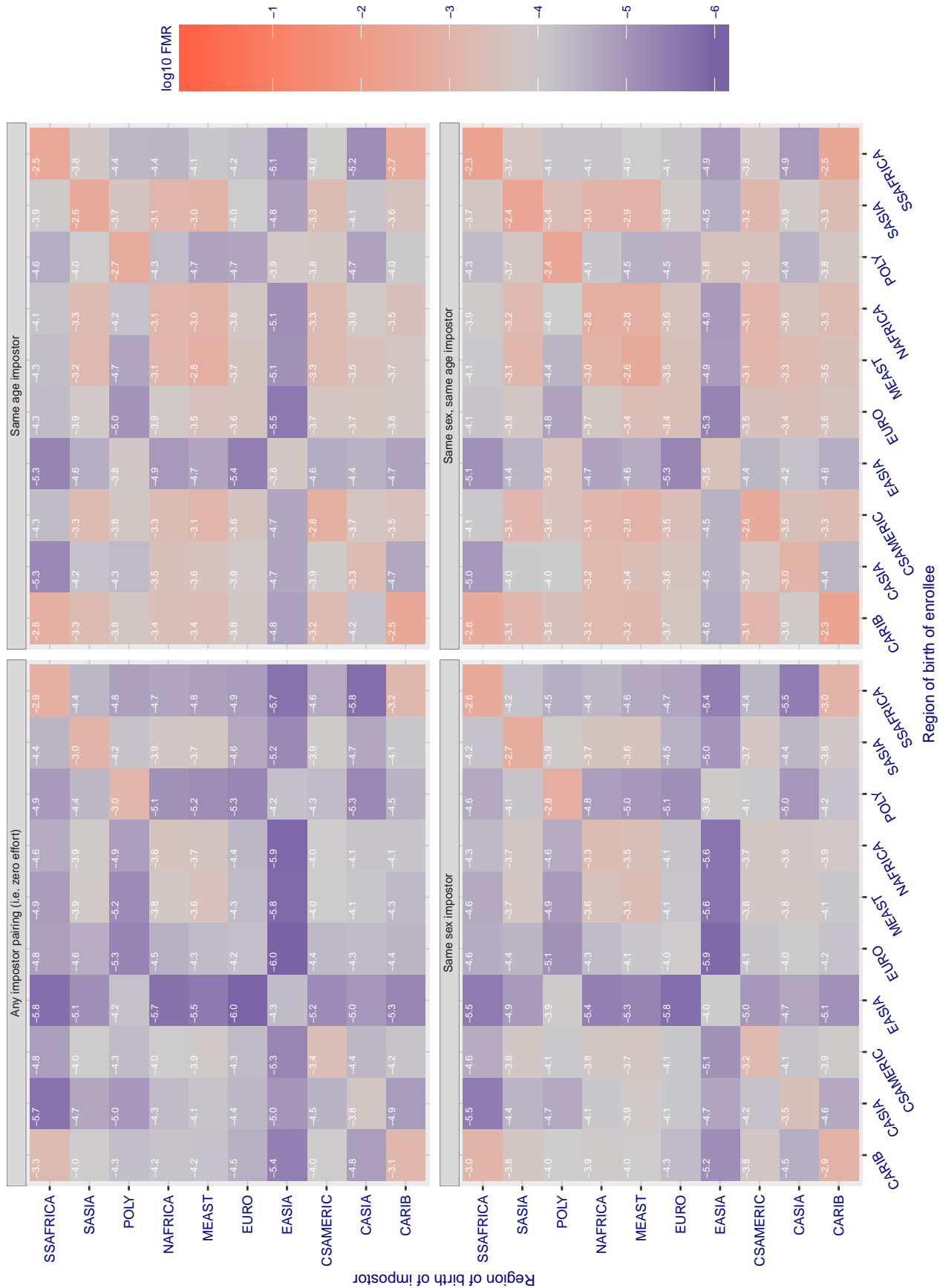


Figure 218: For algorithm imperial-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

**Cross region FMR at threshold T = 1.358 for algorithm imperial\_002, giving FMR(T) = 0.0001 globally.**

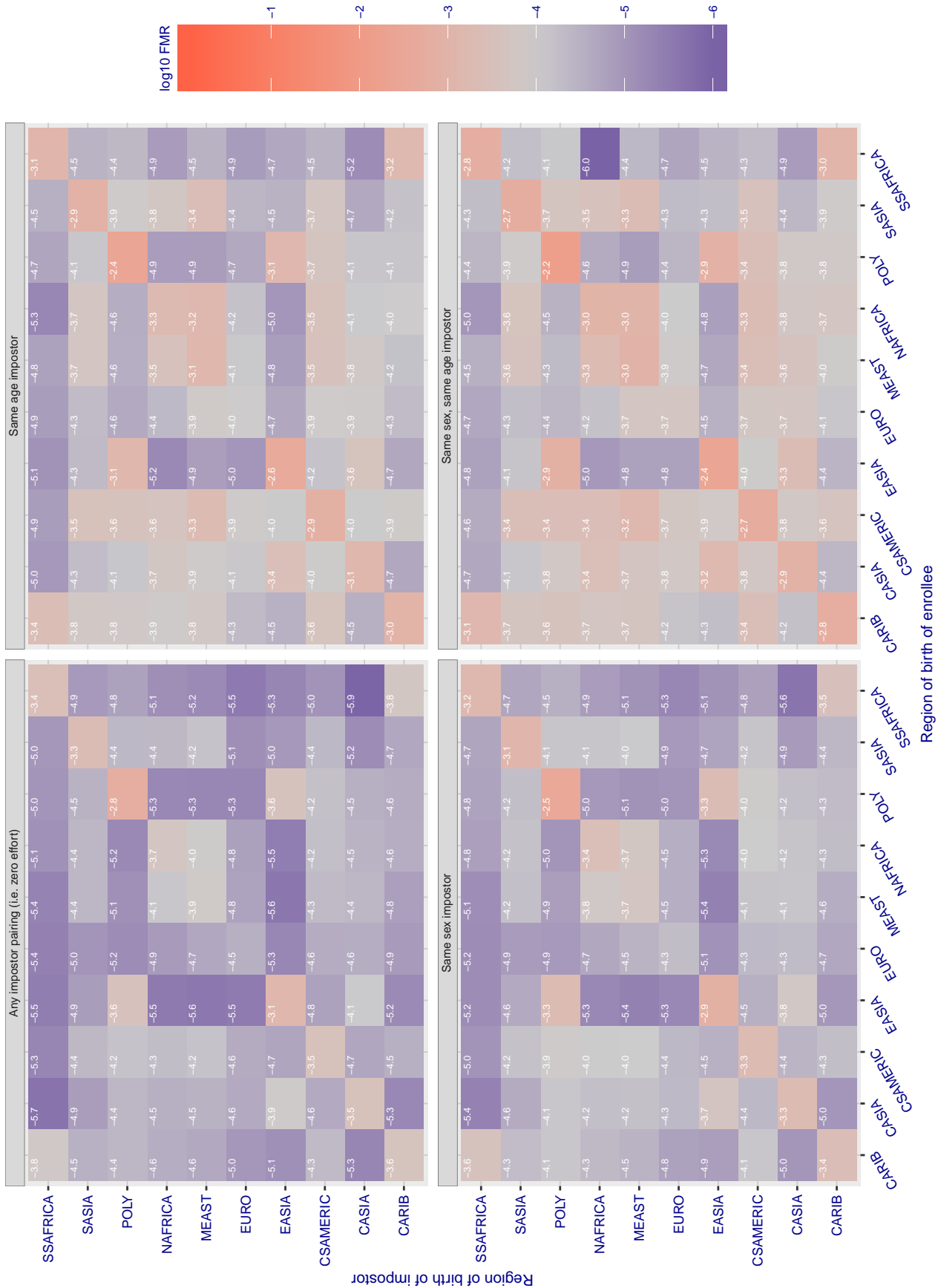


Figure 219: For algorithm imperial-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 1.398$  for algorithm `incde_004`, giving  $FMR(T) = 0.0001$  globally.

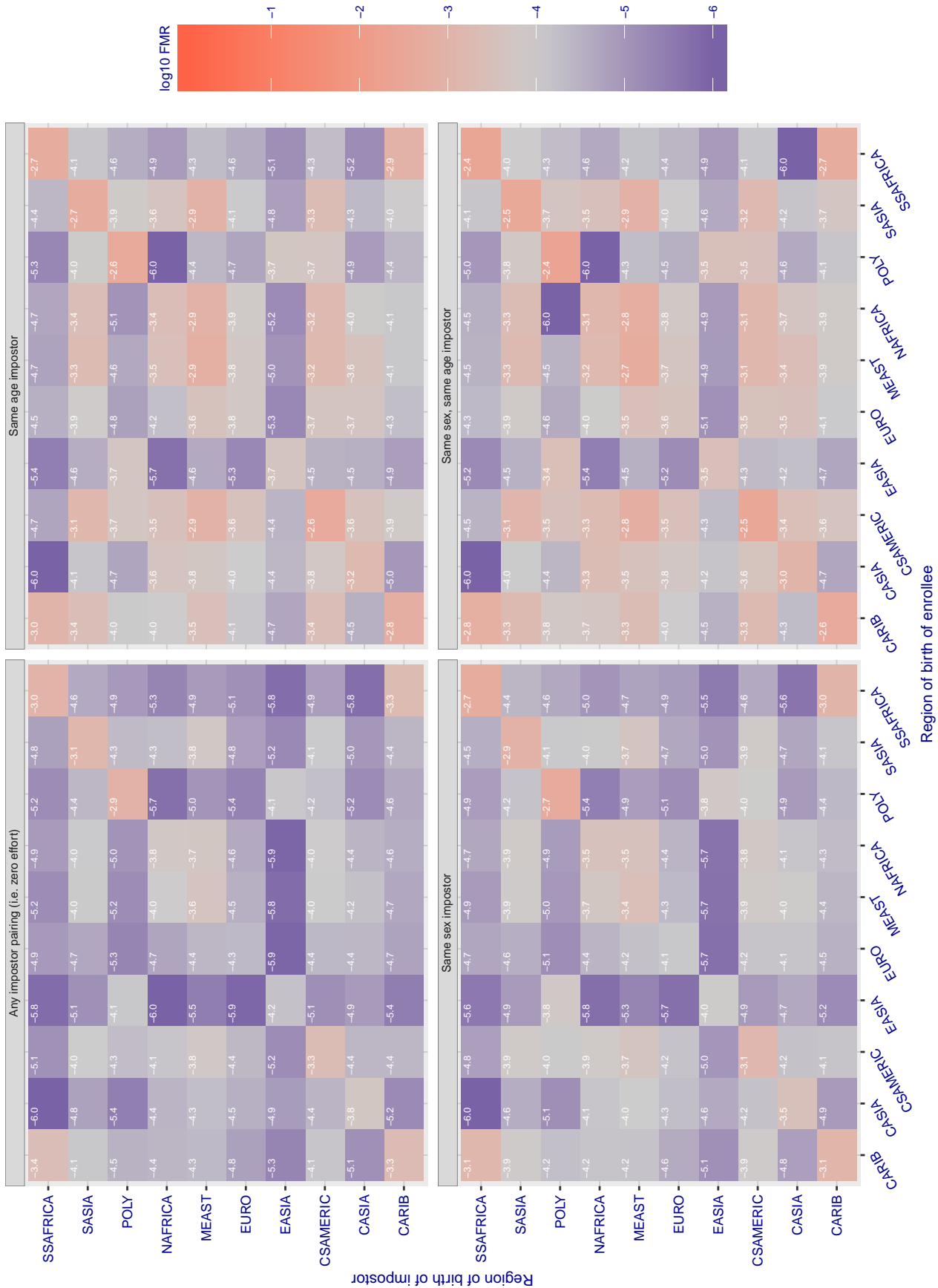


Figure 220: For algorithm `incde-004` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

**Cross region FMR at threshold T = 1.391 for algorithm incde\_005, giving FMR(T) = 0.0001 globally.**

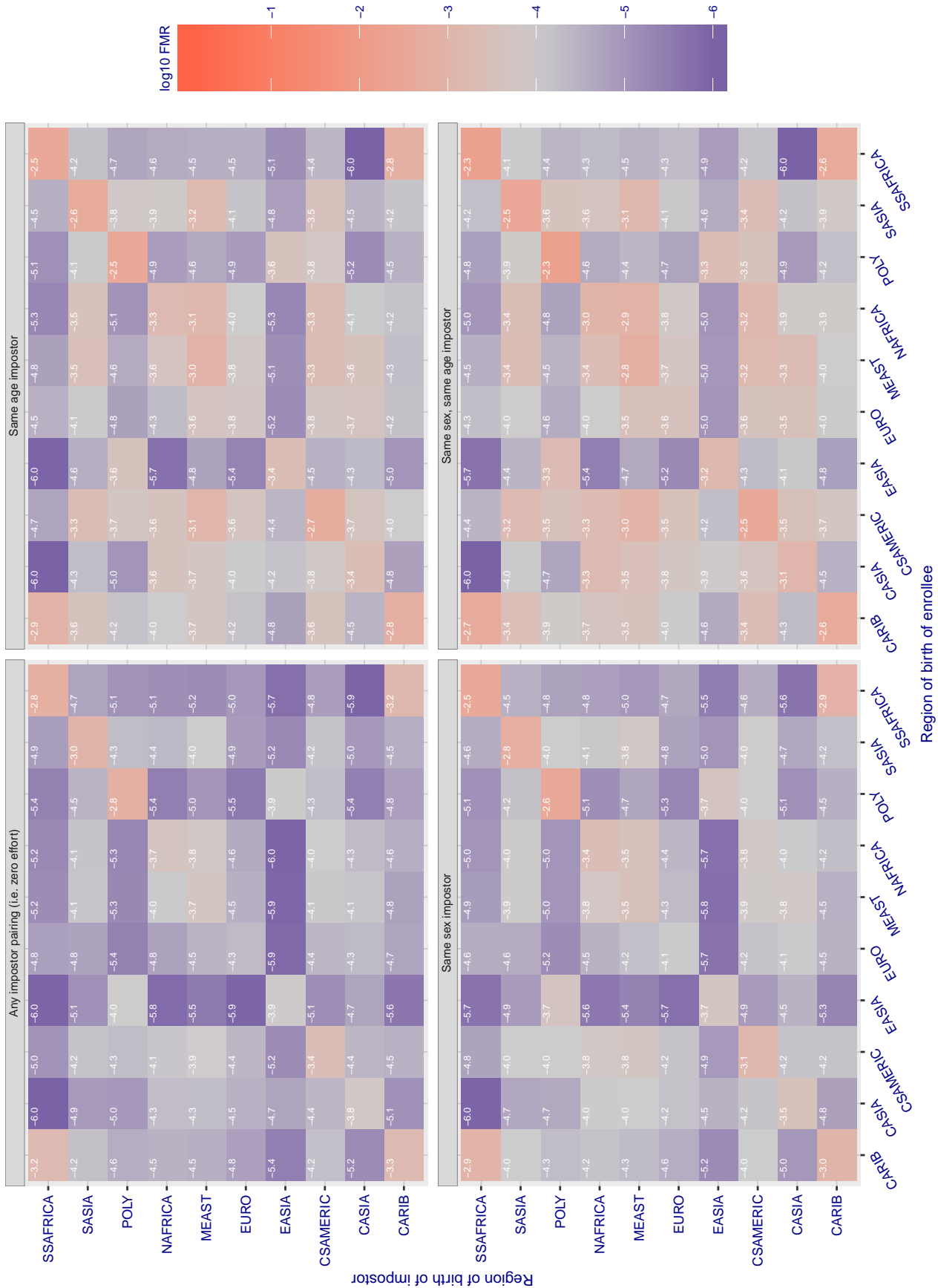


Figure 221: For algorithm incde-005 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.448$  for algorithm `innovativetechnologyld_001`, giving  $FMR(T) = 0.0001$  globally.

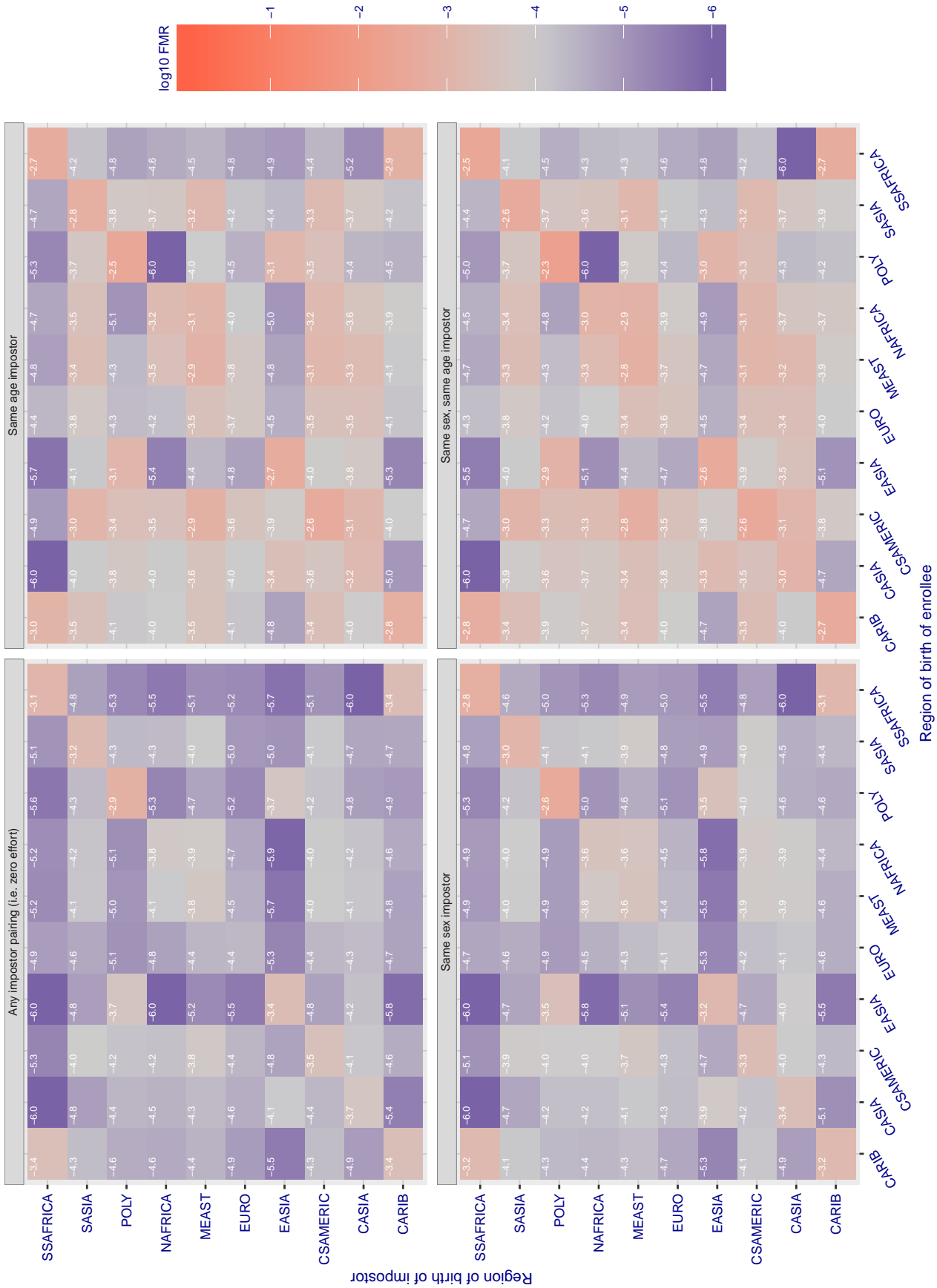


Figure 222: For algorithm `innovativetechnologyld_001` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 29.232$  for algorithm innovatrics\_004, giving  $FMR(T) = 0.0001$  globally.

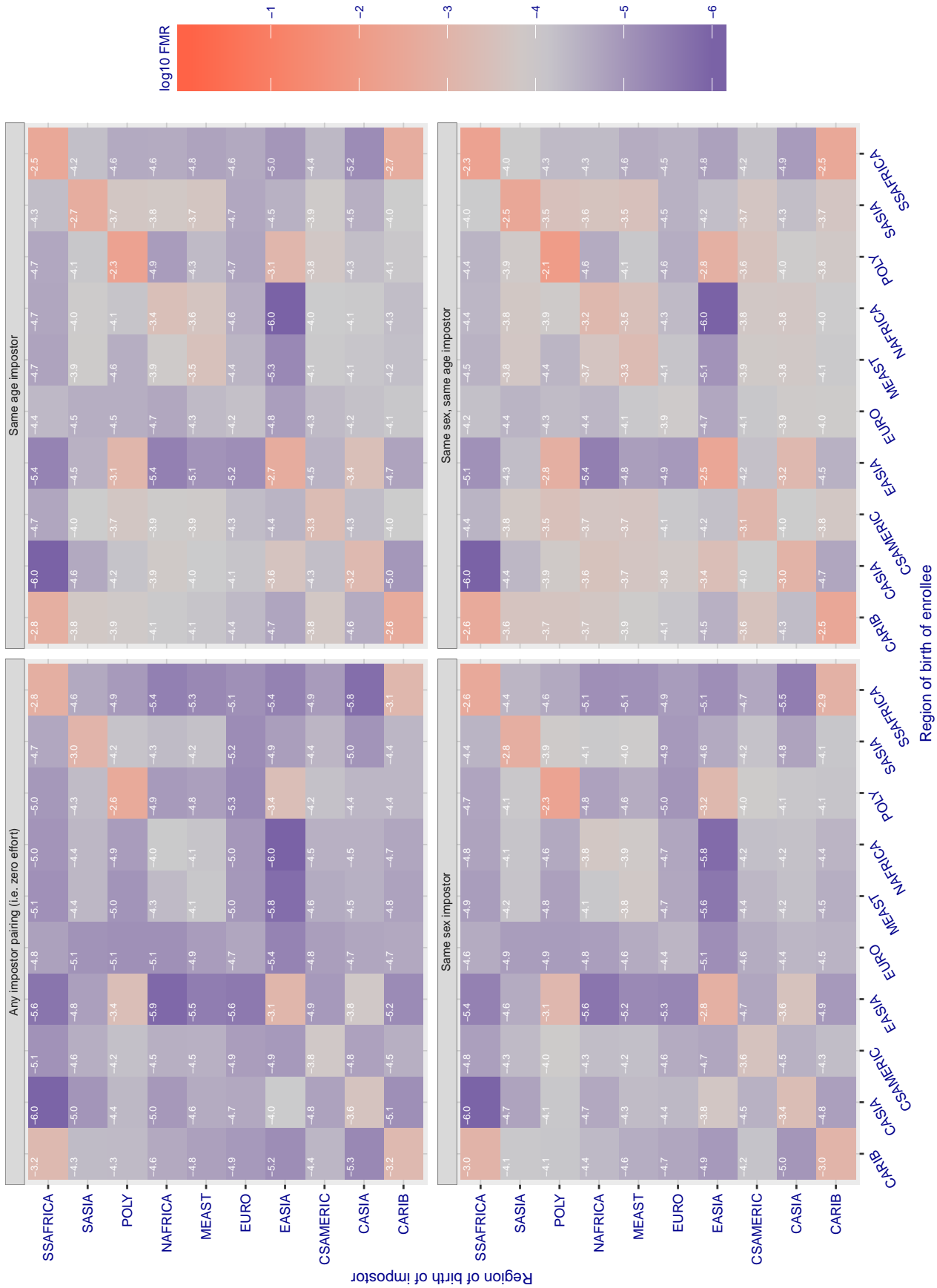


Figure 223: For algorithm innovatrics-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 27.987$  for algorithm innovatrics\_006, giving  $FMR(T) = 0.0001$  globally.

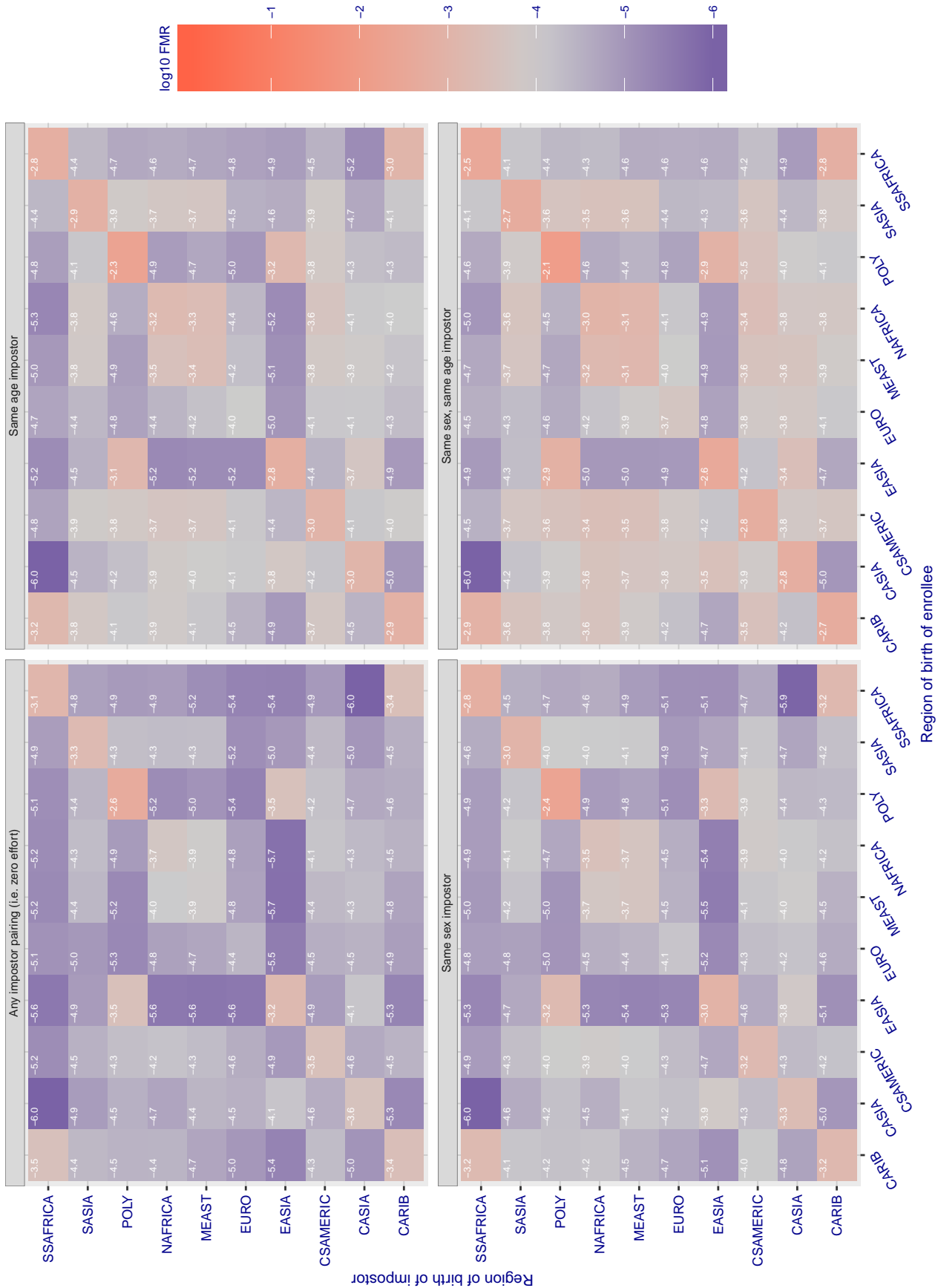


Figure 224: For algorithm innovatrics-006 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 0.705$  for algorithm intellicloudai\_001, giving  $FMR(T) = 0.0001$  globally.

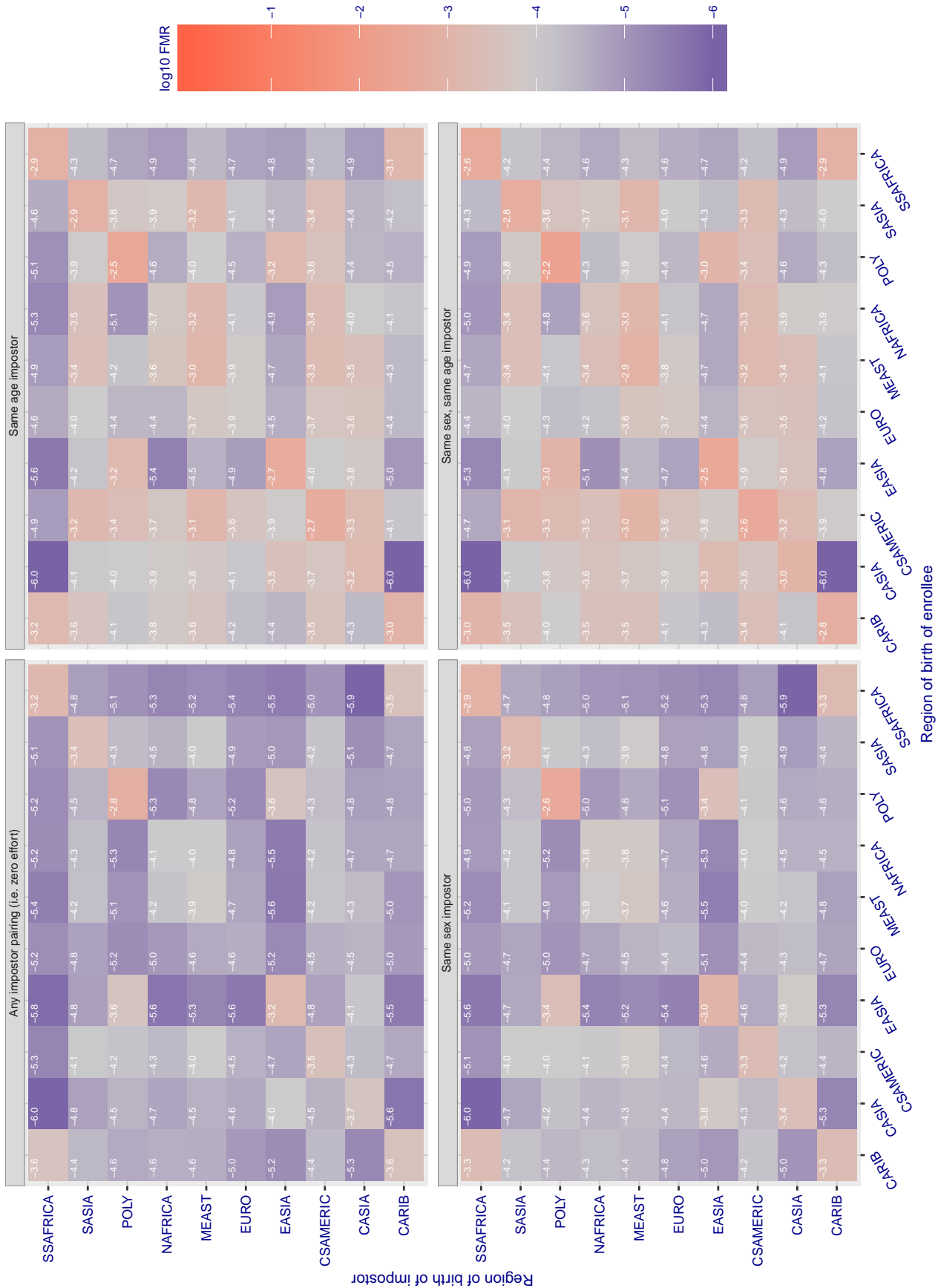


Figure 225: For algorithm intellicloudai-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.300$  for algorithm intellifusion\_001, giving  $FMR(T) = 0.0001$  globally.

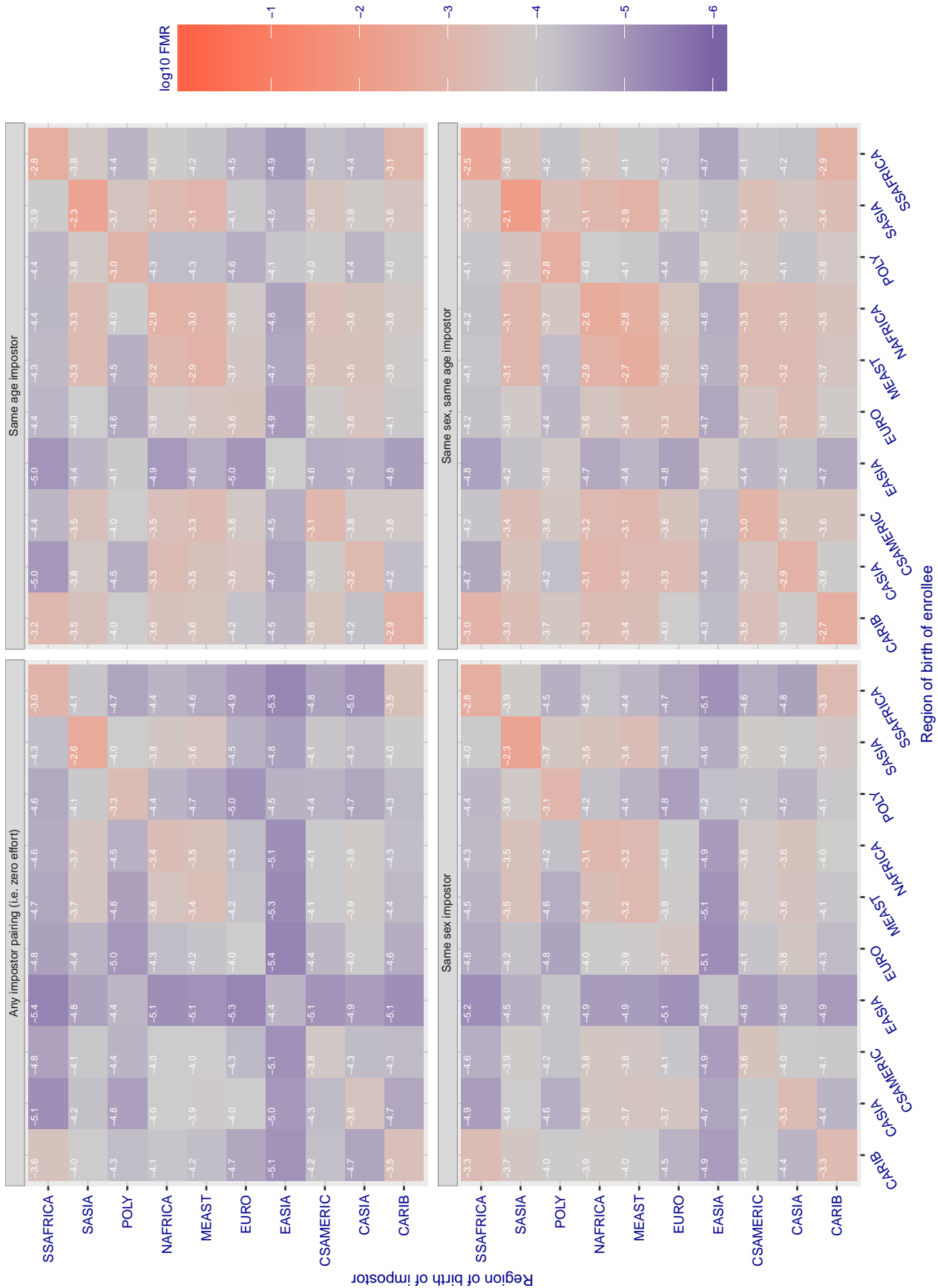


Figure 226: For algorithm intellifusion-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 49.664 for algorithm intellivision\_001, giving FMR(T) = 0.0001 globally.

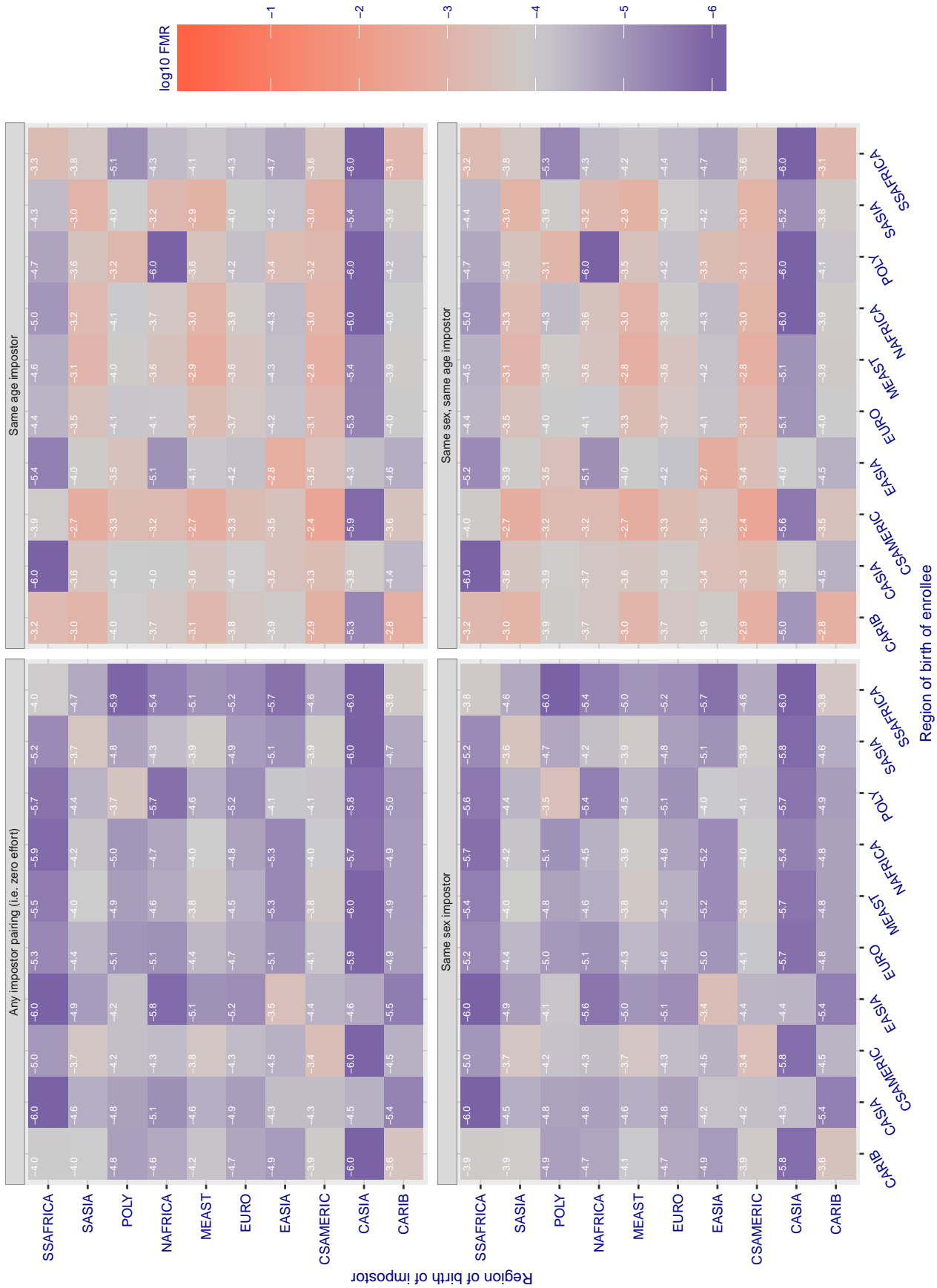


Figure 227: For algorithm intellivision-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of 10<sup>10</sup> impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 44.160 for algorithm intellivision\_002, giving FMR(T) = 0.0001 globally.

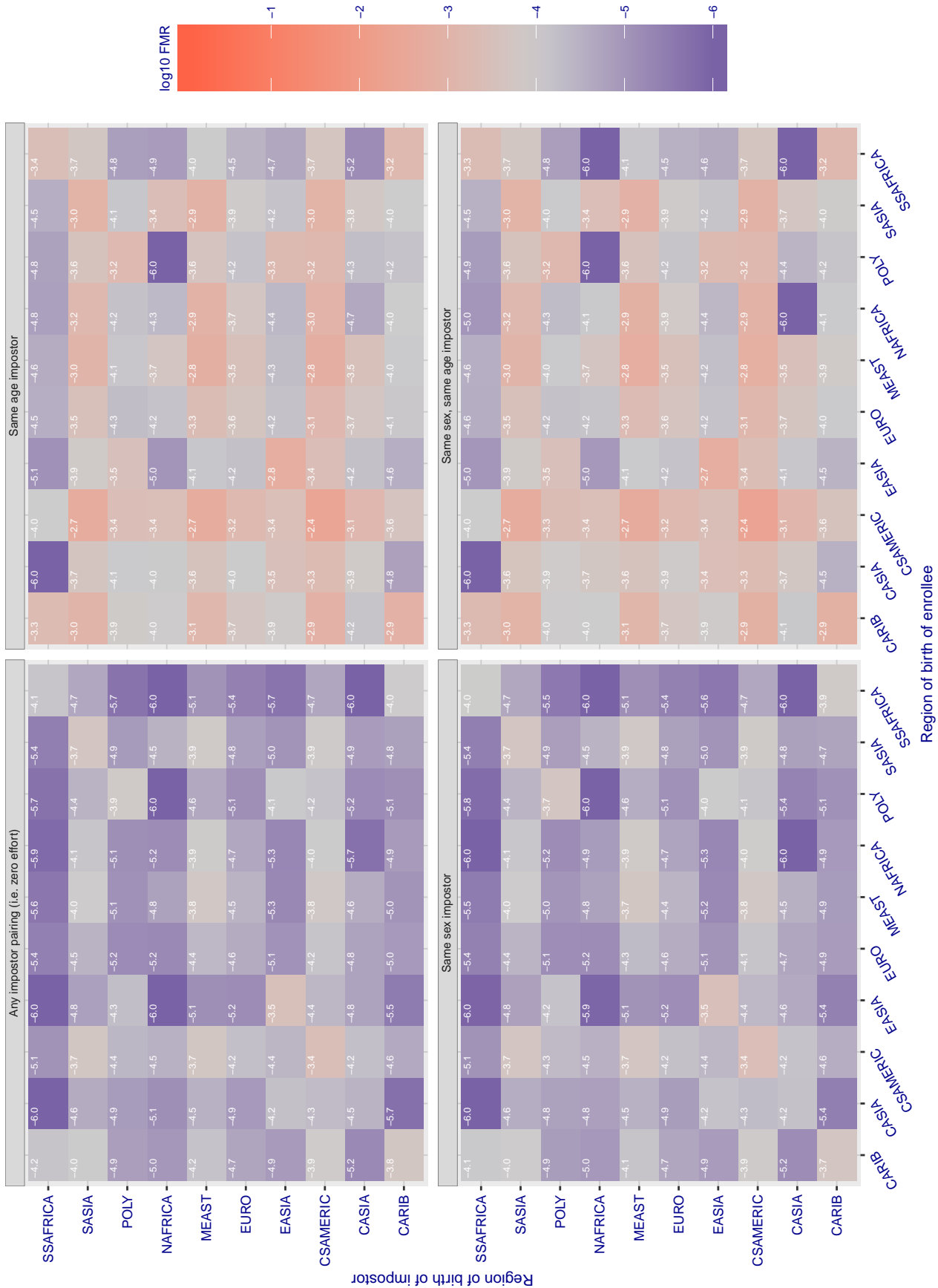


Figure 228: For algorithm intellivision-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 594.014 for algorithm intelresearch\_000, giving FMR(T) = 0.0001 globally.

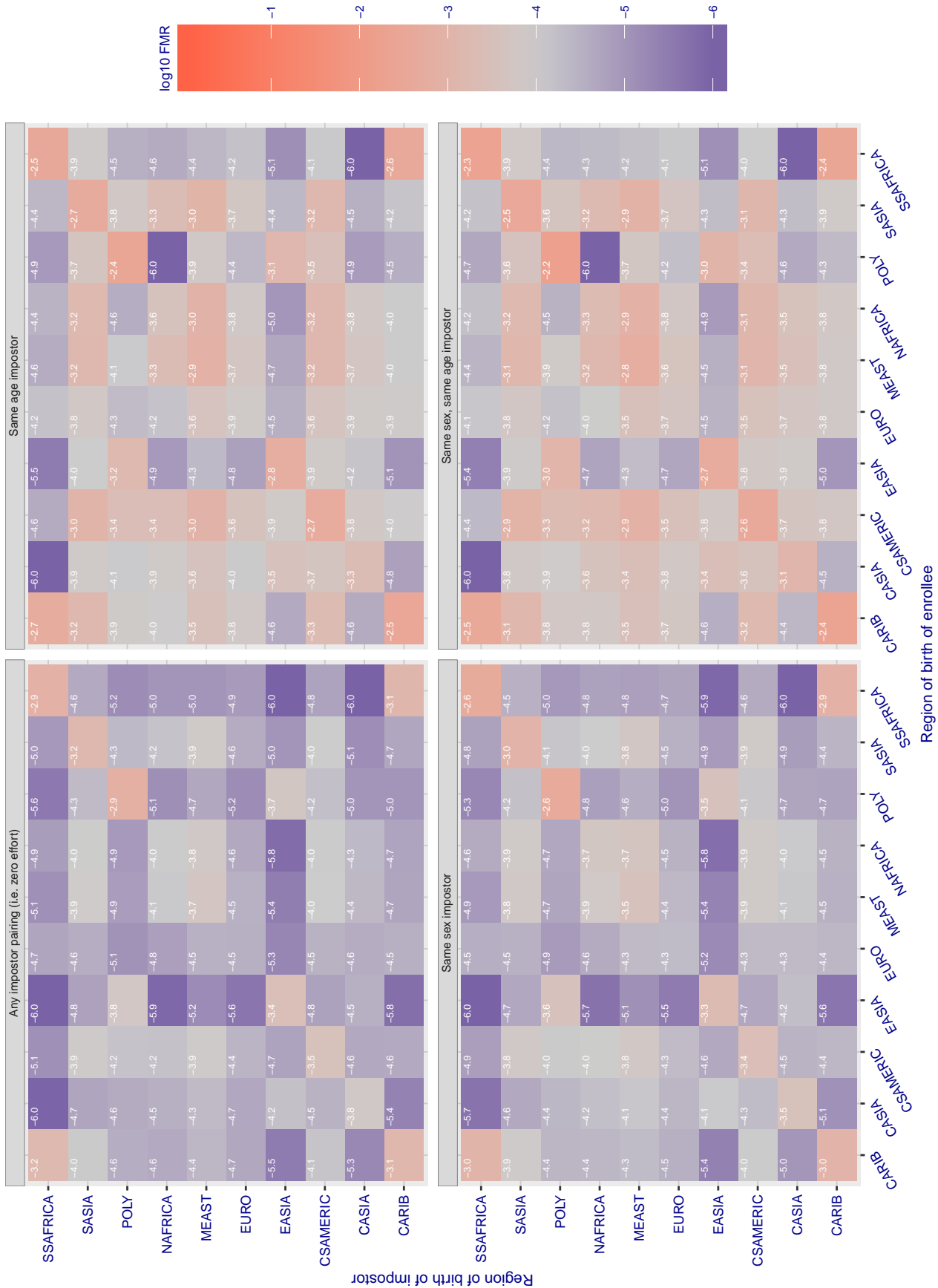


Figure 229: For algorithm intelresearch-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of 10<sup>10</sup> impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 1.389$  for algorithm intsysmsu\_000, giving  $FMR(T) = 0.0001$  globally.

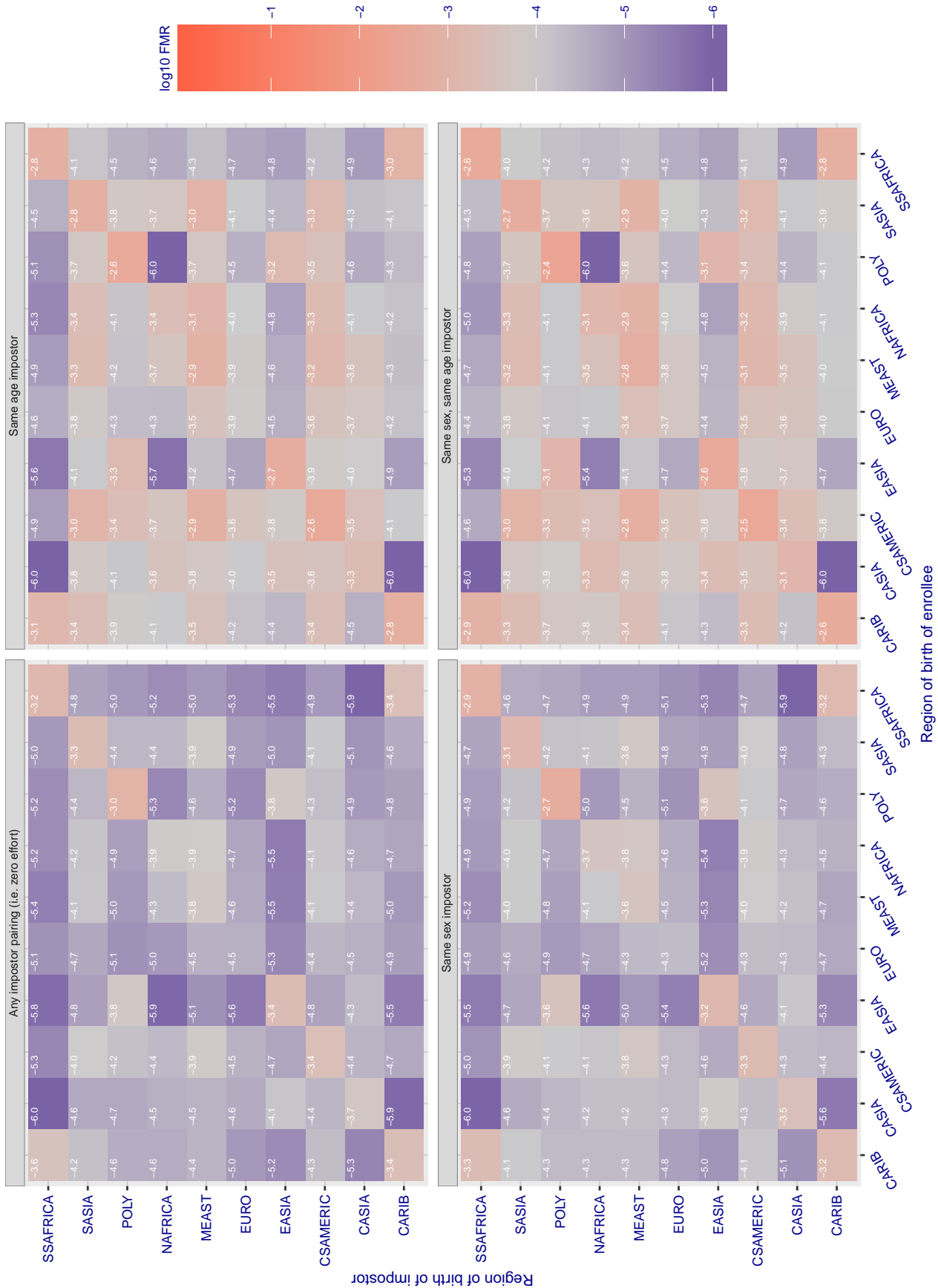


Figure 230: For algorithm intsysmsu-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



**Cross region FMR at threshold  $T = 1.971$  for algorithm intsysmsu\_001, giving  $FMR(T) = 0.0001$  globally.**

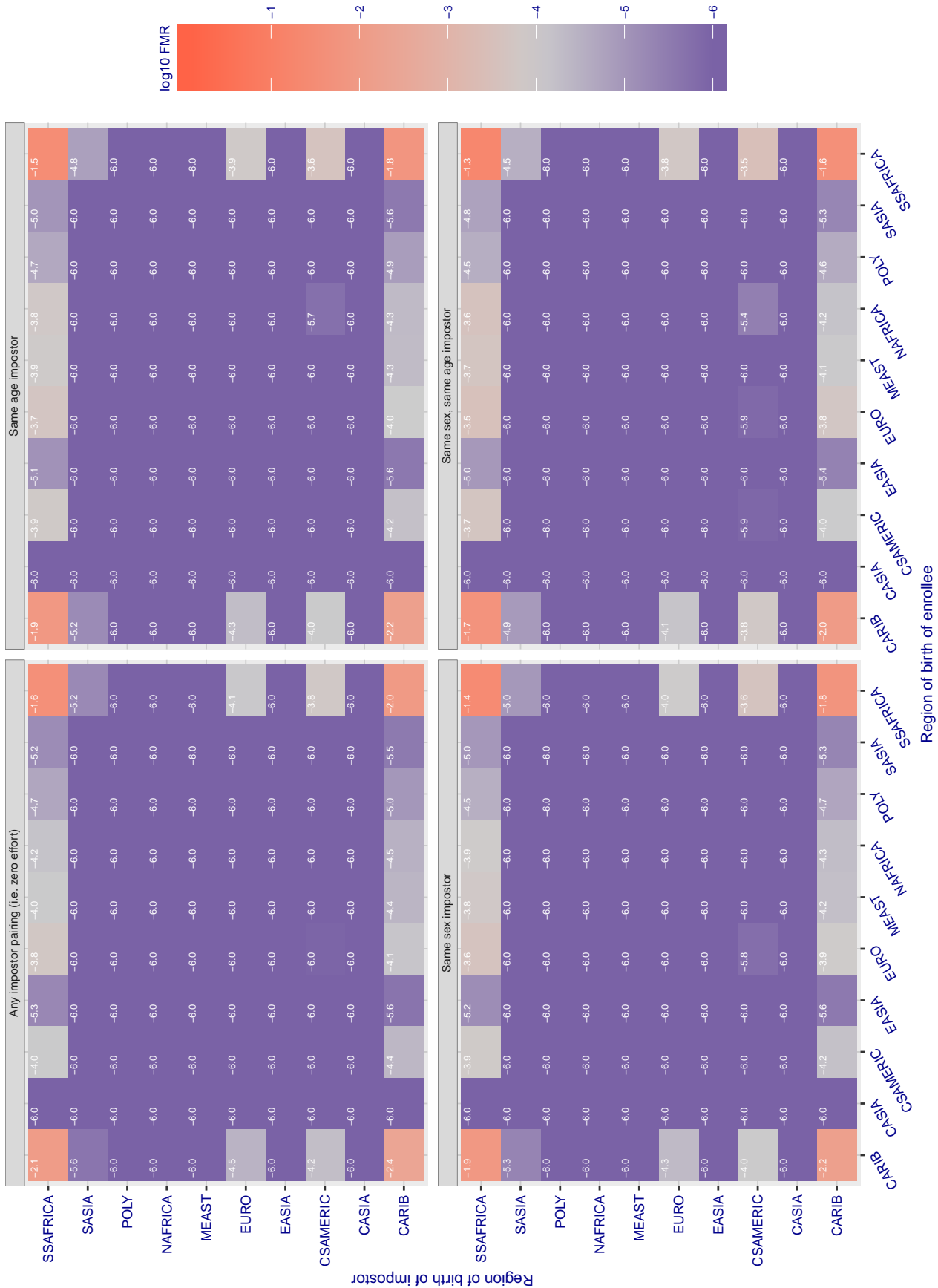


Figure 231: For algorithm intsysmsu-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

**Cross region FMR at threshold  $T = 1.361$  for algorithm iqface\_000, giving  $FMR(T) = 0.0001$  globally.**

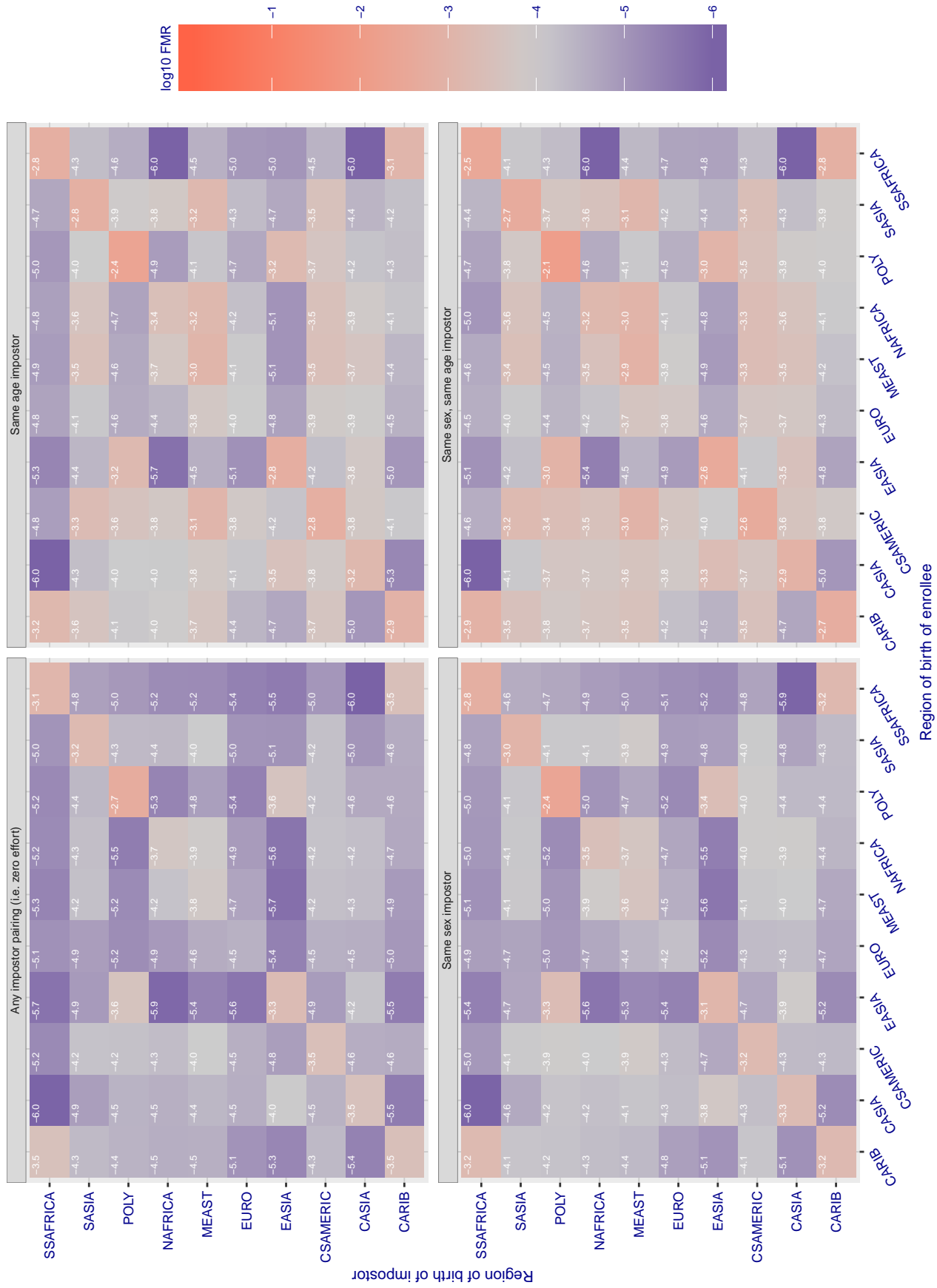


Figure 232: For algorithm iqface-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 0.985$  for algorithm isap\_001, giving  $FMR(T) = 0.0001$  globally.

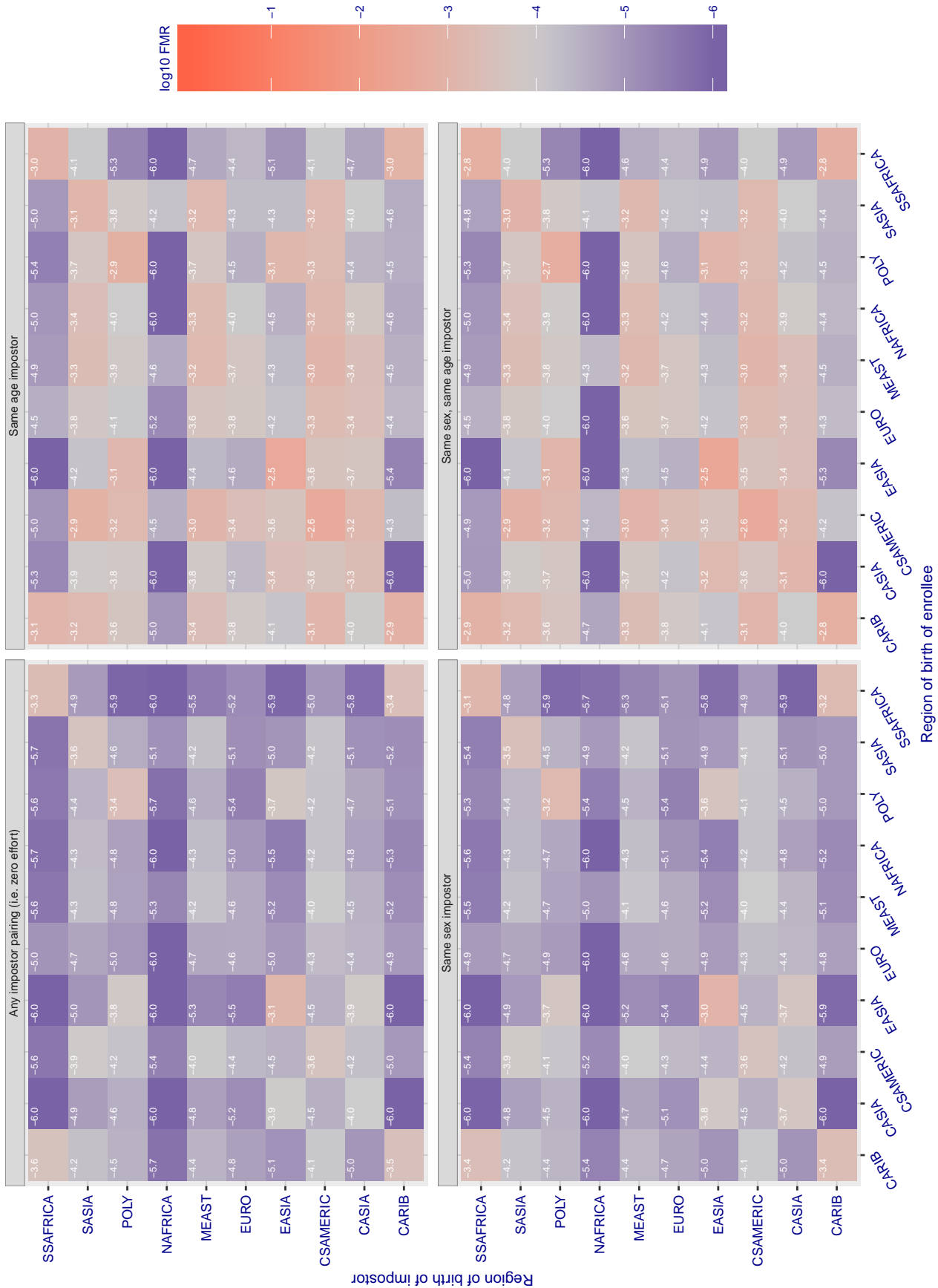


Figure 233: For algorithm isap-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 23.498$  for algorithm isityou\_000, giving  $FMR(T) = 0.0001$  globally.

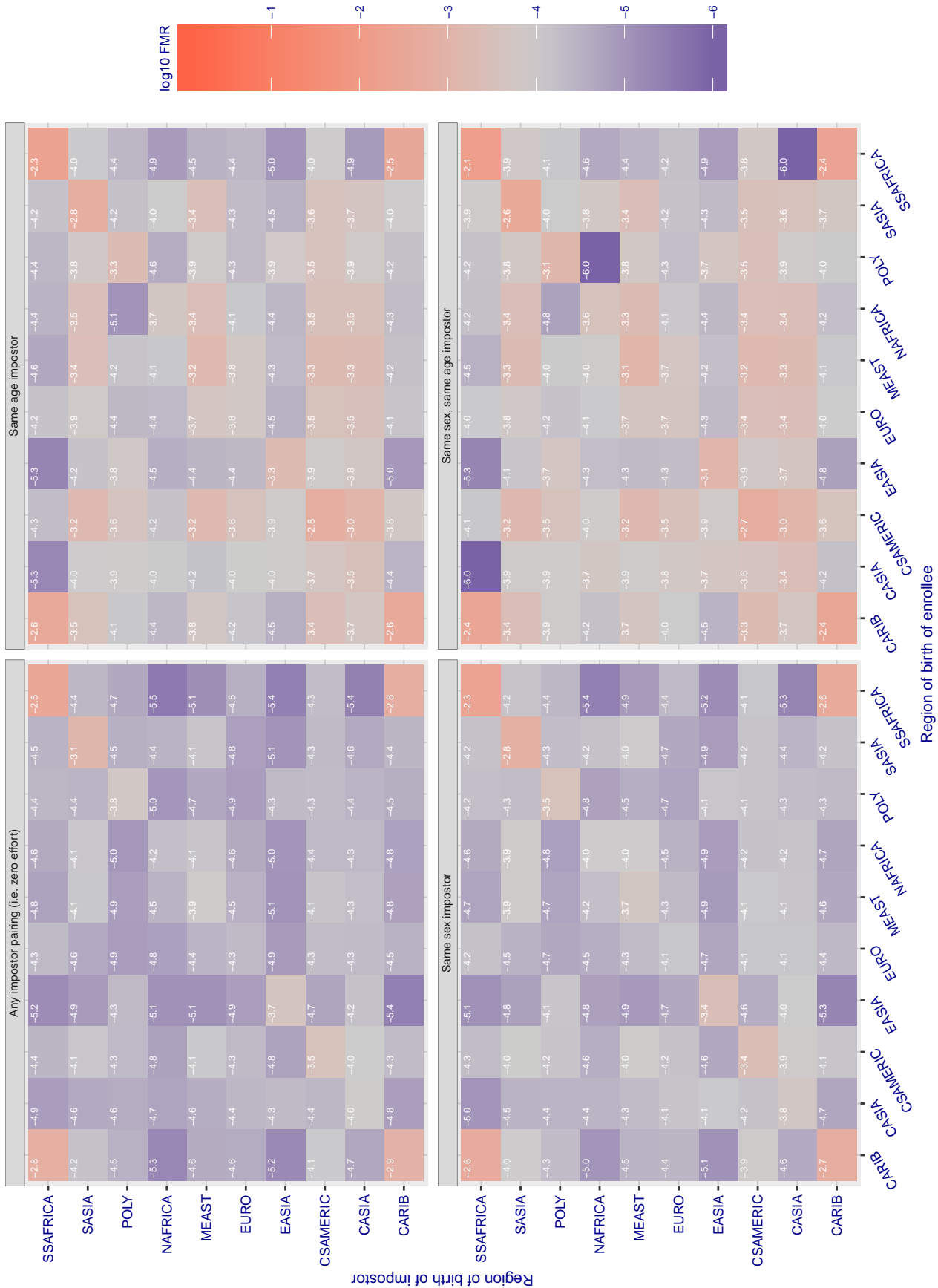


Figure 234: For algorithm isityou-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 0.693 for algorithm isystems\_001, giving FMR(T) = 0.0001 globally.

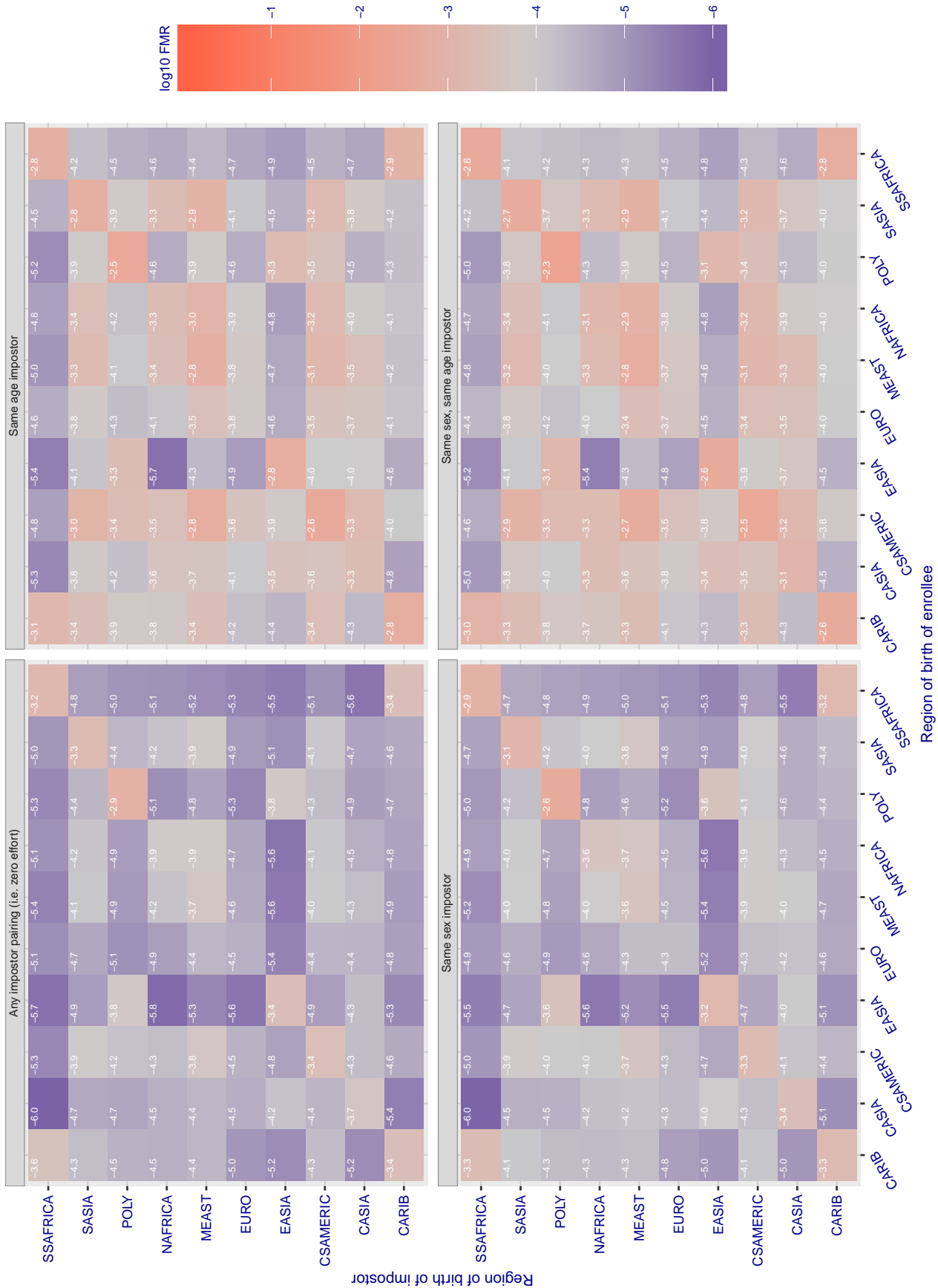


Figure 235: For algorithm isystems-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of 10<sup>10</sup> impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 0.690 for algorithm isystems\_002, giving FMR(T) = 0.0001 globally.

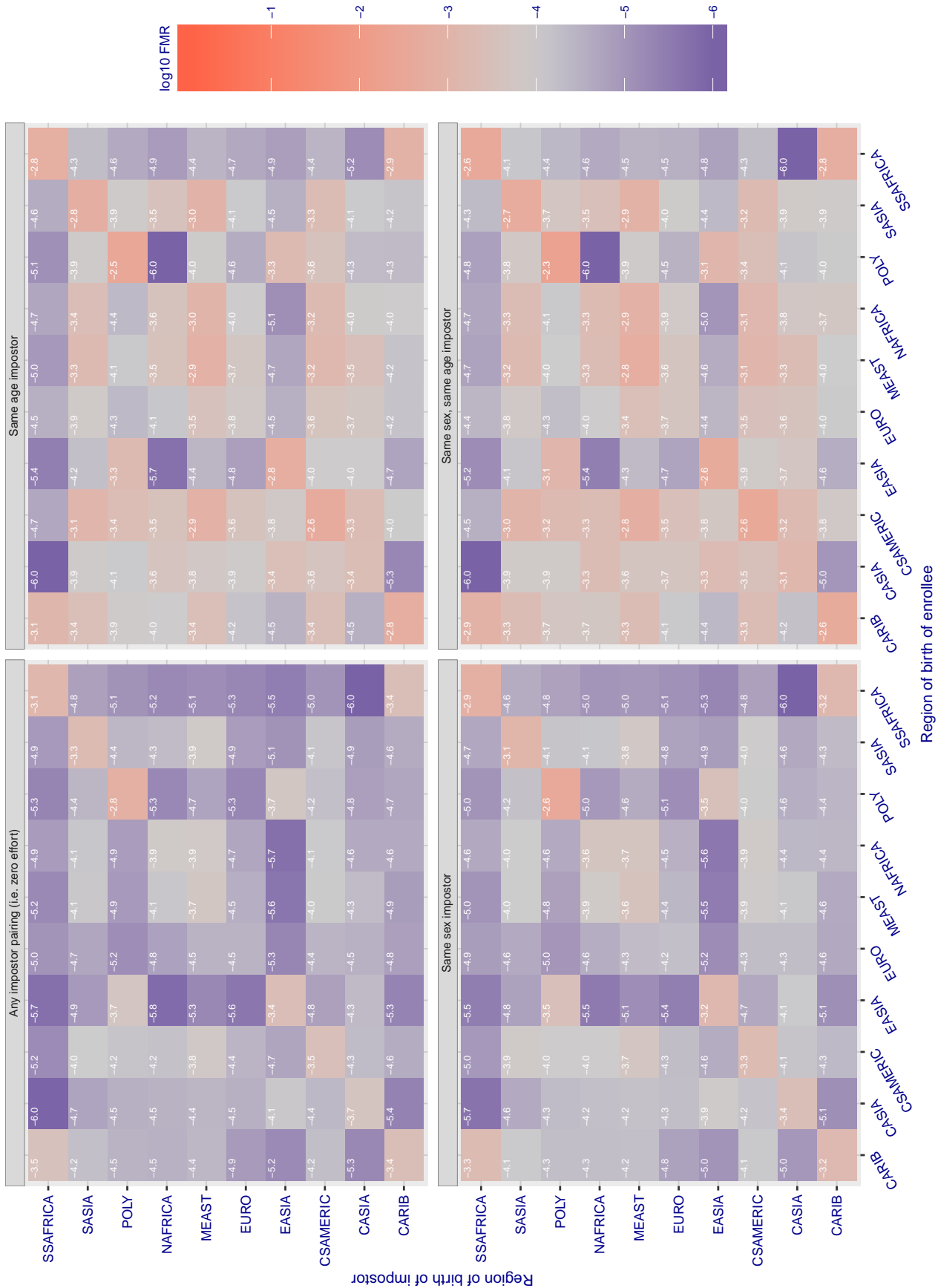


Figure 236: For algorithm isystems-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of 10<sup>10</sup> impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 49.879$  for algorithm itmo\_005, giving  $FMR(T) = 0.0001$  globally.

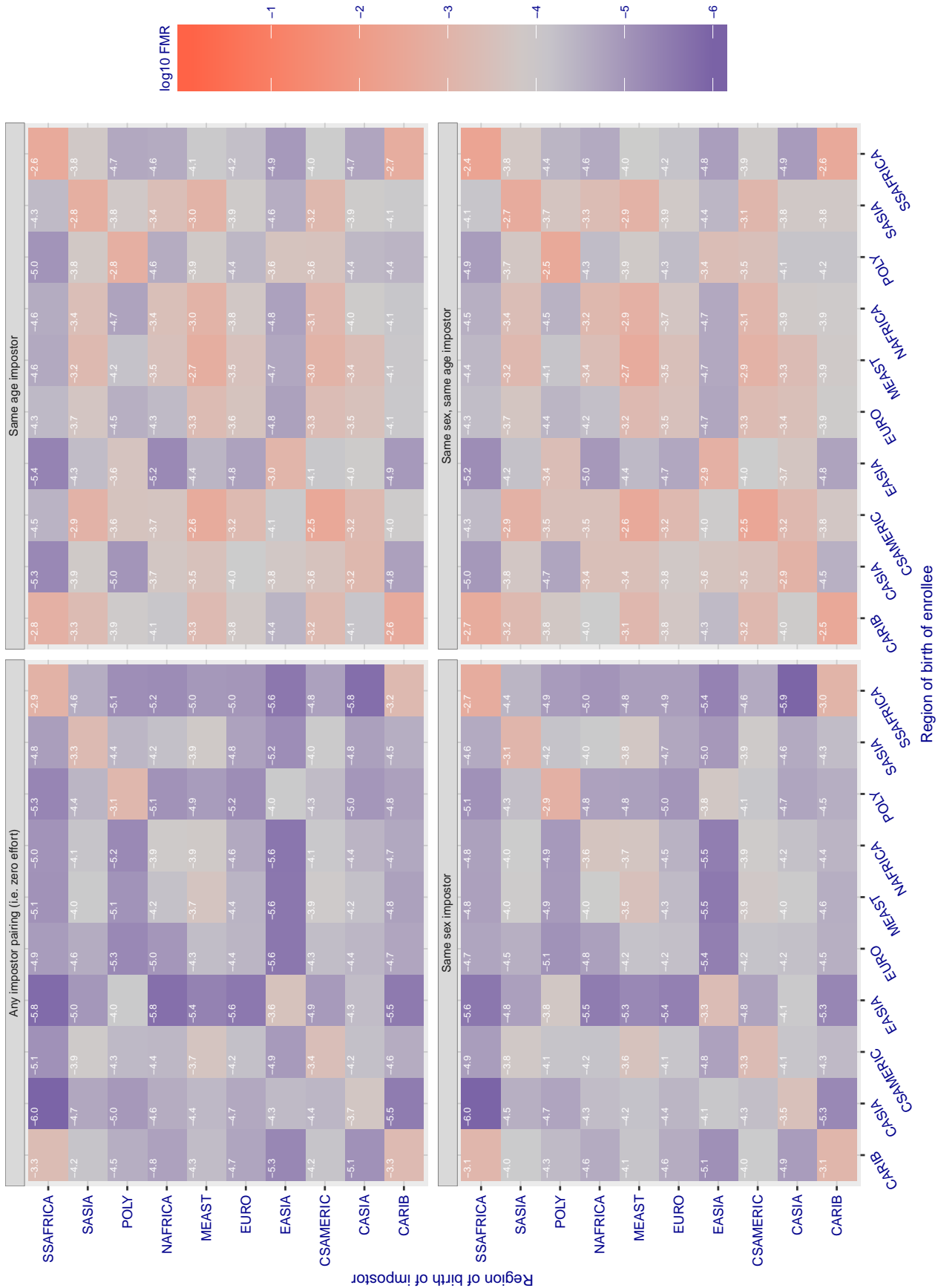


Figure 237: For algorithm itmo-005 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 49.789$  for algorithm itmo\_006, giving  $FMR(T) = 0.0001$  globally.

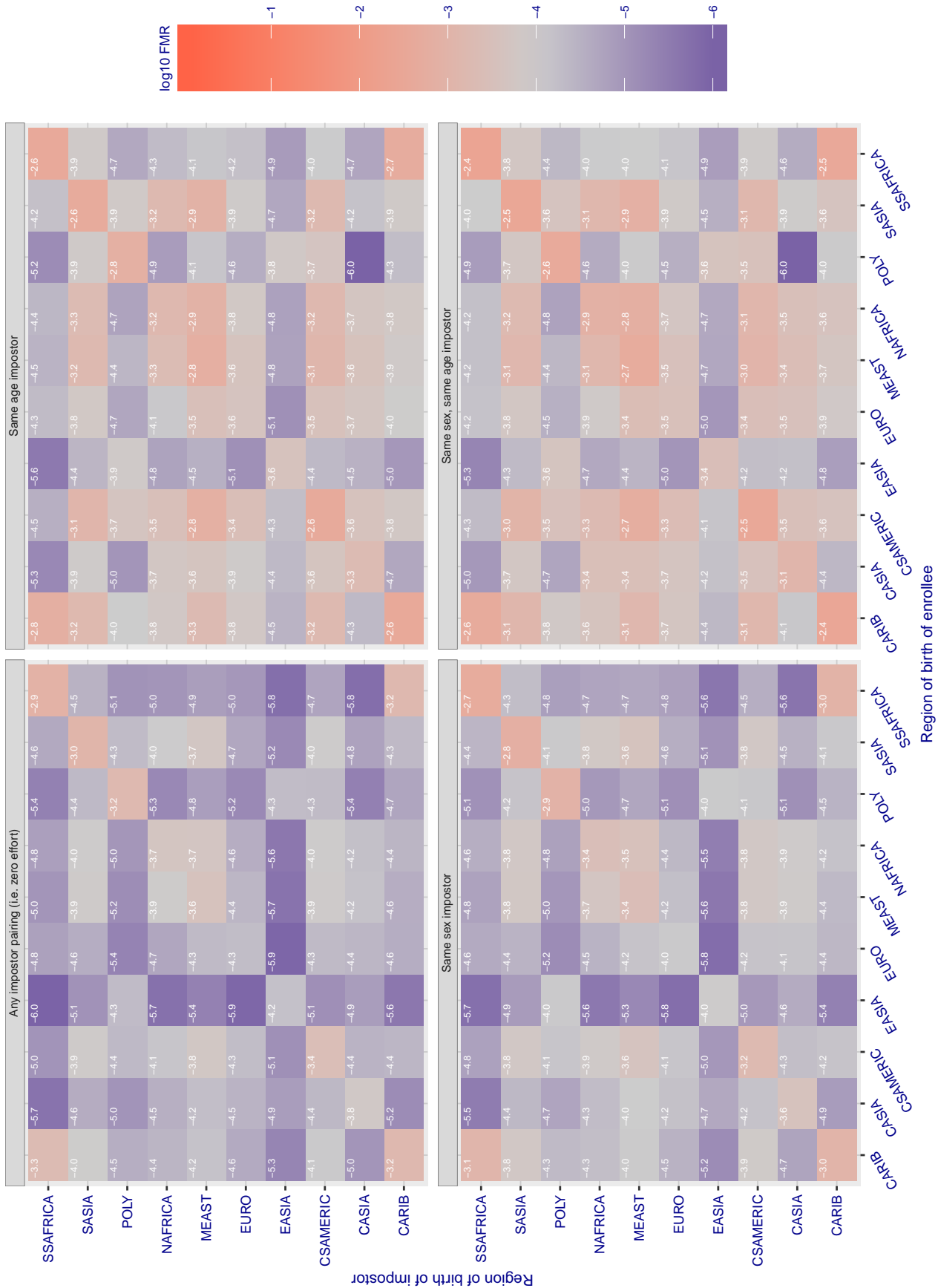


Figure 238: For algorithm itmo-006 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 1.301$  for algorithm kakao\_001, giving  $FMR(T) = 0.0001$  globally.

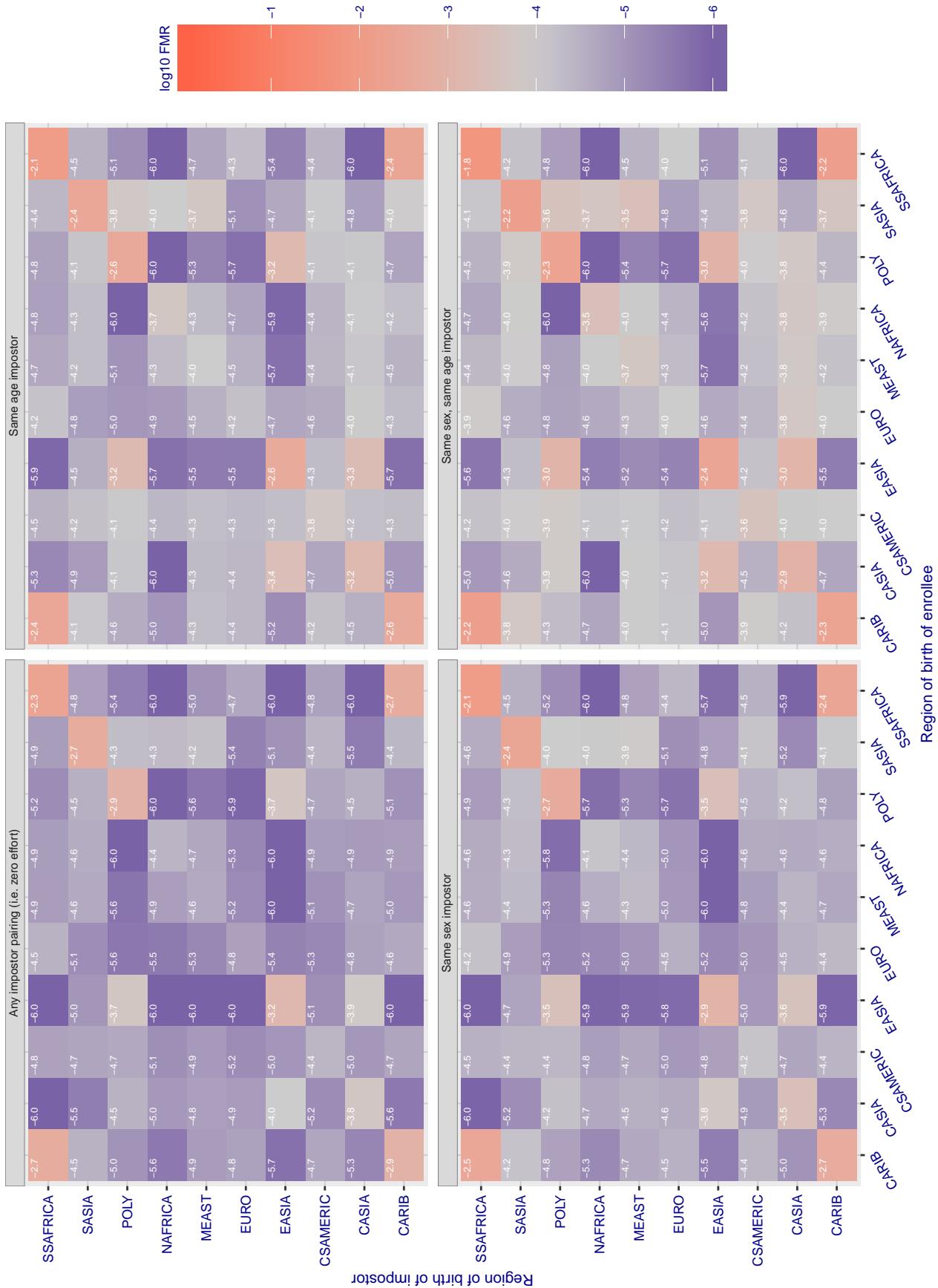


Figure 239: For algorithm kakao-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.929$  for algorithm kakao\_002, giving  $FMR(T) = 0.0001$  globally.

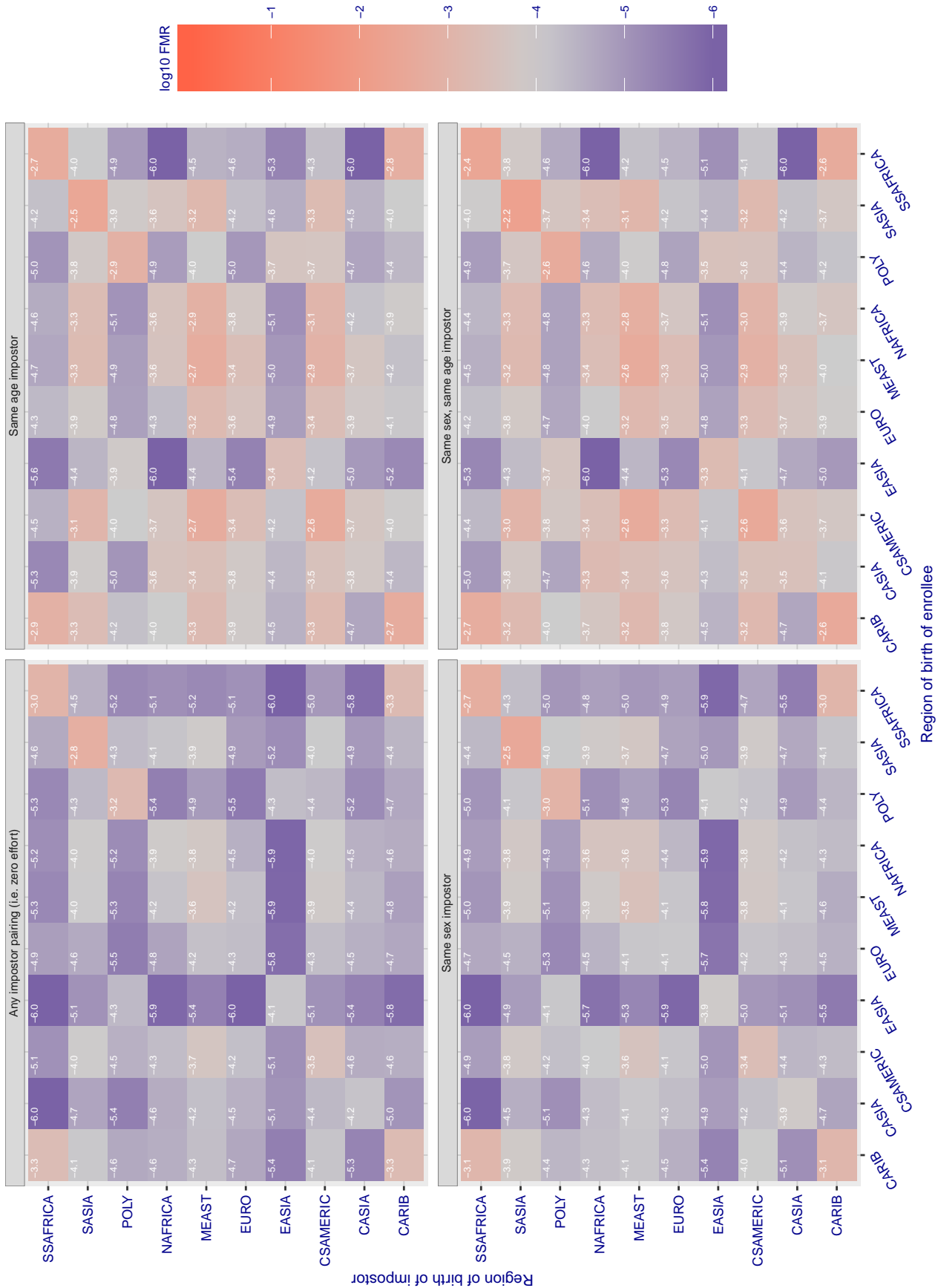


Figure 240: For algorithm kakao-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 0.686$  for algorithm kedadcom\_000, giving  $FMR(T) = 0.0001$  globally.

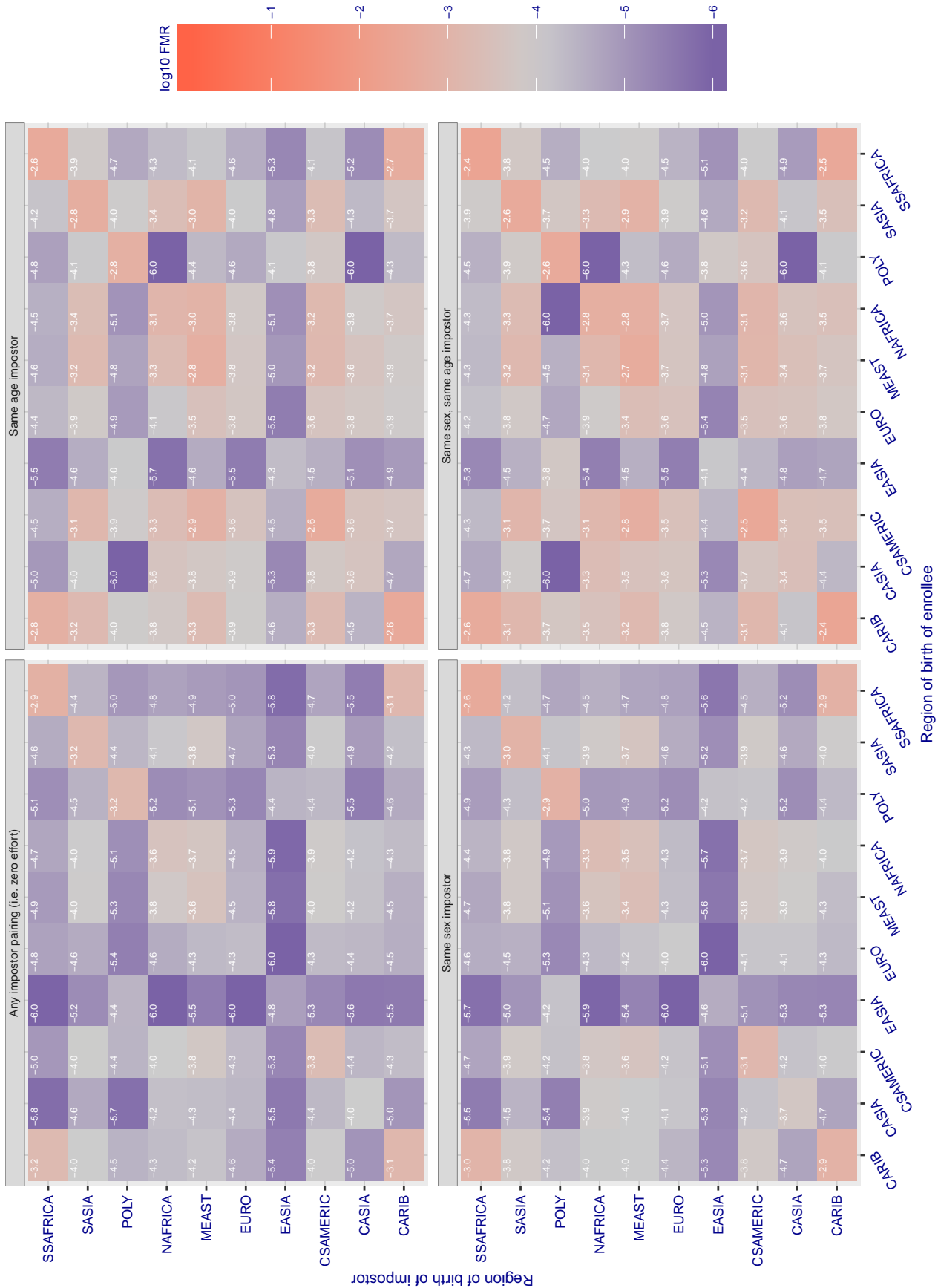


Figure 241: For algorithm kedadcom-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.500$  for algorithm kneron\_003, giving  $FMR(T) = 0.0001$  globally.

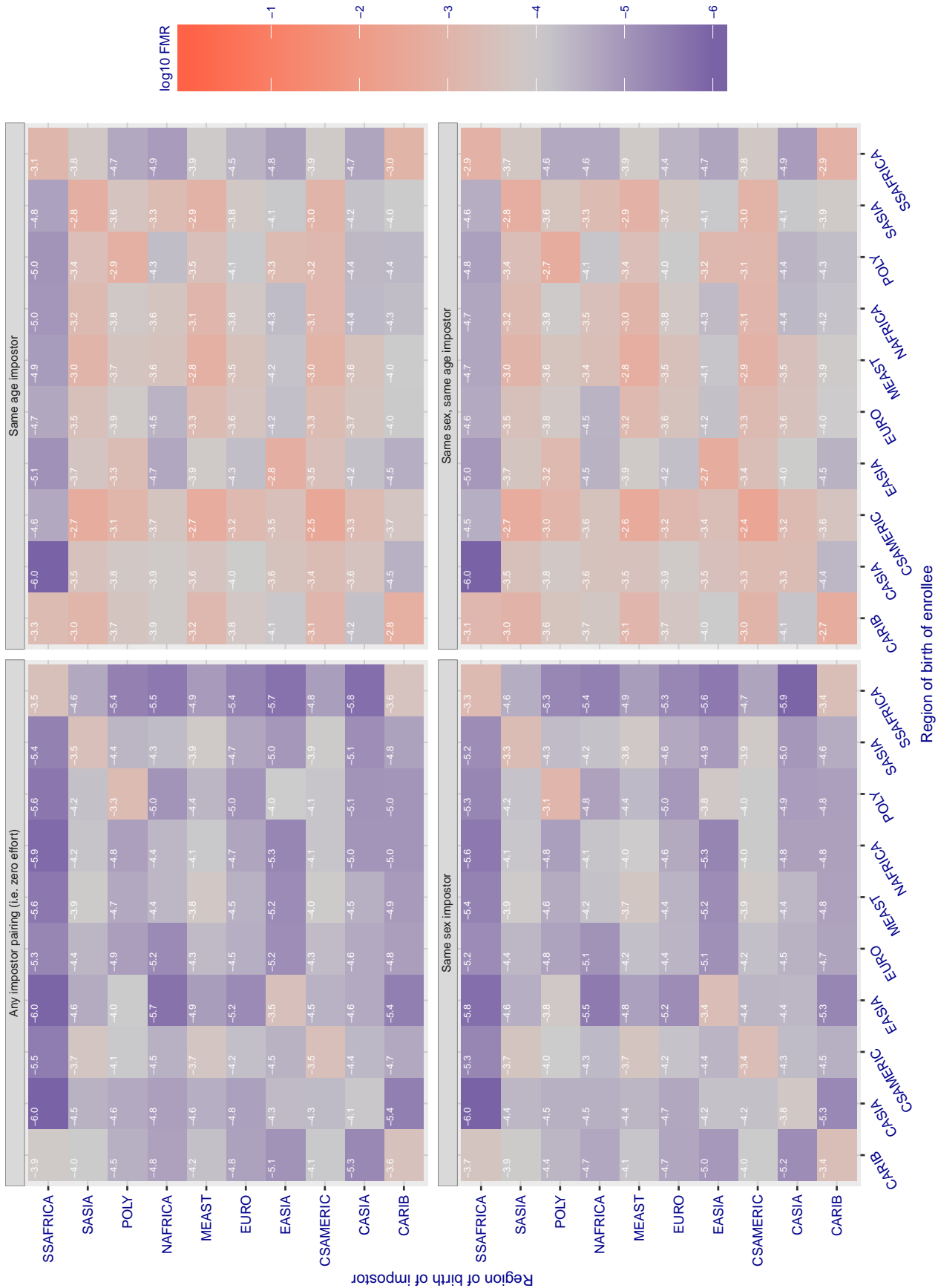


Figure 242: For algorithm kneron-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 0.701 for algorithm lookman\_002, giving FMR(T) = 0.0001 globally.

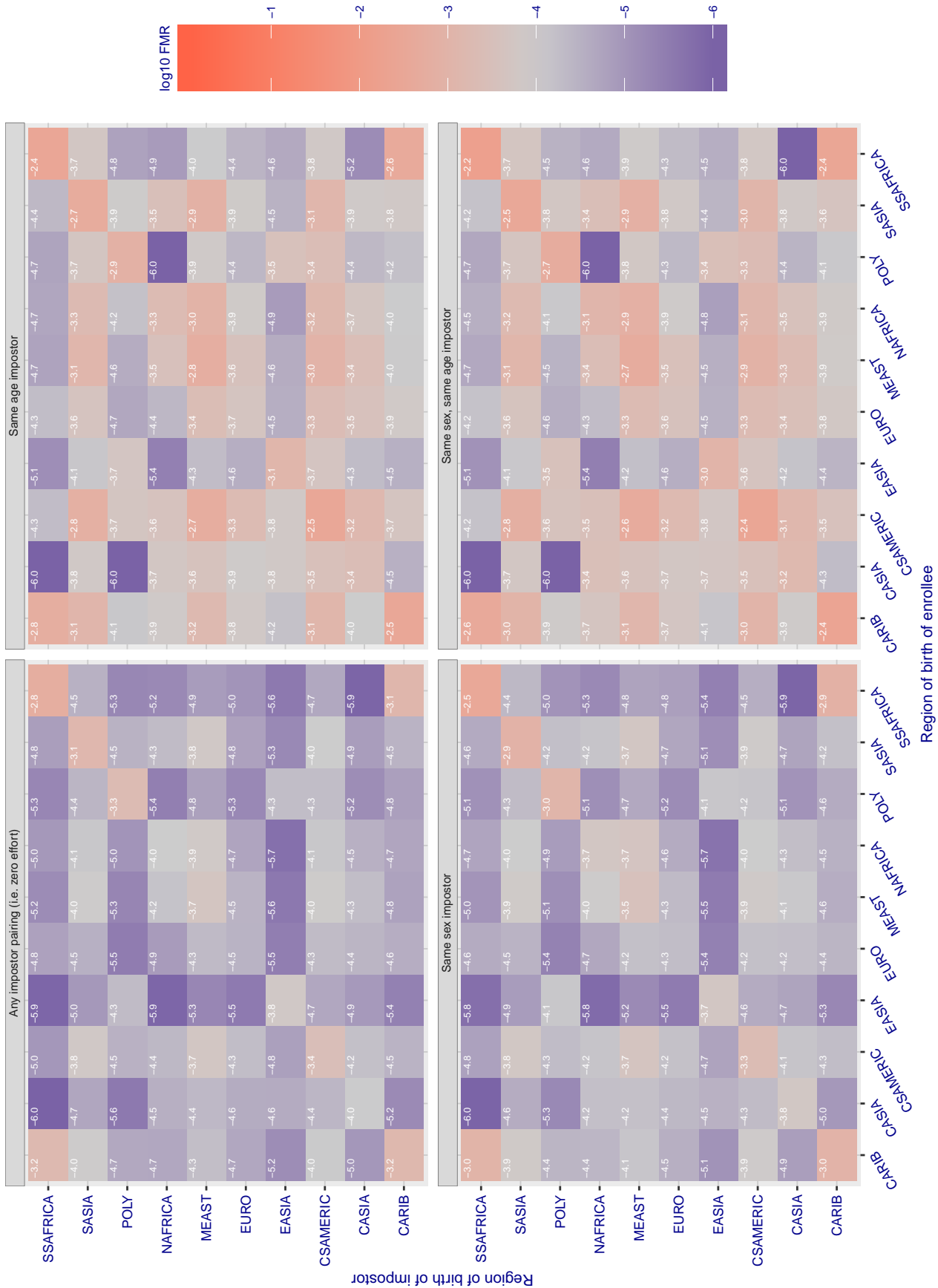


Figure 243: For algorithm lookman-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of 10<sup>10</sup> impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.733$  for algorithm lookman\_004, giving  $FMR(T) = 0.0001$  globally.

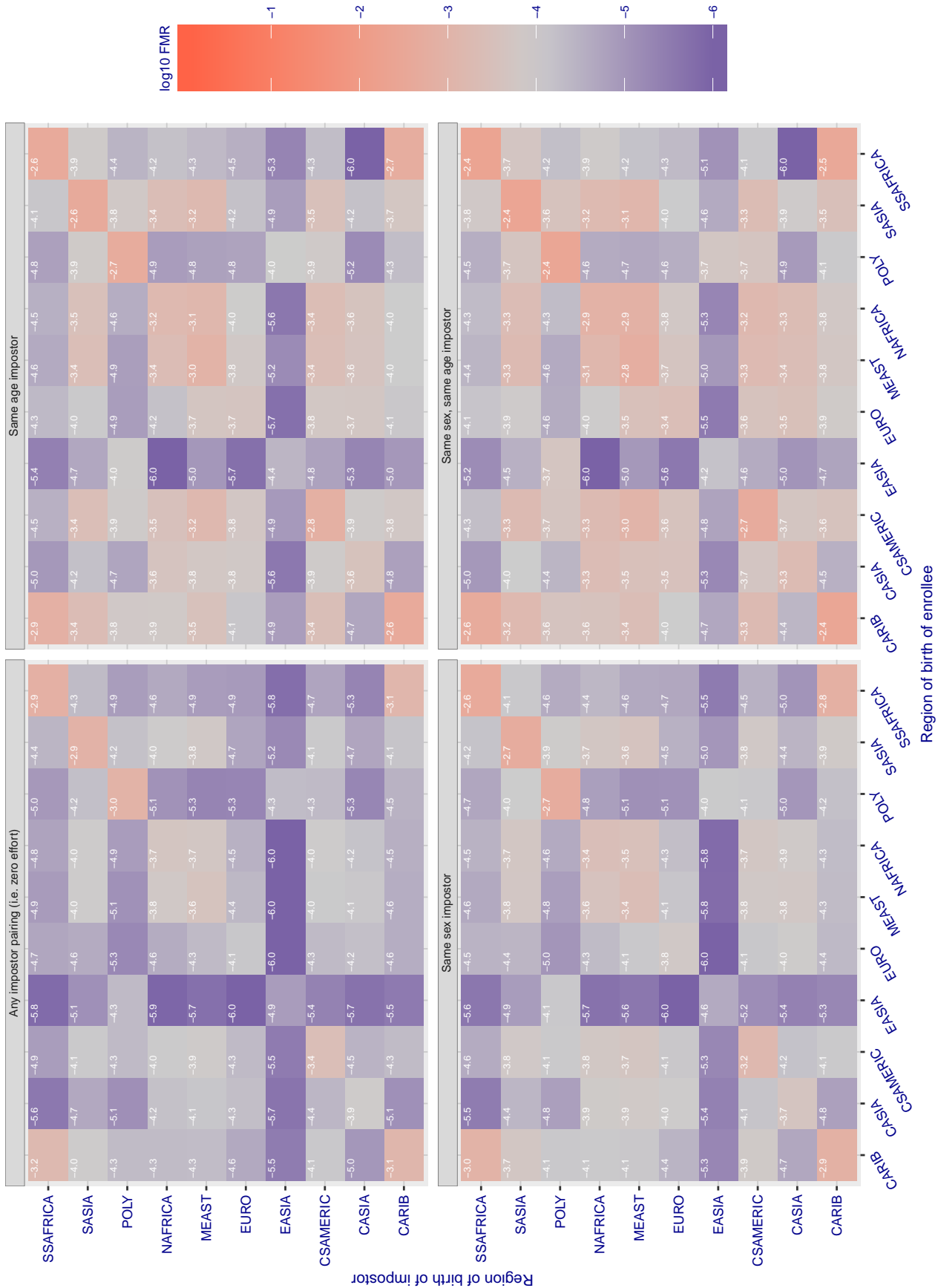


Figure 244: For algorithm lookman-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 74.511$  for algorithm megvii\_001, giving  $FMR(T) = 0.0001$  globally.

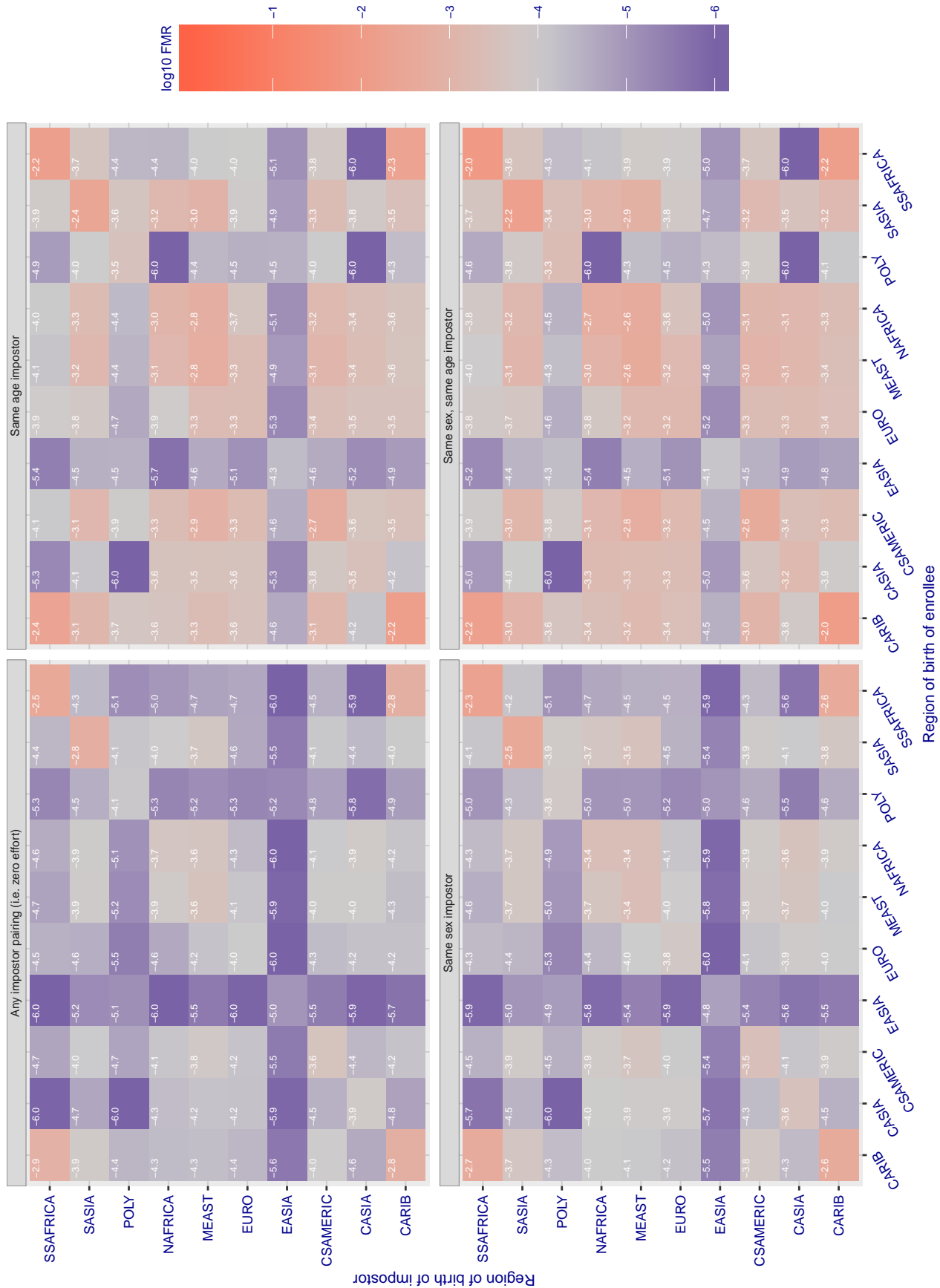


Figure 246: For algorithm megvii-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 66.384$  for algorithm megvii\_002, giving  $FMR(T) = 0.0001$  globally.

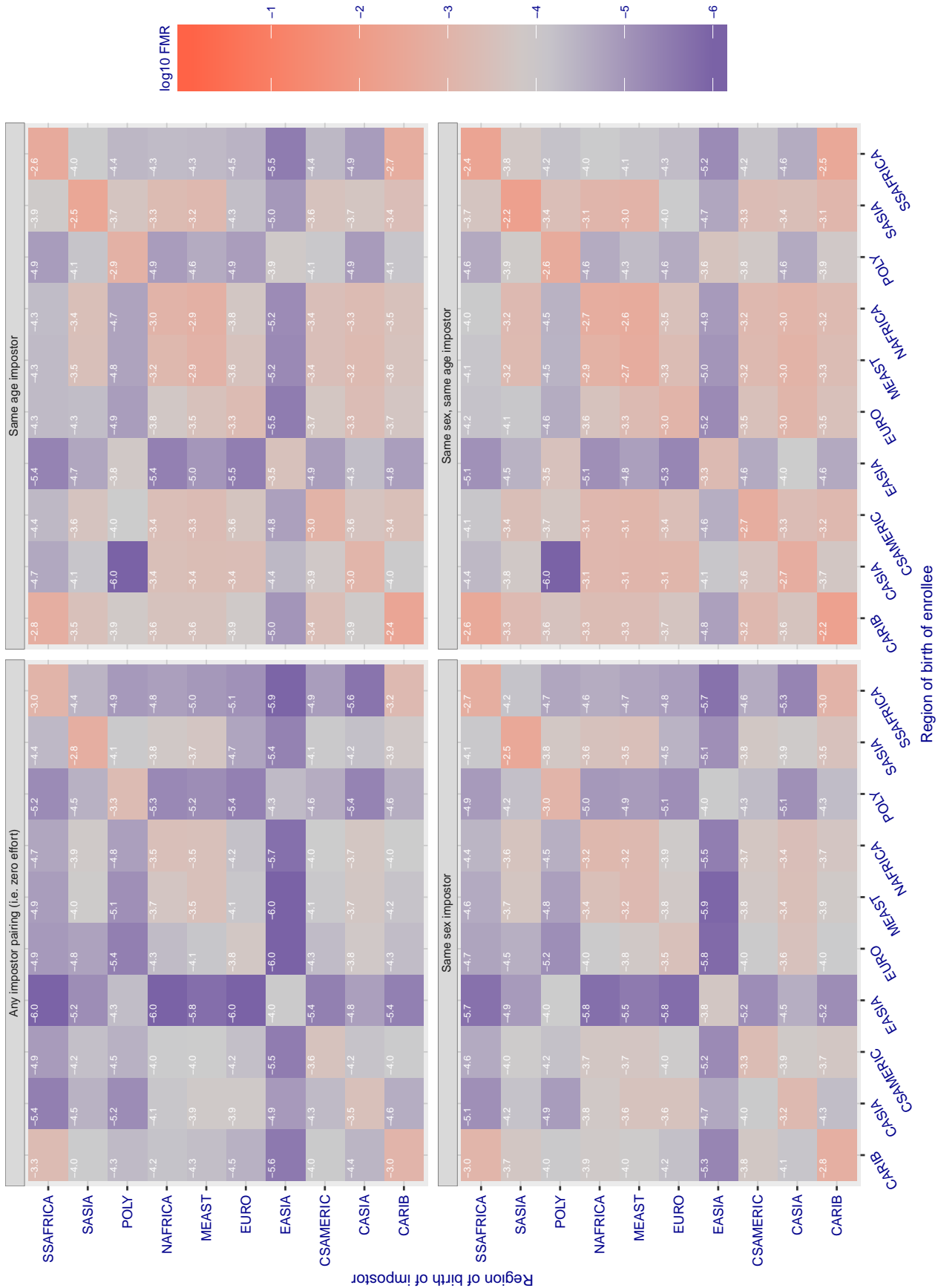


Figure 247: For algorithm megvii-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.425$  for algorithm meiya\_001, giving  $FMR(T) = 0.0001$  globally.

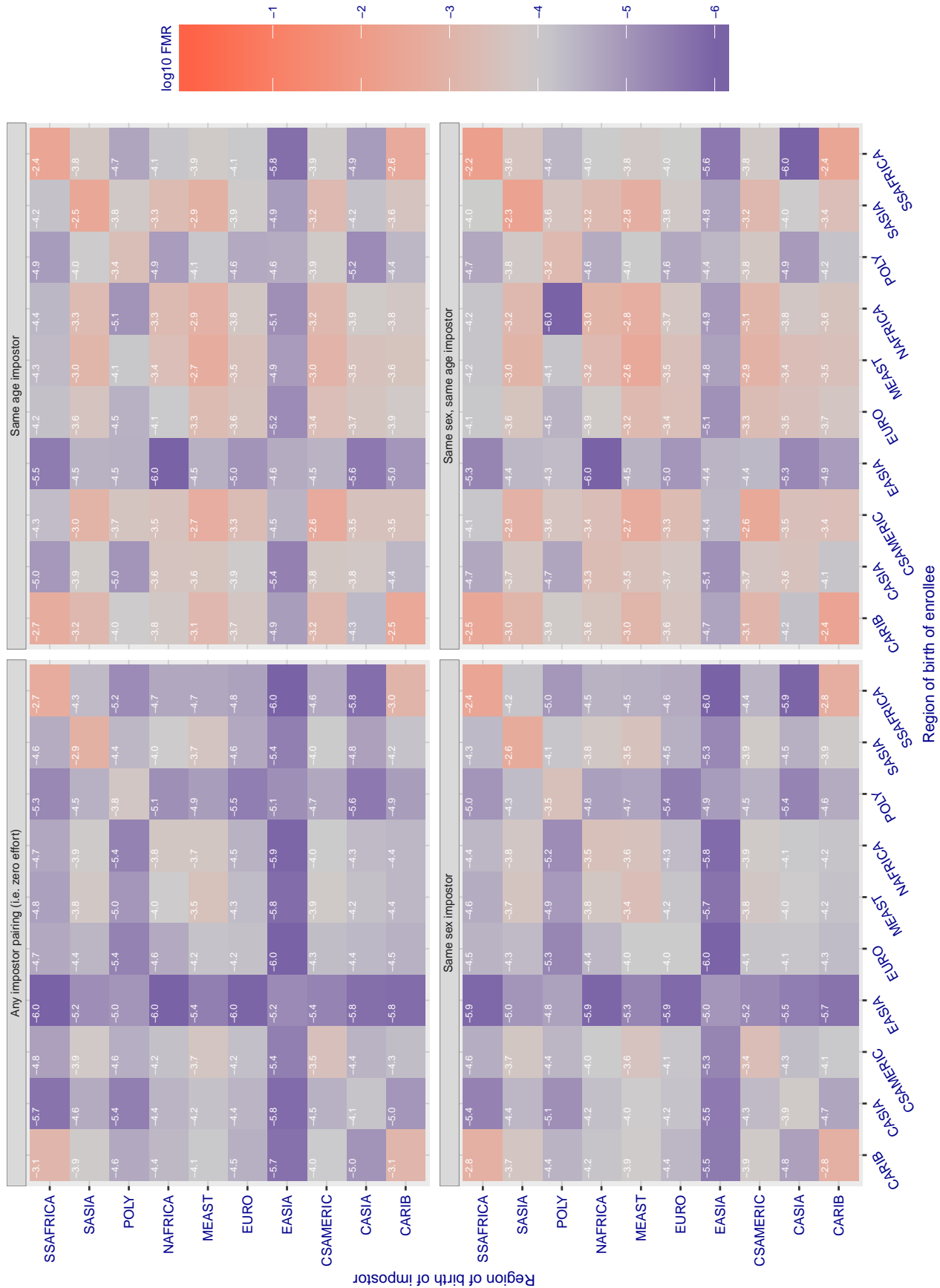


Figure 248: For algorithm meiya-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 0.668$  for algorithm microfocus\_001, giving  $FMR(T) = 0.0001$  globally.

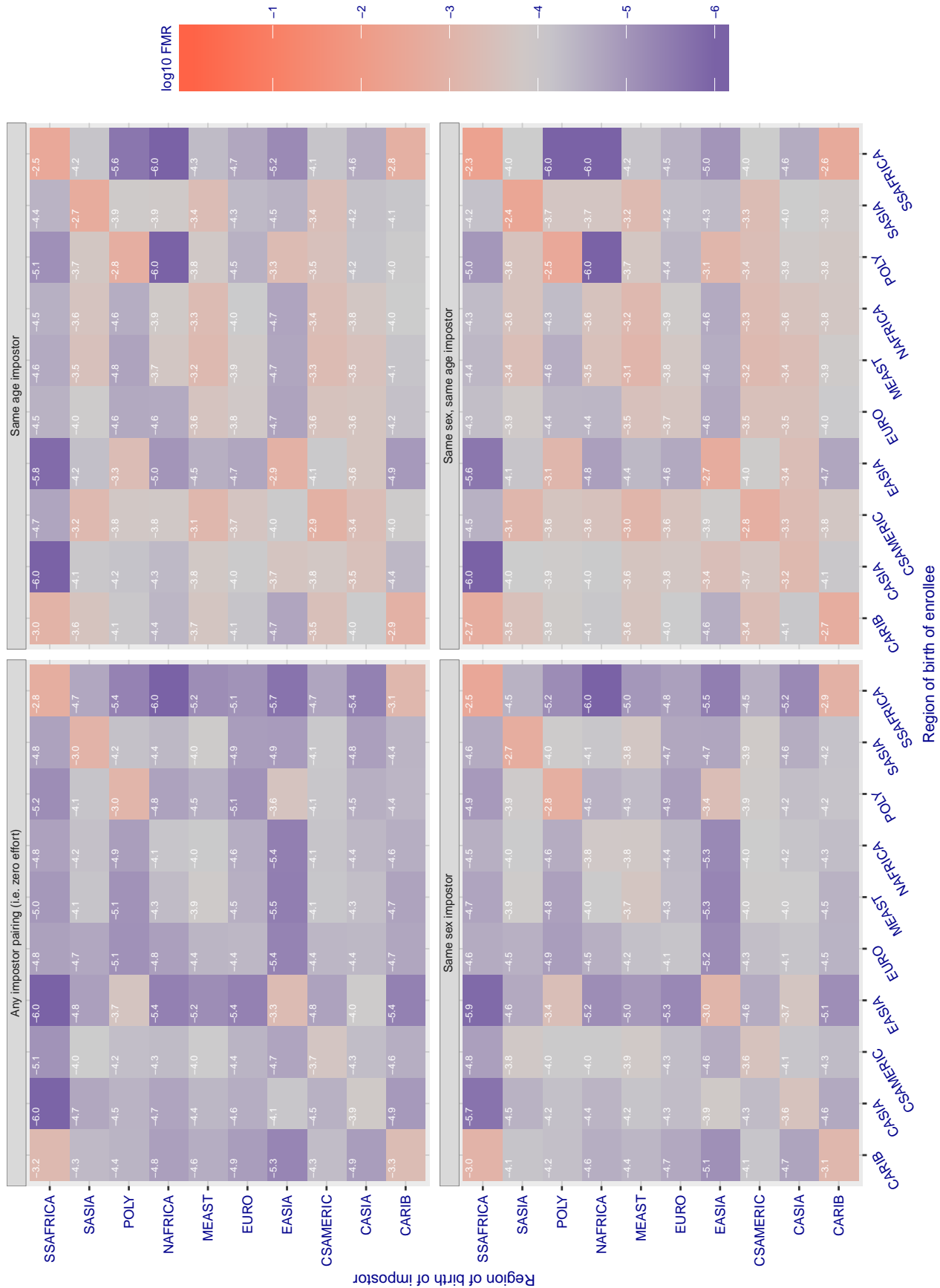


Figure 249: For algorithm microfocus-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

**Cross region FMR at threshold T = 0.602 for algorithm microfocus\_002, giving FMR(T) = 0.0001 globally.**

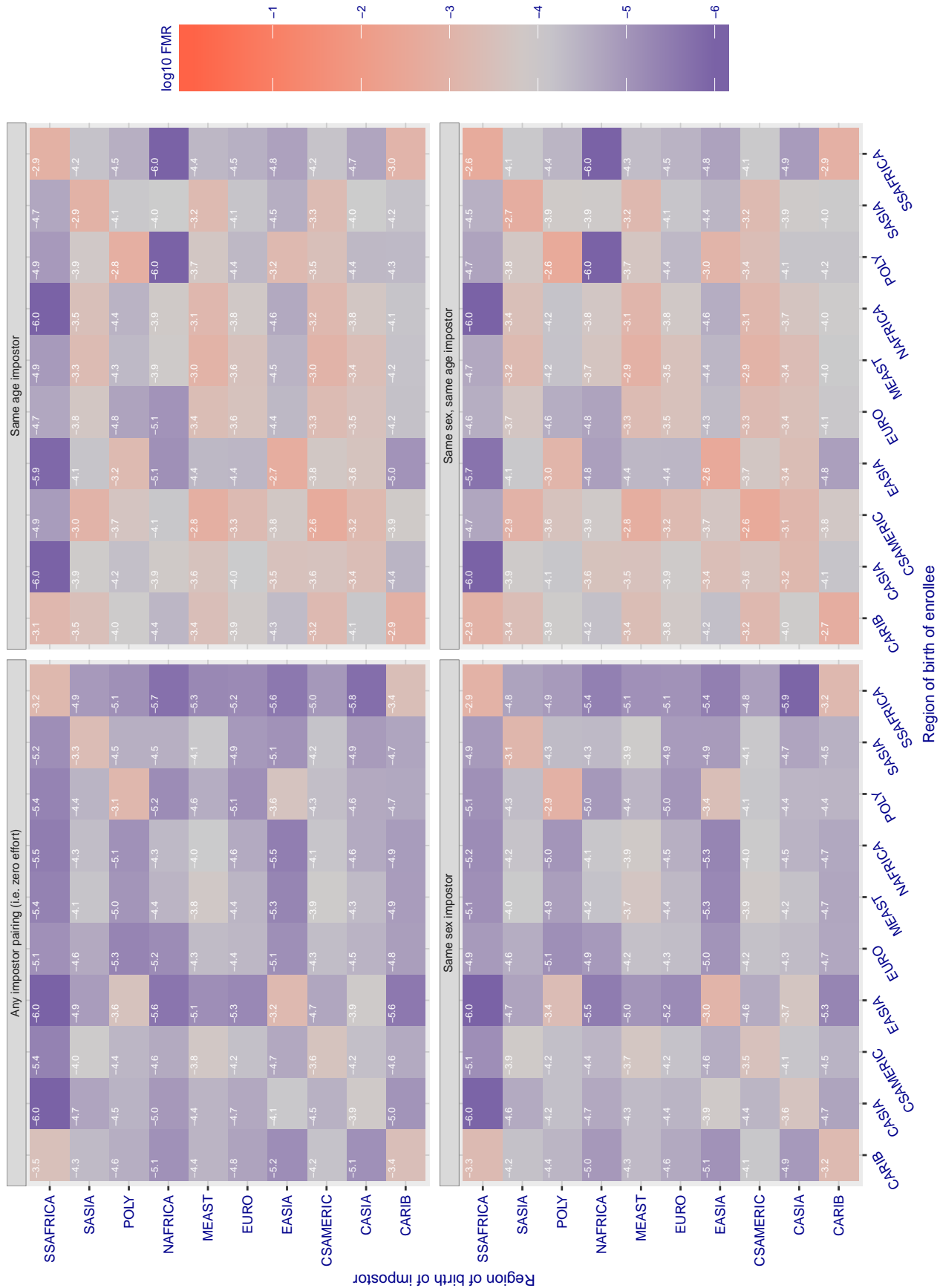


Figure 250: For algorithm microfocus-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 1.394$  for algorithm mt\_000, giving  $FMR(T) = 0.0001$  globally.

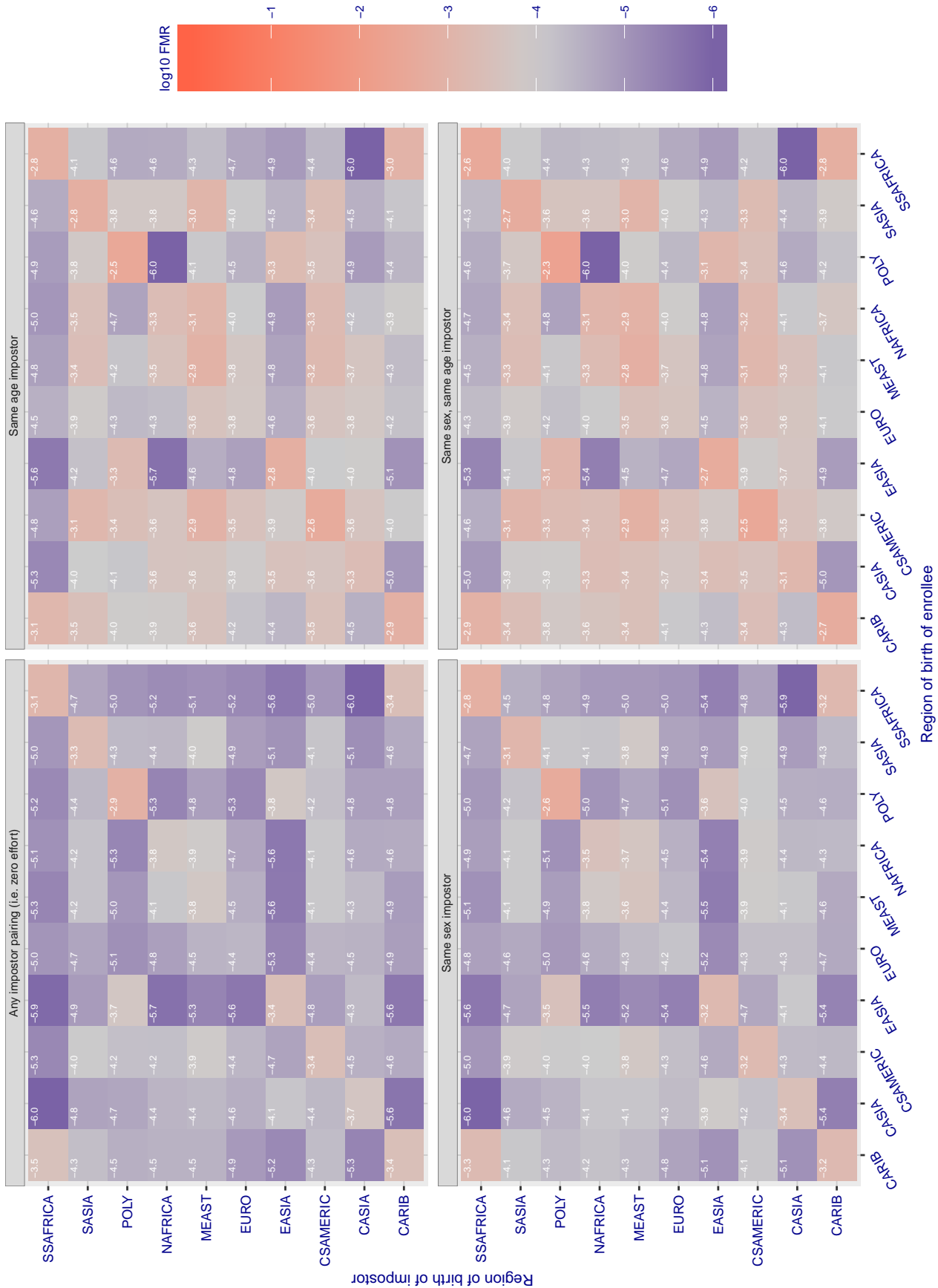


Figure 251: For algorithm mt-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.719$  for algorithm `mvision_001`, giving  $FMR(T) = 0.0001$  globally.

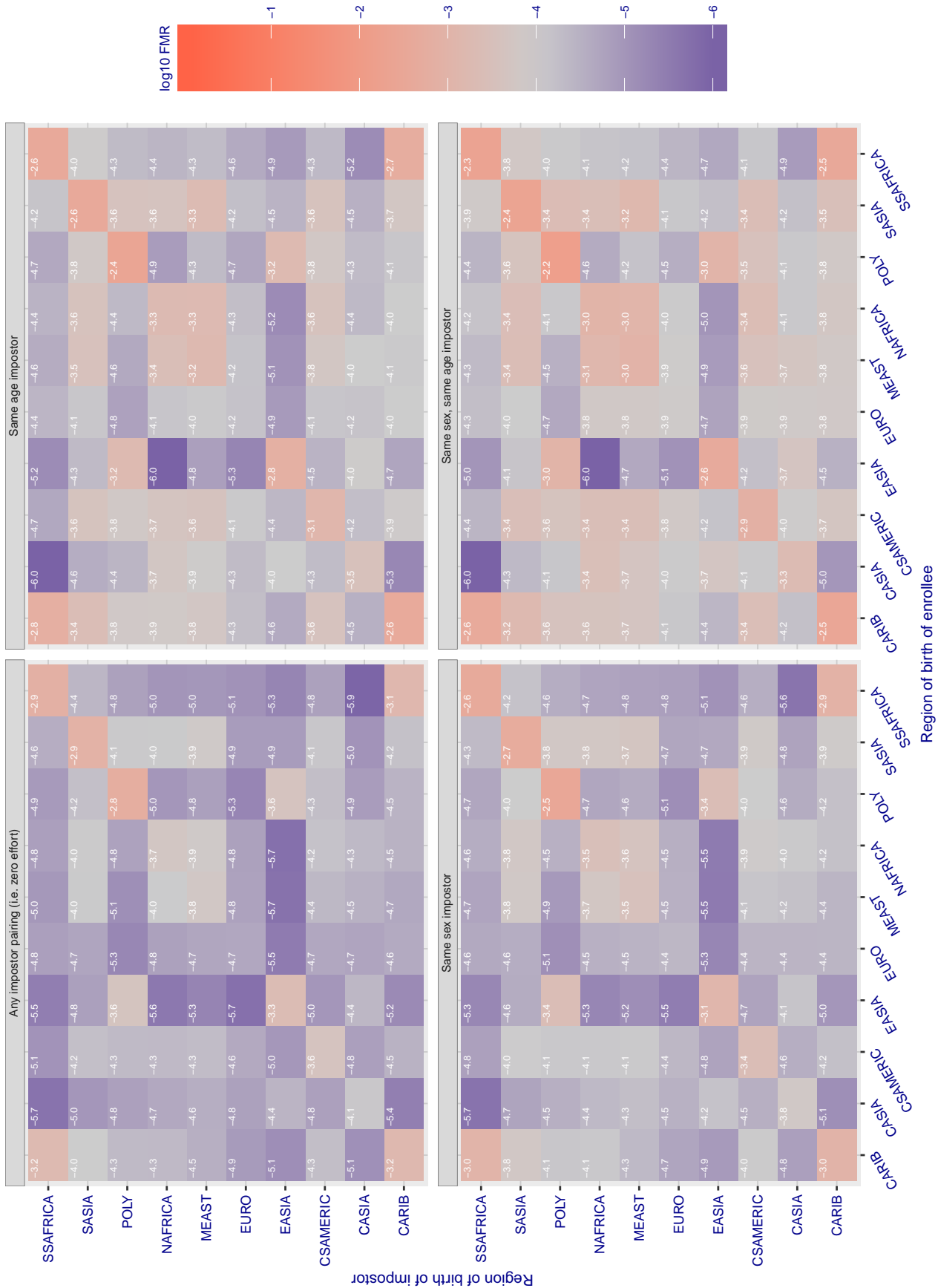


Figure 252: For algorithm `mvision-001` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 46.101$  for algorithm neurotechnology\_005, giving  $FMR(T) = 0.0001$  globally.

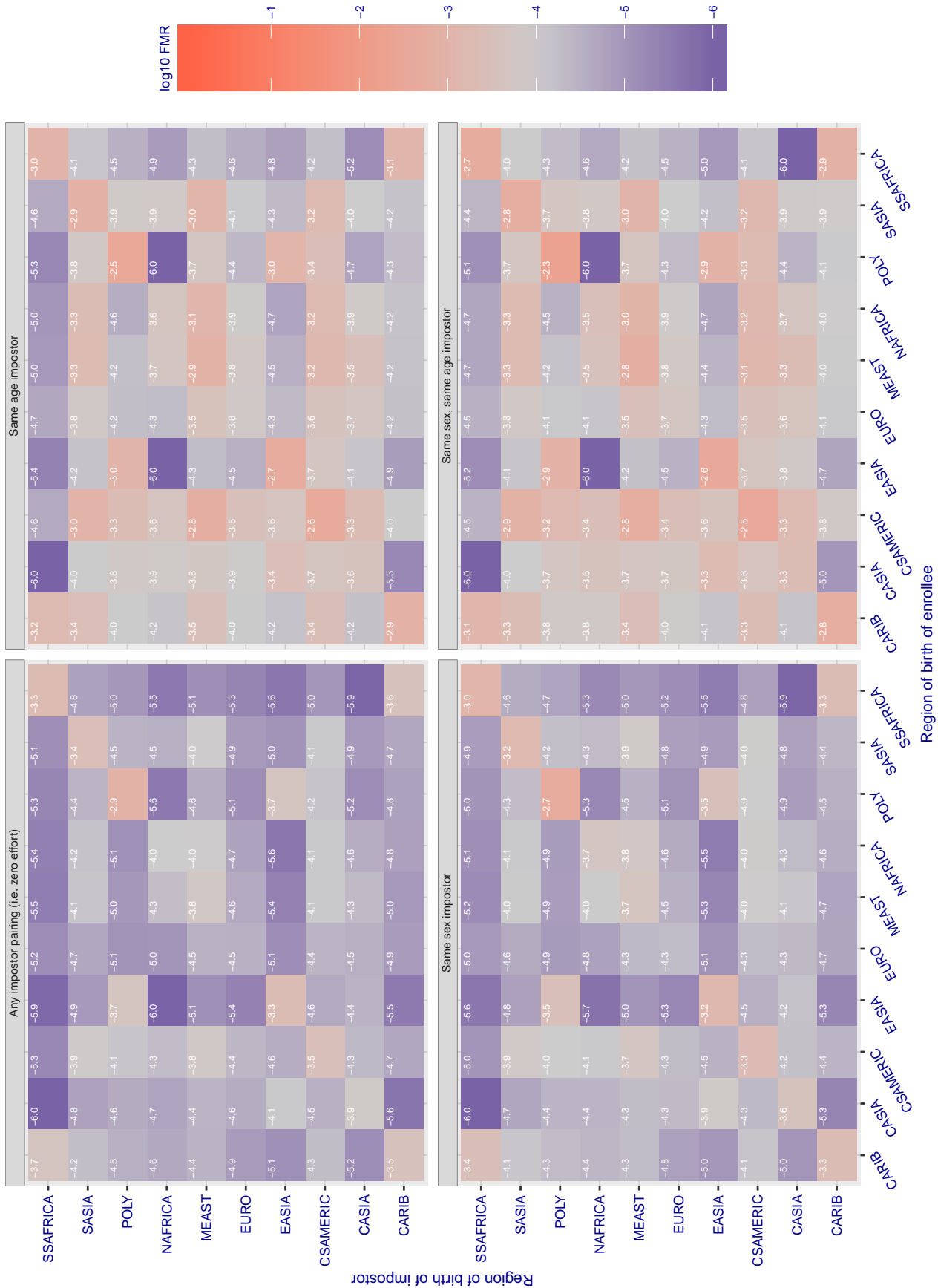


Figure 253: For algorithm neurotechnology-005 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{1.0}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 2044.000 for algorithm neurotechnology\_006, giving FMR(T) = 0.0001 globally.

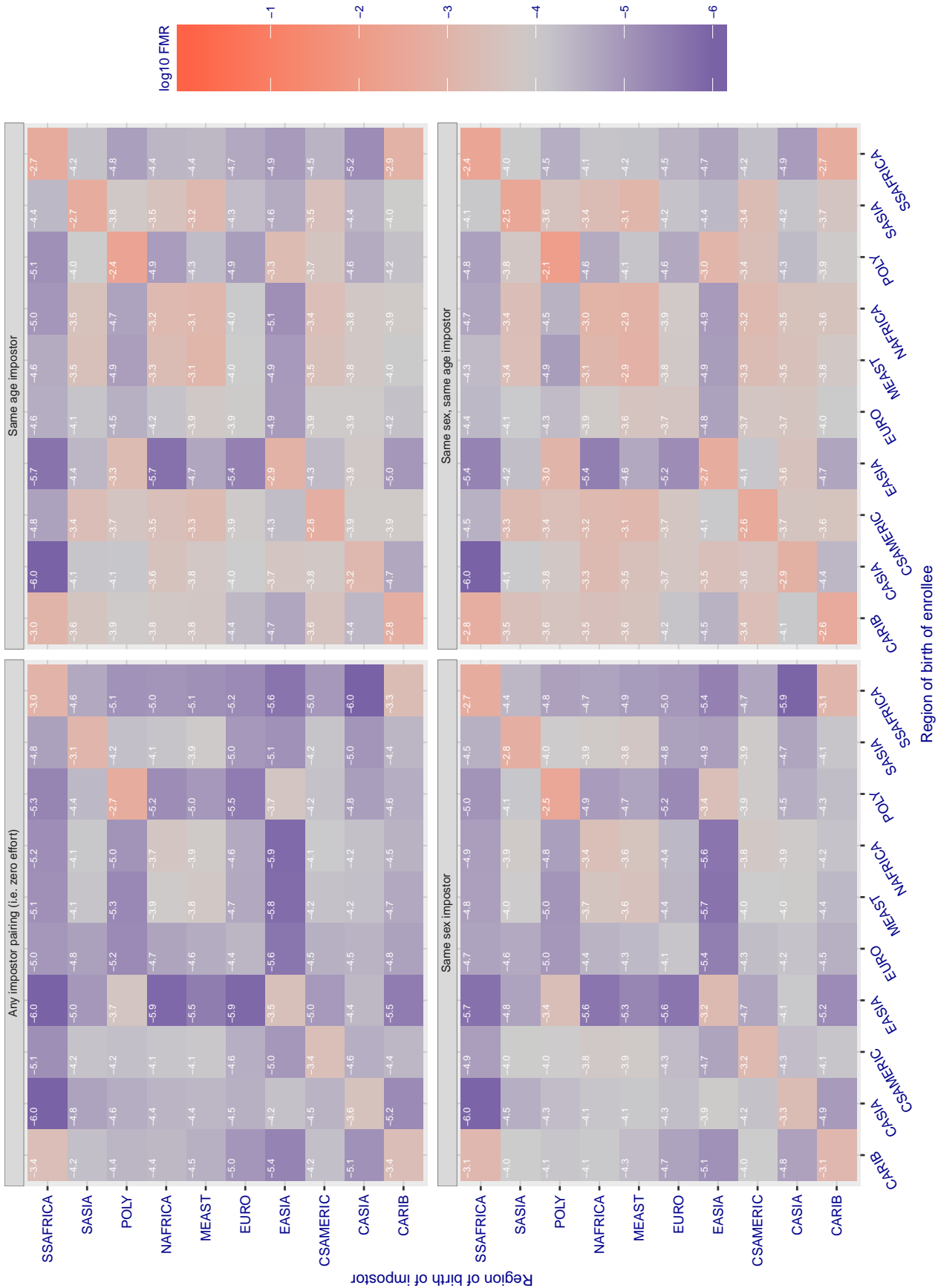


Figure 254: For algorithm neurotechnology-006 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{1.0}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 1.000$  for algorithm nodeflux\_001, giving  $FMR(T) = 0.0001$  globally.

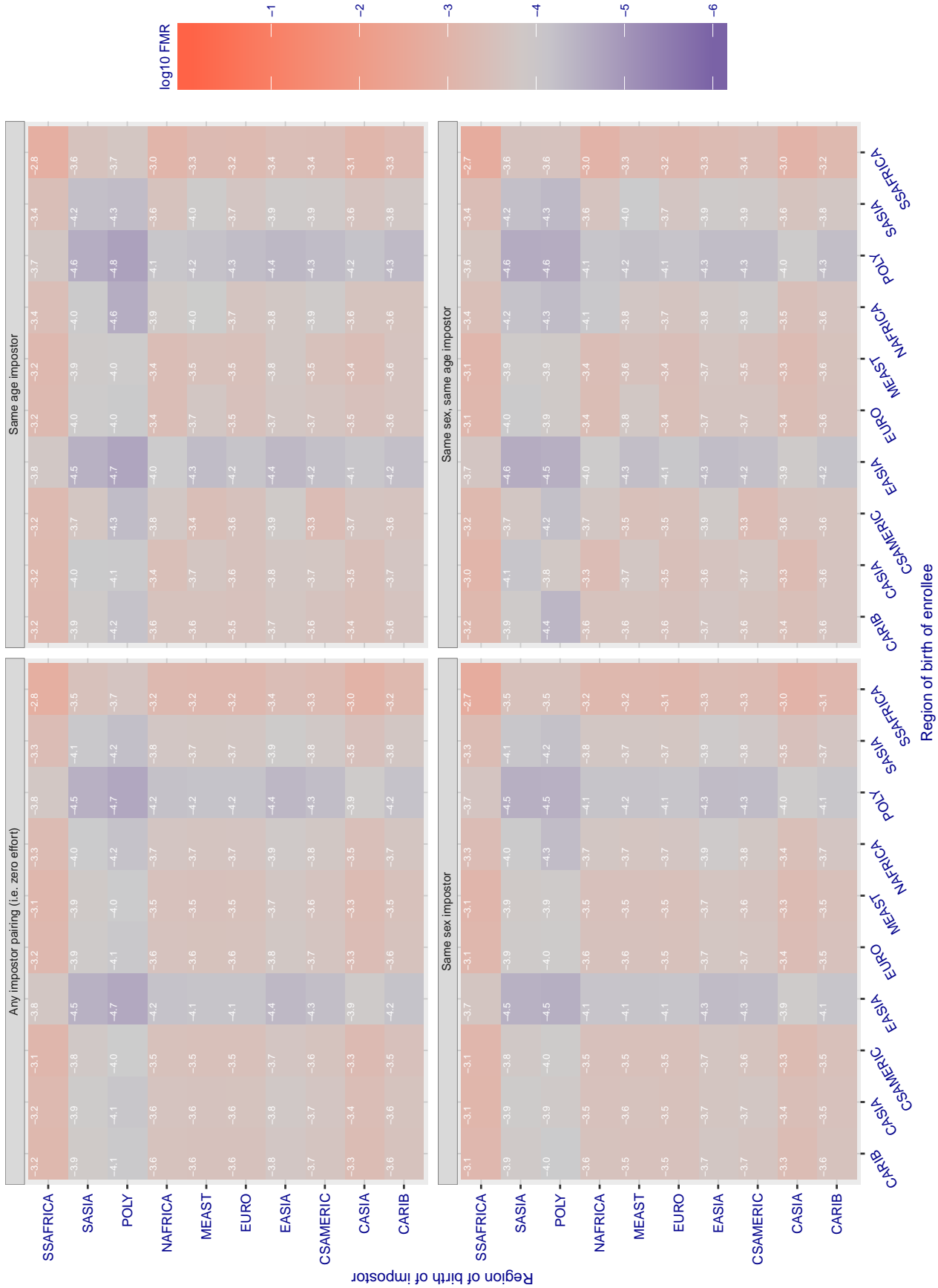


Figure 255: For algorithm nodeflux-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

**Cross region FMR at threshold T = 0.455 for algorithm nodeflux\_002, giving FMR(T) = 0.0001 globally.**

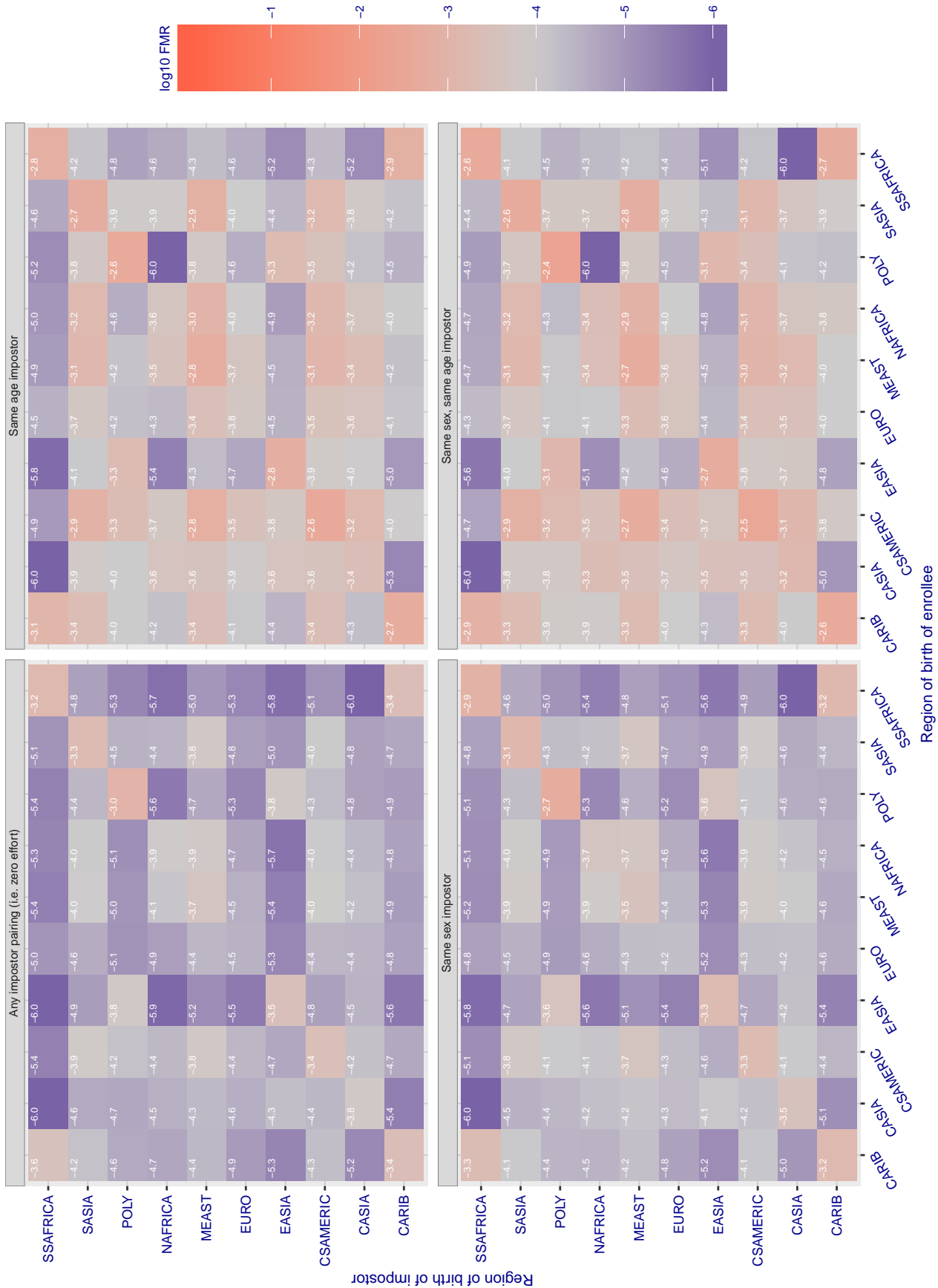


Figure 256: For algorithm nodeflux-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold T = 16846383821648700779774369791310334462380752812000954299625965117711518105060865483

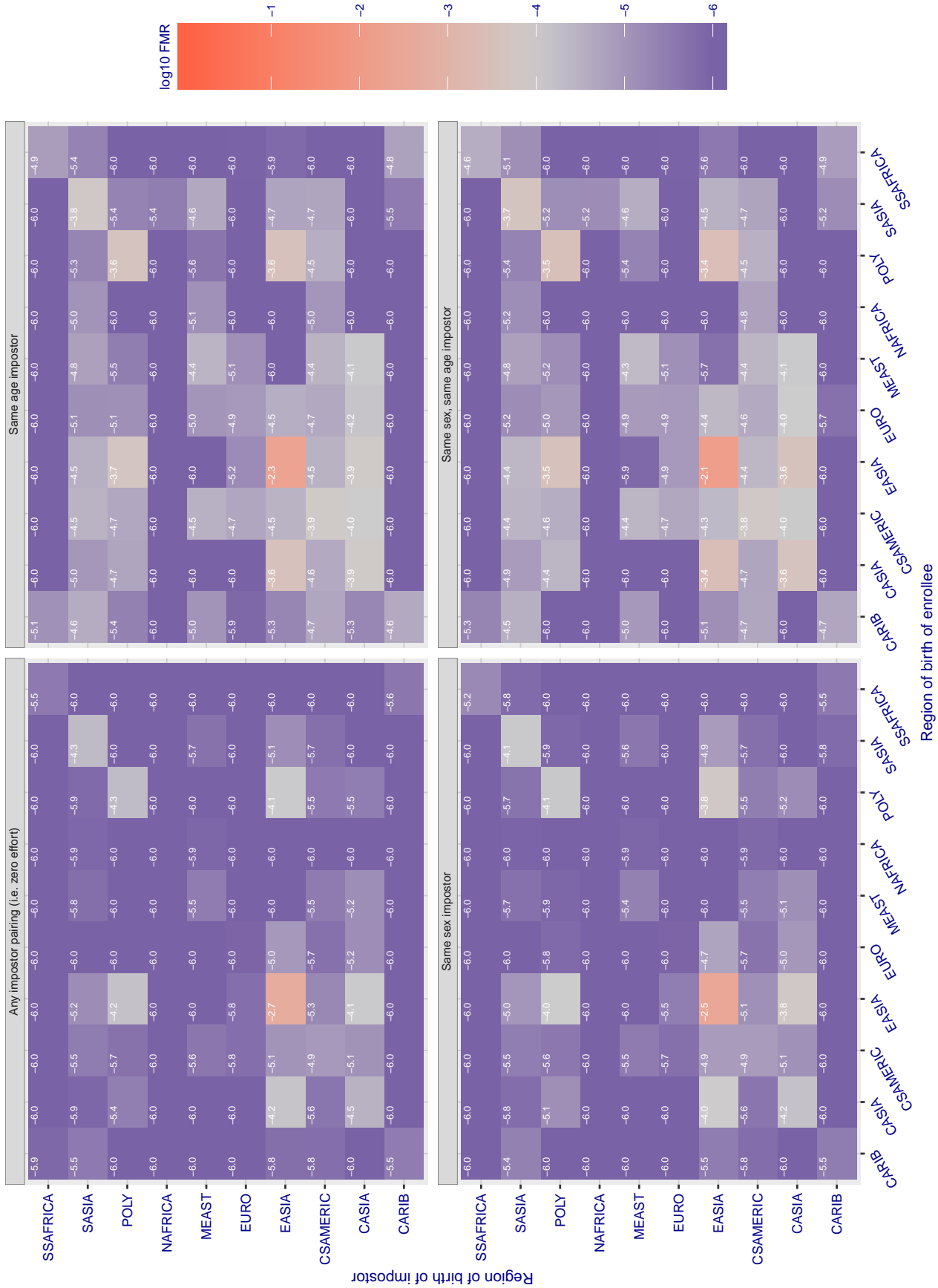


Figure 257: For algorithm notiontag-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

**Cross region FMR at threshold T = 1.997 for algorithm ntechlab\_006, giving FMR(T) = 0.0001 globally.**

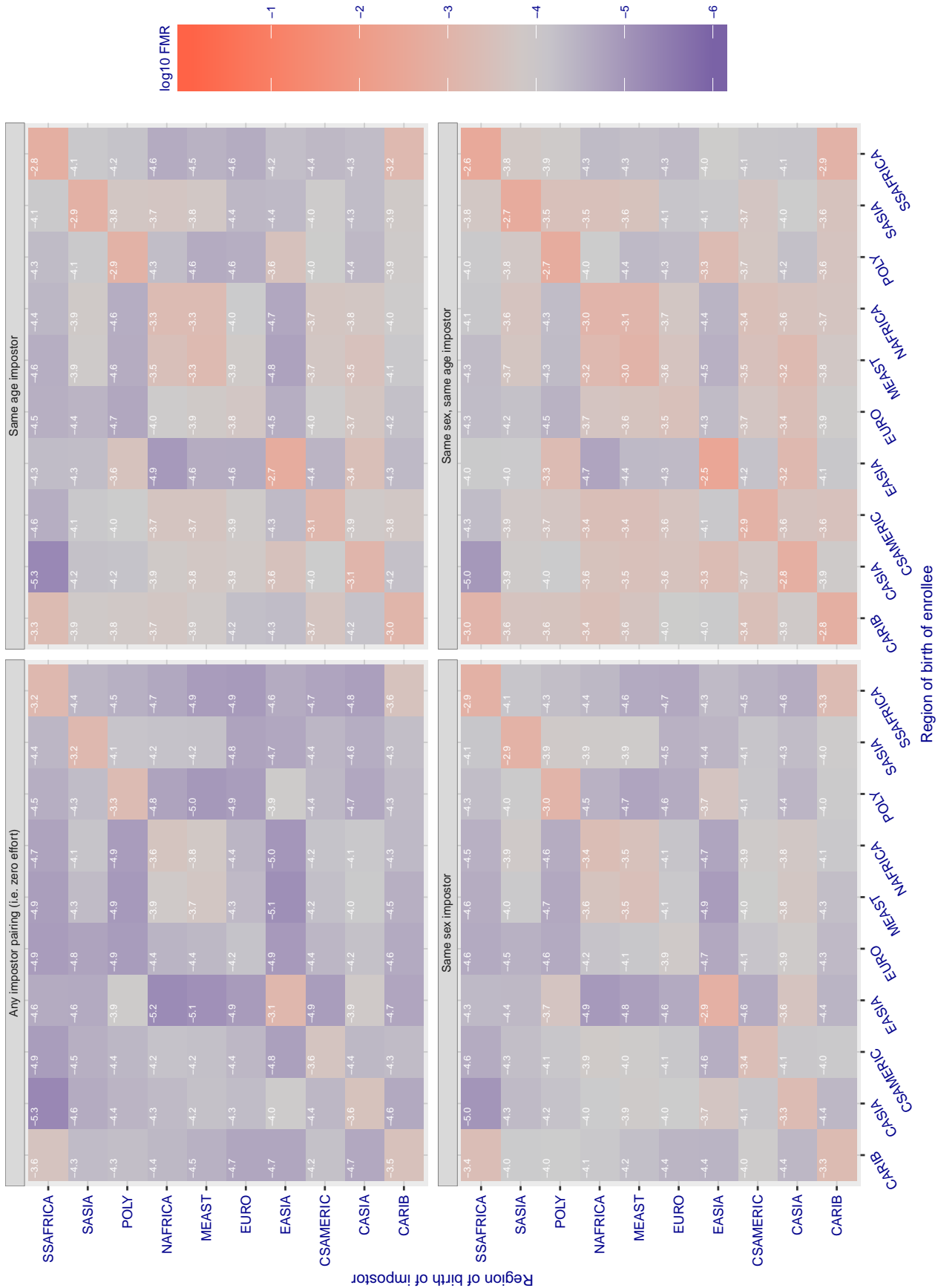


Figure 258: For algorithm ntechlab-006 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 1.416 for algorithm ntechlab\_007, giving FMR(T) = 0.0001 globally.

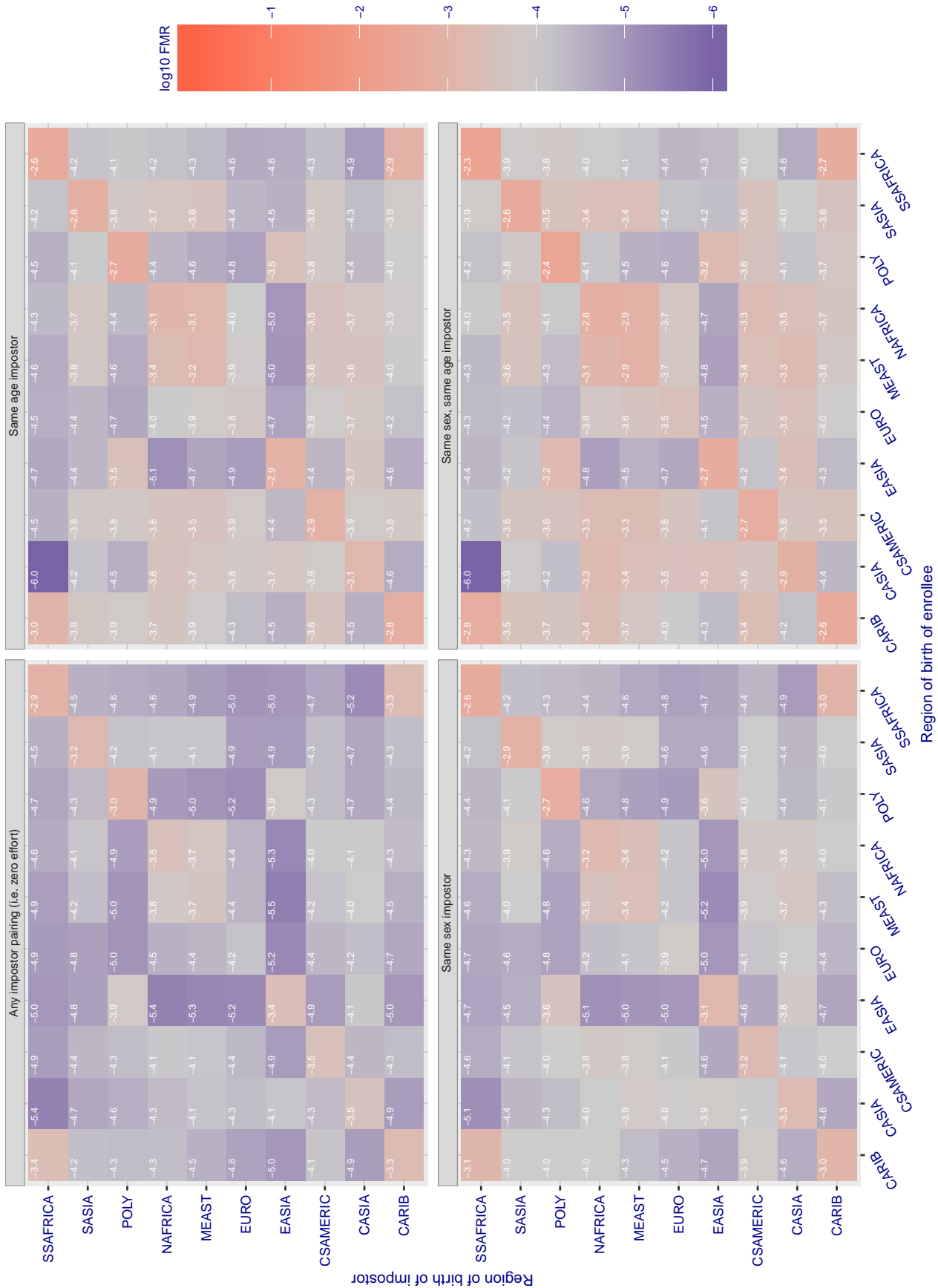


Figure 259: For algorithm ntechlab-007 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.428$  for algorithm pixelall\_002, giving  $FMR(T) = 0.0001$  globally.

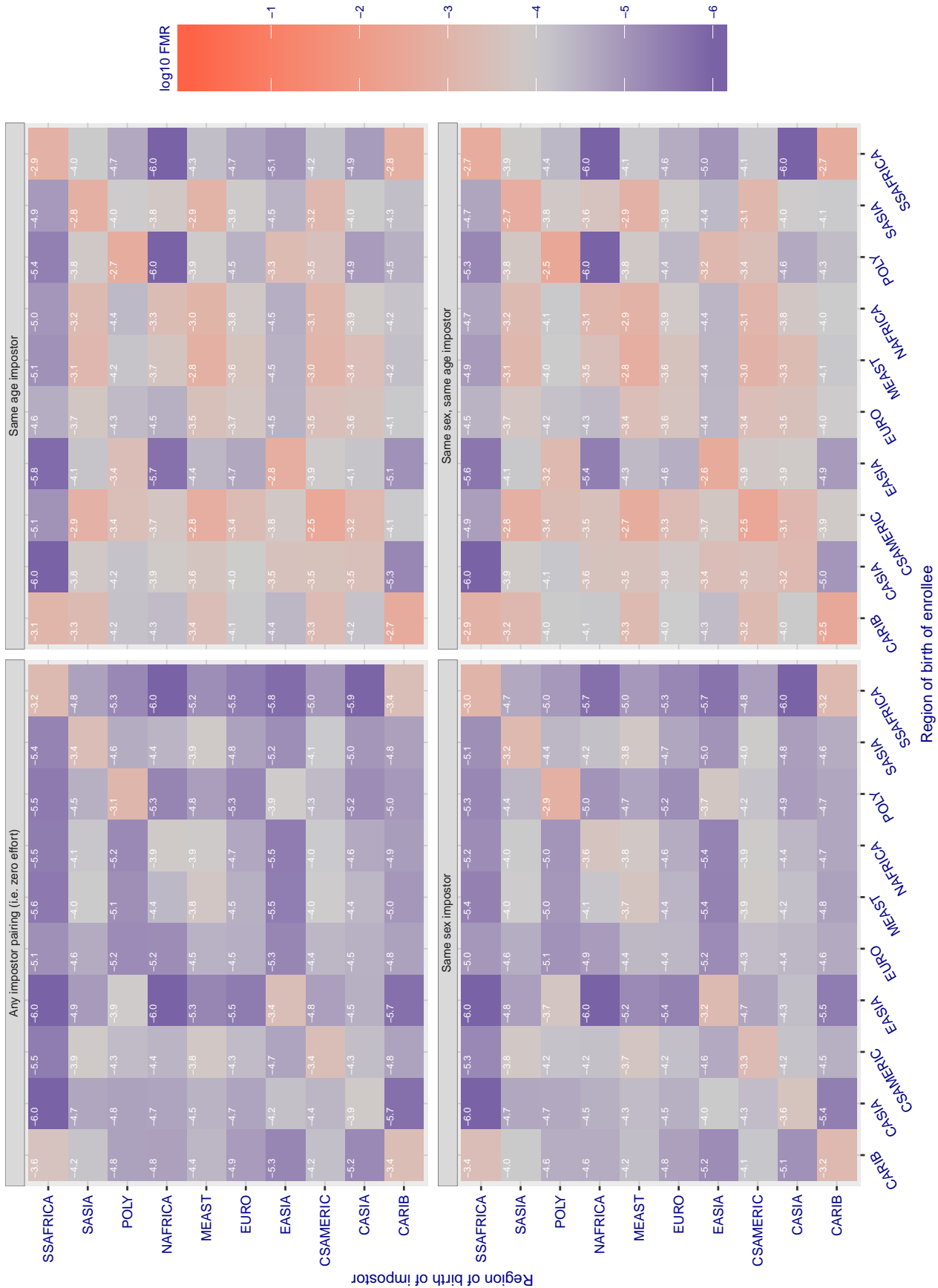


Figure 260: For algorithm pixelall-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.389$  for algorithm pixelall\_003, giving  $FMR(T) = 0.0001$  globally.

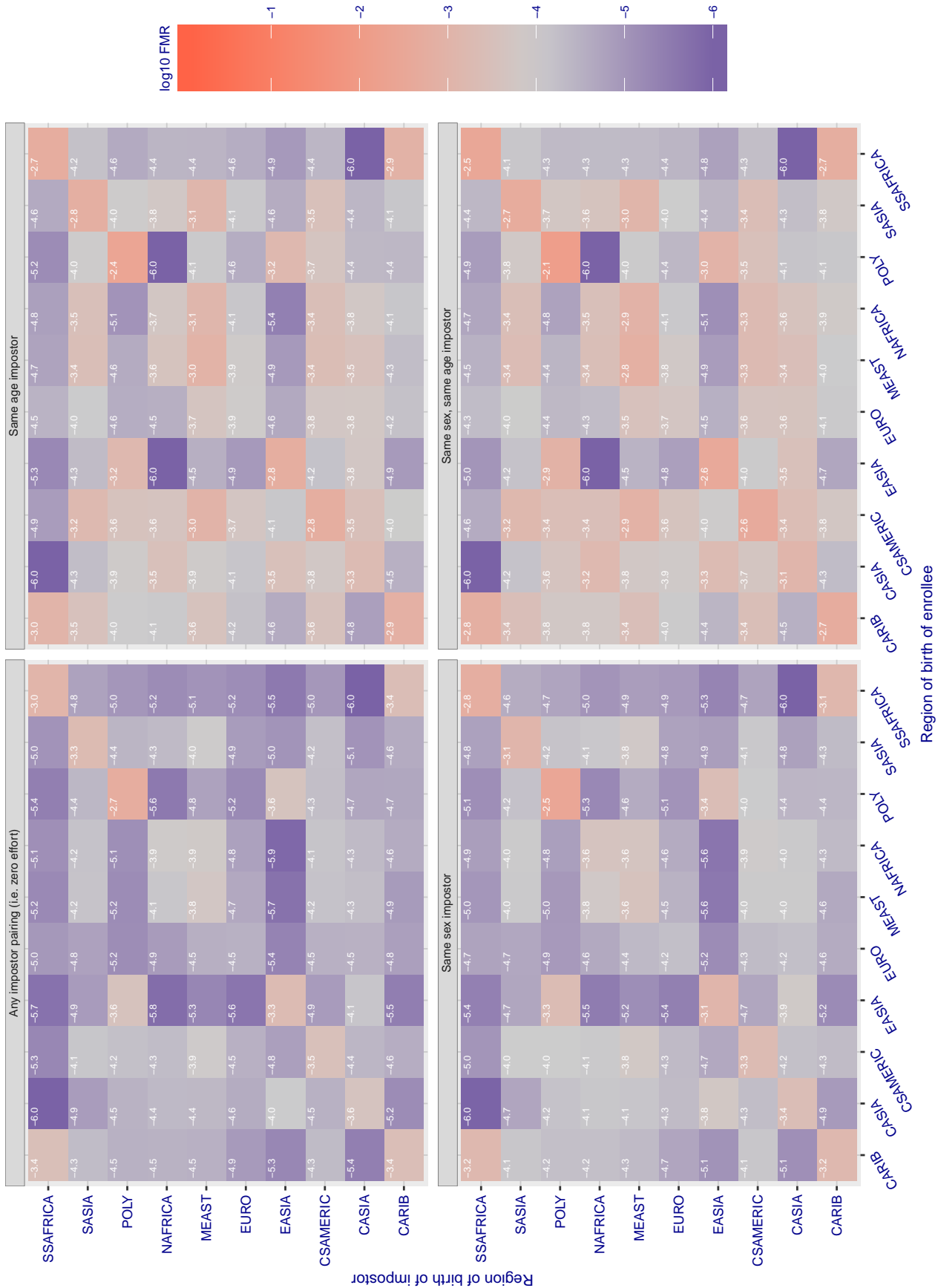


Figure 261: For algorithm pixelall-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.353$  for algorithm `psl_002`, giving  $FMR(T) = 0.0001$  globally.

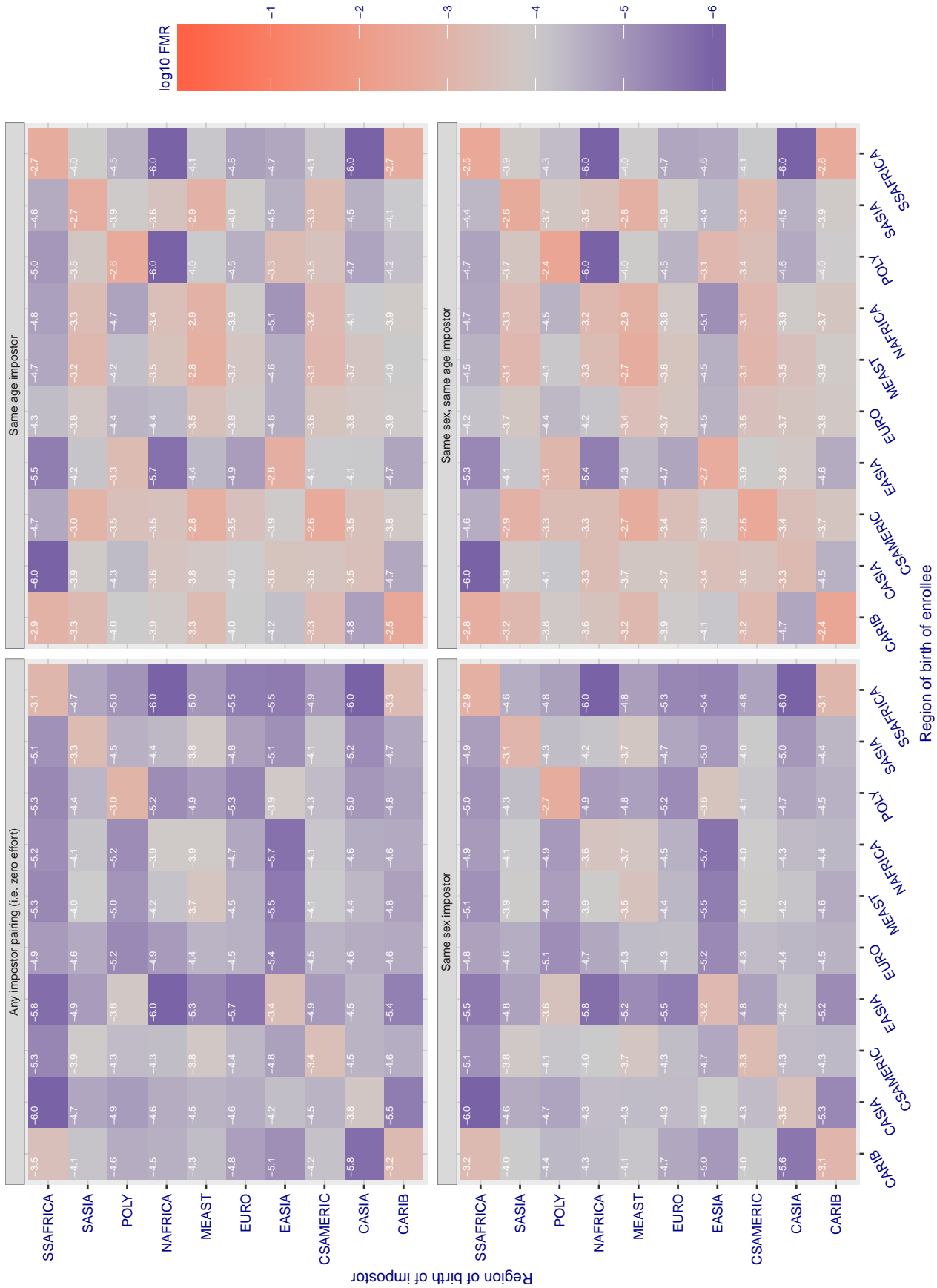


Figure 262: For algorithm `psl-002` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold T = 0.668 for algorithm psl\_003, giving FMR(T) = 0.0001 globally.

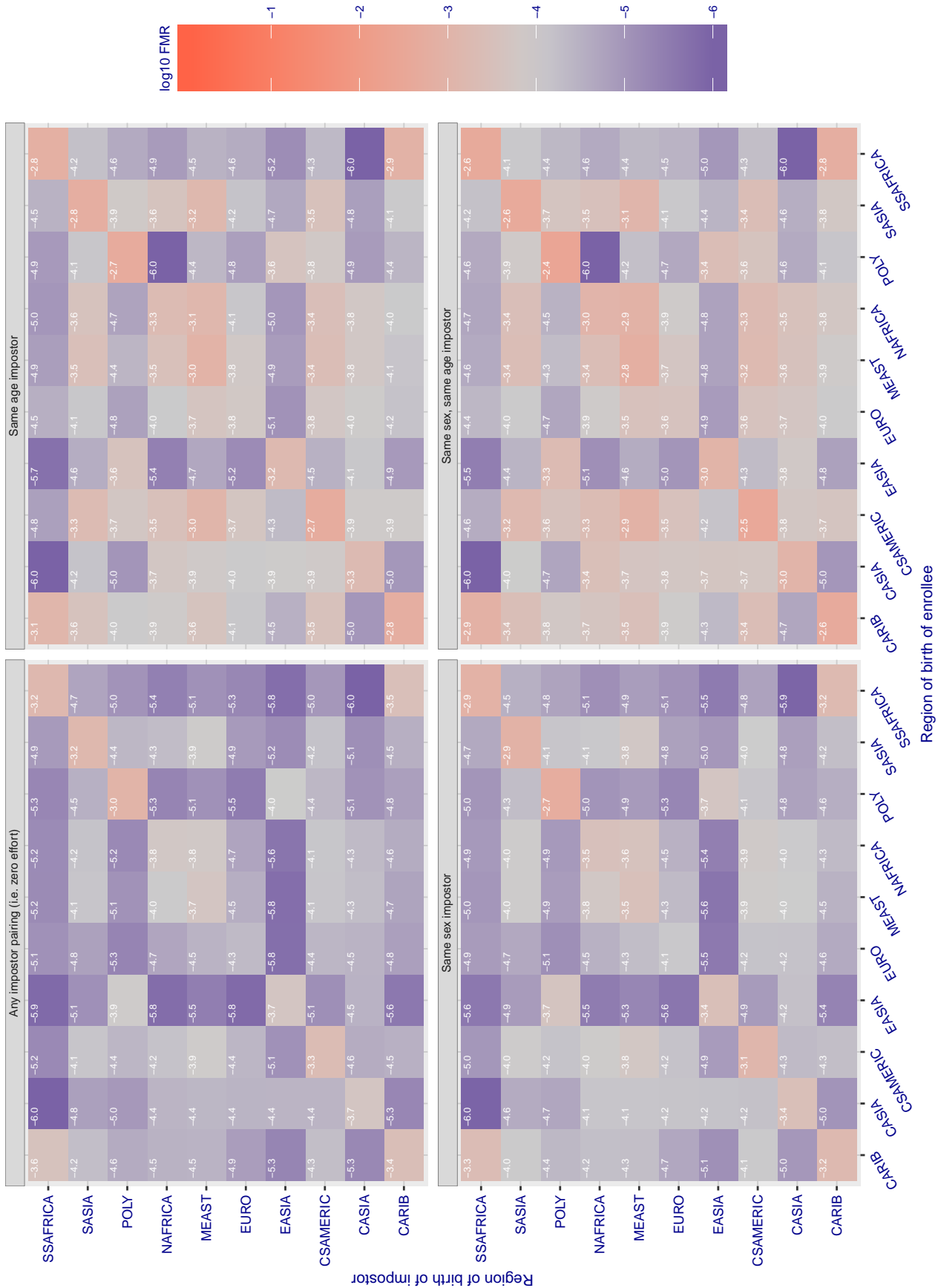


Figure 263: For algorithm psl-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 53.178$  for algorithm pyramid\_000, giving  $FMR(T) = 0.0001$  globally.

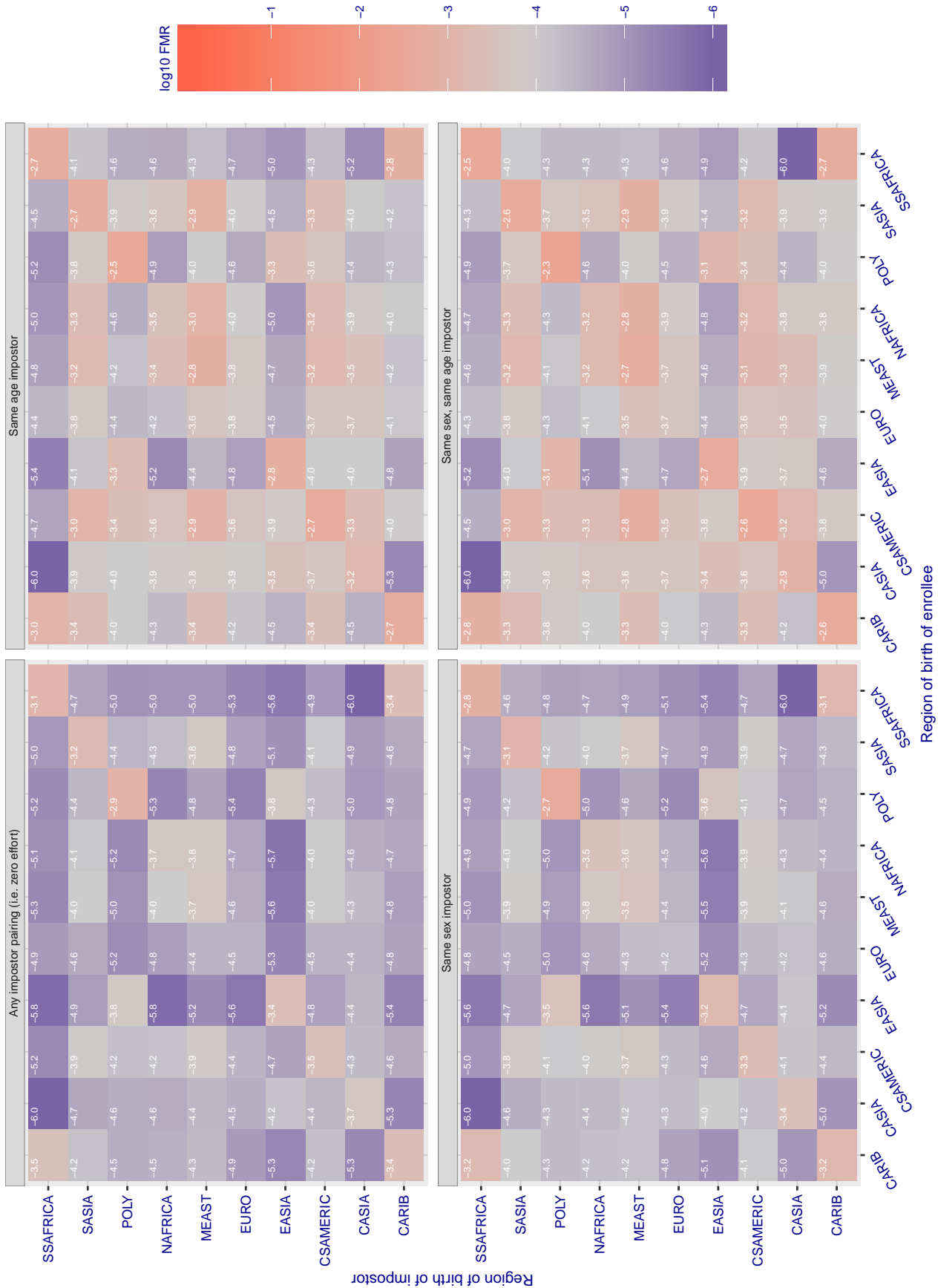


Figure 264: For algorithm pyramid-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



**Cross region FMR at threshold T = 0.661 for algorithm rankone\_007, giving FMR(T) = 0.0001 globally.**

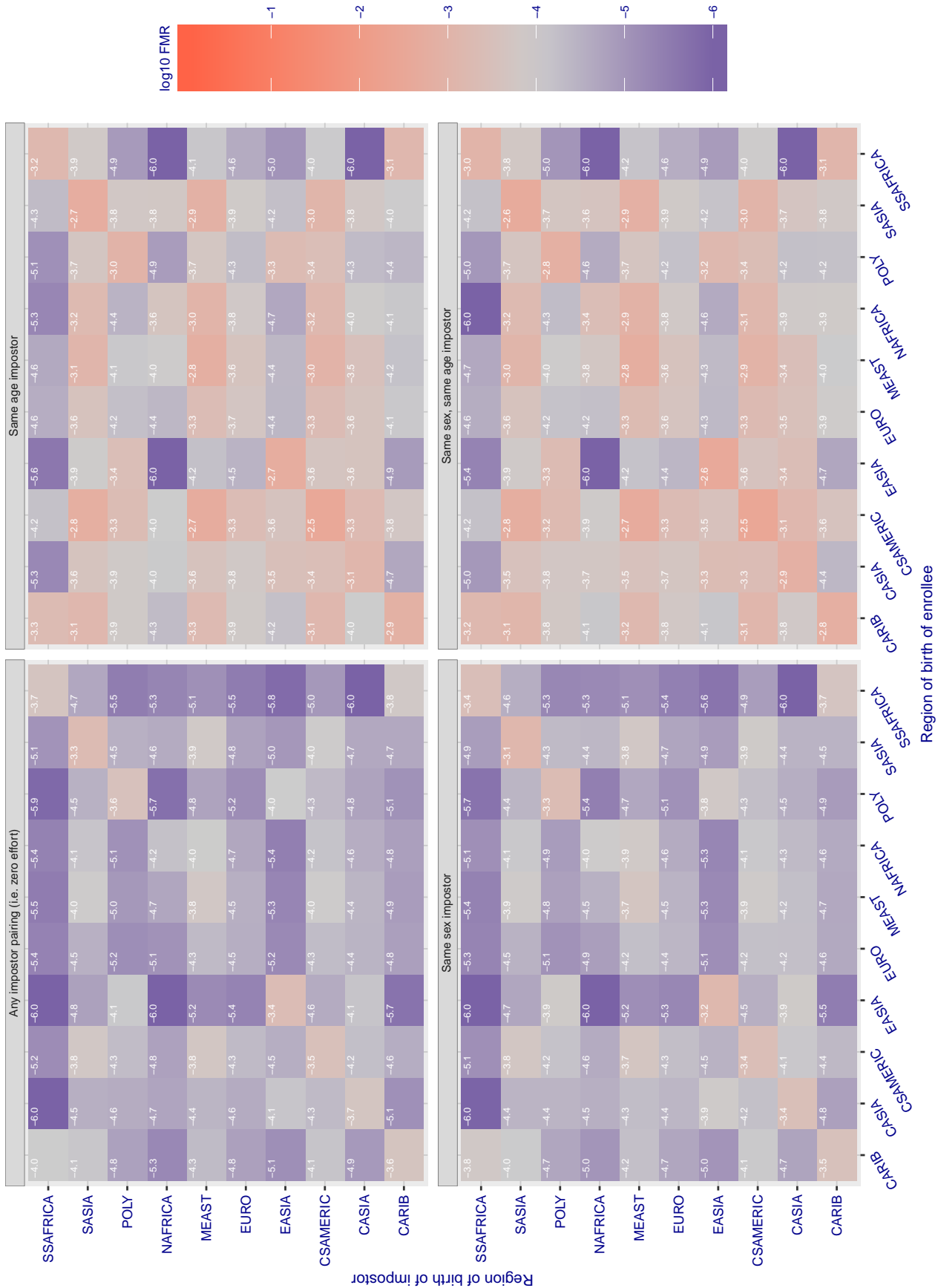


Figure 265: For algorithm rankone-007 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.774$  for algorithm rankone\_008, giving  $FMR(T) = 0.0001$  globally.

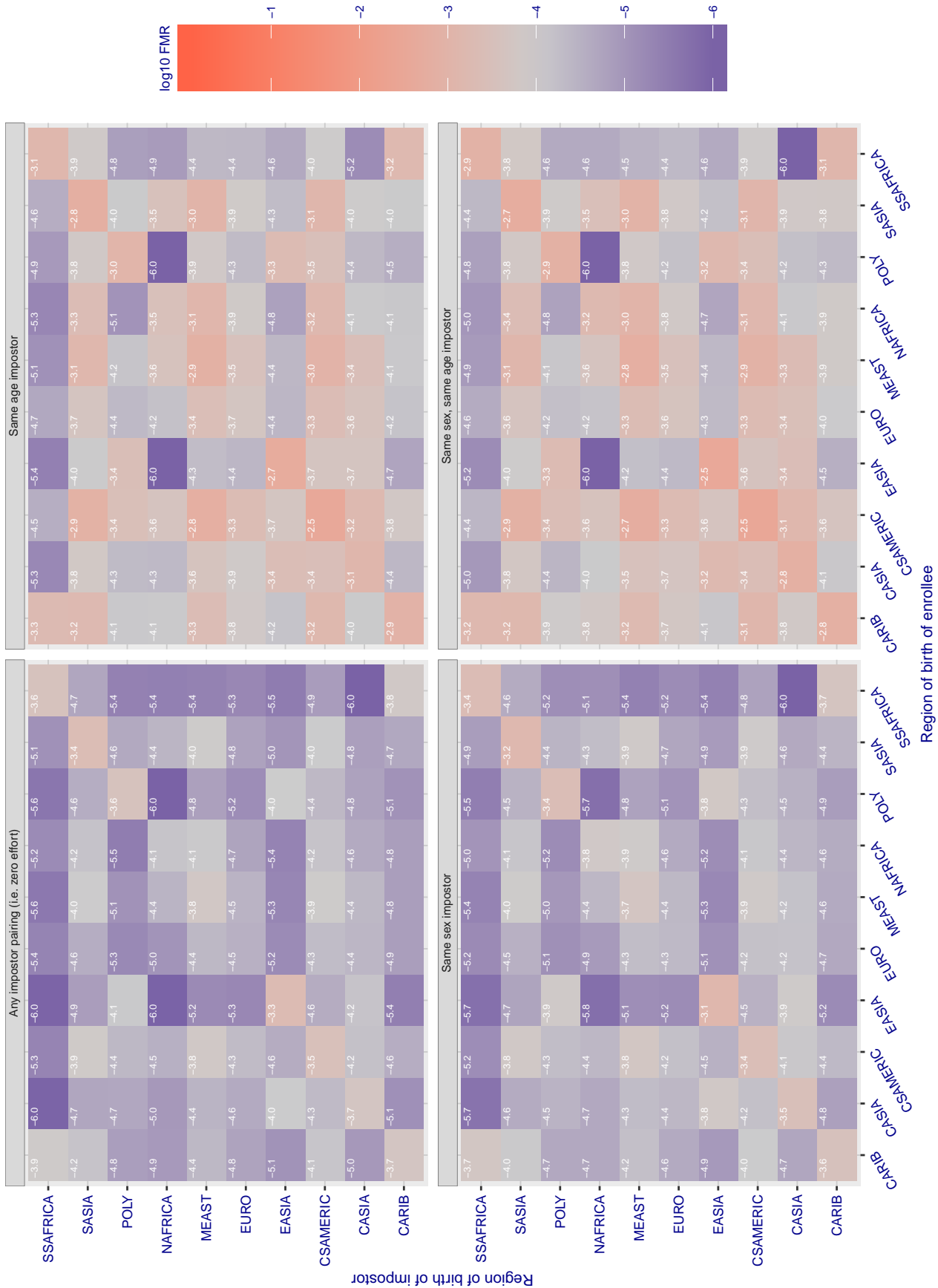


Figure 266: For algorithm rankone-008 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.883$  for algorithm realnetworks\_002, giving  $FMR(T) = 0.0001$  globally.

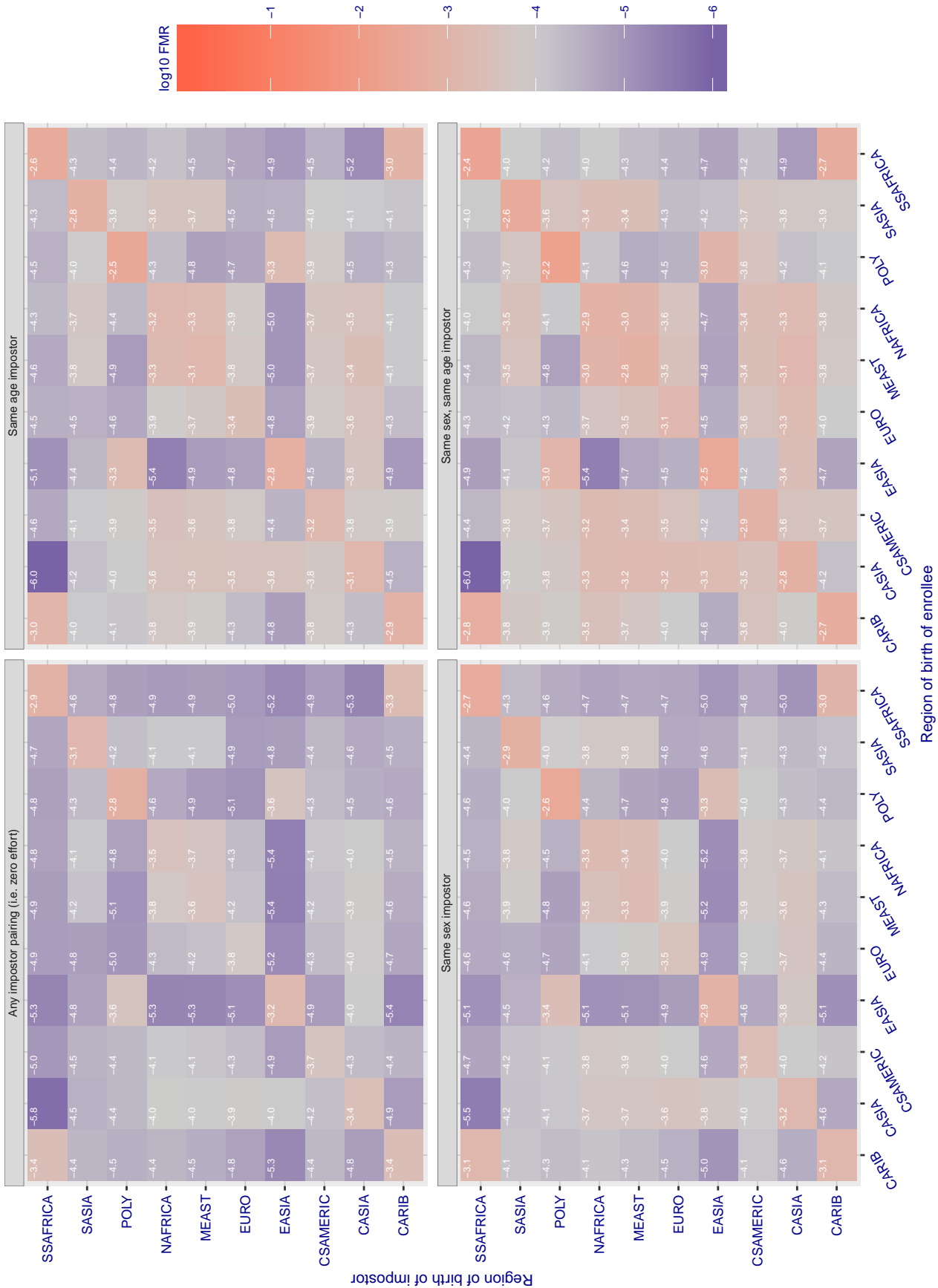


Figure 267: For algorithm realnetworks-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.886$  for algorithm realnetworks\_003, giving  $FMR(T) = 0.0001$  globally.

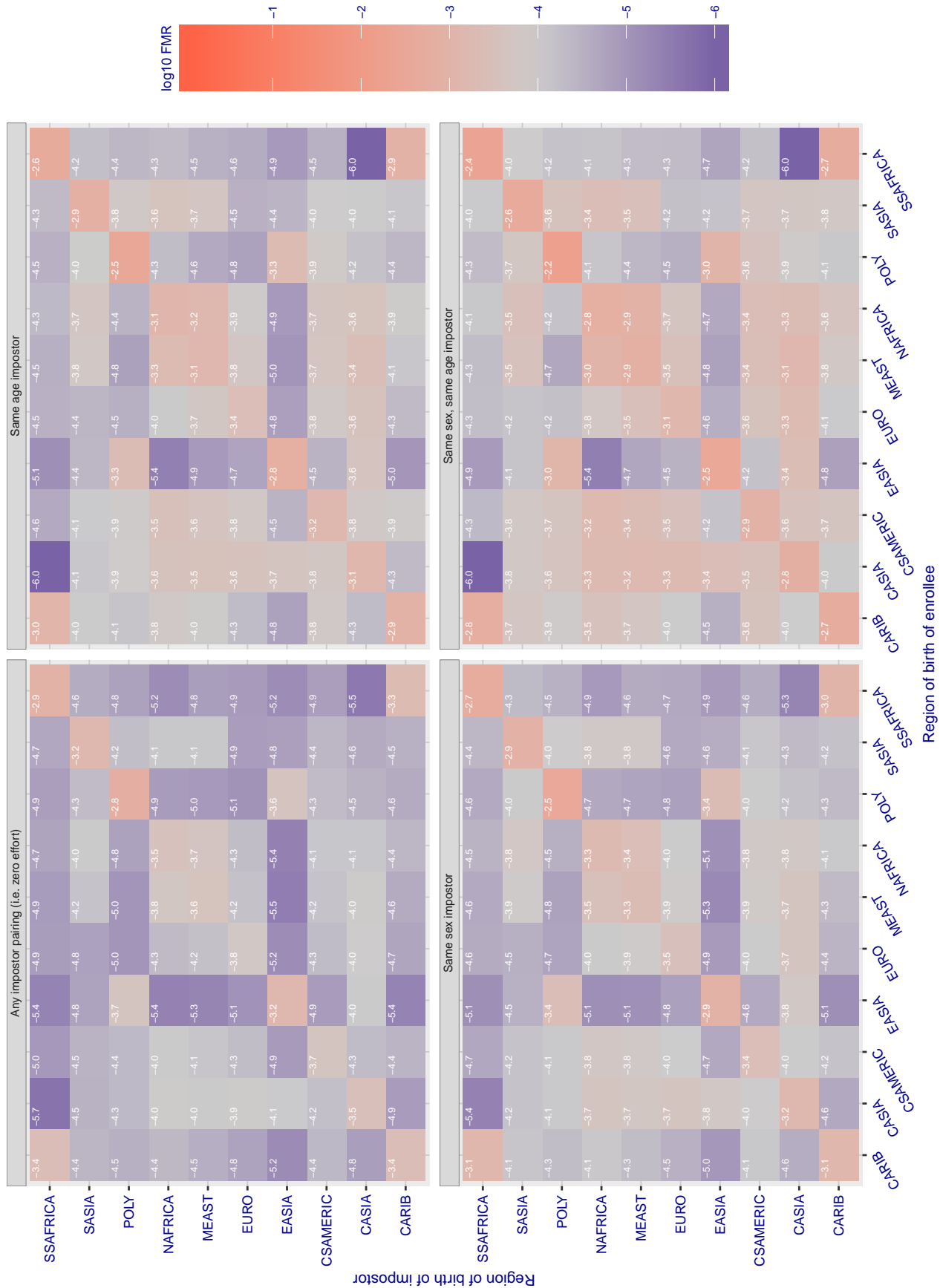


Figure 268: For algorithm realnetworks-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 70.373$  for algorithm remarkai\_000, giving  $FMR(T) = 0.0001$  globally.

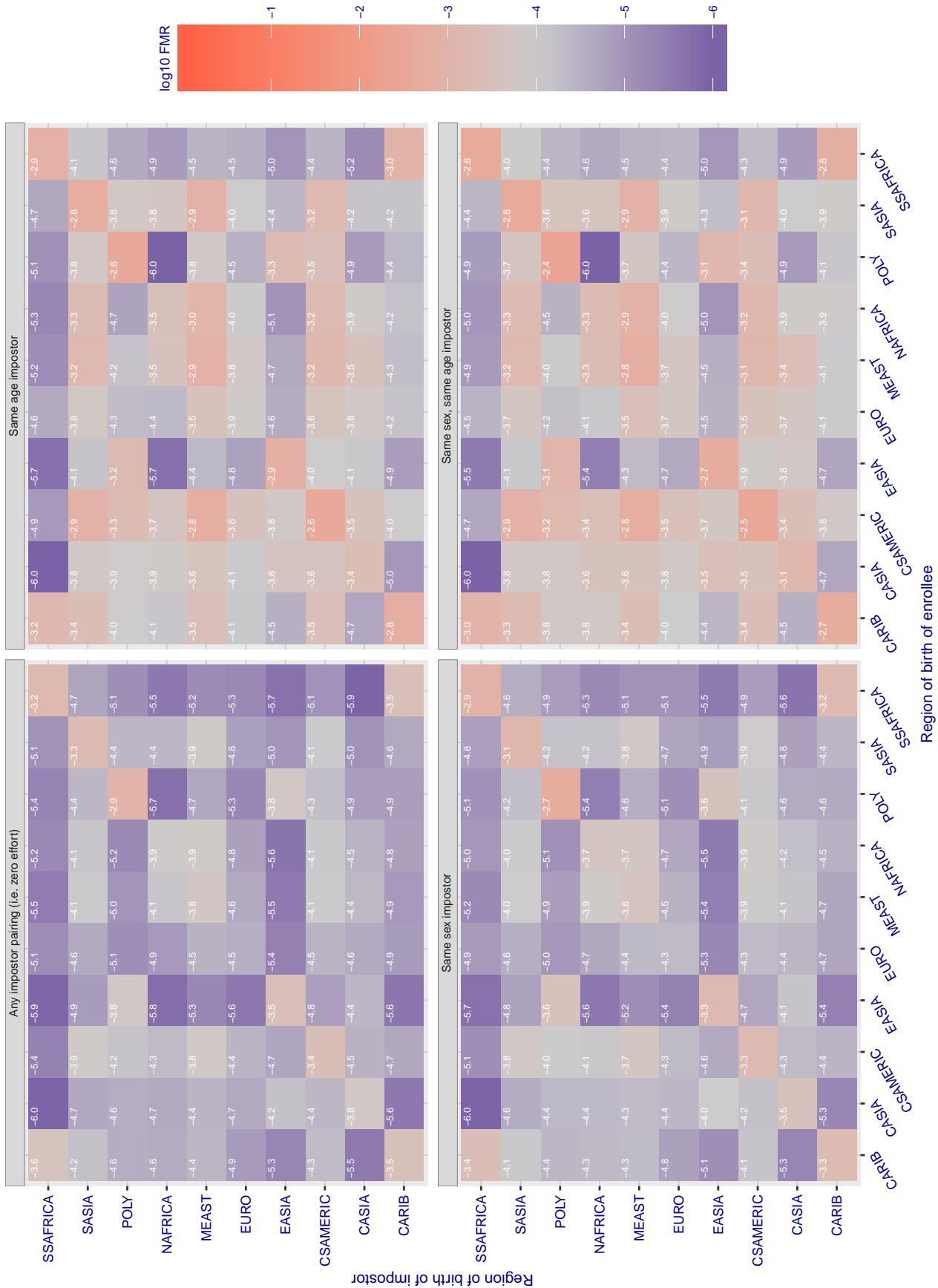


Figure 269: For algorithm remarkai-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 70.384 for algorithm remarkai\_001, giving FMR(T) = 0.0001 globally.

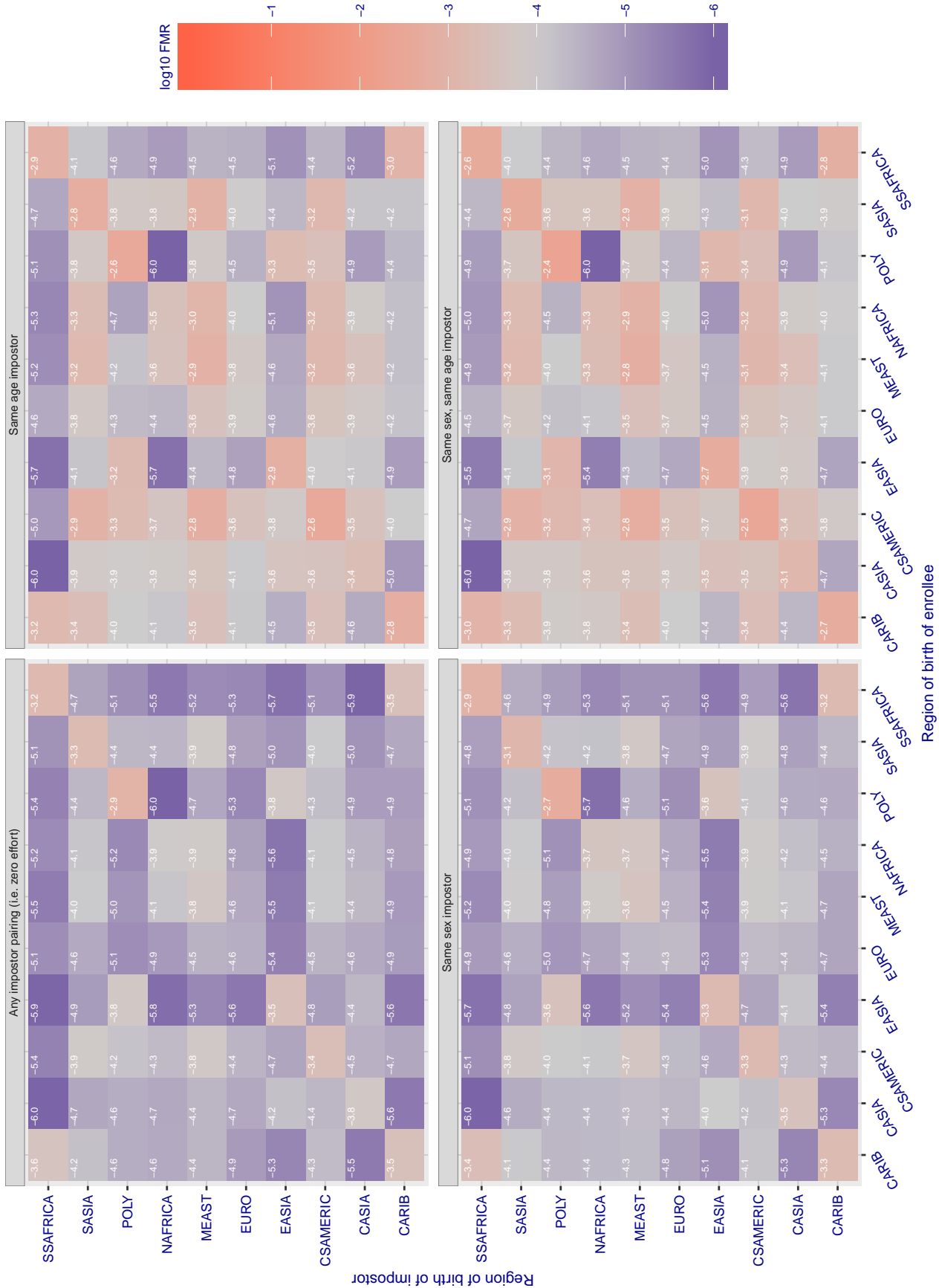


Figure 270: For algorithm remarkai-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



**Cross region FMR at threshold  $T = 0.663$  for algorithm rokid\_000, giving  $FMR(T) = 0.0001$  globally.**

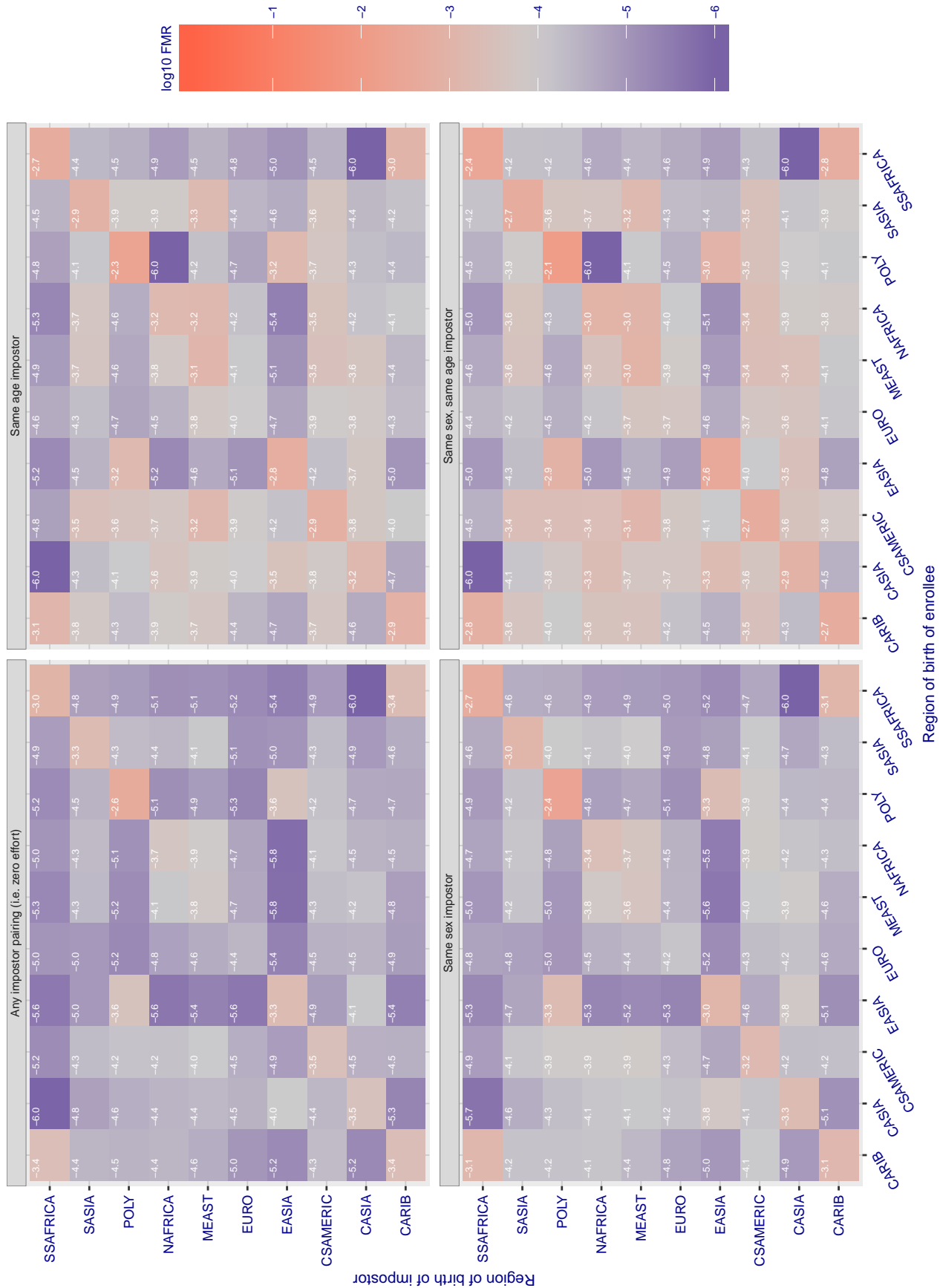


Figure 271: For algorithm rokid-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.682$  for algorithm safe\_001, giving  $FMR(T) = 0.0001$  globally.

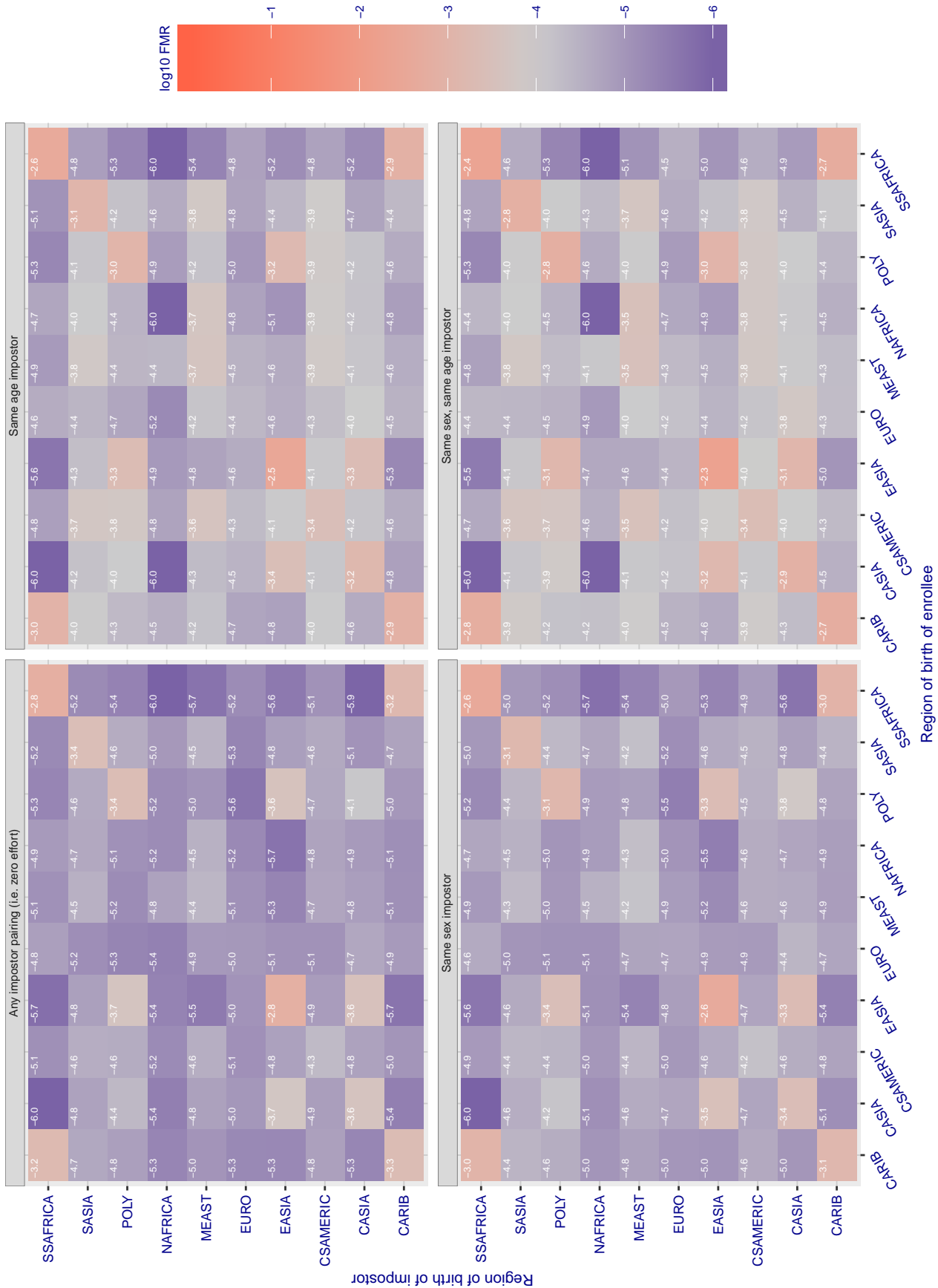


Figure 272: For algorithm safe-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 0.383$  for algorithm safe\_002, giving  $FMR(T) = 0.0001$  globally.

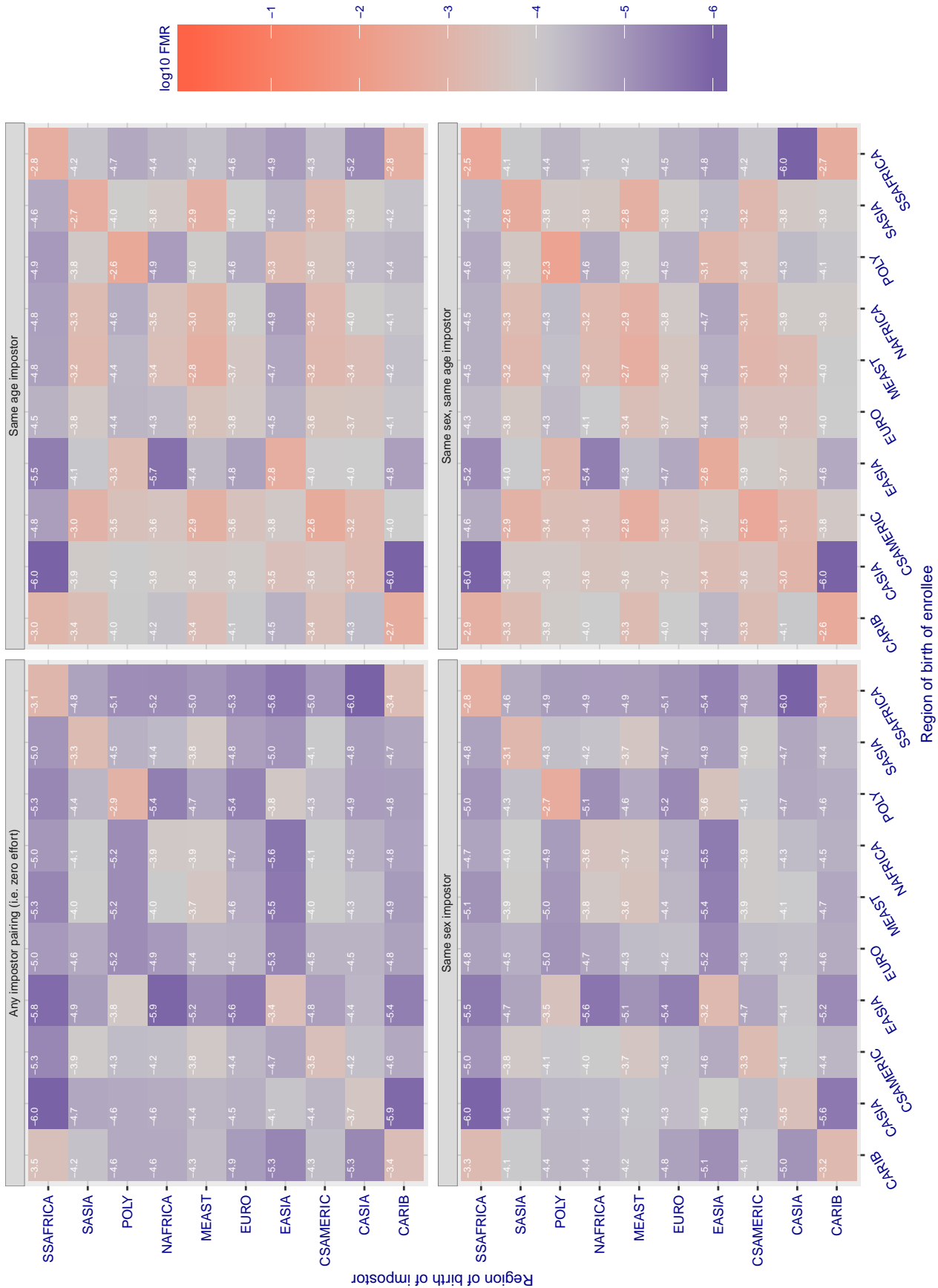


Figure 273: For algorithm safe-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 56.107$  for algorithm samtech\_001, giving  $FMR(T) = 0.0001$  globally.

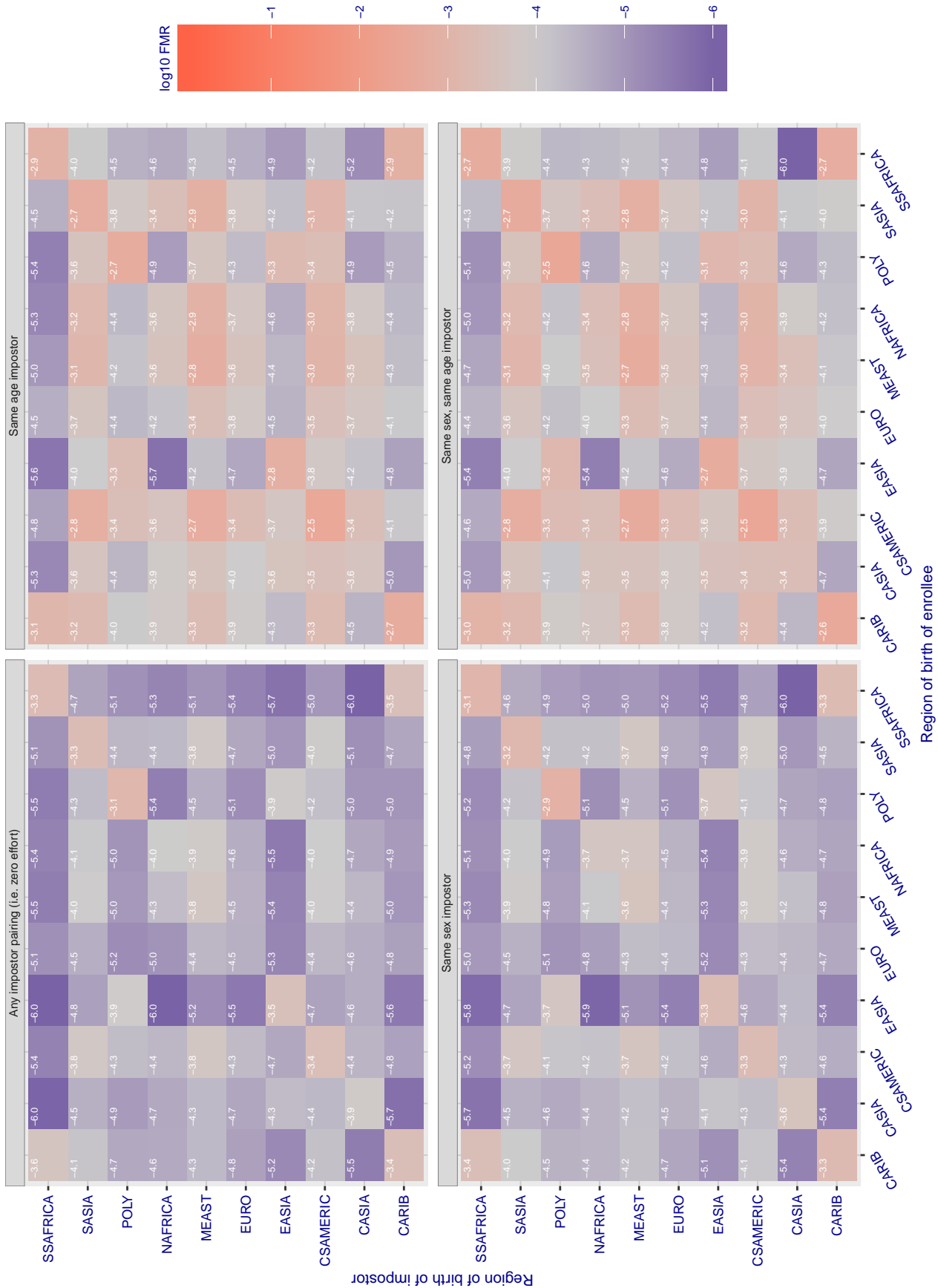


Figure 274: For algorithm samtech-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 0.683 for algorithm scanovate\_001, giving FMR(T) = 0.0001 globally.

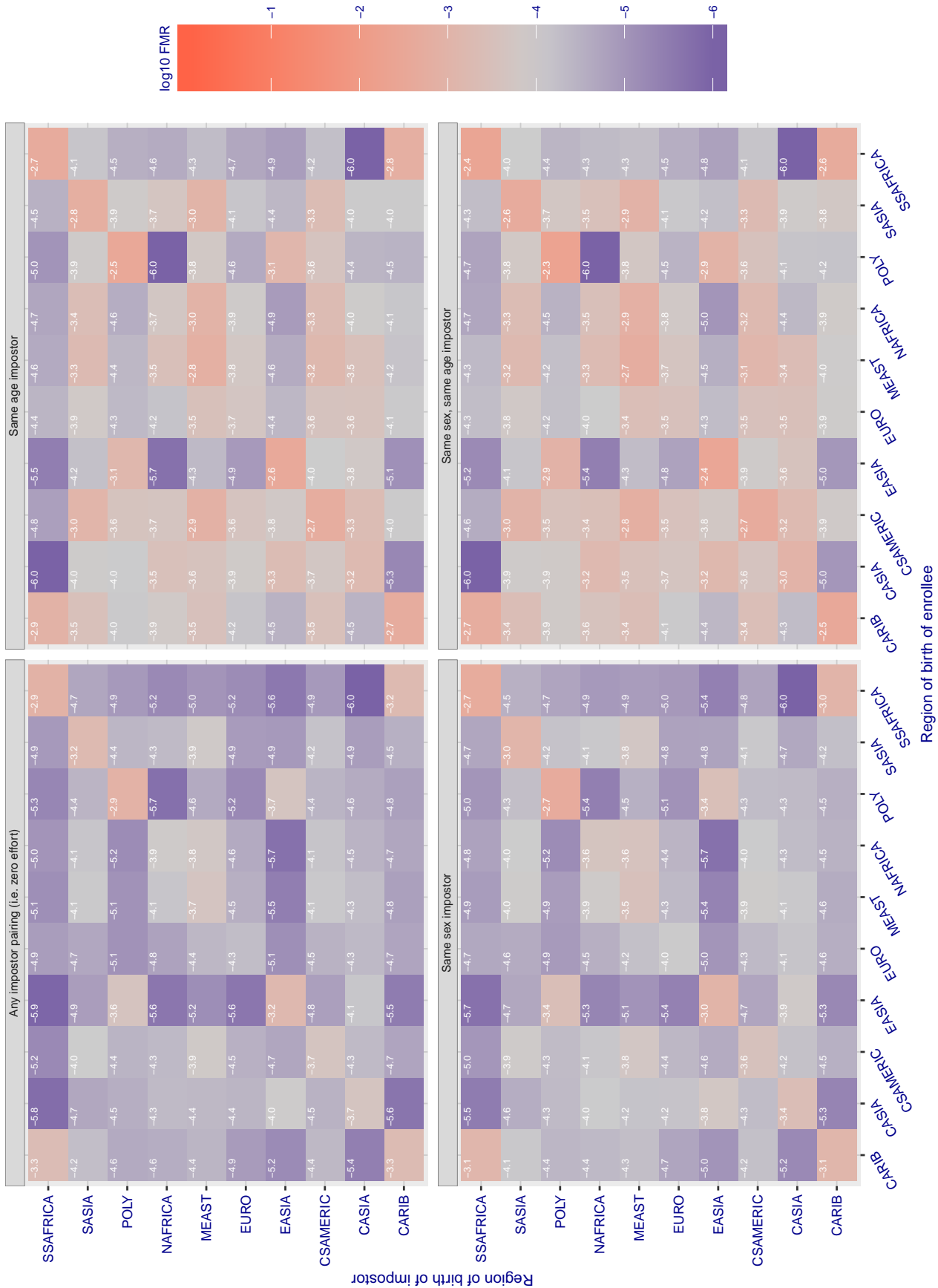


Figure 275: For algorithm scanovate-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of 10<sup>10</sup> impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.390$  for algorithm `sensetime_001`, giving  $FMR(T) = 0.0001$  globally.

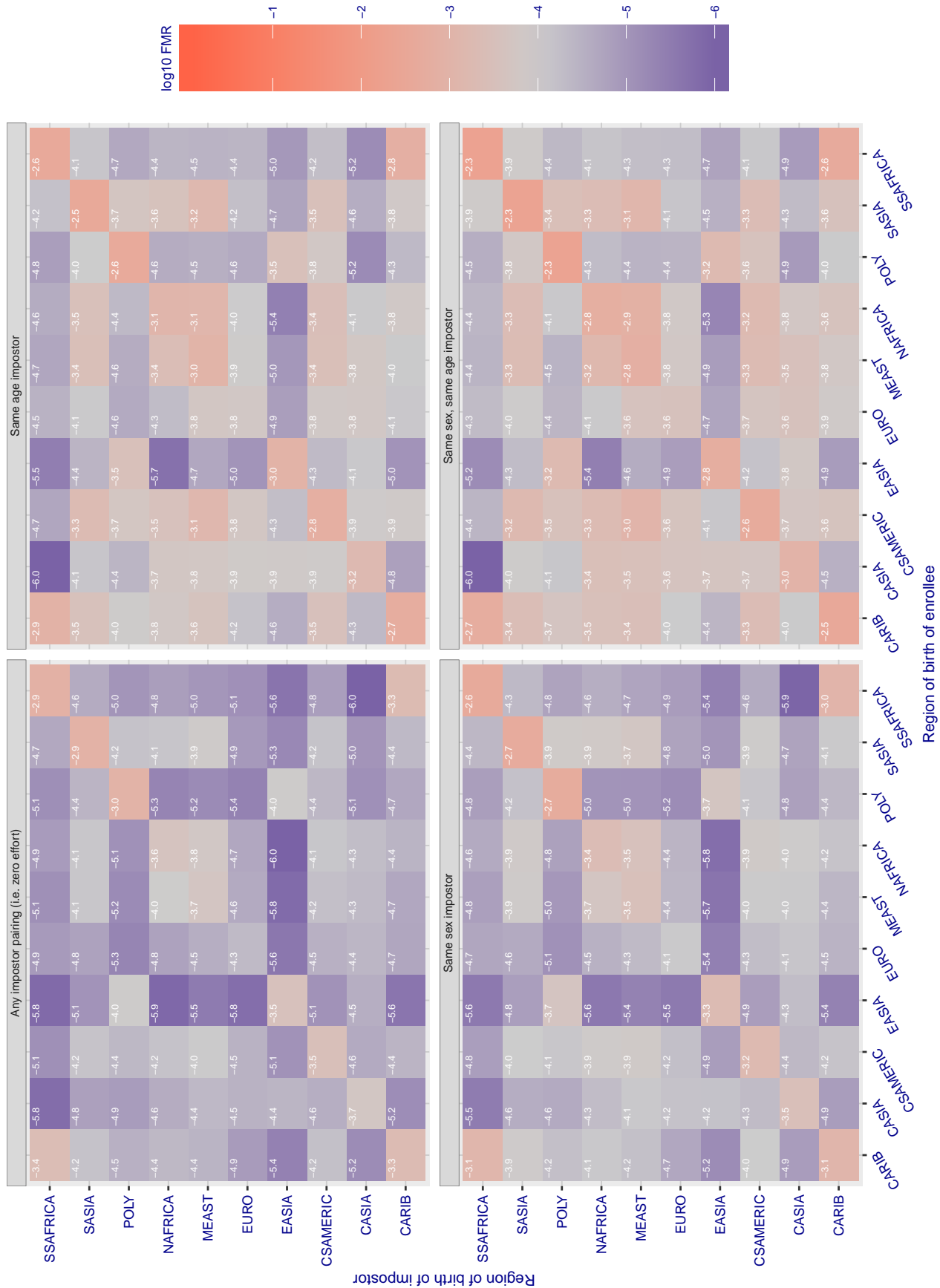


Figure 276: For algorithm `sensetime-001` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

**Cross region FMR at threshold T = 0.390 for algorithm sensetime\_002, giving FMR(T) = 0.0001 globally.**

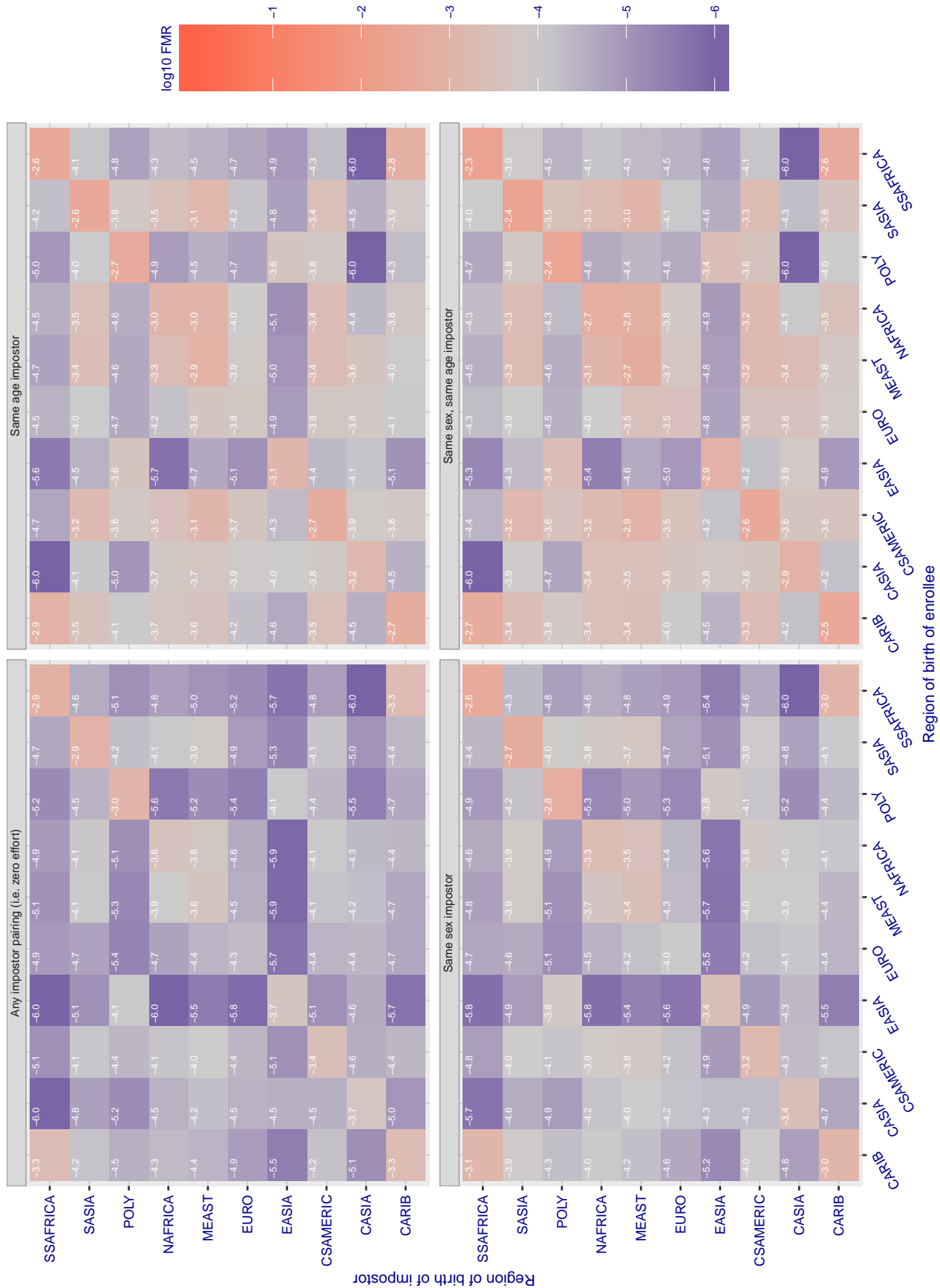


Figure 277: For algorithm sensetime-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of 10<sup>10</sup> impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.713$  for algorithm  $\text{sertis}_{000}$ , giving  $\text{FMR}(T) = 0.0001$  globally.

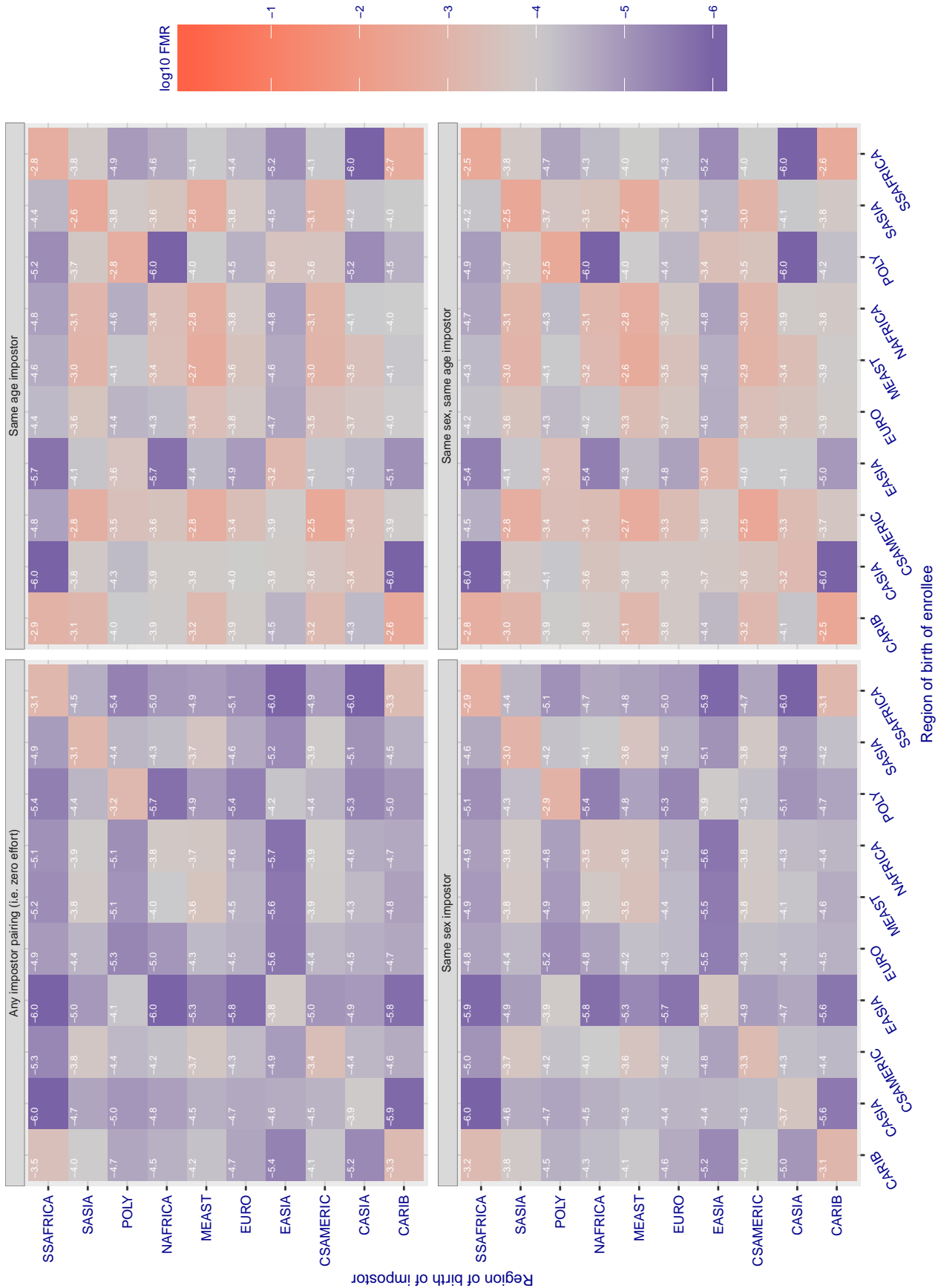


Figure 278: For algorithm  $\text{sertis}_{000}$  operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



**Cross region FMR at threshold  $T = 0.970$  for algorithm shaman\_000, giving  $FMR(T) = 0.0001$  globally.**

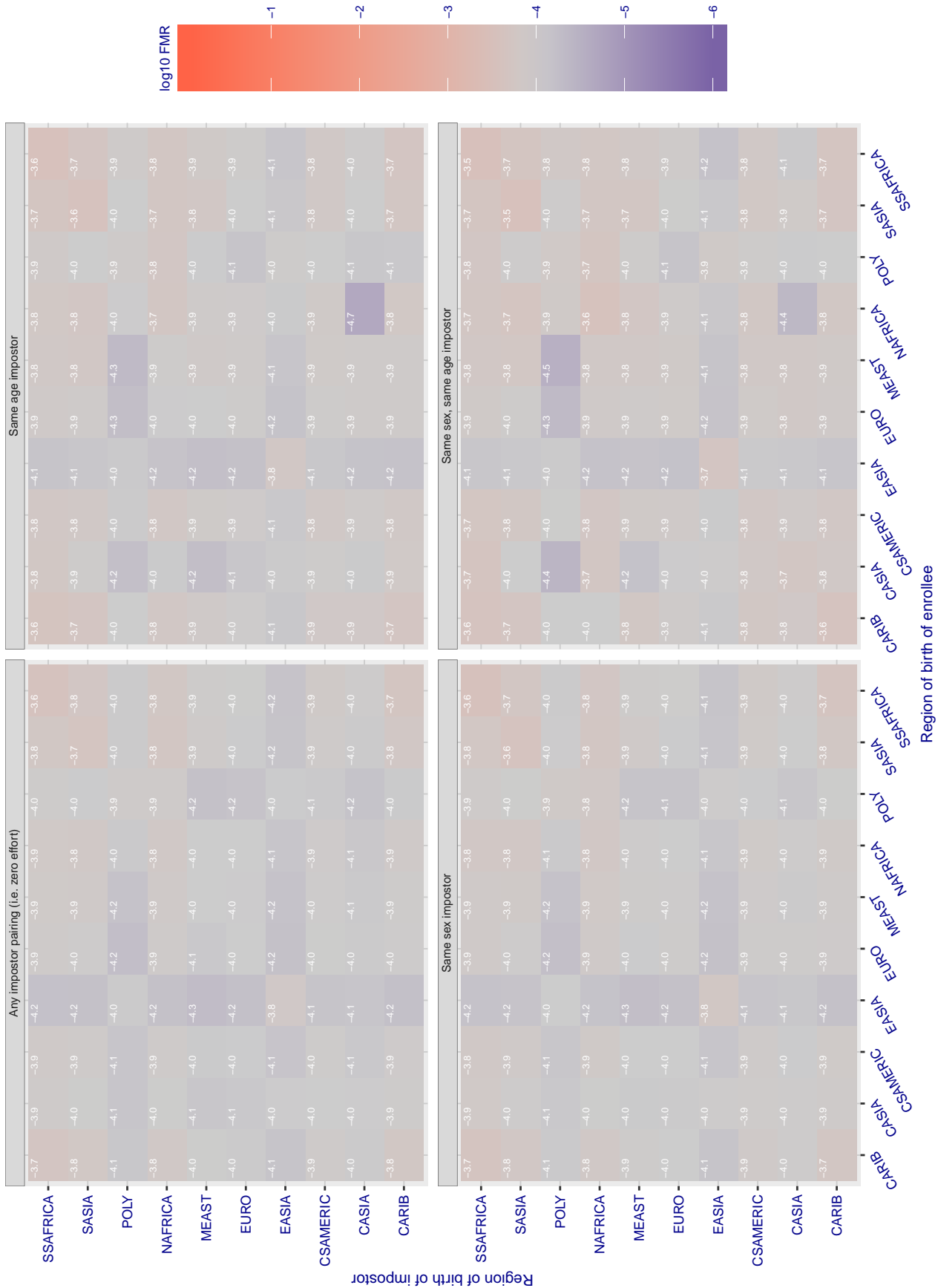


Figure 279: For algorithm shaman-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.725$  for algorithm shaman\_001, giving  $FMR(T) = 0.0001$  globally.

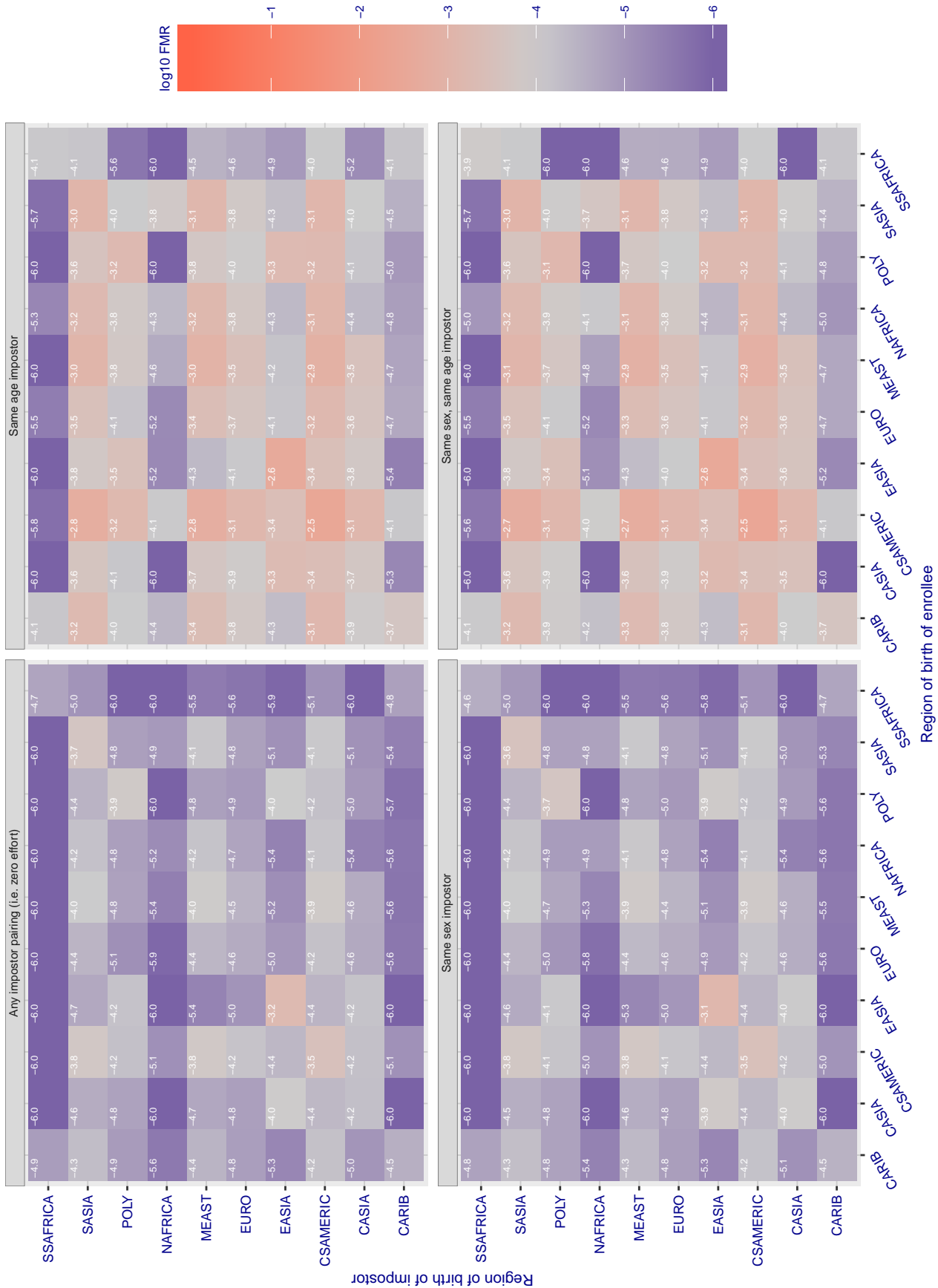


Figure 280: For algorithm shaman-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 0.400$  for algorithm shu\_001, giving  $FMR(T) = 0.0001$  globally.

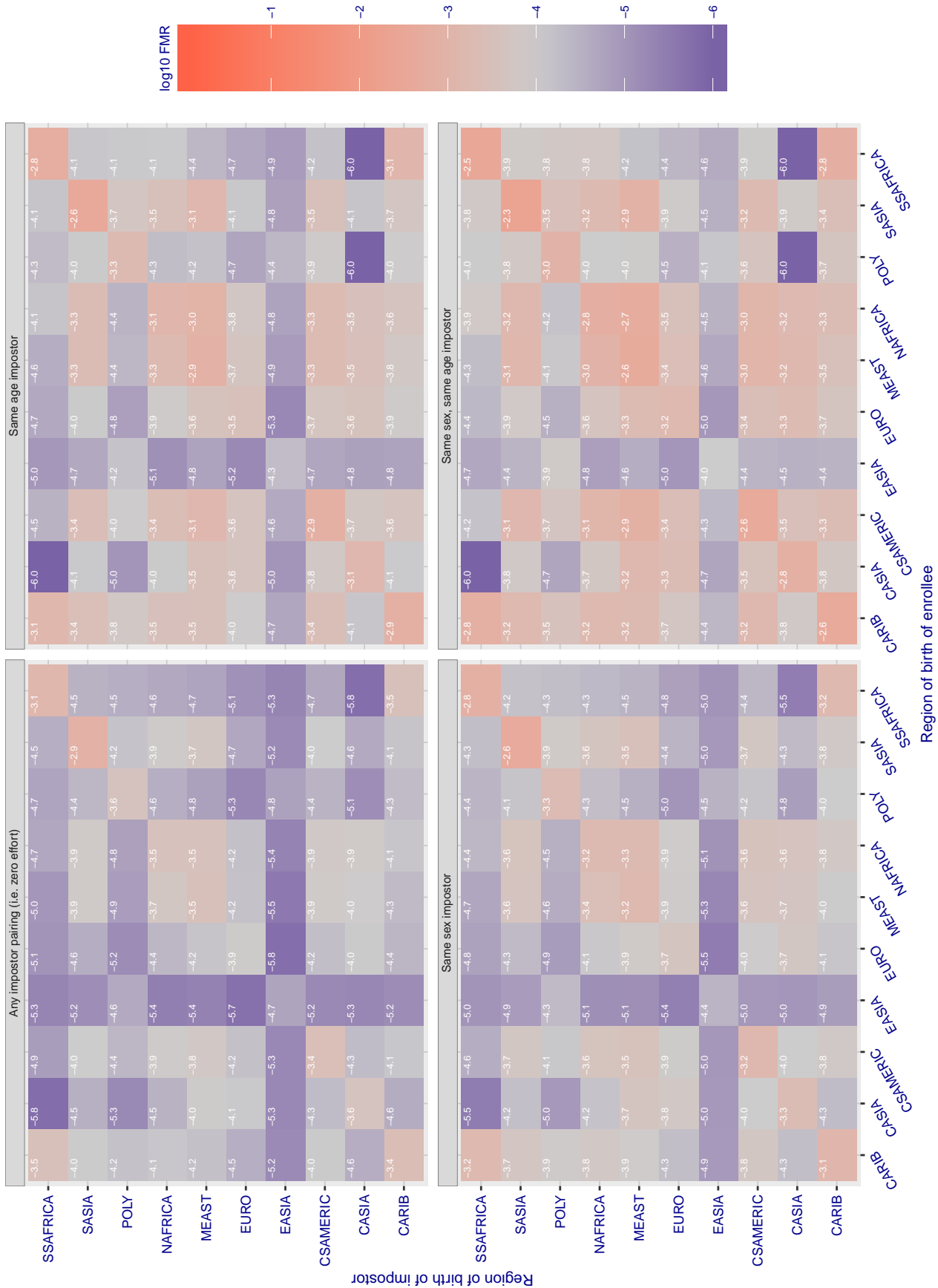


Figure 281: For algorithm shu-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.390$  for algorithm `siat_002`, giving  $FMR(T) = 0.0001$  globally.

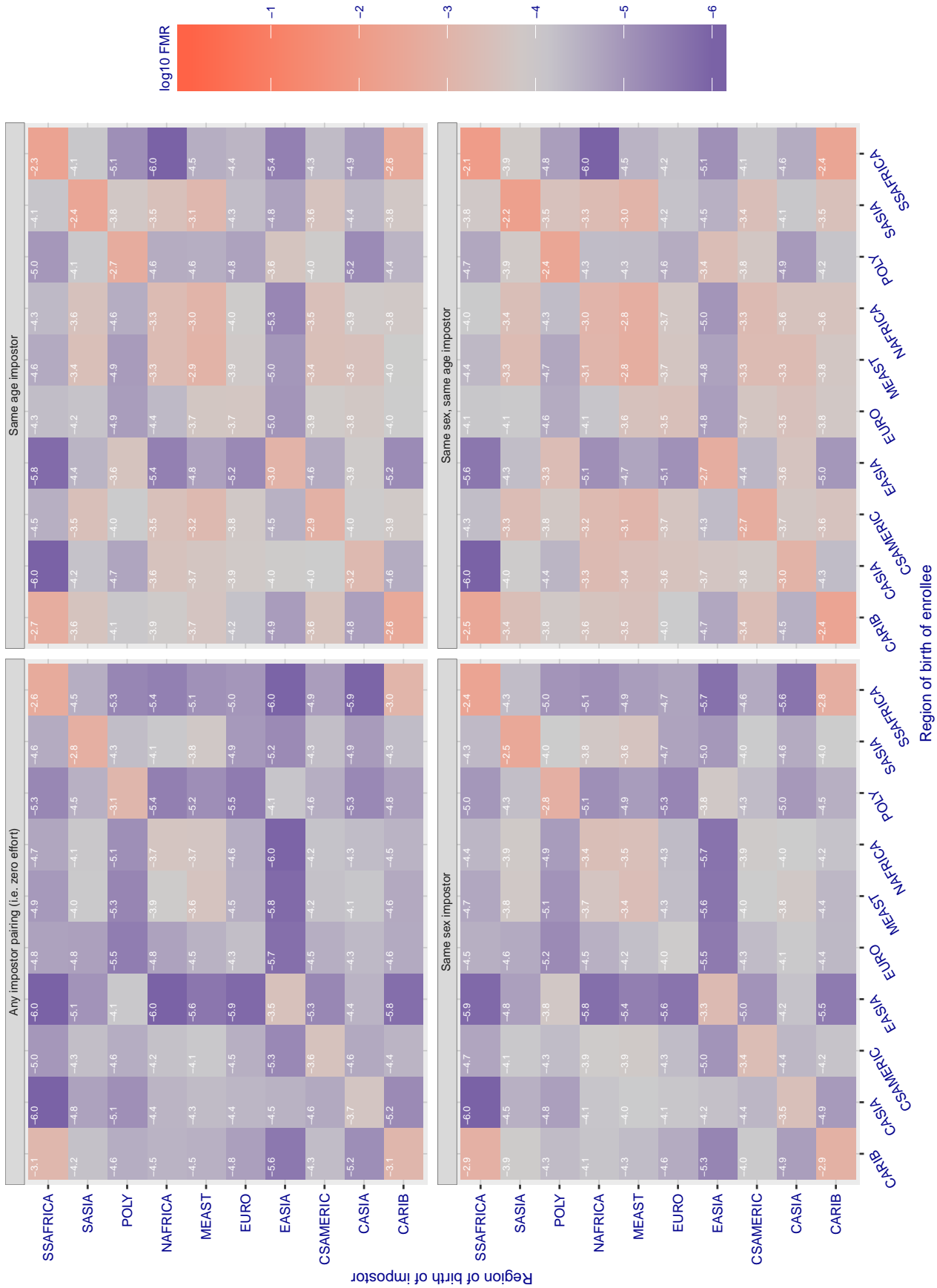


Figure 282: For algorithm `siat-002` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 0.393 for algorithm siat\_004, giving FMR(T) = 0.0001 globally.

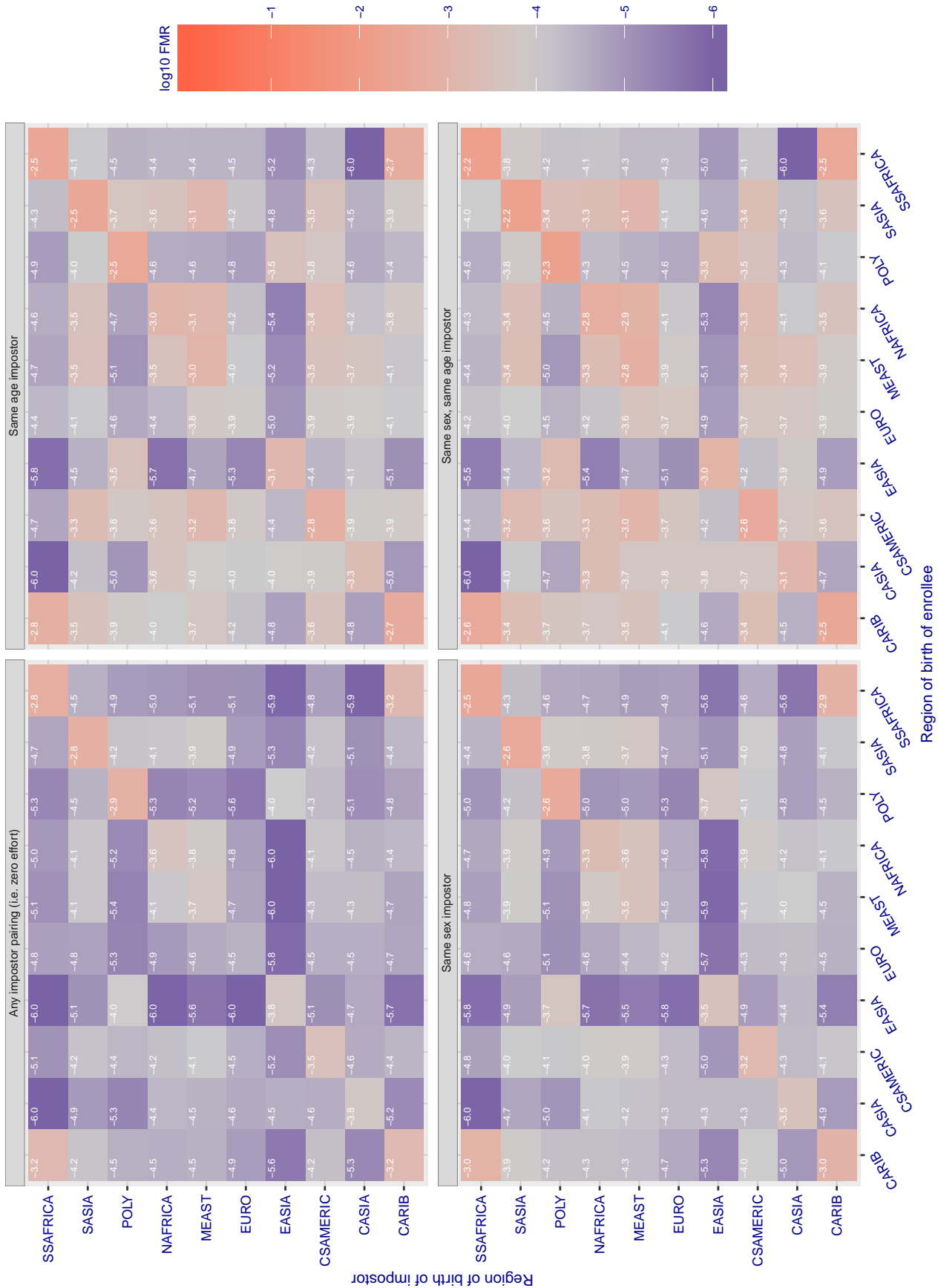


Figure 283: For algorithm siat-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 1.206$  for algorithm sjtu\_001, giving  $FMR(T) = 0.0001$  globally.

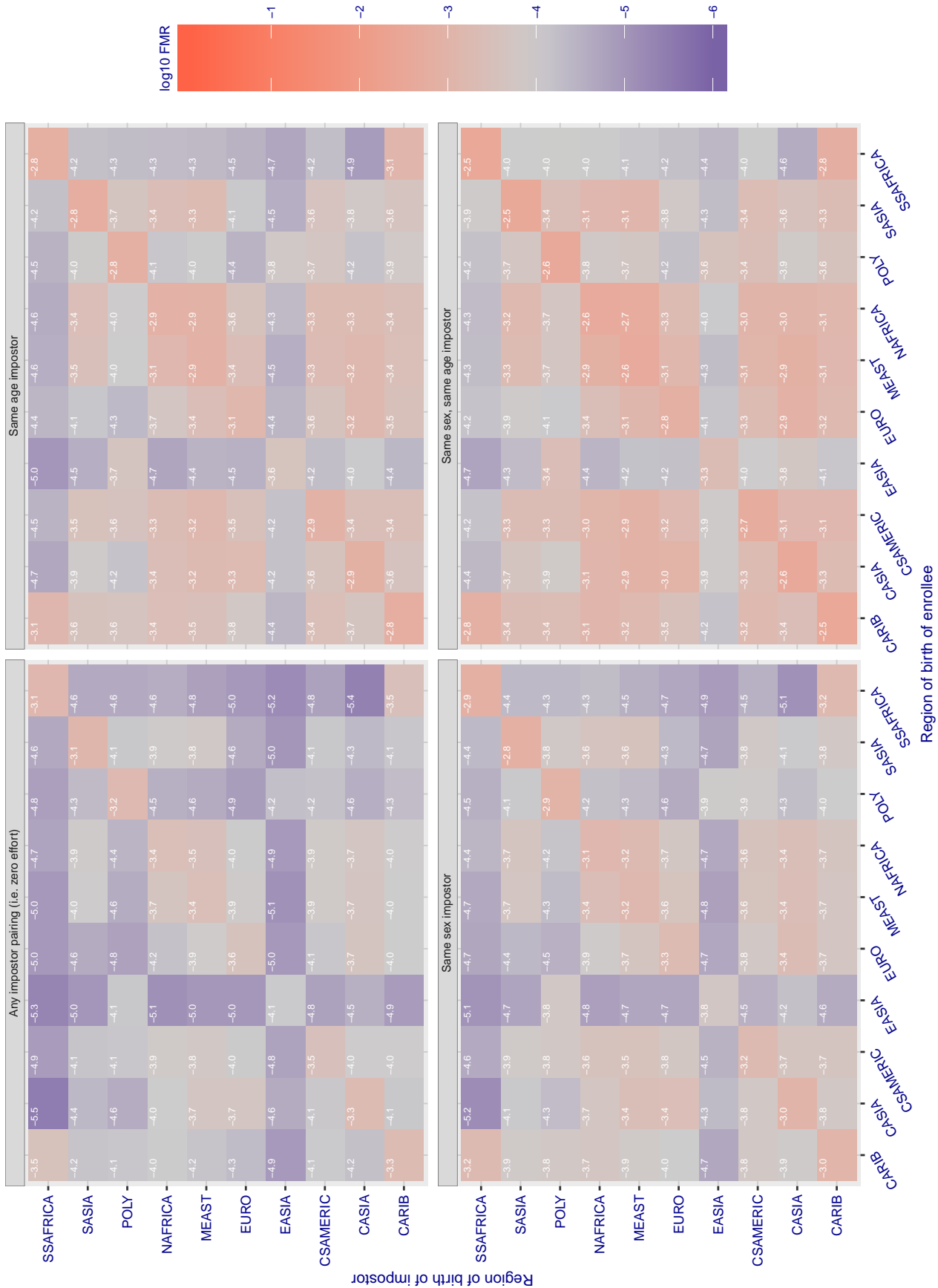


Figure 284: For algorithm sjtu-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.598$  for algorithm smilart\_002, giving  $FMR(T) = 0.0001$  globally.

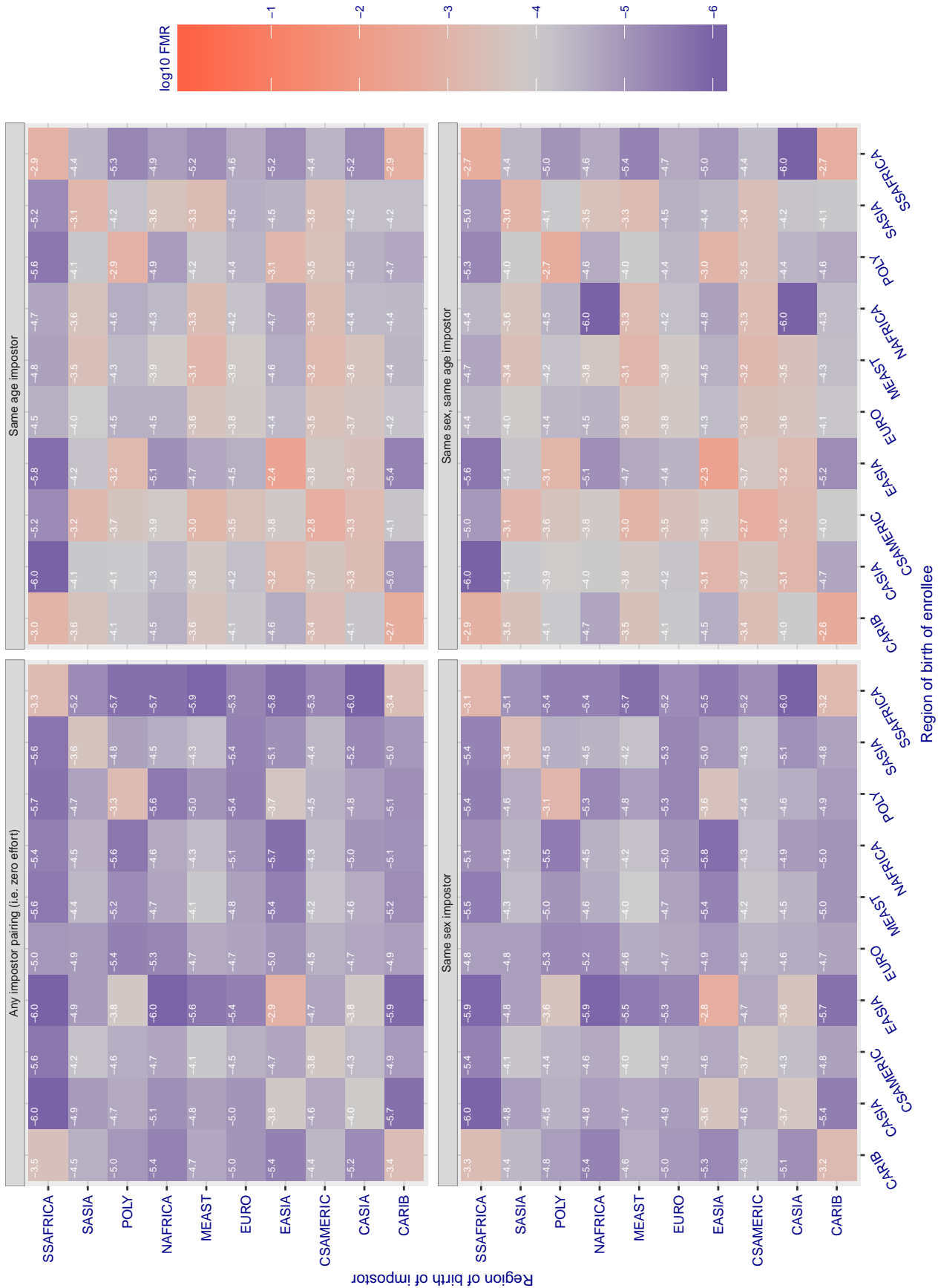


Figure 285: For algorithm smilart-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.654$  for algorithm smilart\_003, giving  $FMR(T) = 0.0001$  globally.

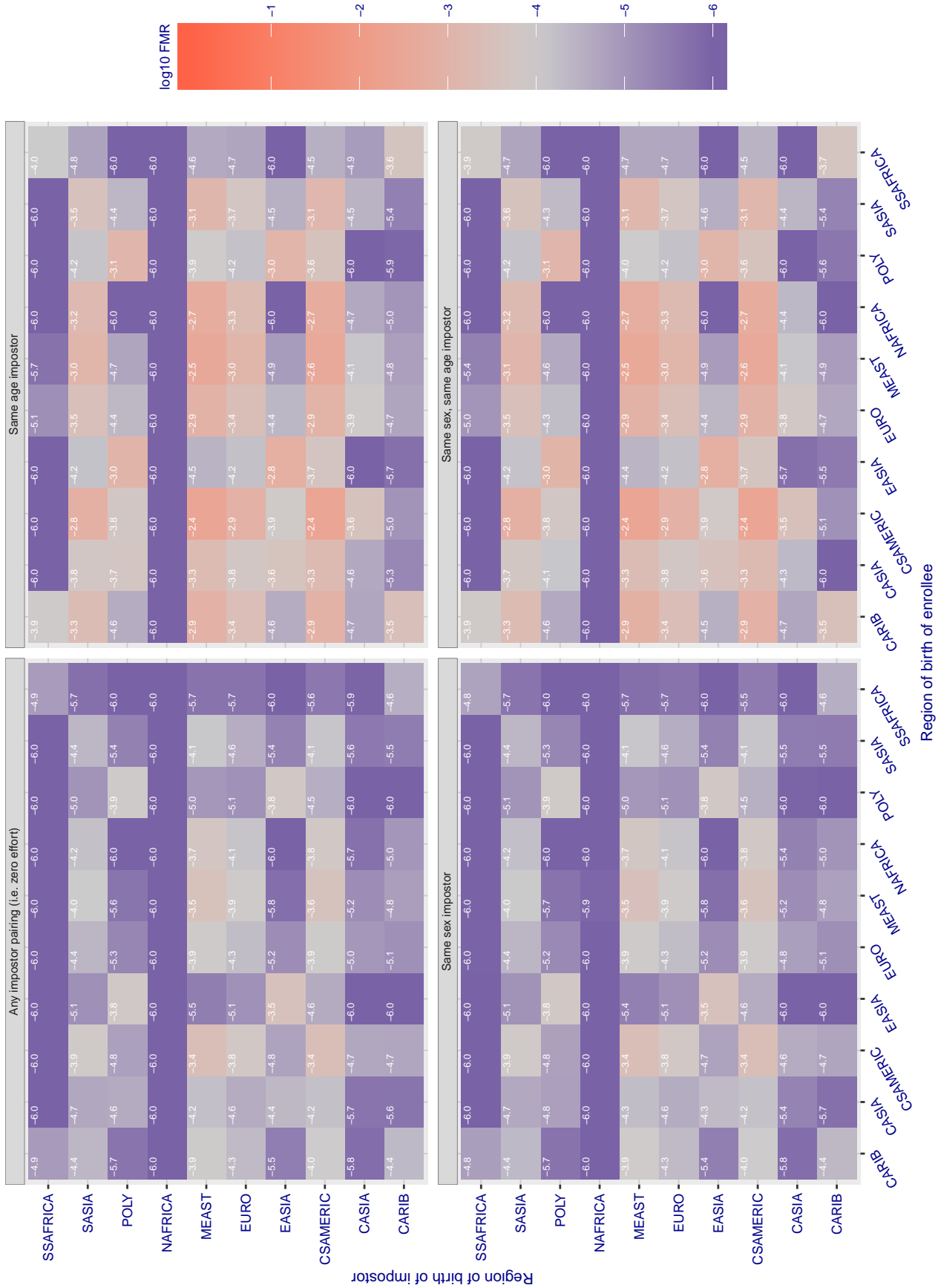


Figure 286: For algorithm smilart-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 0.314$  for algorithm starhybrid\_001, giving  $FMR(T) = 0.0001$  globally.

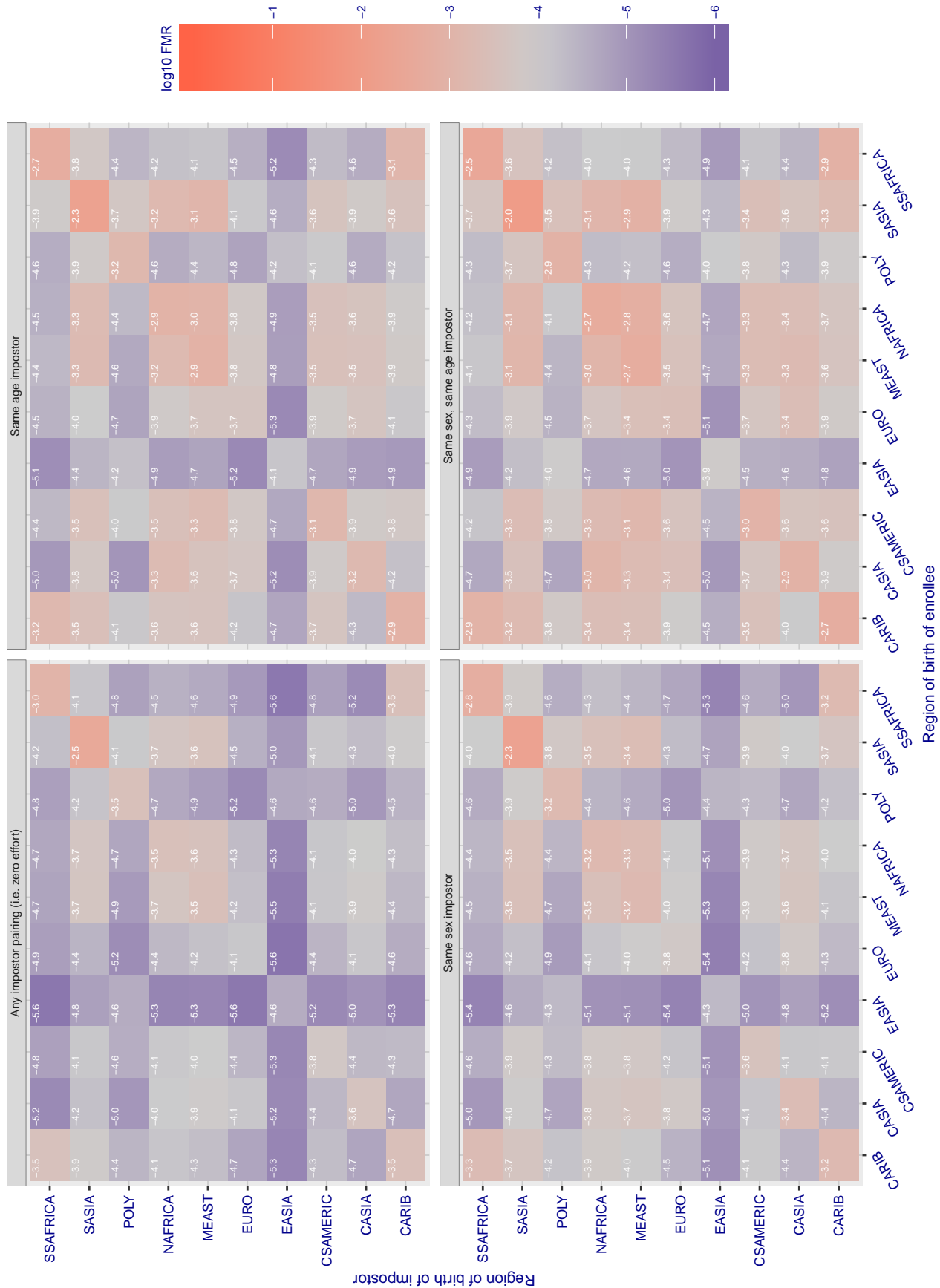


Figure 287: For algorithm starhybrid-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 0.356 for algorithm synthesis\_005, giving FMR(T) = 0.0001 globally.

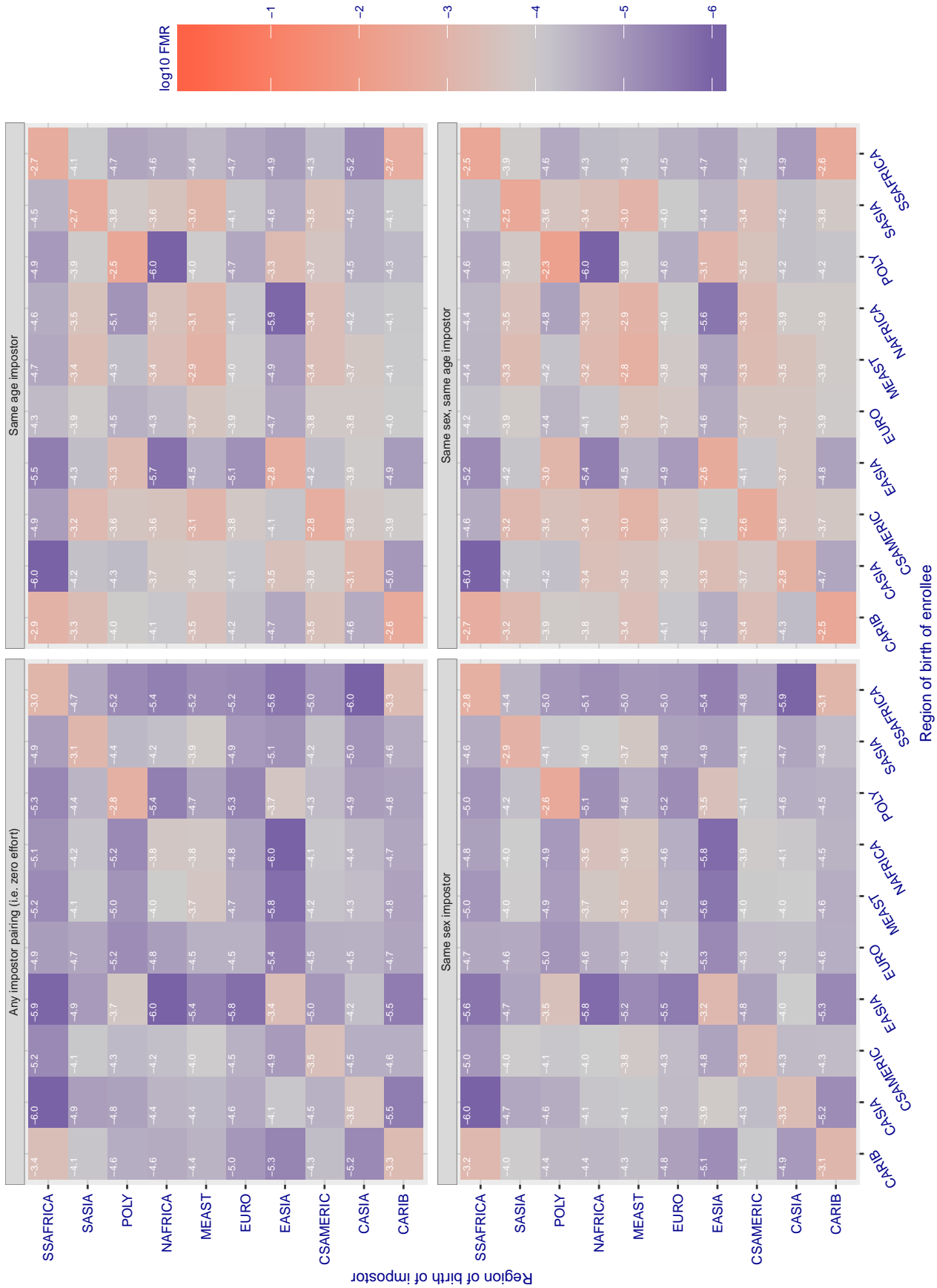


Figure 288: For algorithm synthesis-005 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold T = 0.375 for algorithm synthesis\_006, giving FMR(T) = 0.0001 globally.

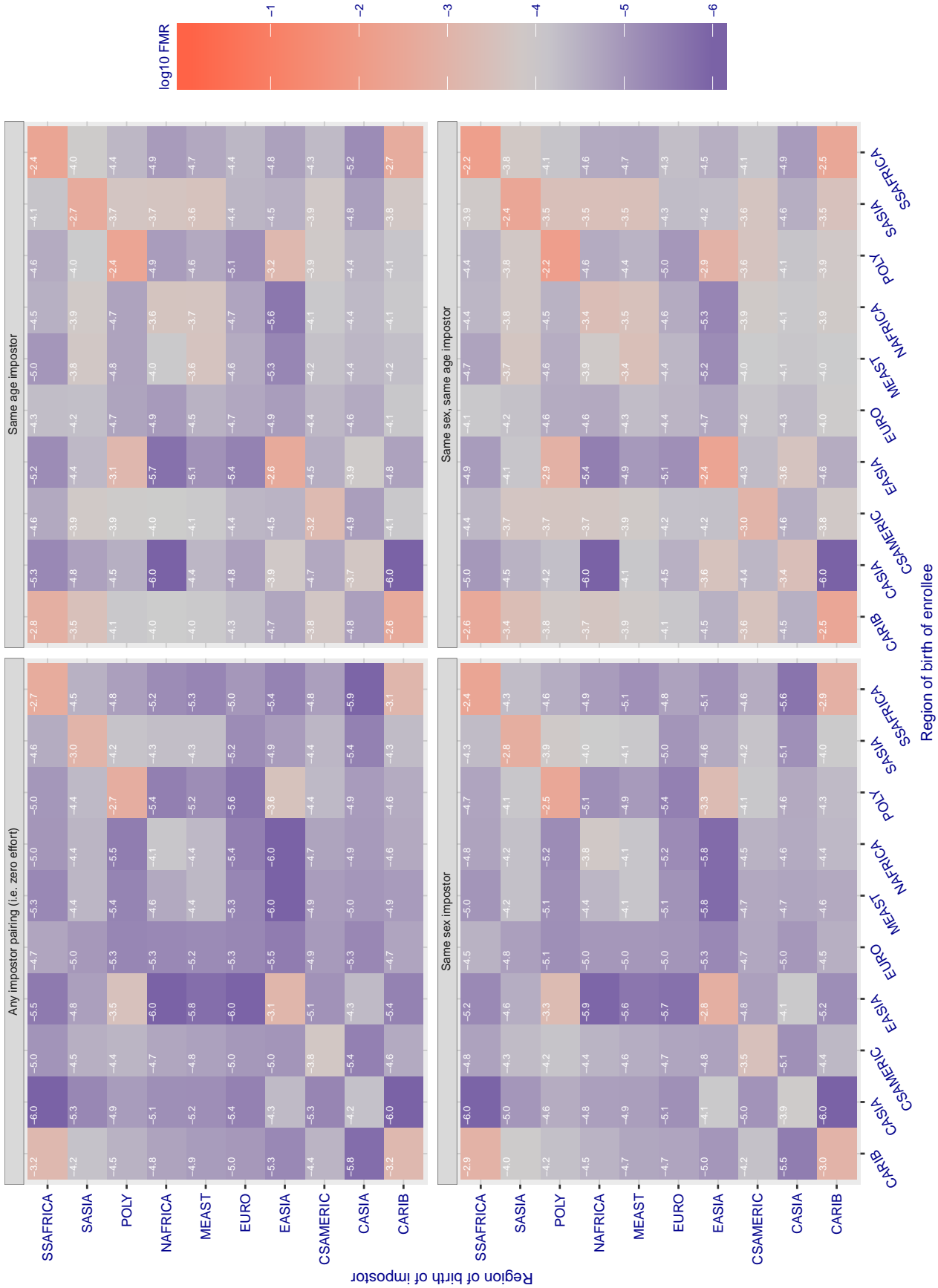


Figure 289: For algorithm synthesis-006 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of 10<sup>10</sup> impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 0.430 for algorithm synology\_000, giving FMR(T) = 0.0001 globally.

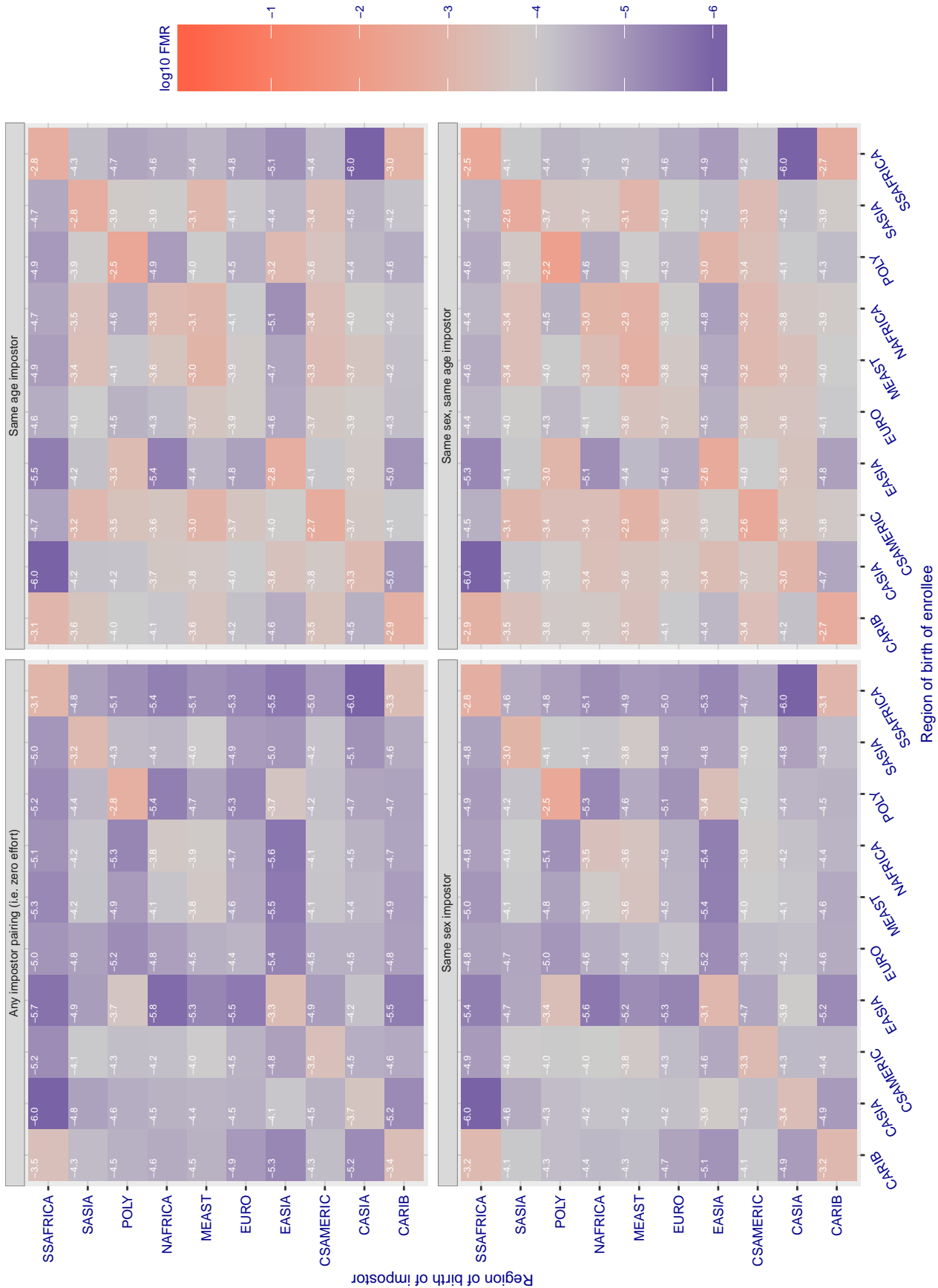


Figure 290: For algorithm synology-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of 10<sup>10</sup> impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 147.661 for algorithm tech5\_002, giving FMR(T) = 0.0001 globally.

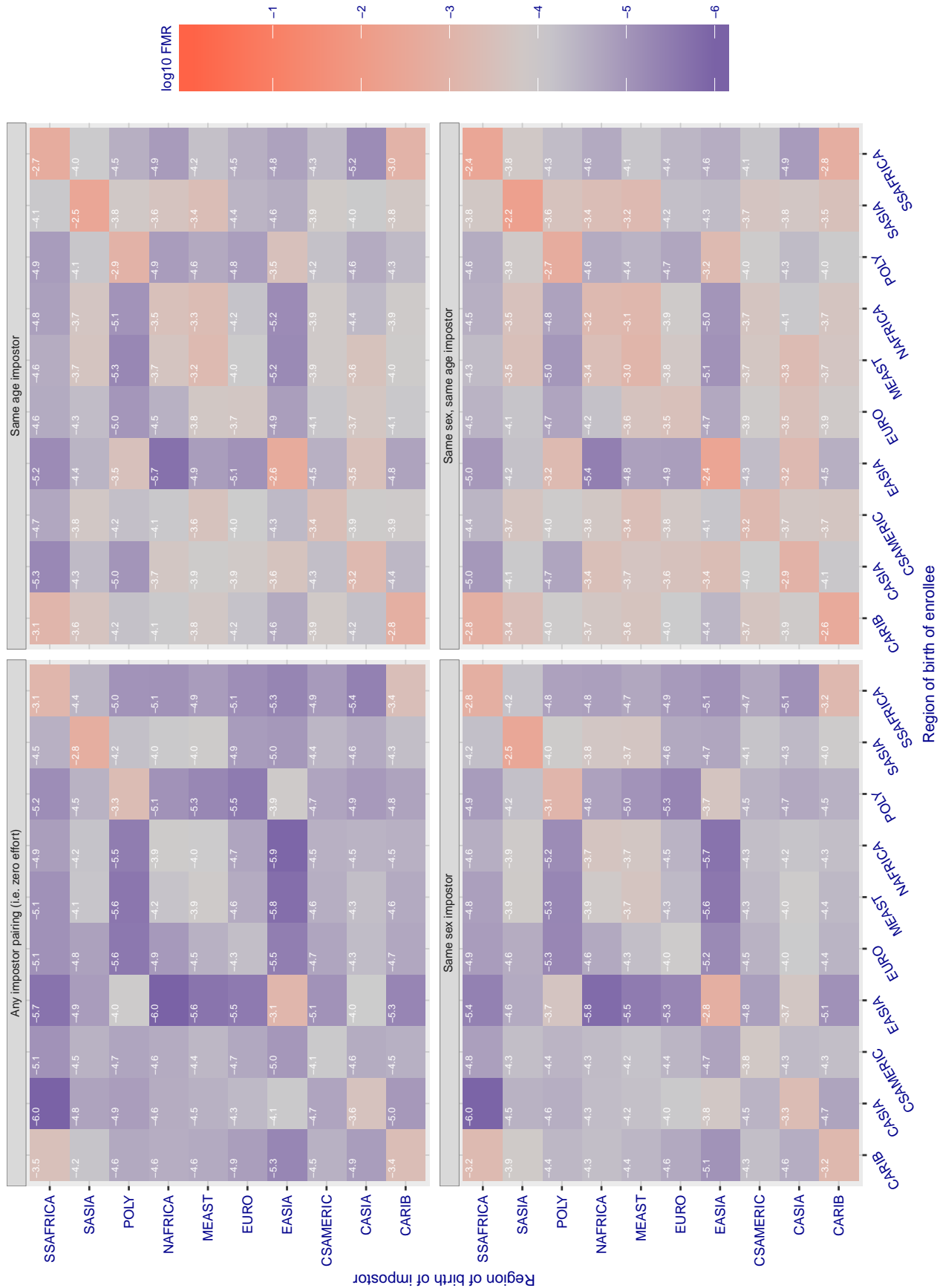


Figure 291: For algorithm tech5-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of 10<sup>10</sup> impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 147.080 for algorithm tech5\_003, giving FMR(T) = 0.0001 globally.

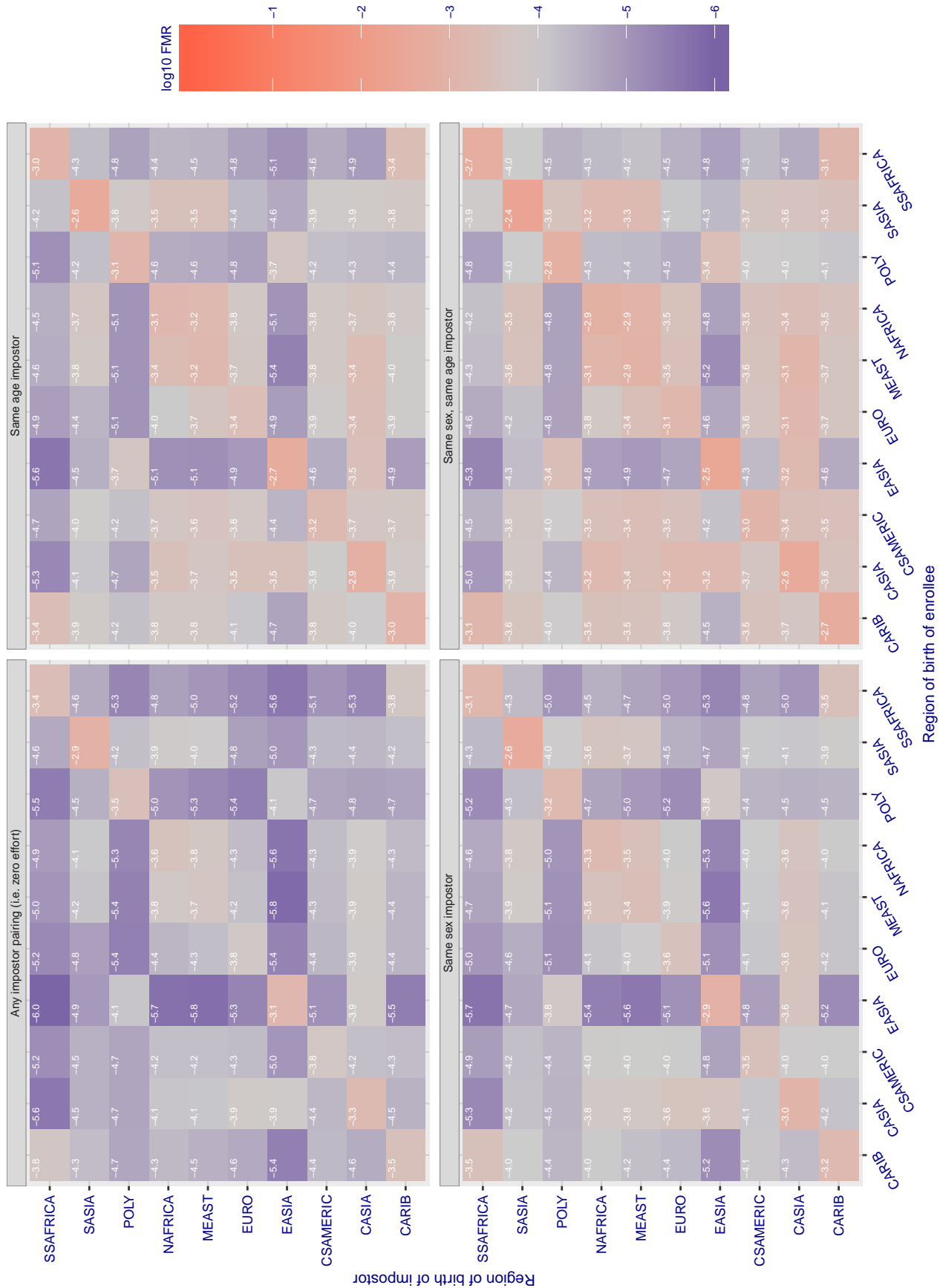


Figure 292: For algorithm tech5-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.896$  for algorithm tevia\_004, giving  $FMR(T) = 0.0001$  globally.

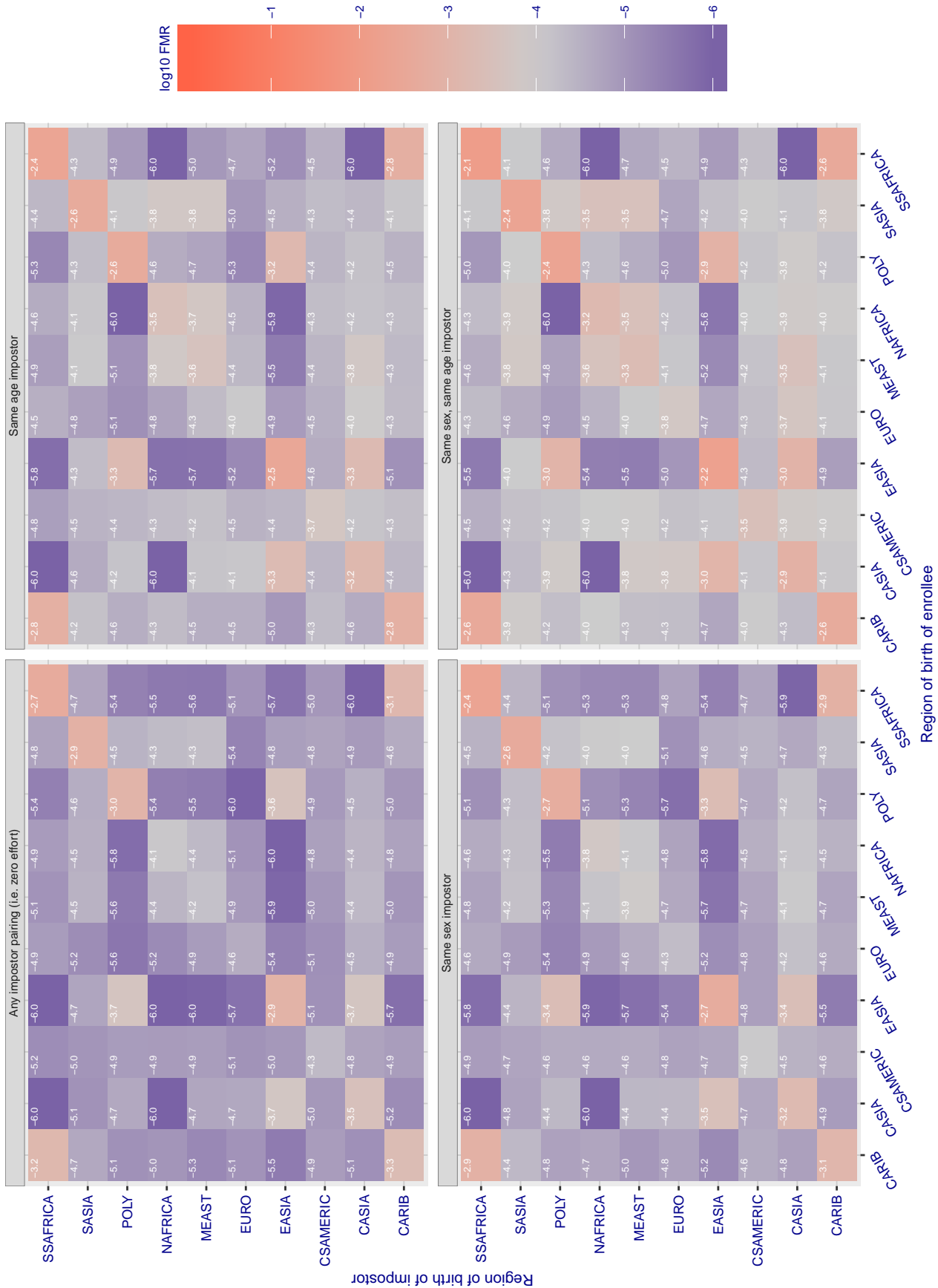


Figure 293: For algorithm tevia-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.854$  for algorithm tevia-005, giving  $FMR(T) = 0.0001$  globally.

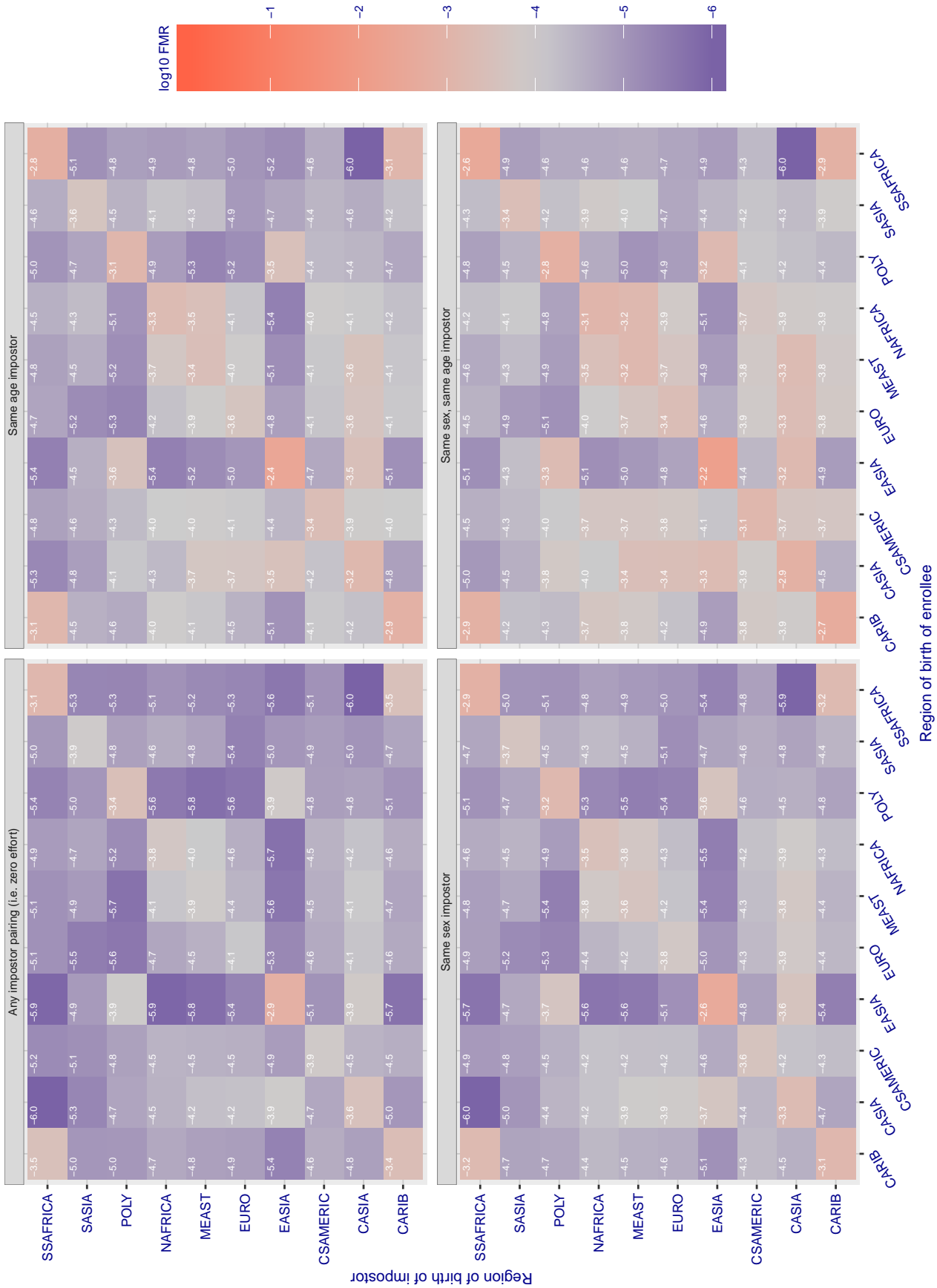


Figure 294: For algorithm tevia-005 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 151.011$  for algorithm tiger\_002, giving  $FMR(T) = 0.0001$  globally.

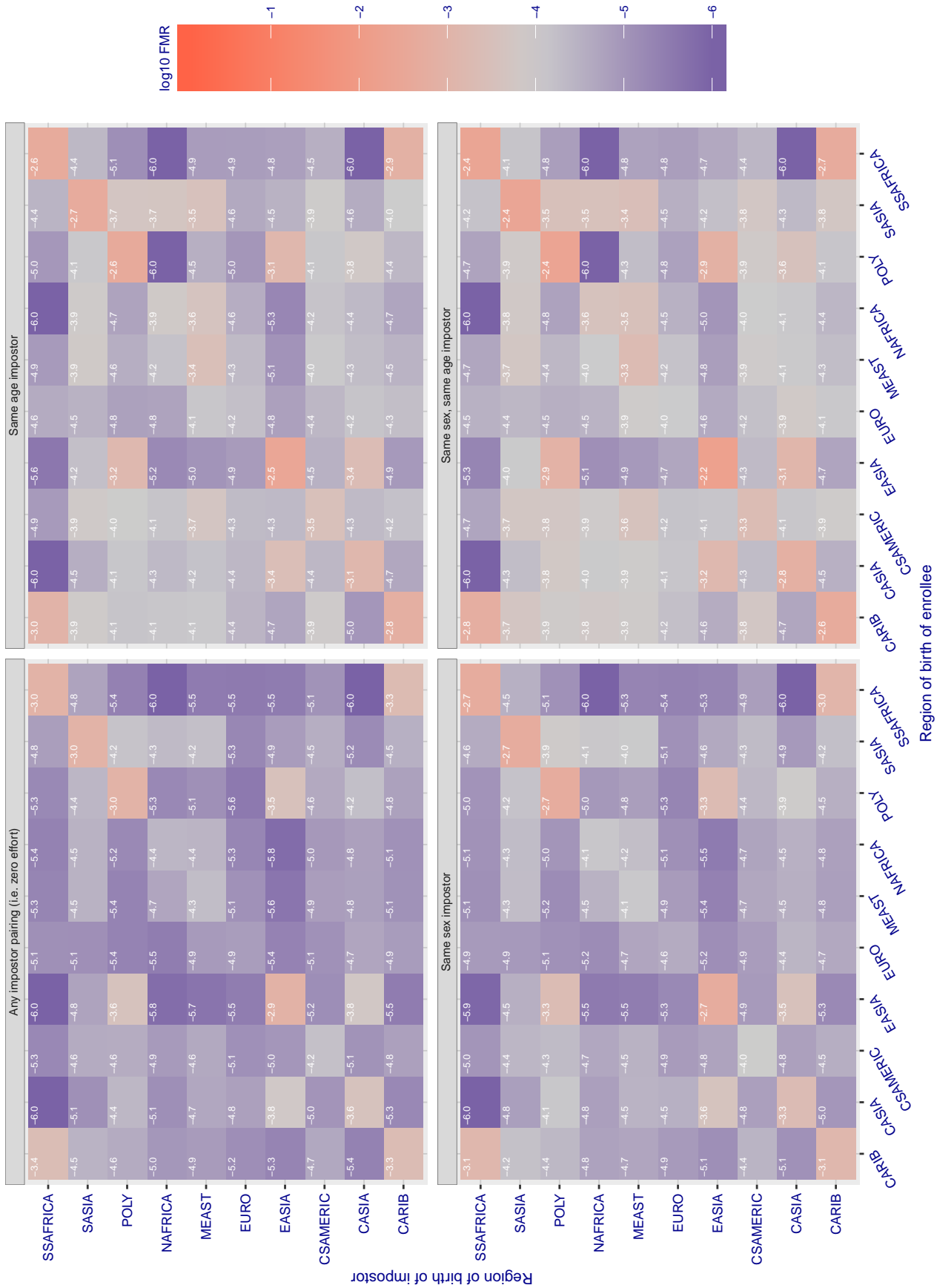


Figure 295: For algorithm tiger-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 149.313$  for algorithm tiger\_003, giving  $FMR(T) = 0.0001$  globally.

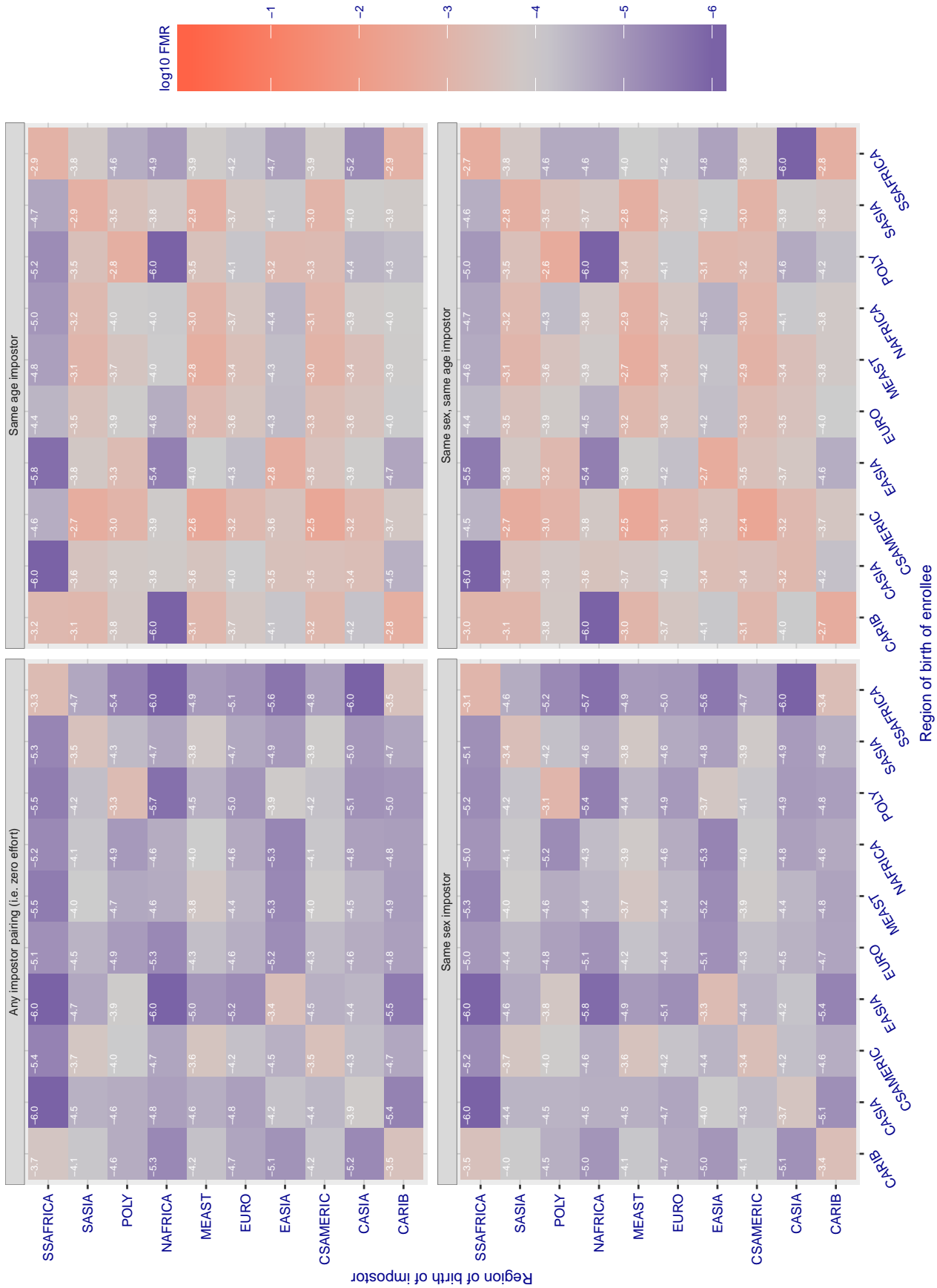


Figure 29c: For algorithm tiger-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 43.677$  for algorithm tongyi\_005, giving  $FMR(T) = 0.0001$  globally.

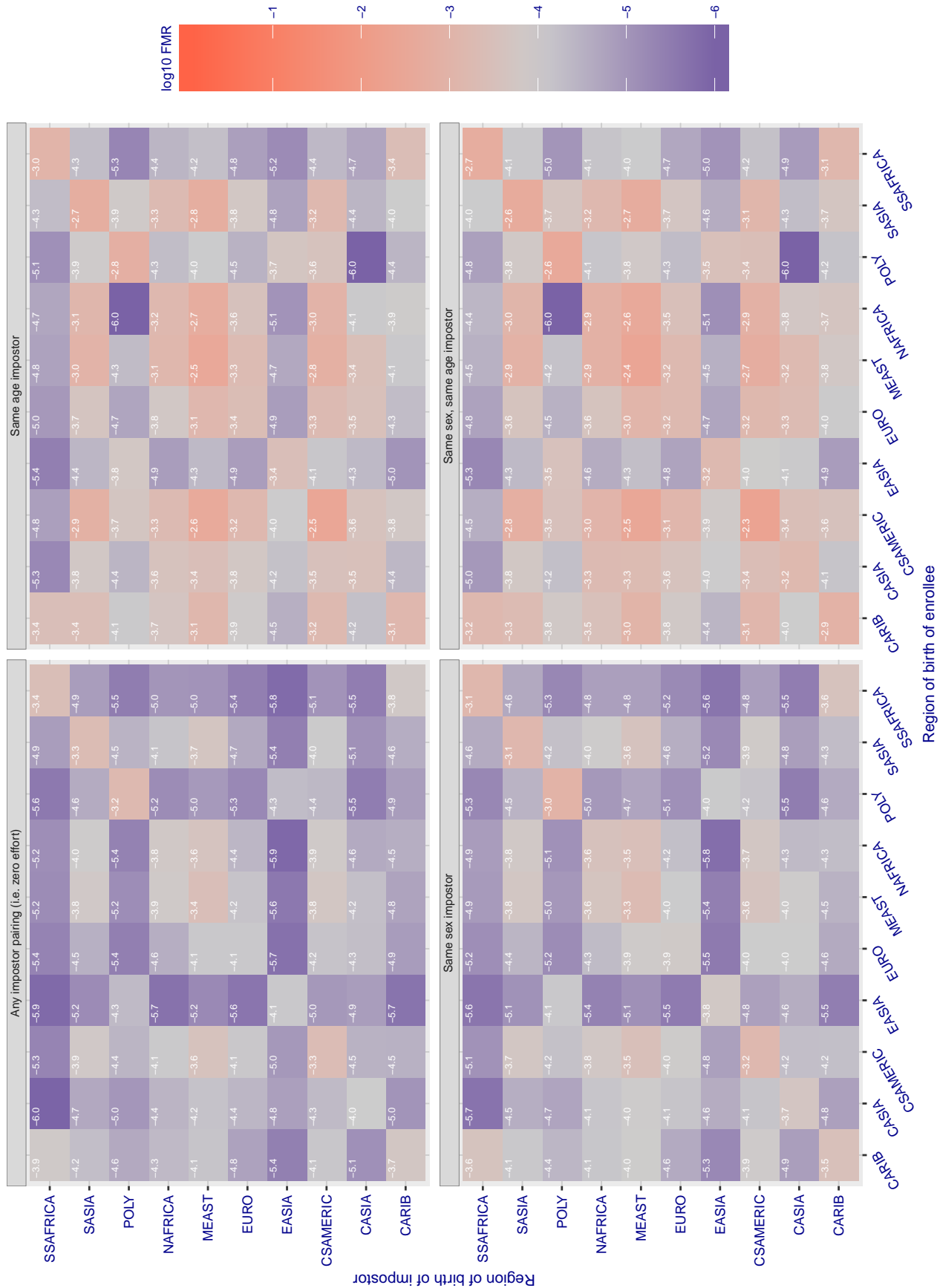


Figure 297: For algorithm tongyi-005 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 0.628 for algorithm toshiba\_002, giving FMR(T) = 0.0001 globally.

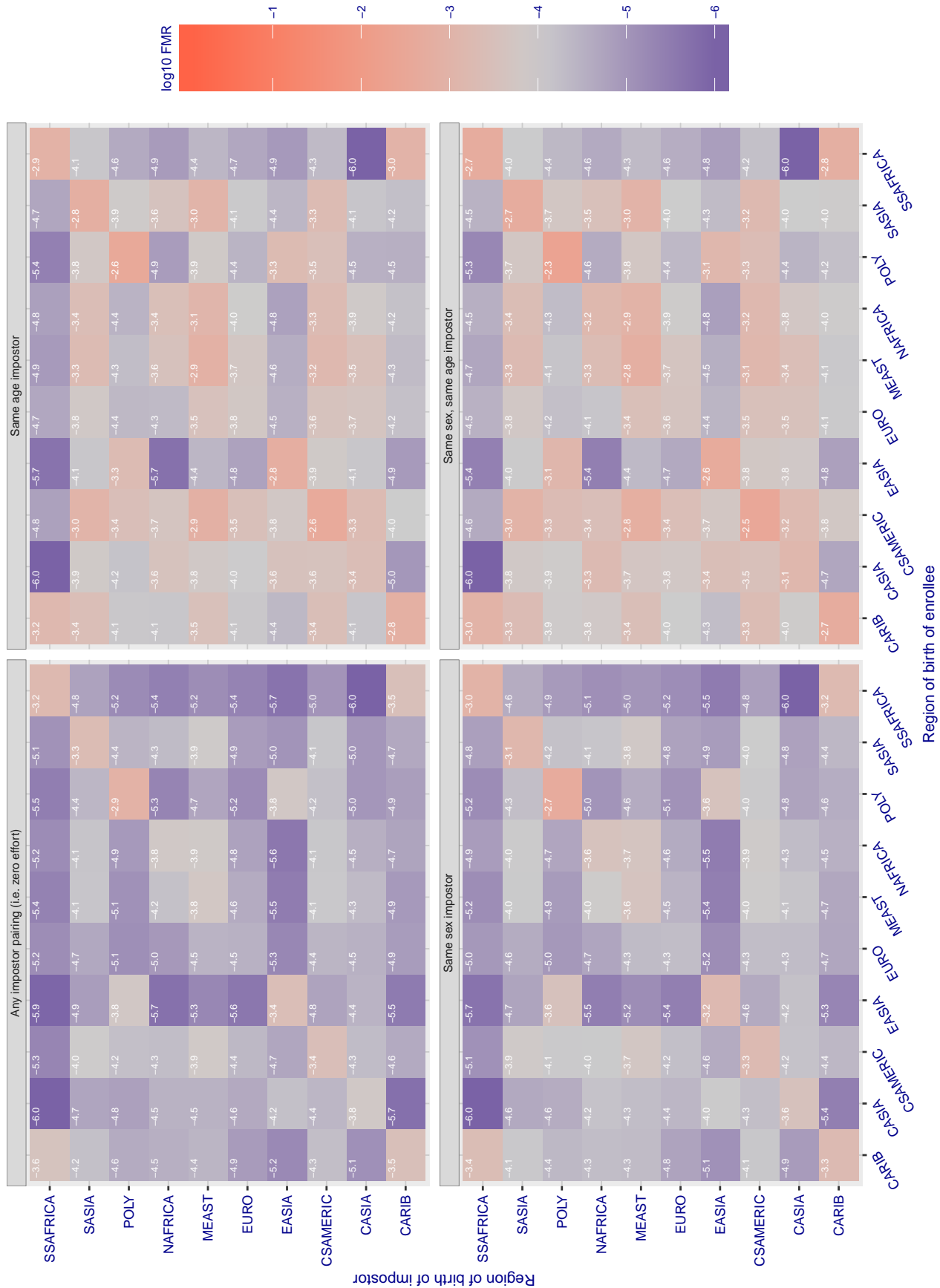


Figure 298: For algorithm toshiba-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of 10<sup>10</sup> impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 0.626 for algorithm toshiba\_003, giving FMR(T) = 0.0001 globally.

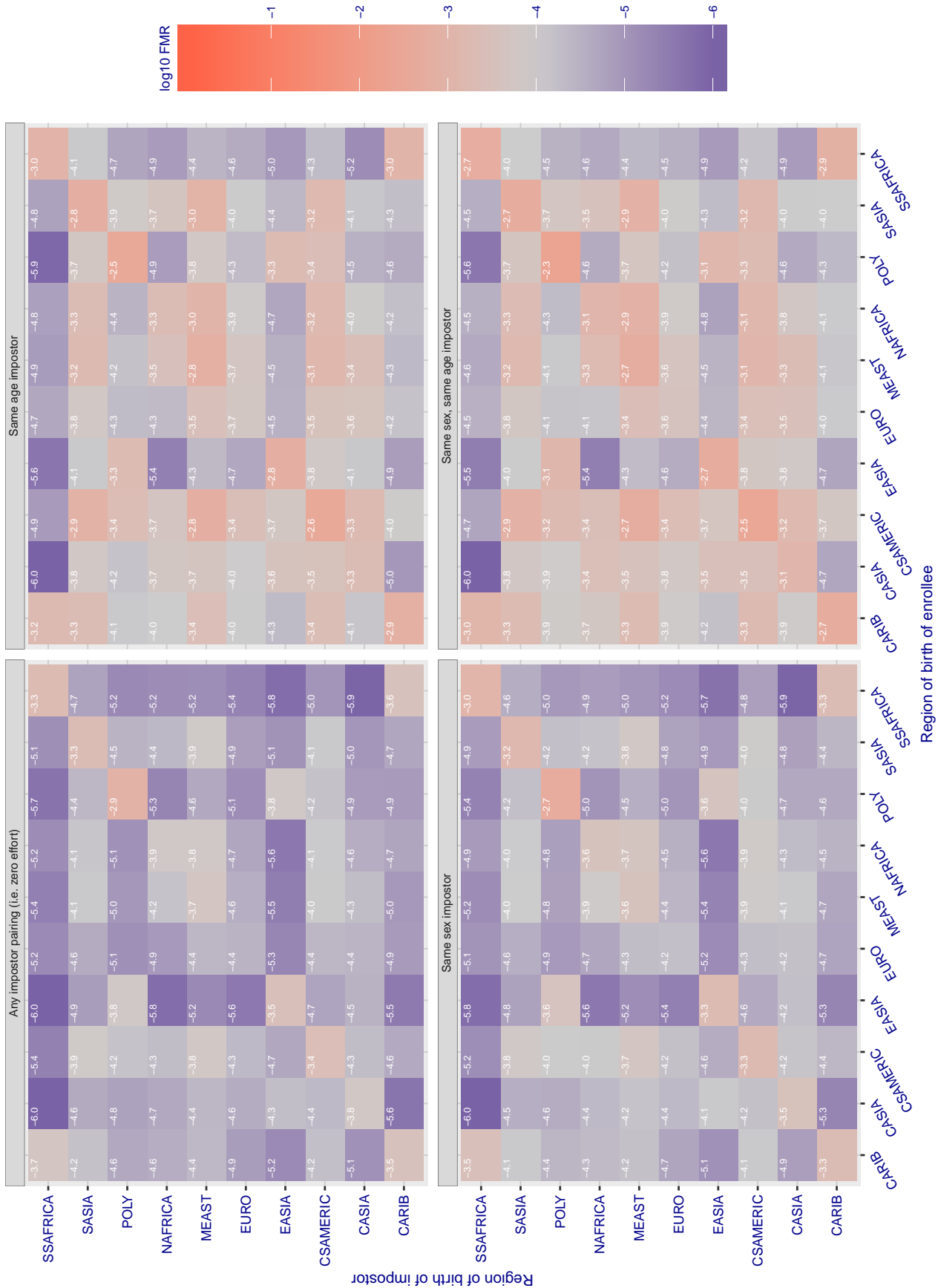


Figure 299: For algorithm toshiba-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of 10<sup>10</sup> impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.368$  for algorithm trueface\_000, giving  $FMR(T) = 0.0001$  globally.

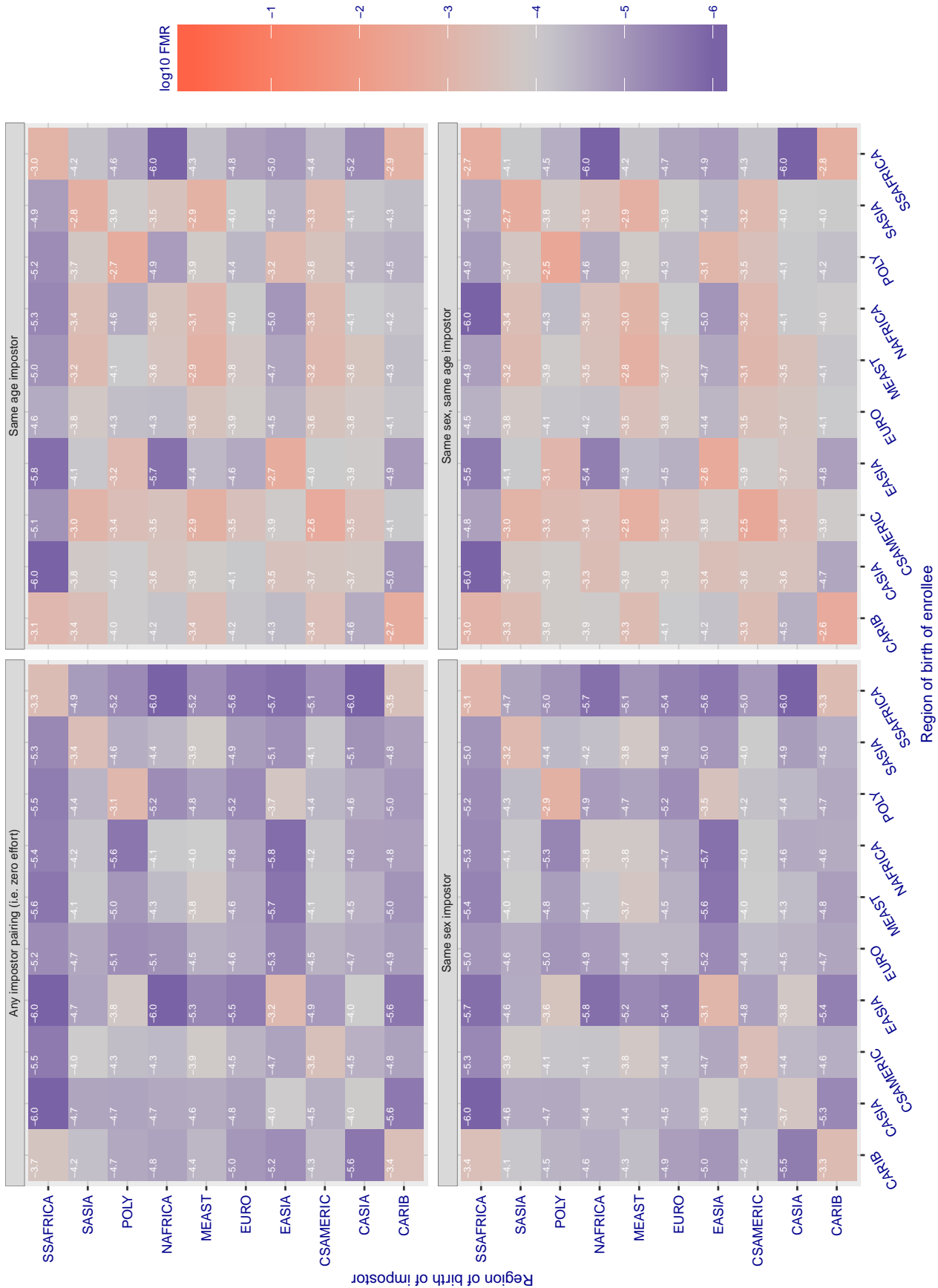


Figure 300: For algorithm trueface-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.371$  for algorithm tuputech\_000, giving  $FMR(T) = 0.0001$  globally.

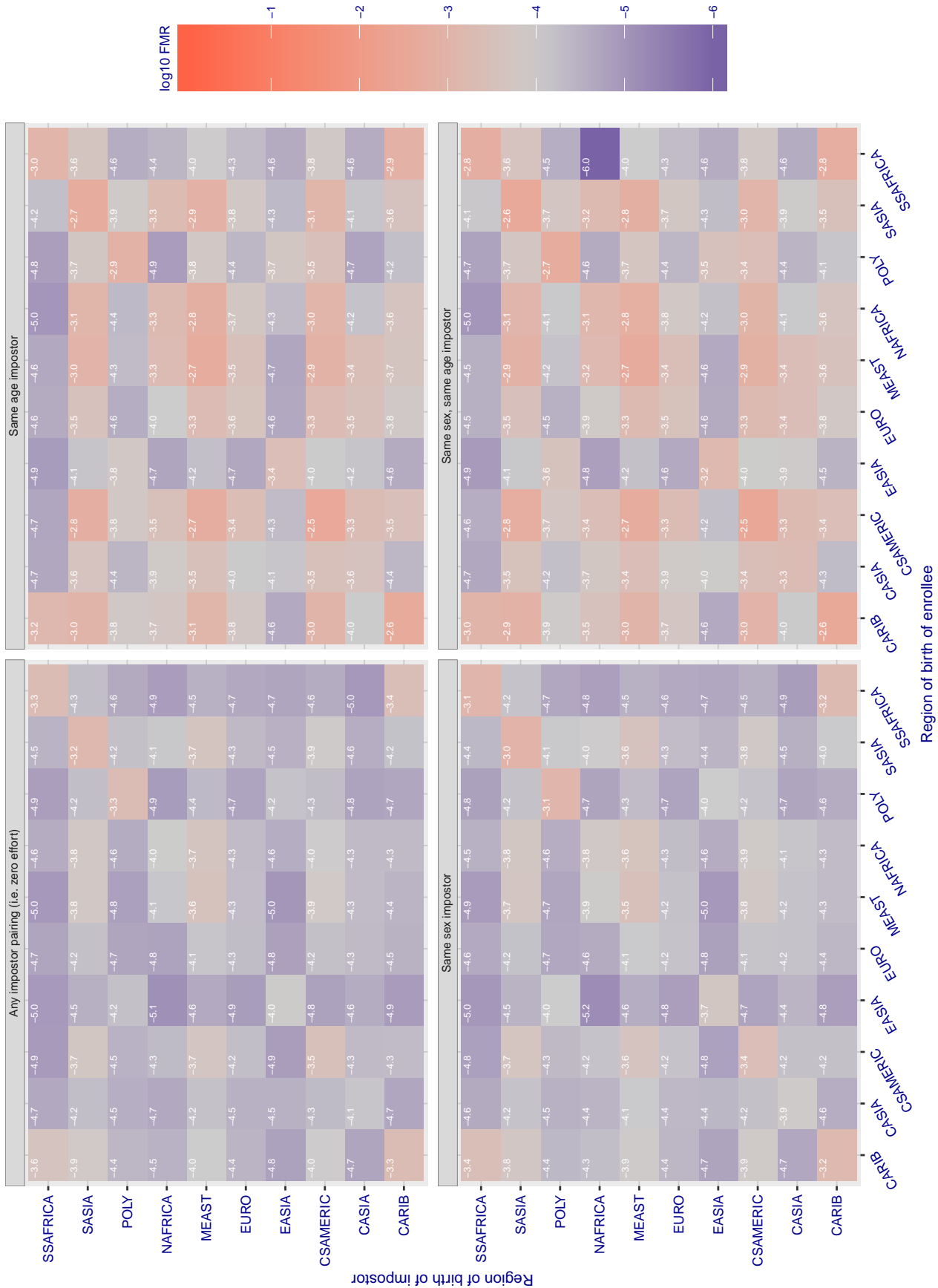


Figure 301: For algorithm tuputech-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.151$  for algorithm ulsee\_001, giving  $FMR(T) = 0.0001$  globally.

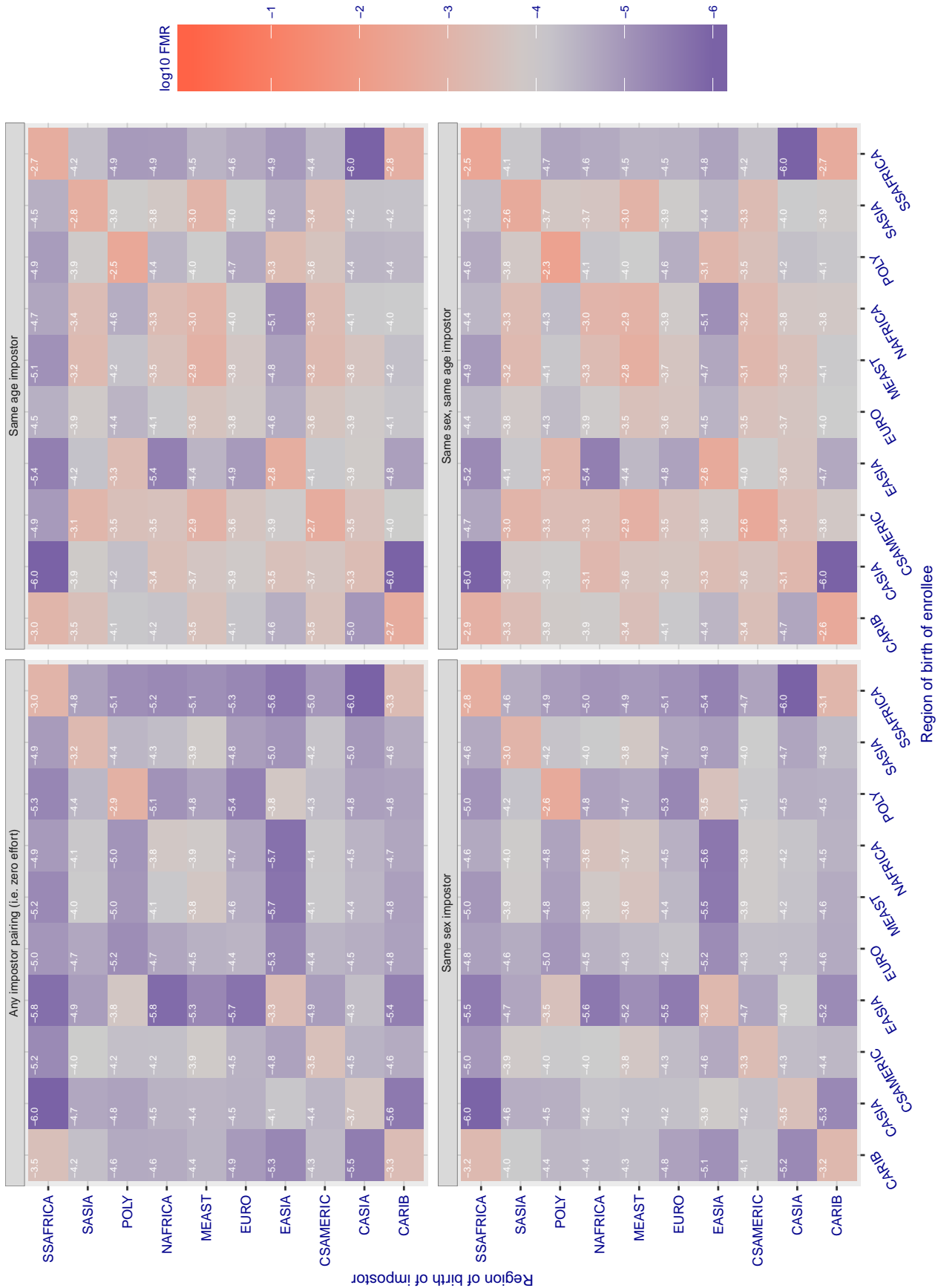


Figure 302: For algorithm ulsee-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 0.771$  for algorithm uluface\_002, giving  $FMR(T) = 0.0001$  globally.

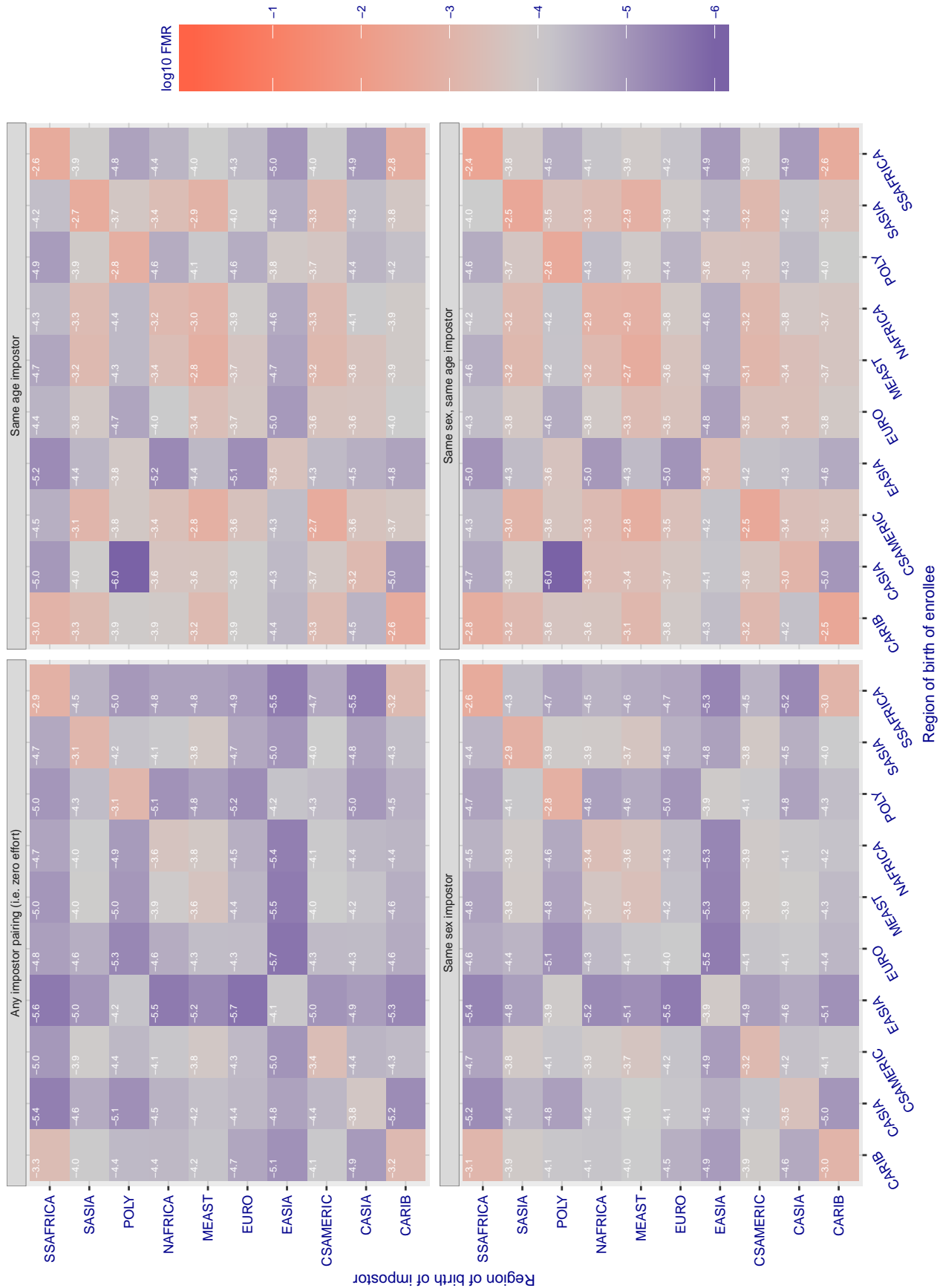


Figure 303: For algorithm uluface-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 0.838 for algorithm uluface\_003, giving FMR(T) = 0.0001 globally.

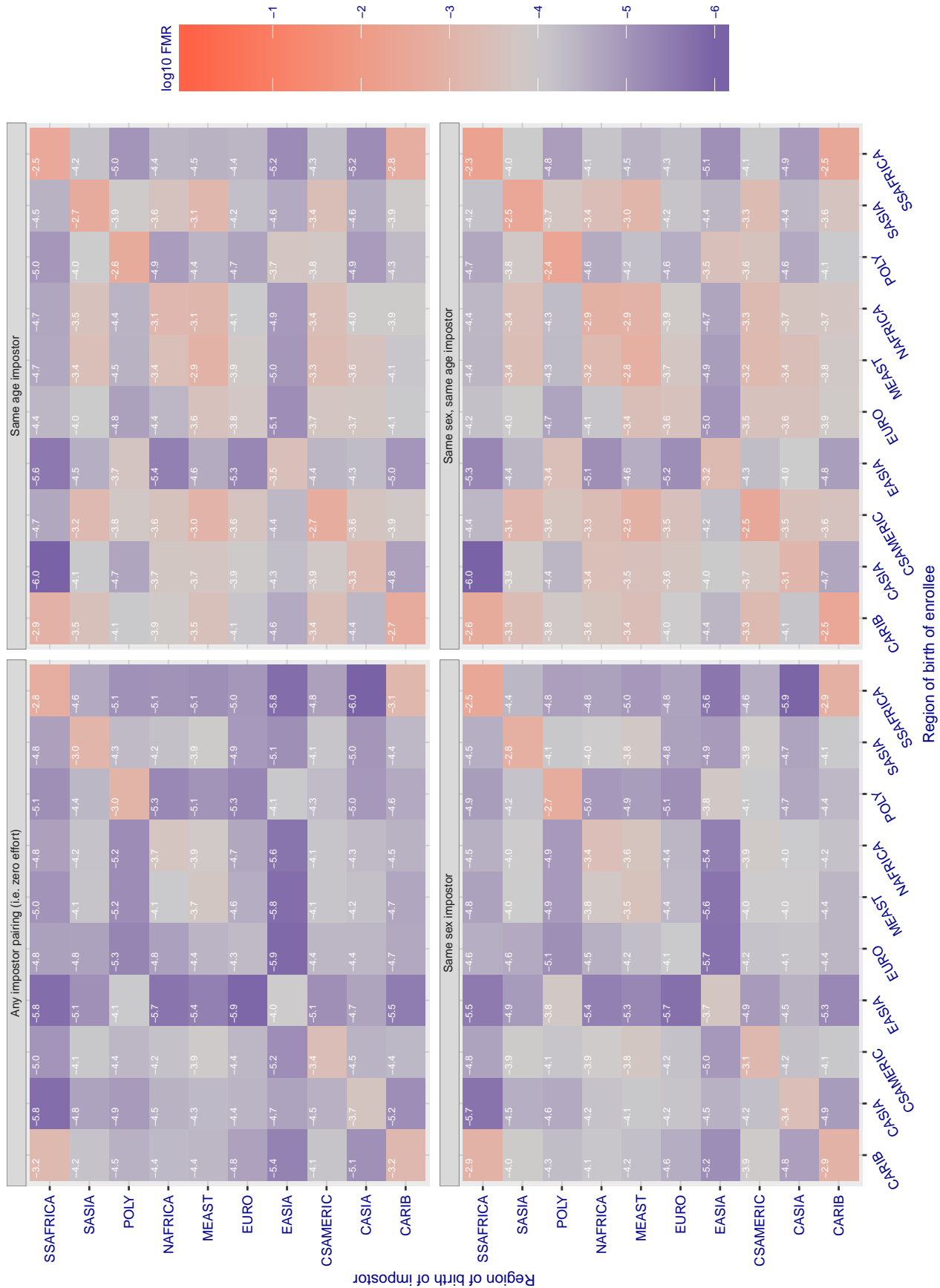


Figure 304: For algorithm uluface-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of 10<sup>10</sup> impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold  $T = 0.482$  for algorithm upc\_001, giving  $FMR(T) = 0.0001$  globally.

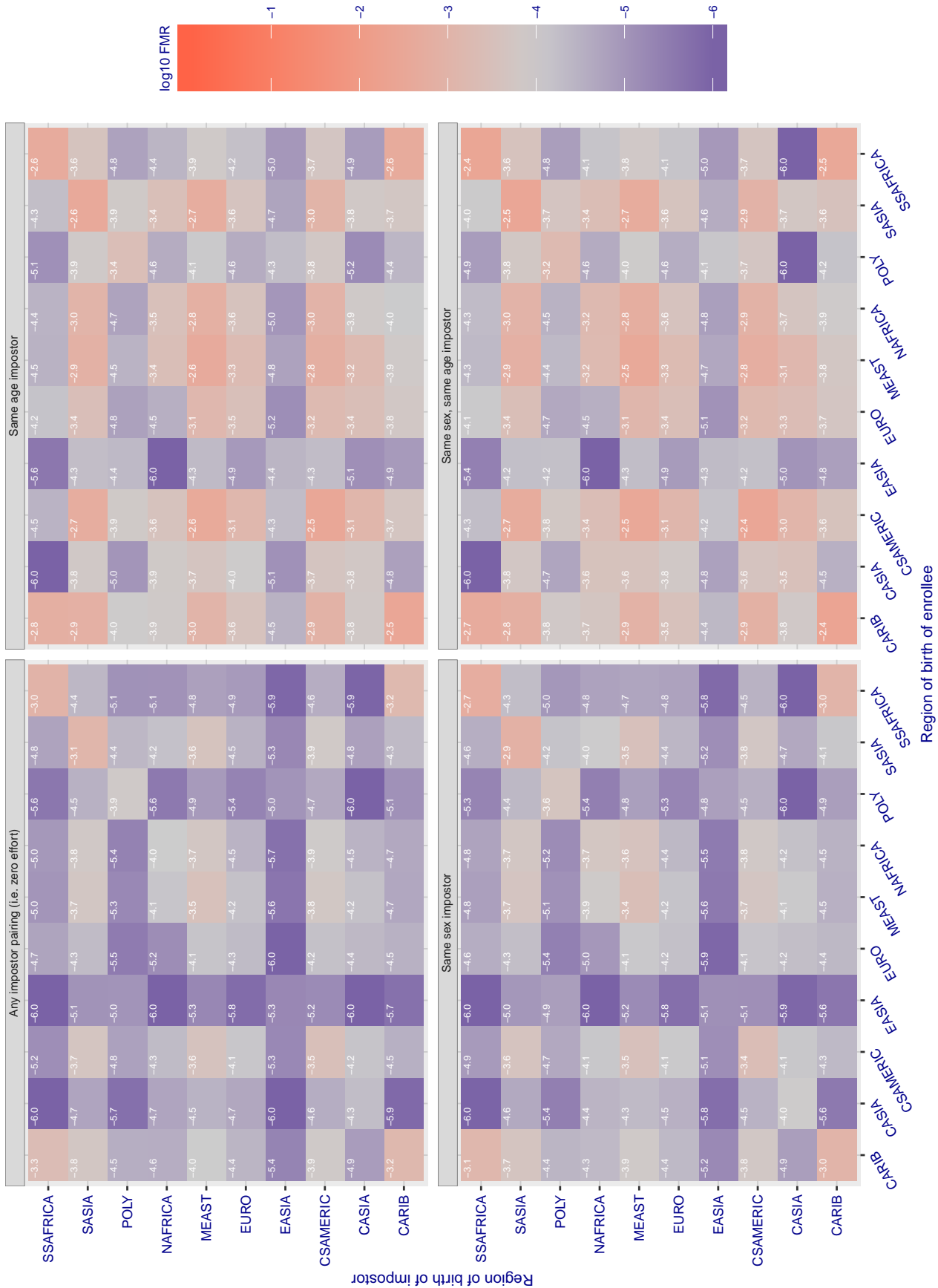


Figure 305: For algorithm upc-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.428$  for algorithm vcog\_002, giving  $FMR(T) = 0.0001$  globally.

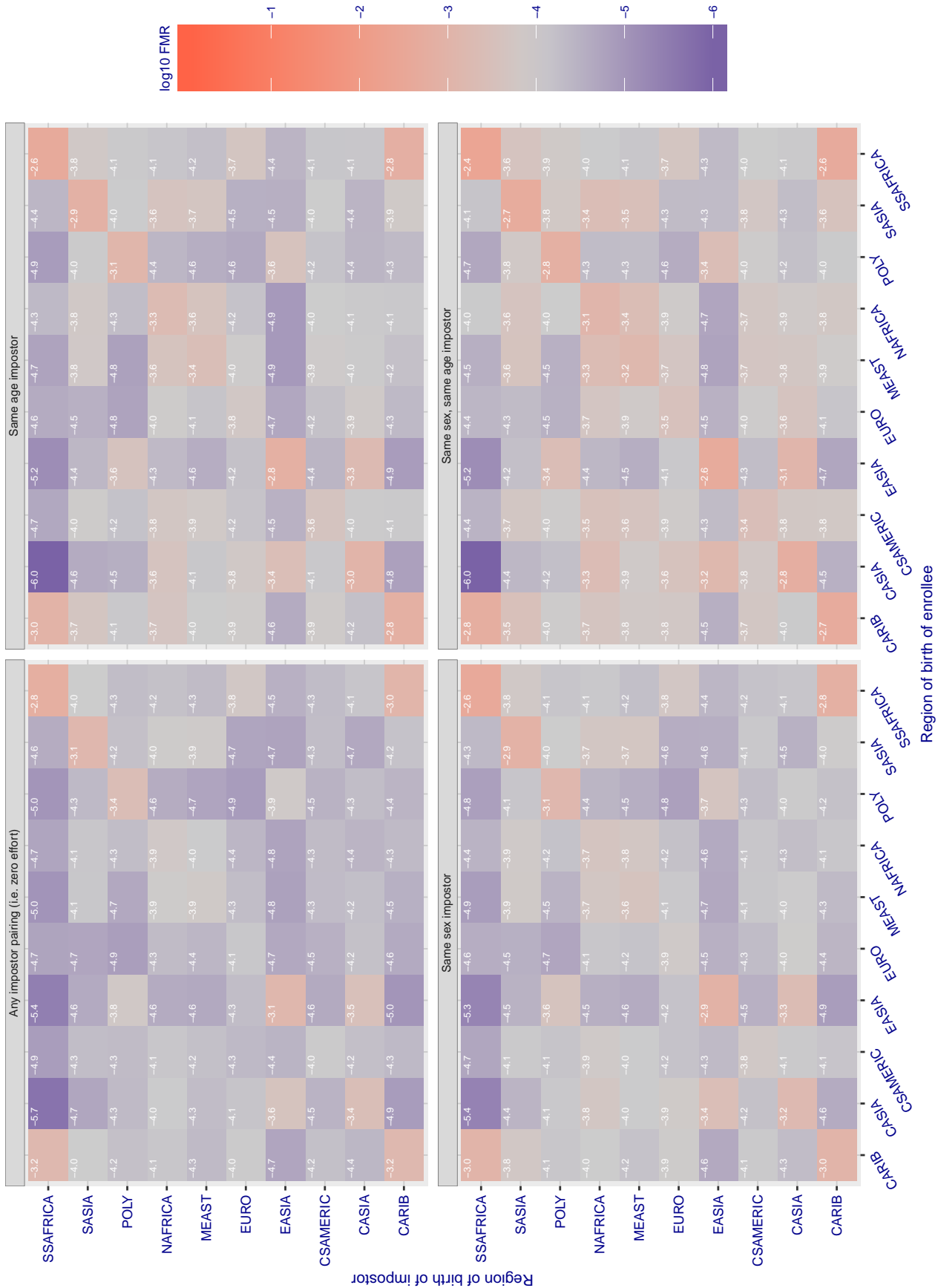


Figure 306: For algorithm vcog-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 71.529 for algorithm vd\_001, giving FMR(T) = 0.0001 globally.

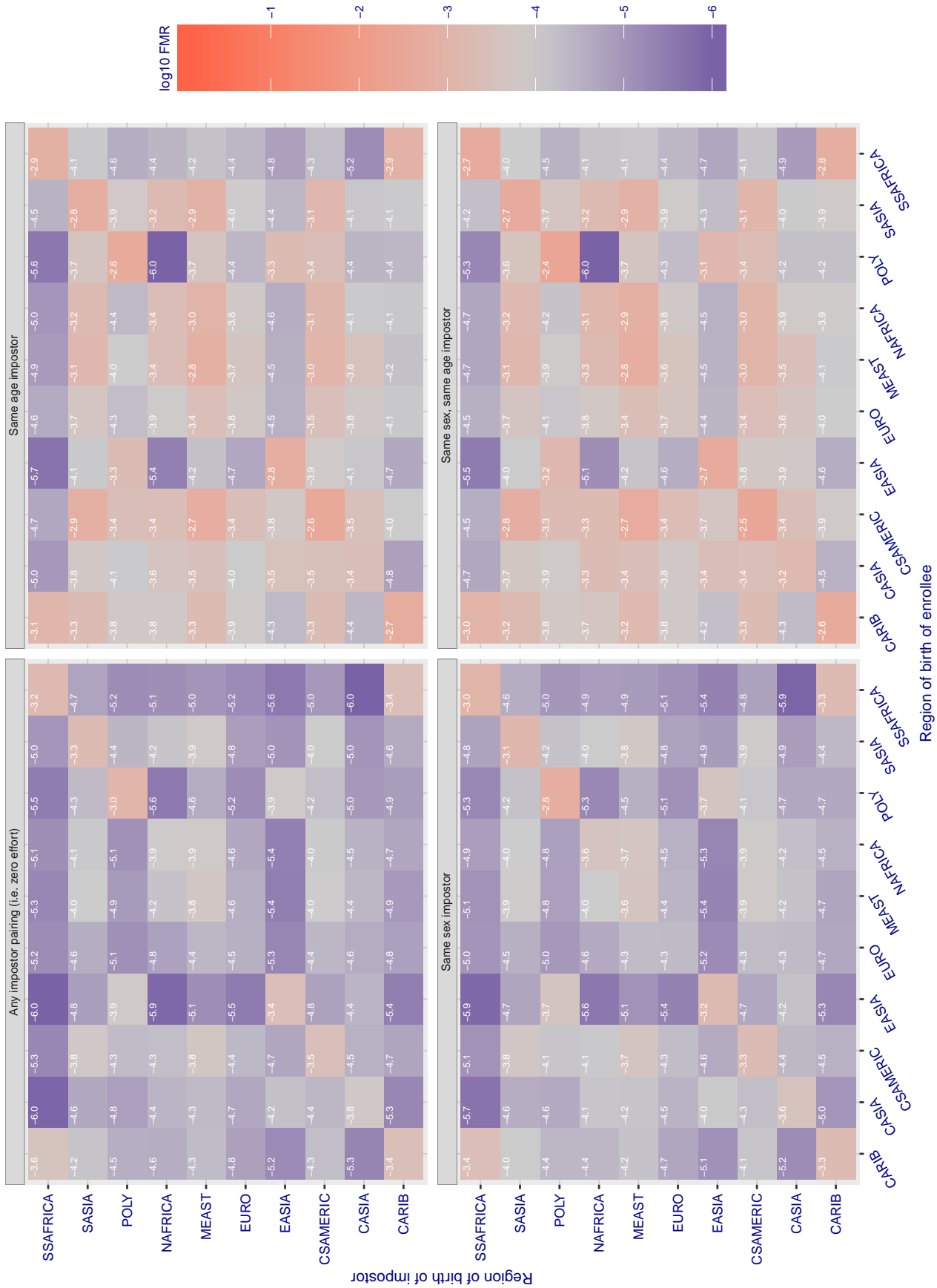


Figure 307: For algorithm vd-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 3.325$  for algorithm veridas\_001, giving  $FMR(T) = 0.0001$  globally.

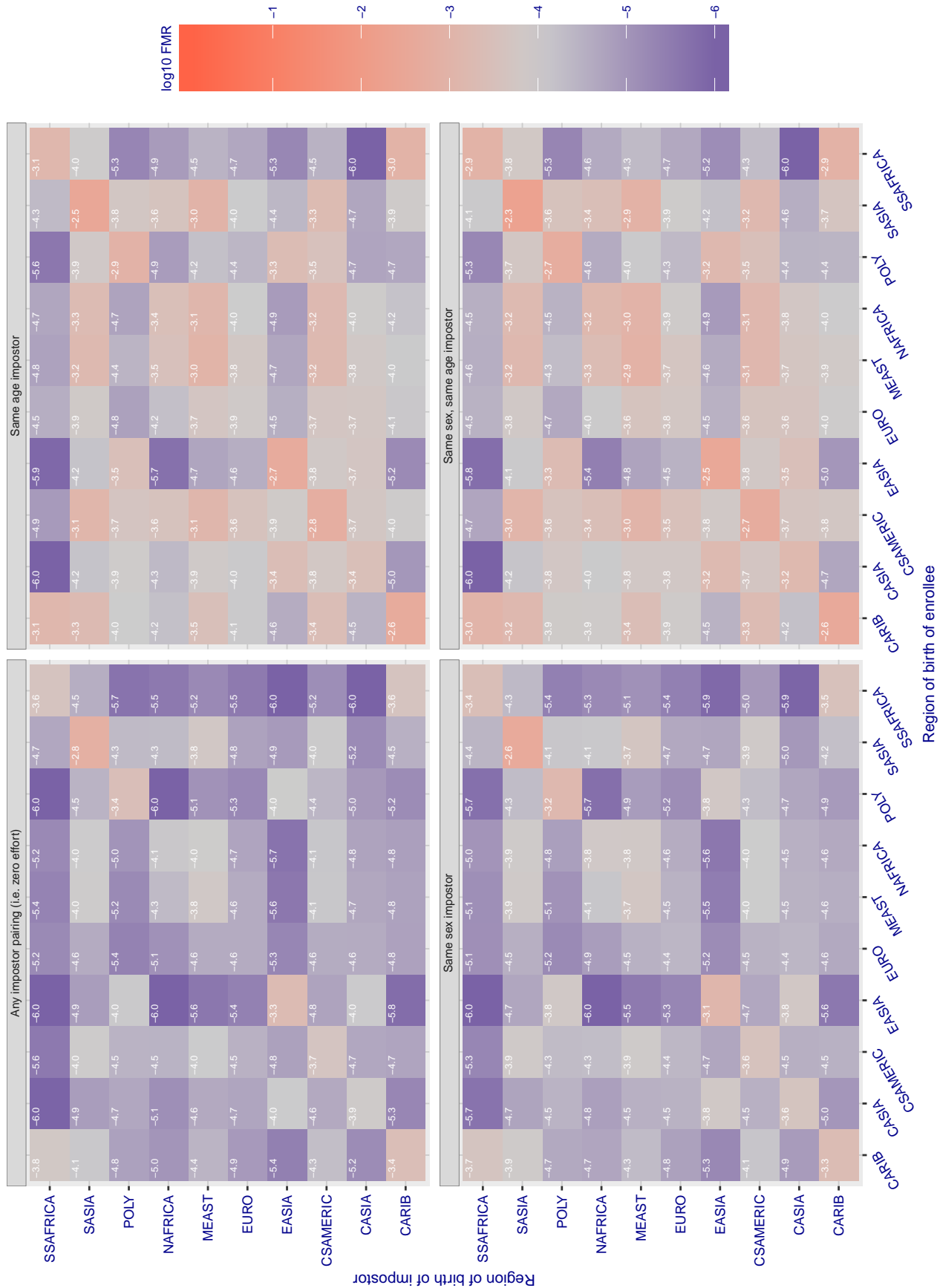


Figure 308: For algorithm veridas-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 3.389 for algorithm veridas\_002, giving FMR(T) = 0.0001 globally.

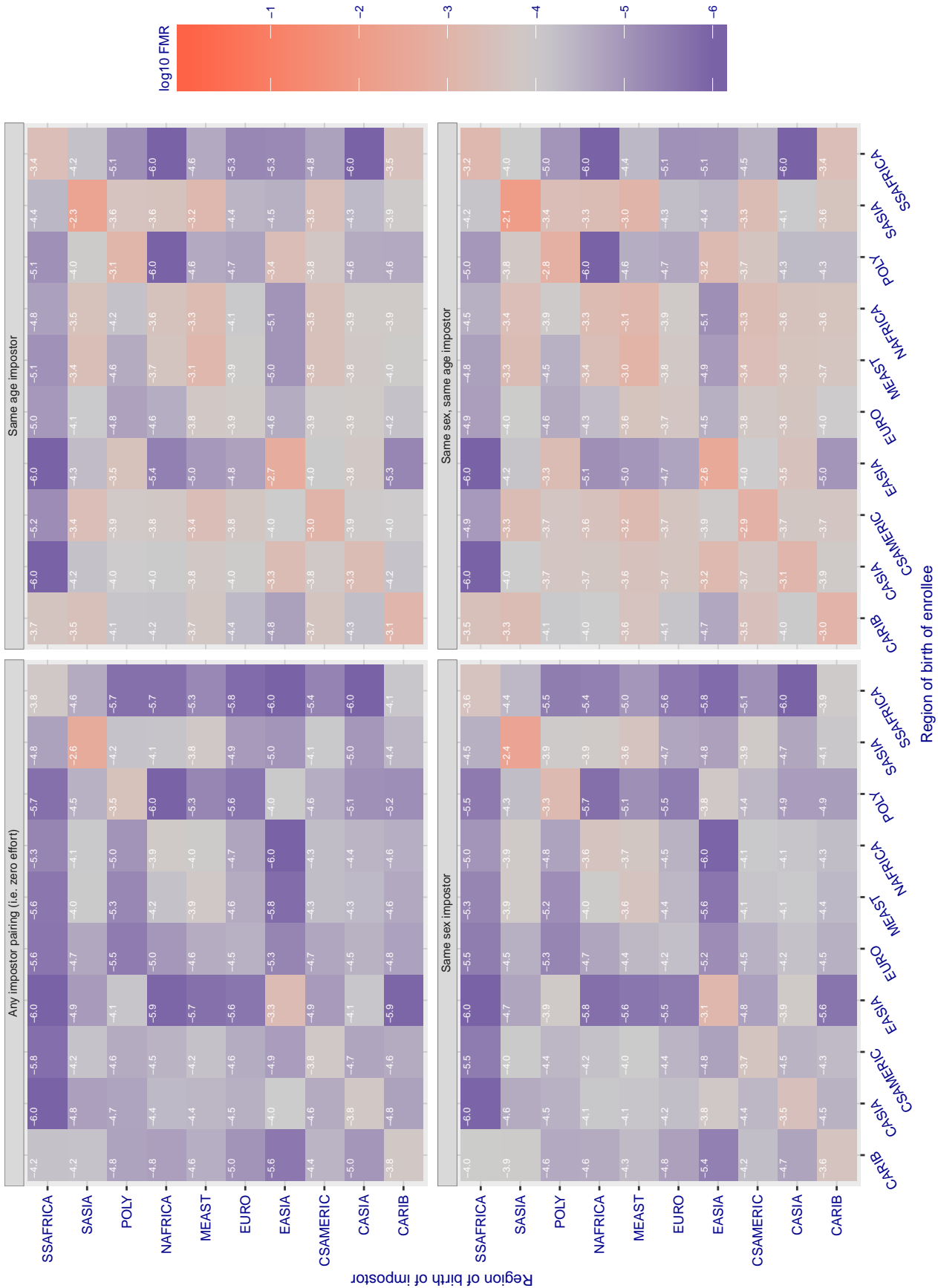


Figure 309: For algorithm veridas-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of 10<sup>10</sup> impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 2.859 for algorithm via\_000, giving FMR(T) = 0.0001 globally.

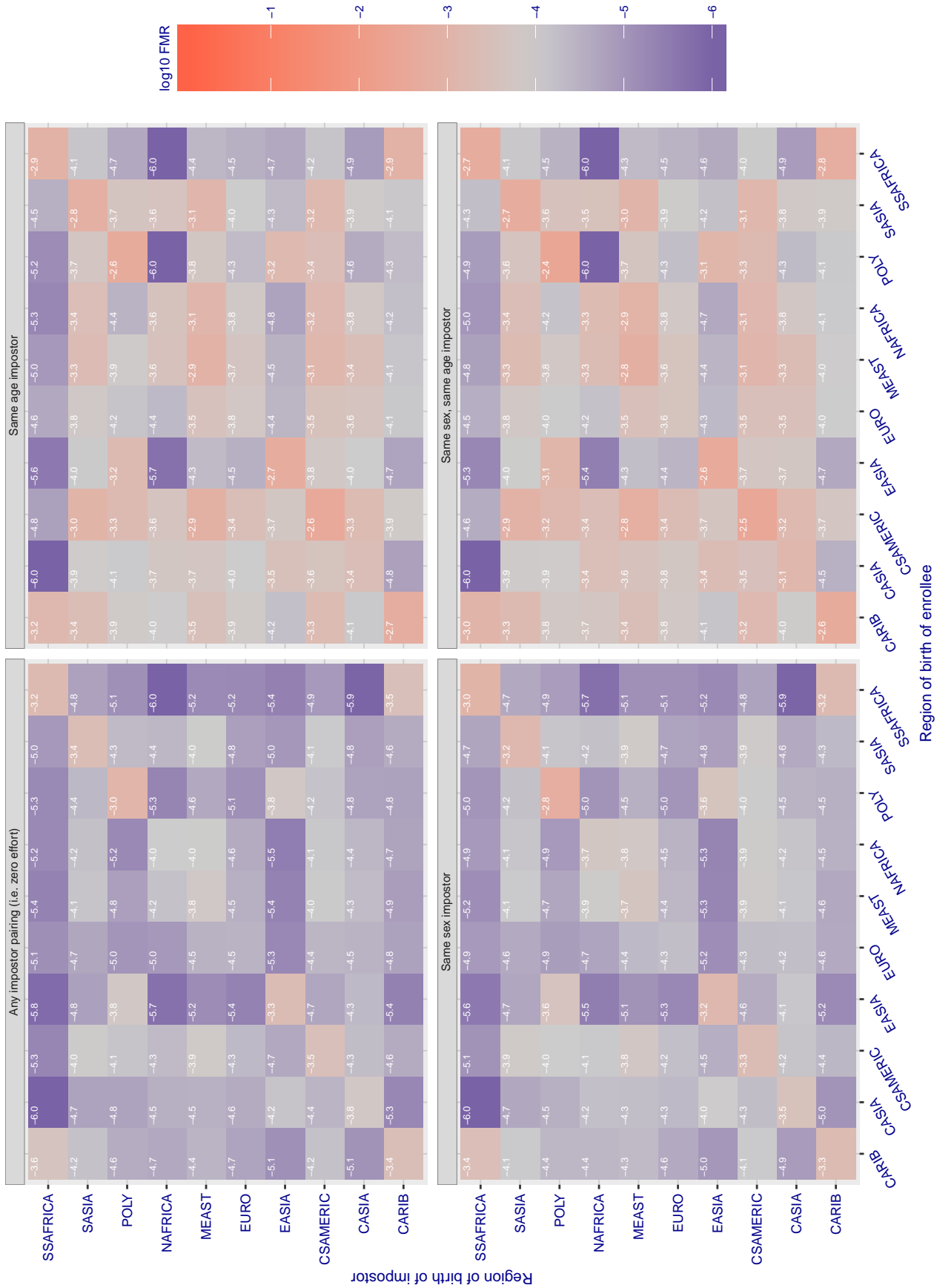


Figure 310: For algorithm via-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



**Cross region FMR at threshold  $T = 0.842$  for algorithm videonetics\_001, giving  $FMR(T) = 0.0001$  globally.**

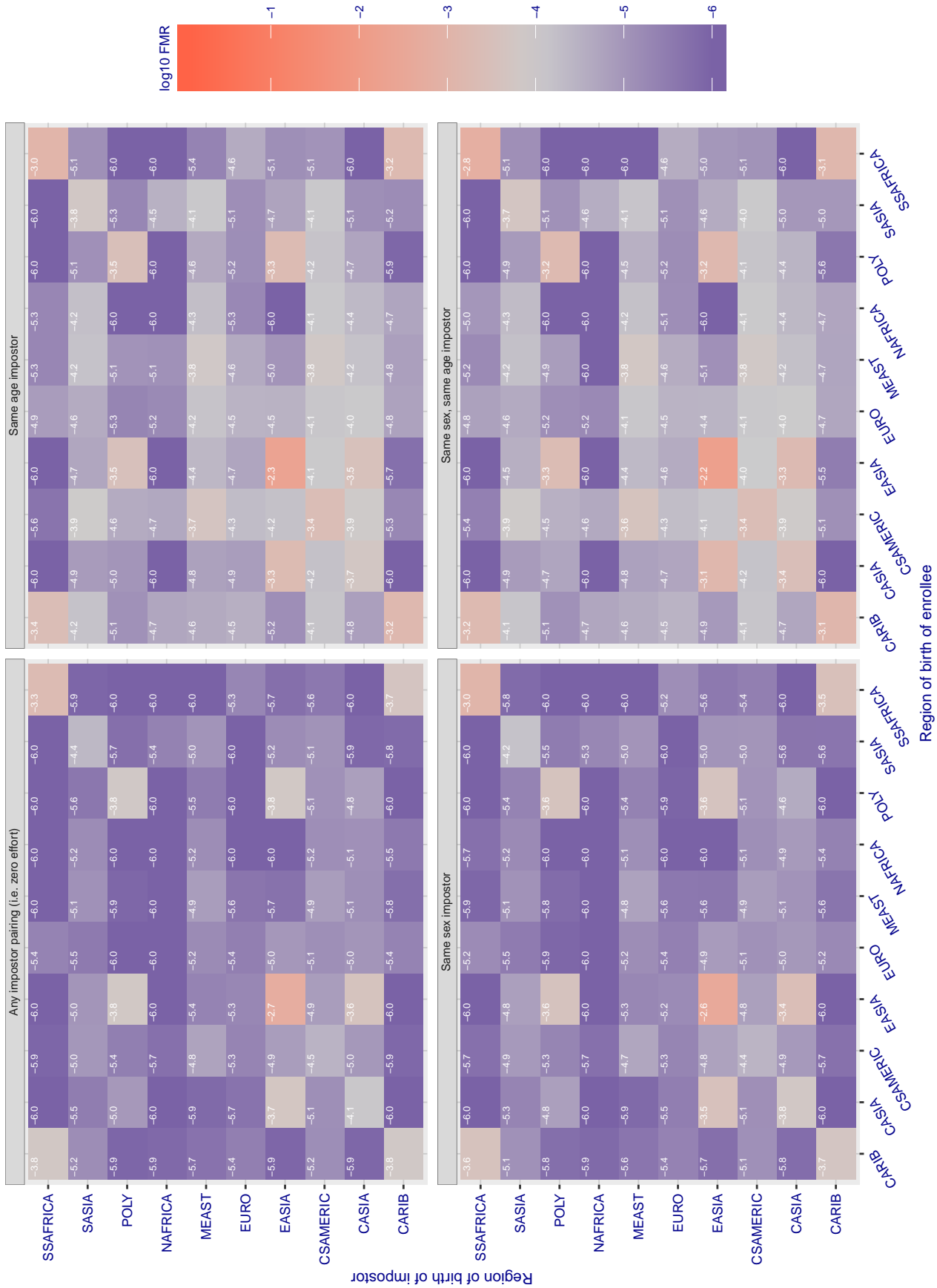


Figure 311: For algorithm videonetics-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 3.057$  for algorithm *vigilantsolutions\_006*, giving  $FMR(T) = 0.0001$  globally.

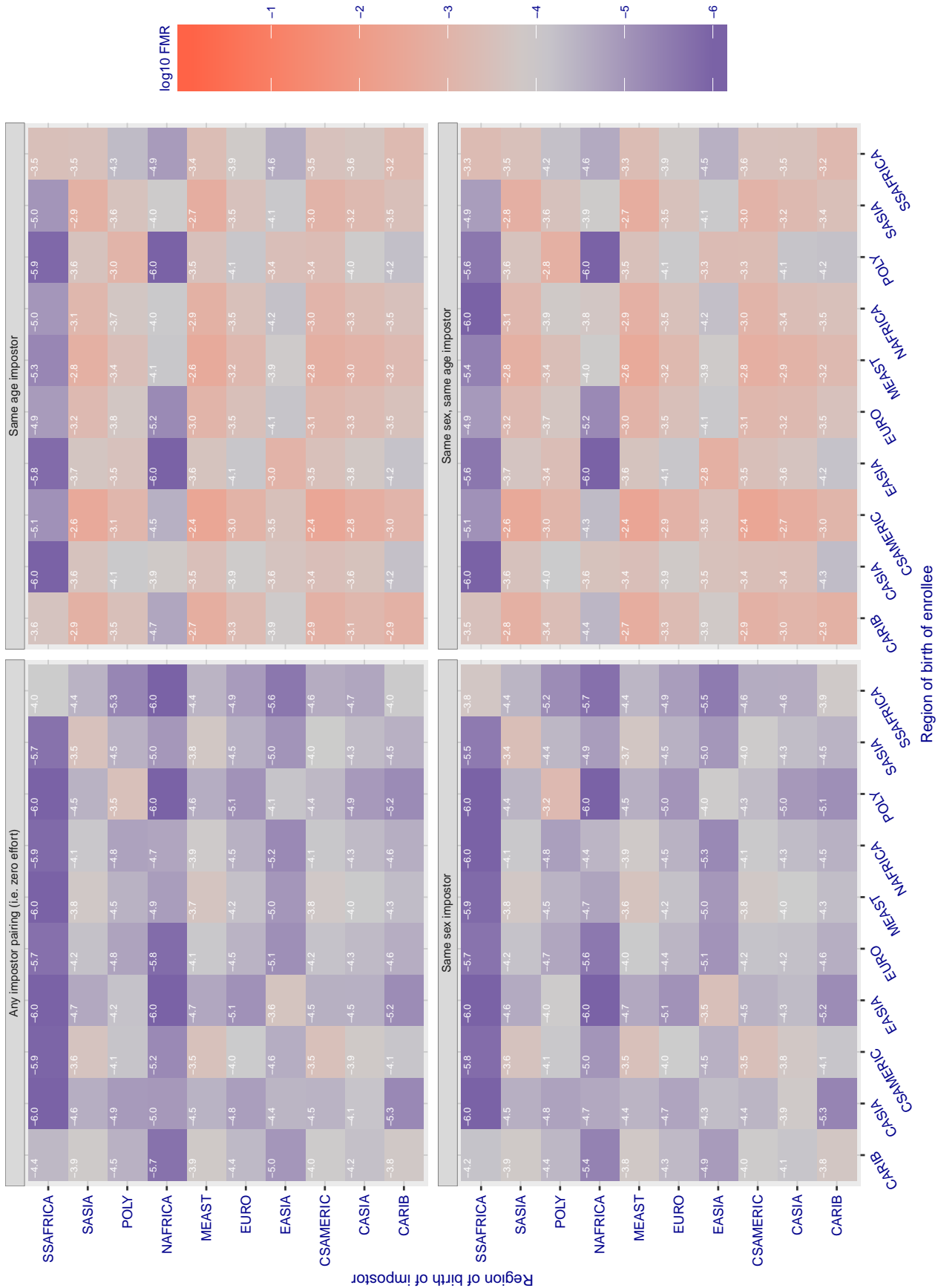


Figure 312: For algorithm *vigilantsolutions-006* operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold T = 2.926 for algorithm vigilantsolutions\_007, giving FMR(T) = 0.0001 globally.

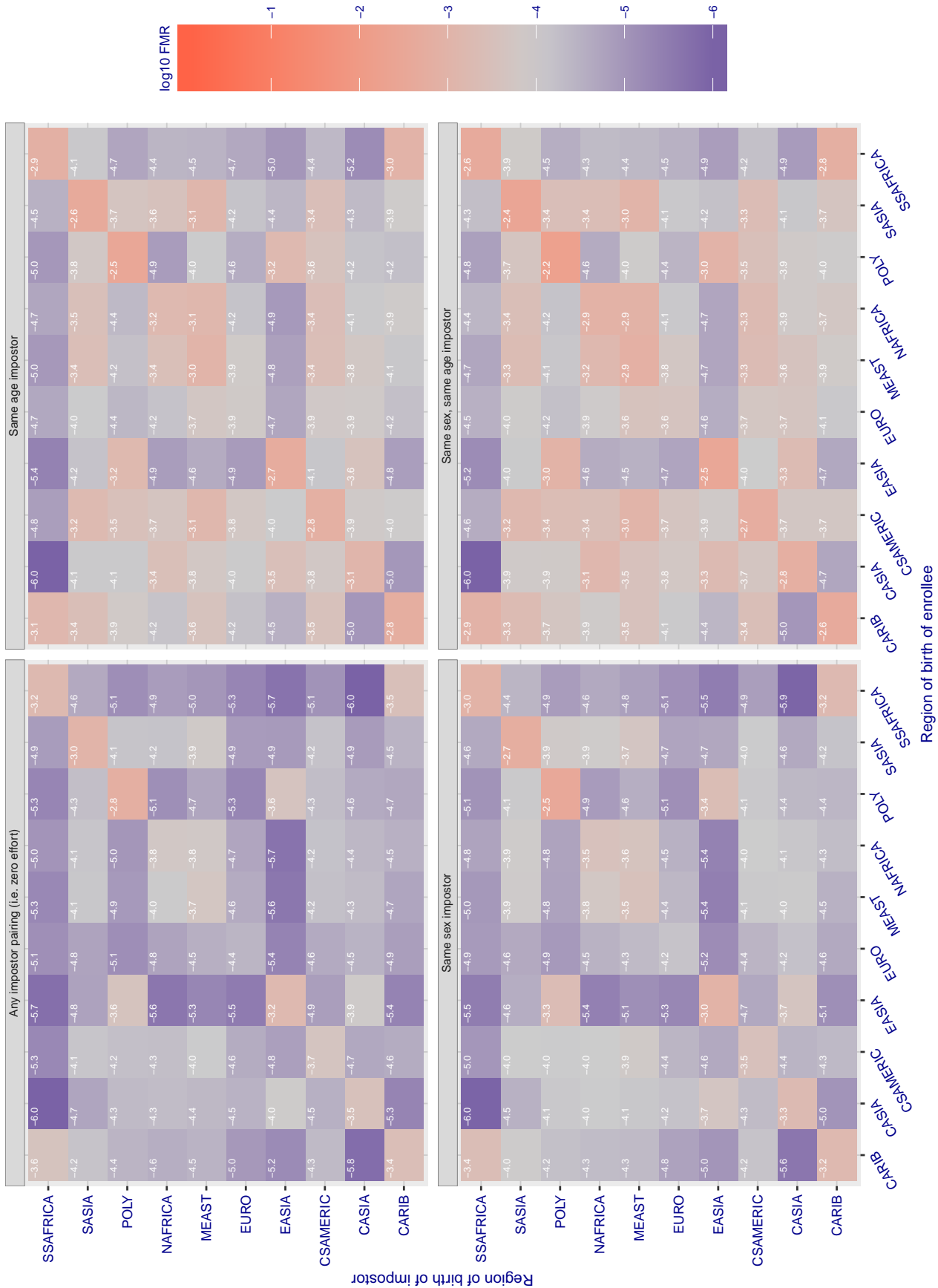


Figure 313: For algorithm vigilantsolutions-007 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of 10<sup>10</sup> impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.432$  for algorithm  $\text{vion}_{000}$ , giving  $\text{FMR}(T) = 0.0001$  globally.

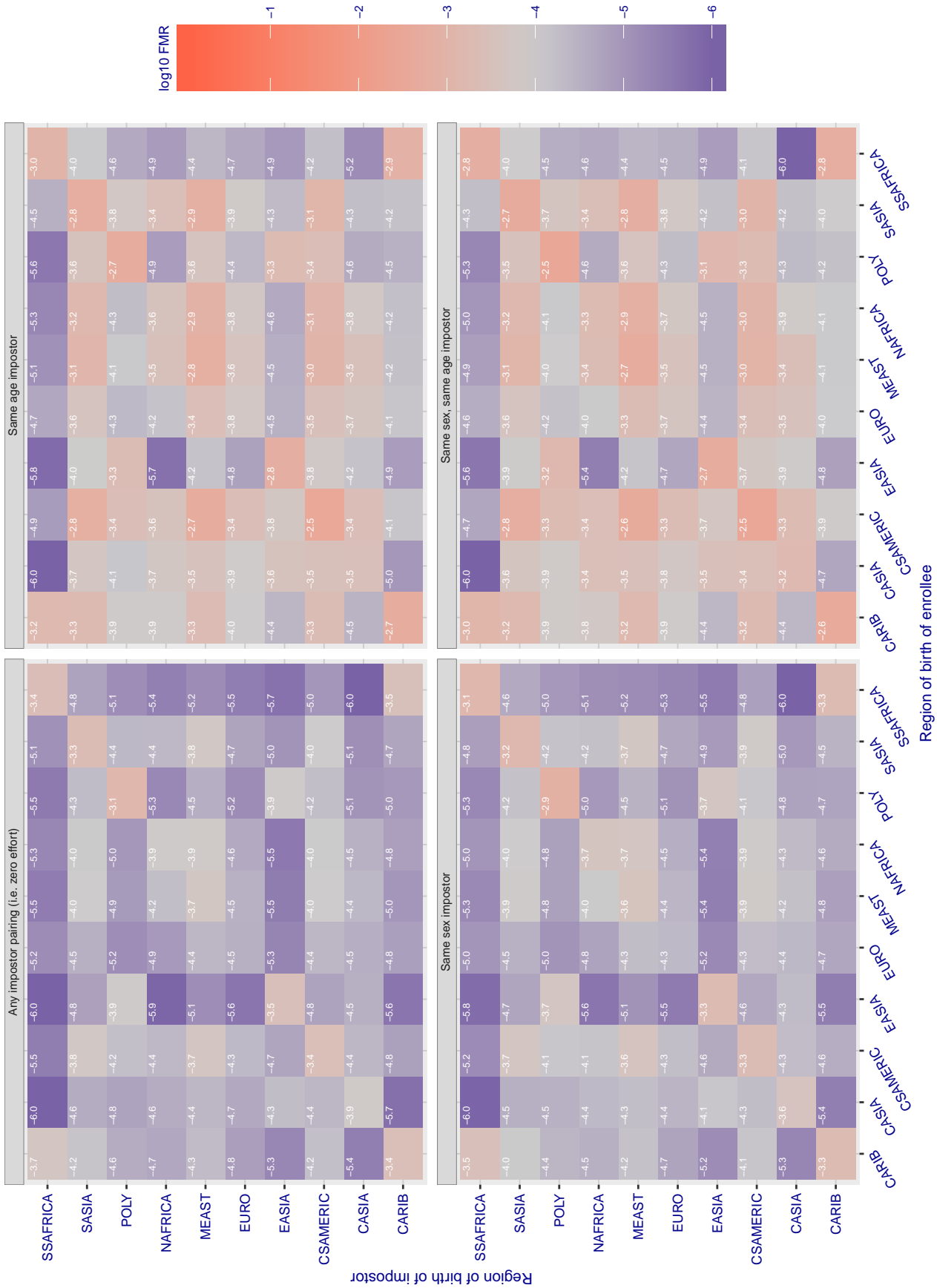


Figure 314: For algorithm  $\text{vion}_{000}$  operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

**Cross region FMR at threshold T = 0.433 for algorithm visionbox\_000, giving FMR(T) = 0.0001 globally.**

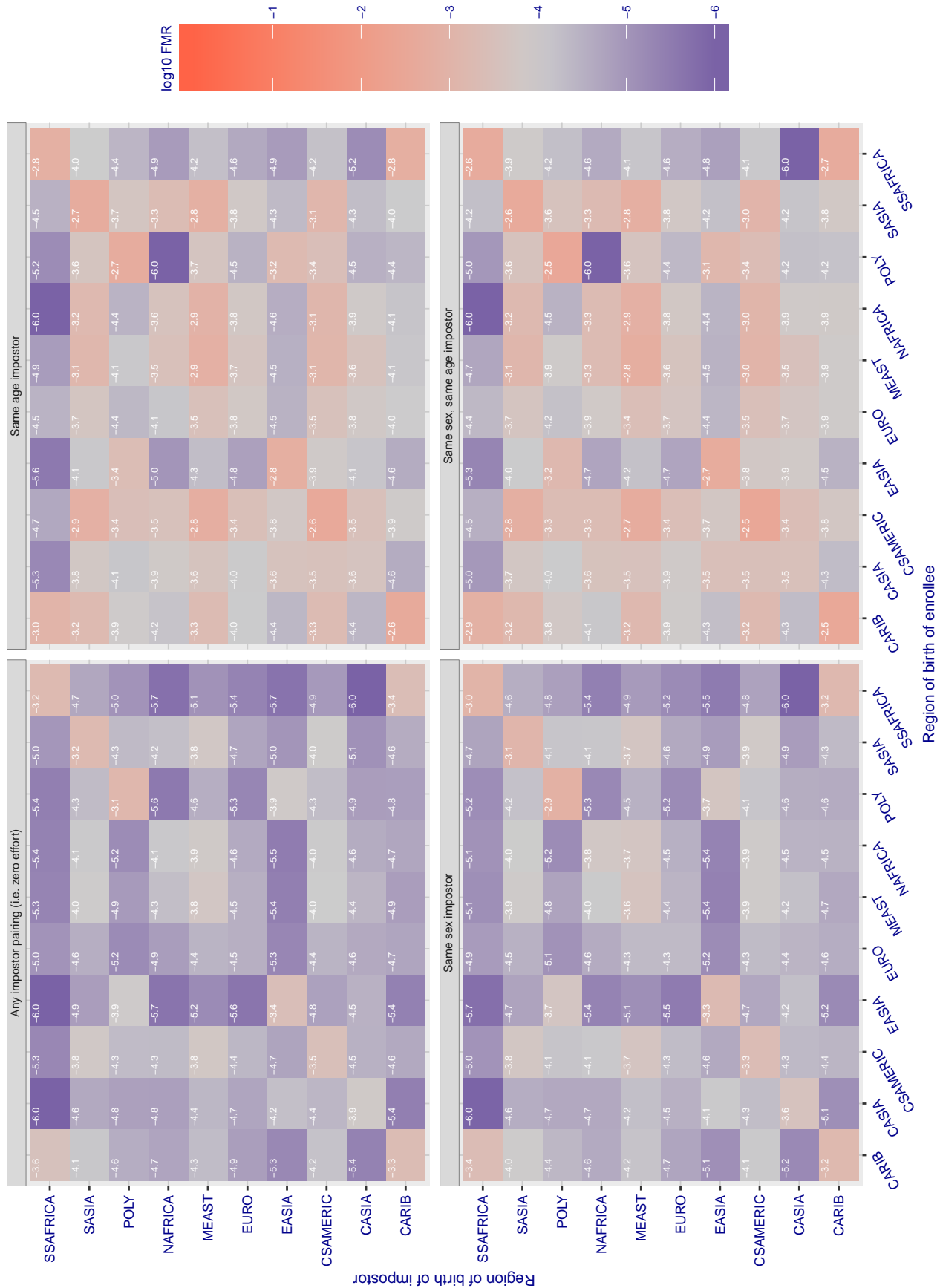


Figure 315: For algorithm visionbox-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.382$  for algorithm visionbox\_001, giving FMR(T) = 0.0001 globally.

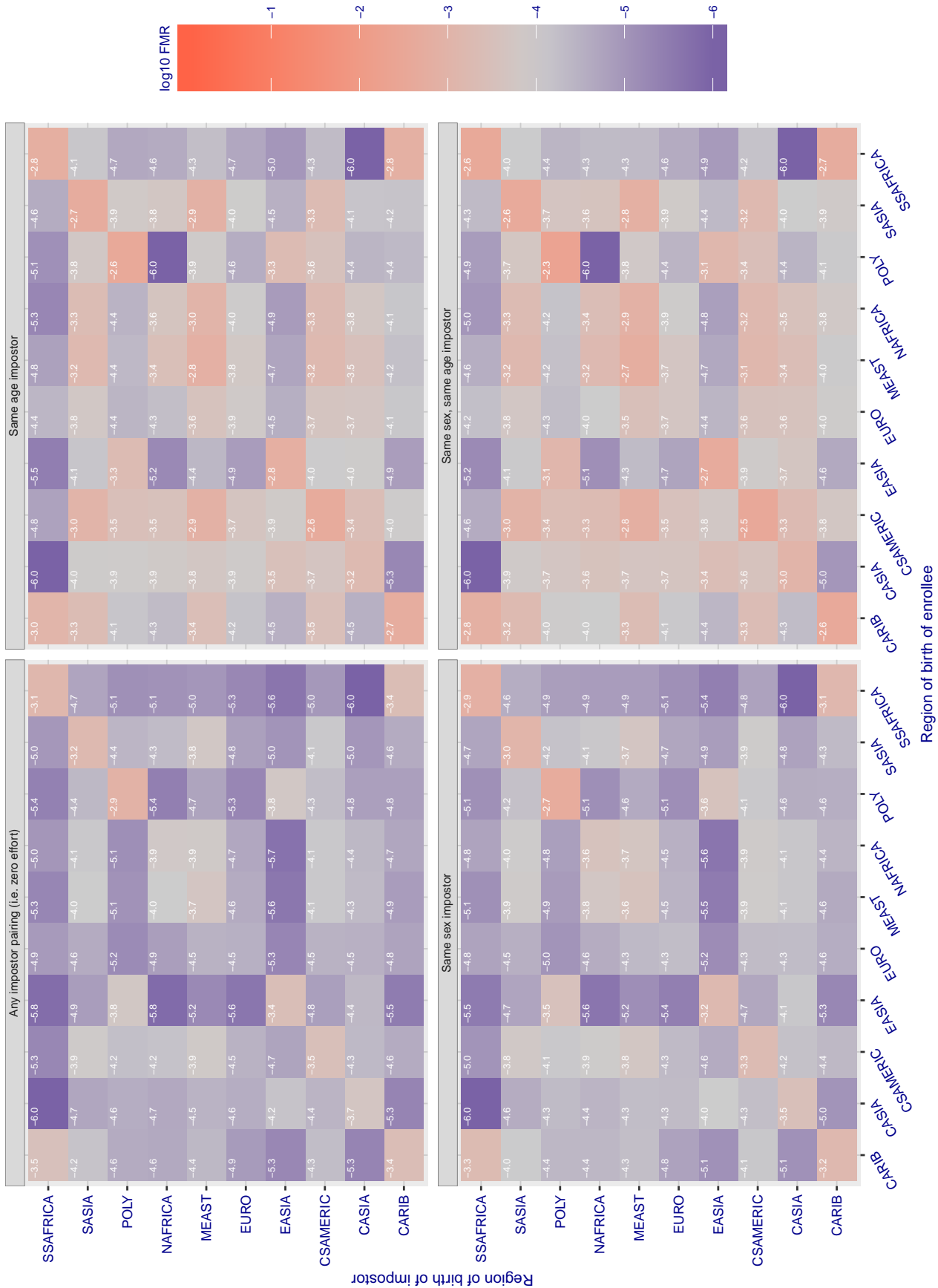


Figure 316: For algorithm visionbox-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.669$  for algorithm visionlabs\_006, giving  $FMR(T) = 0.0001$  globally.

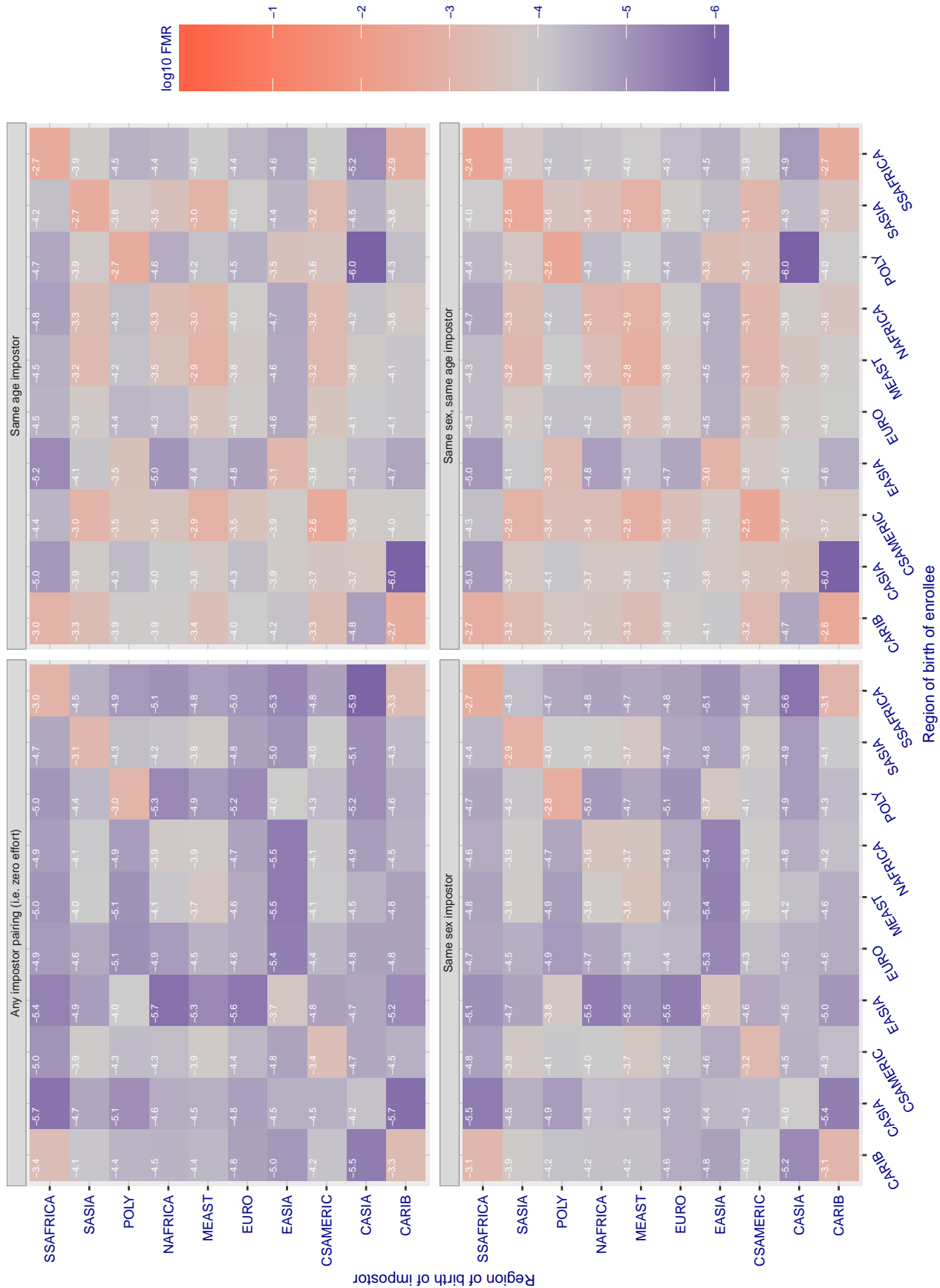


Figure 317: For algorithm visionlabs-006 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 0.657 for algorithm visionlabs\_007, giving FMR(T) = 0.0001 globally.

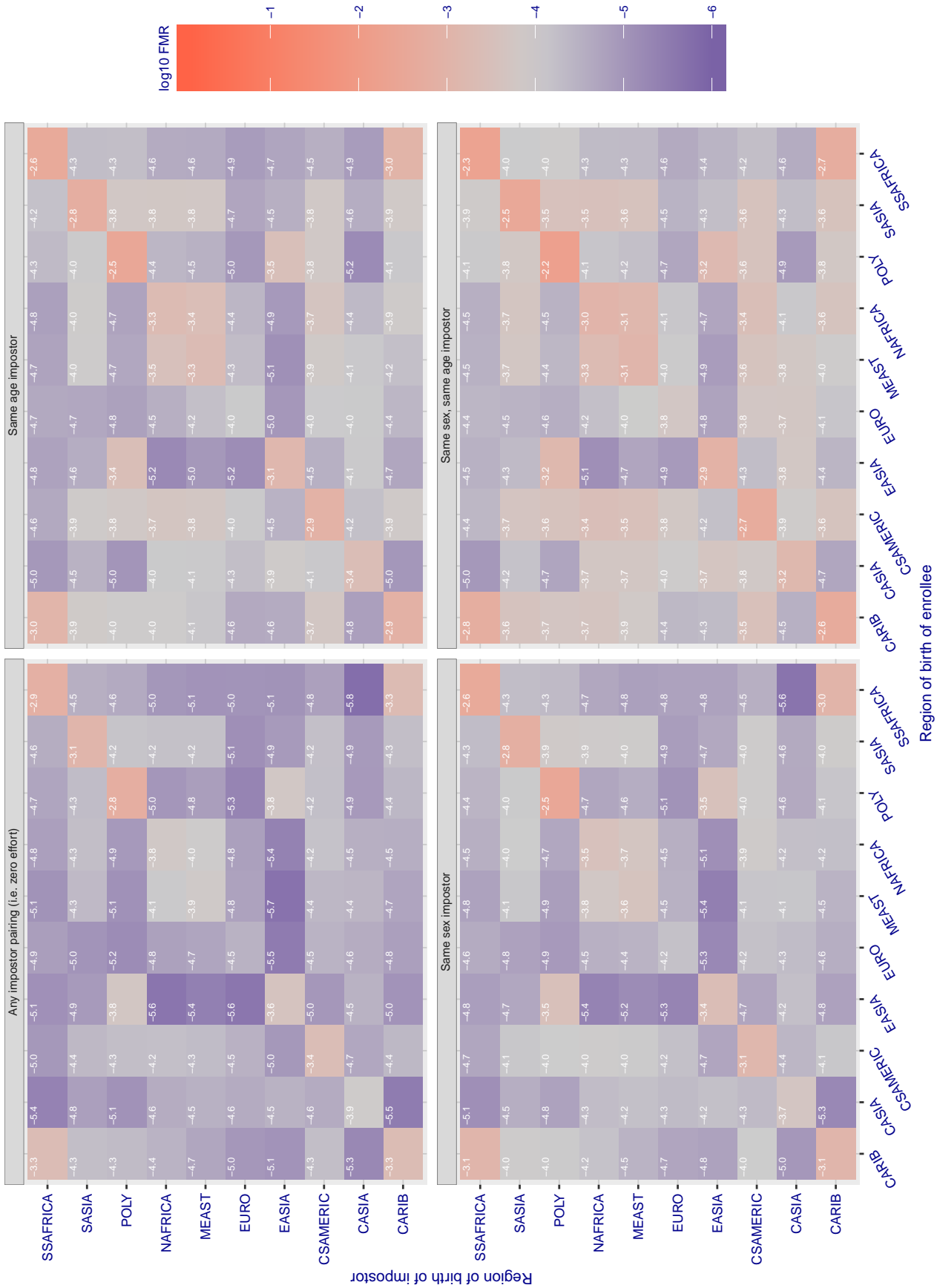


Figure 318: For algorithm visionlabs-007 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of 10<sup>10</sup> impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold T = 995.898 for algorithm vocord\_006, giving FMR(T) = 0.0001 globally.

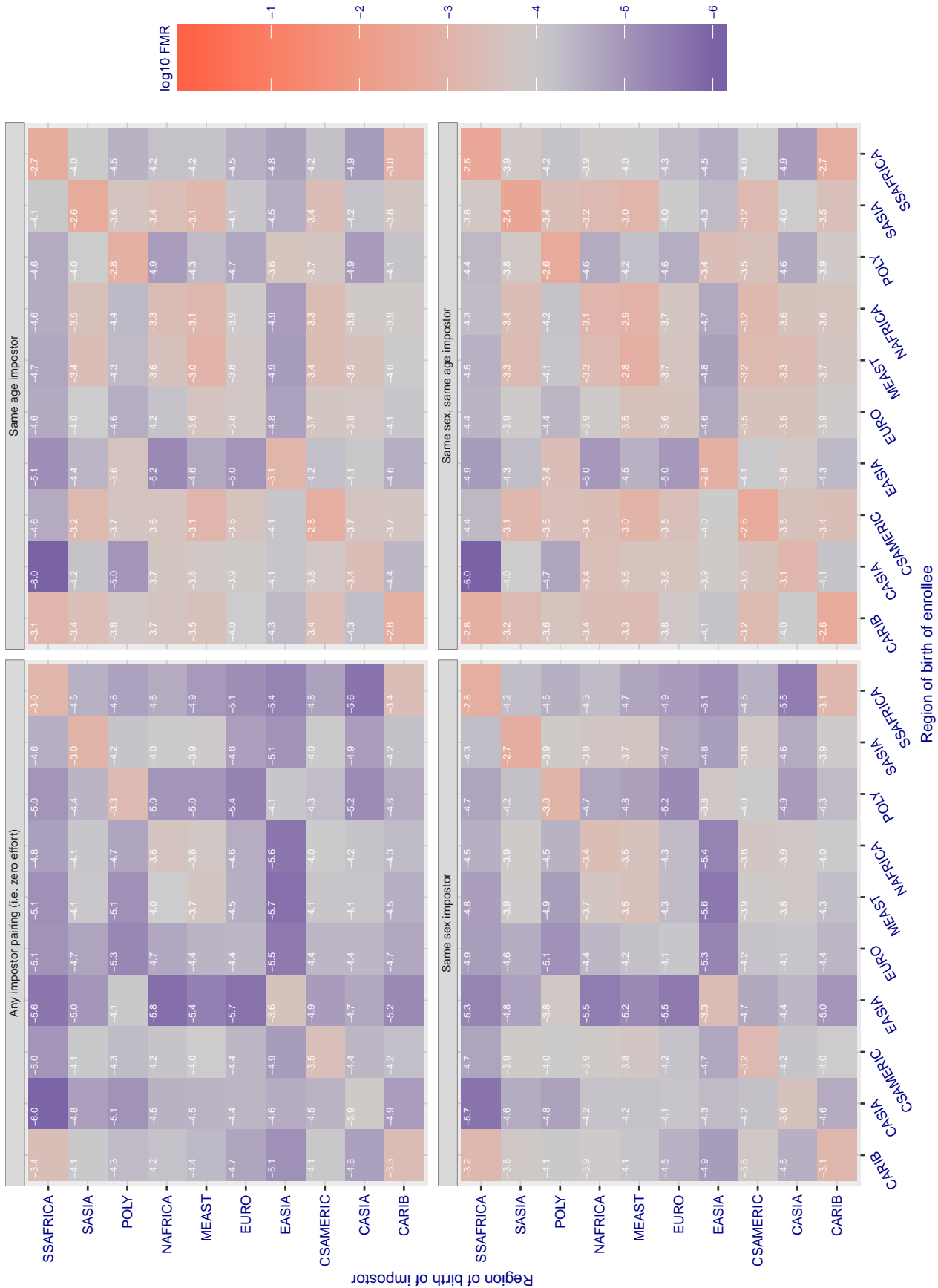


Figure 319: For algorithm vocord-006 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of 10<sup>10</sup> impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 995.241 for algorithm vocord\_007, giving FMR(T) = 0.0001 globally.

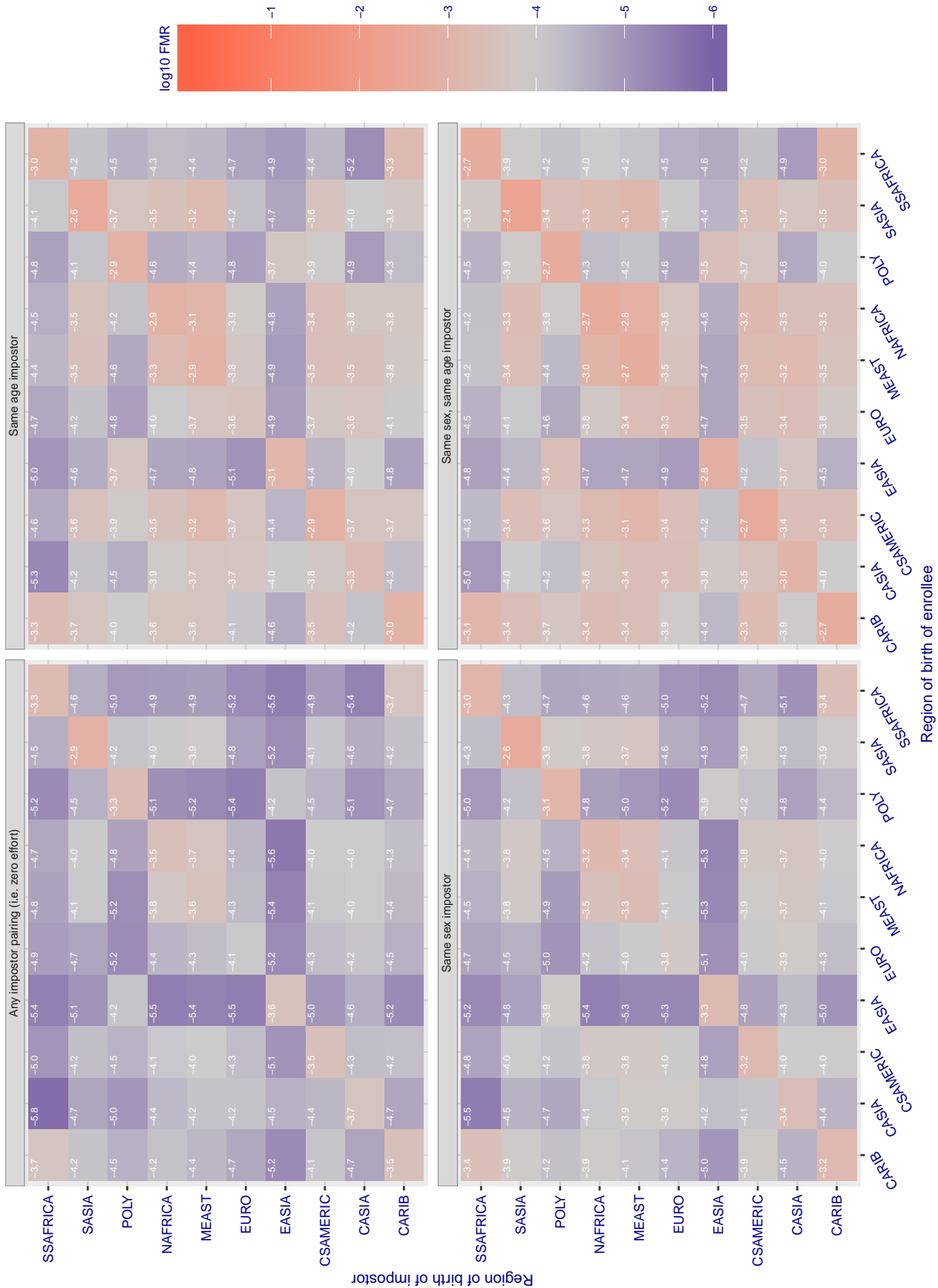


Figure 320: For algorithm vocord-007 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross region FMR at threshold T = 0.400 for algorithm winsense\_000, giving FMR(T) = 0.0001 globally.

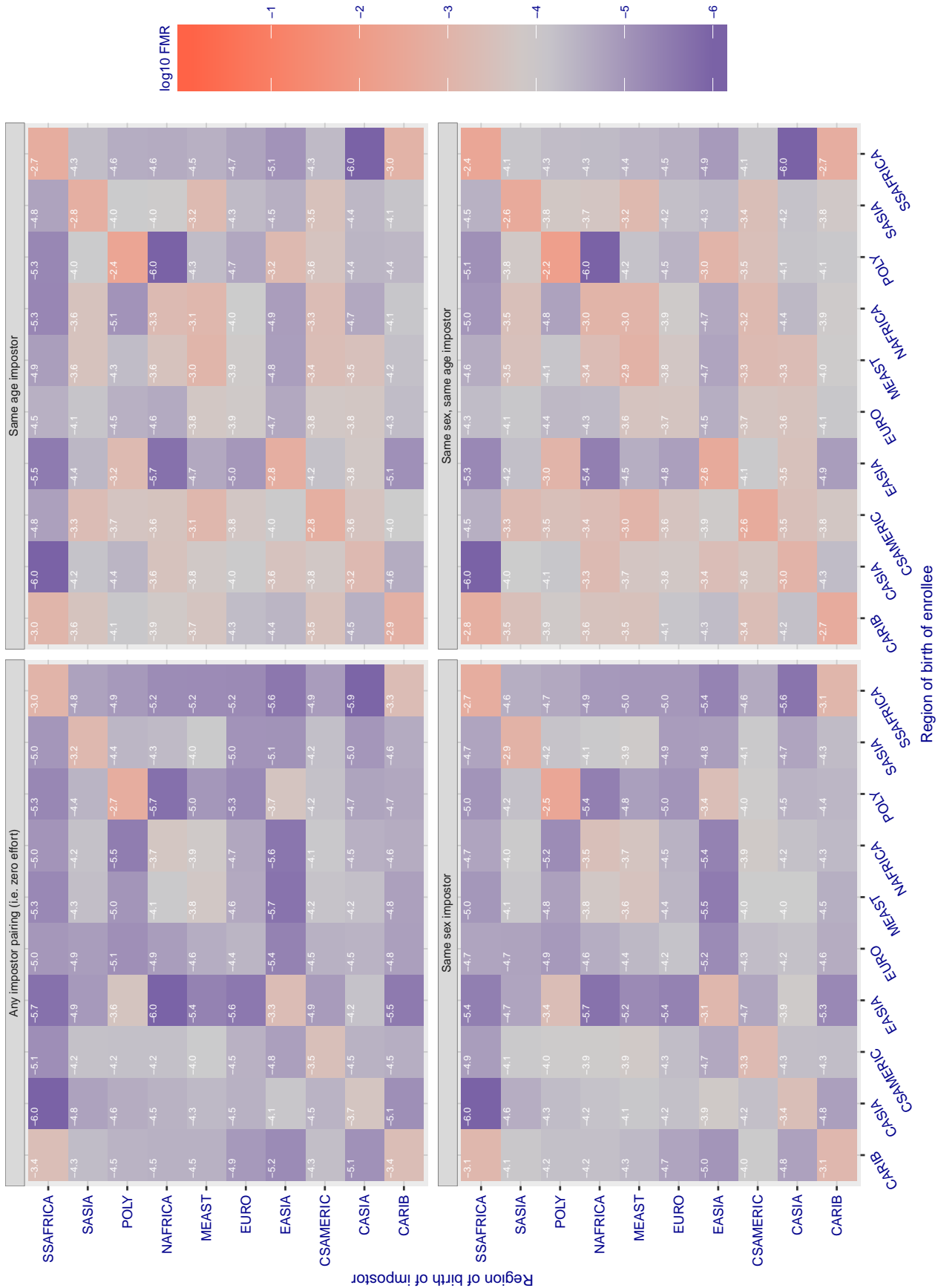


Figure 321: For algorithm winsense-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of 10<sup>10</sup> impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.322$  for algorithm winsense\_001, giving  $FMR(T) = 0.0001$  globally.

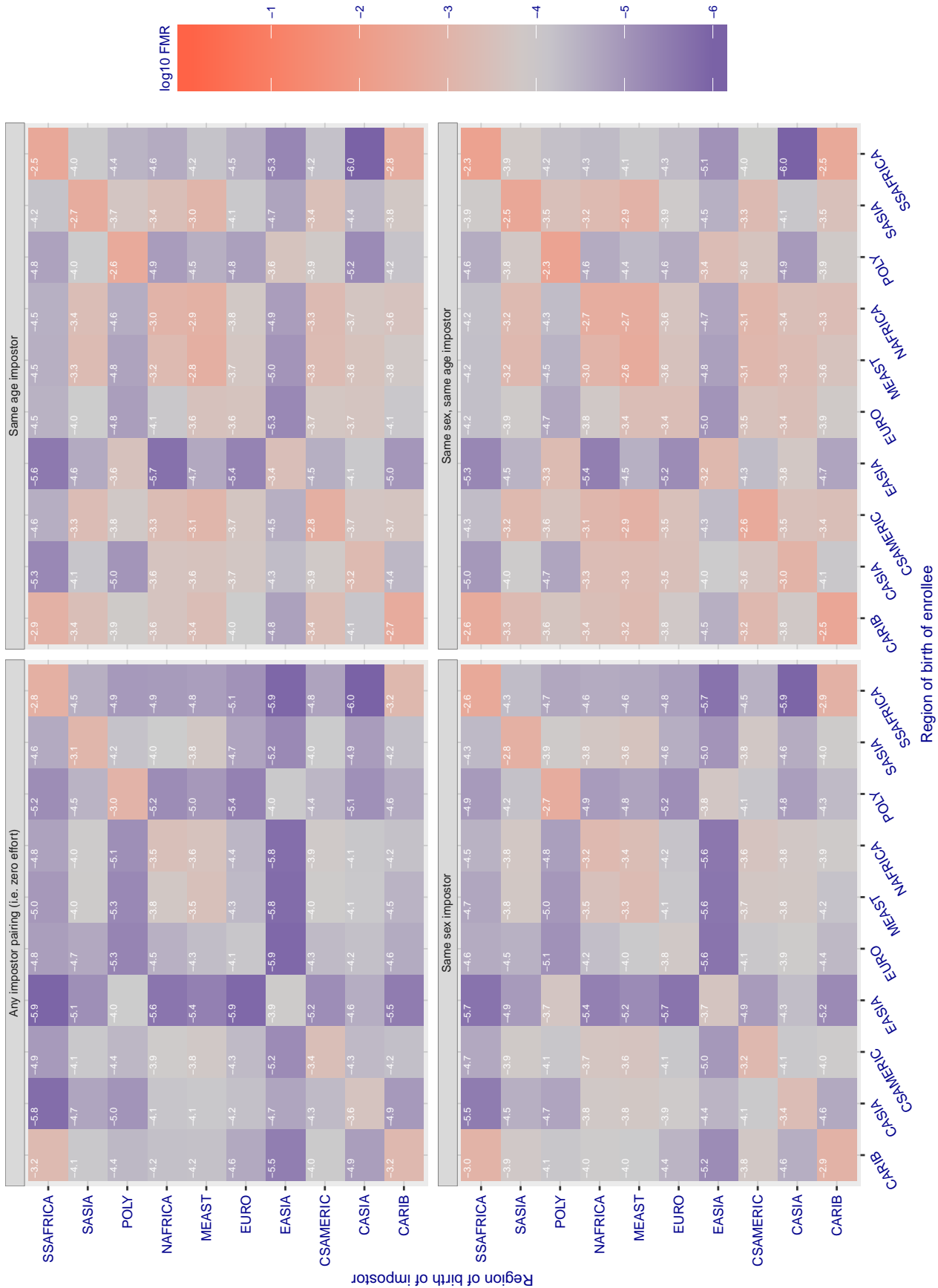


Figure 322: For algorithm winsense-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 0.404$  for algorithm  $x$ -laboratory\_000, giving  $FMR(T) = 0.0001$  globally.

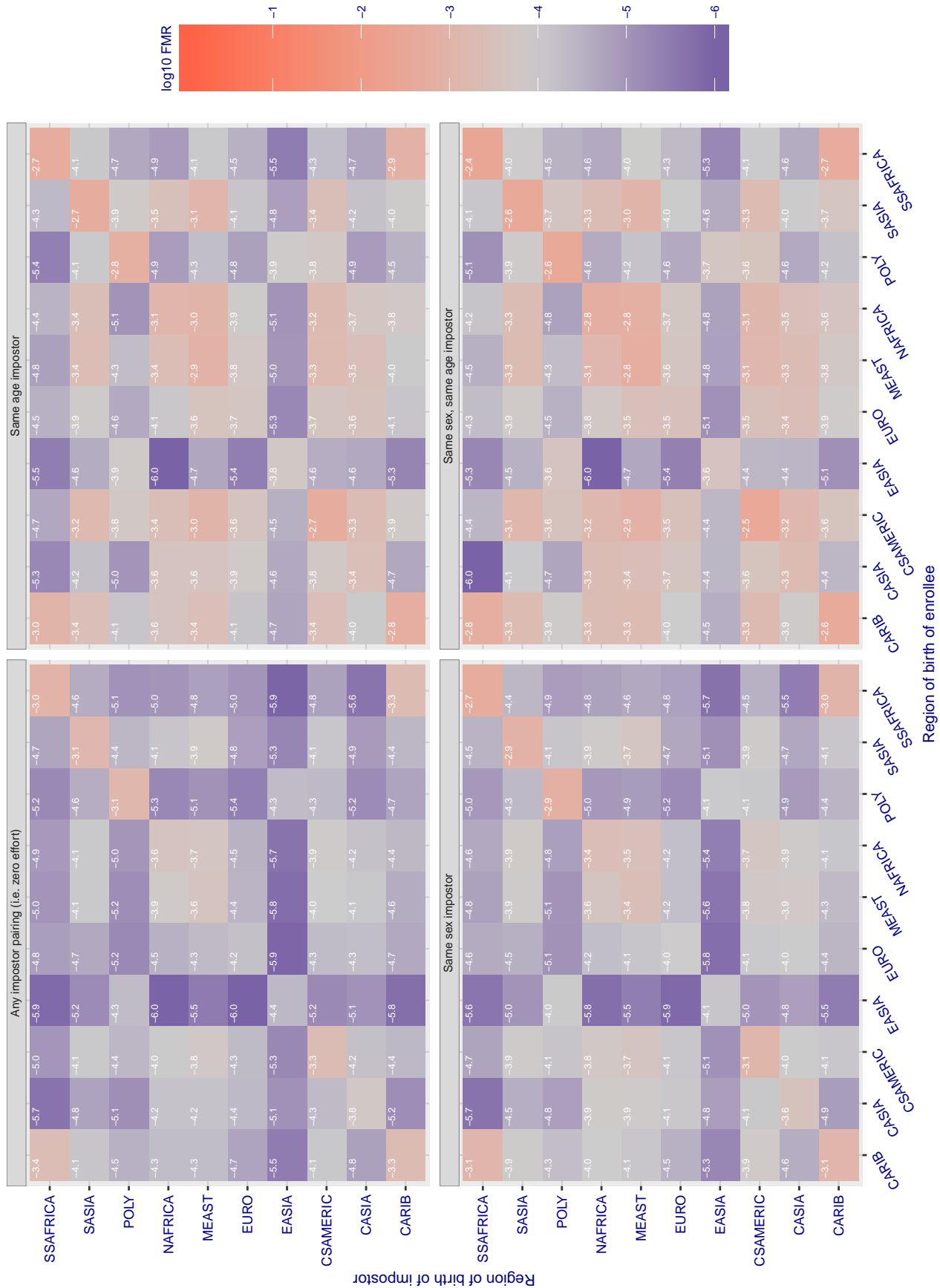


Figure 323: For algorithm  $x$ -laboratory-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold T = 5.544 for algorithm yisheng\_004, giving FMR(T) = 0.0001 globally.

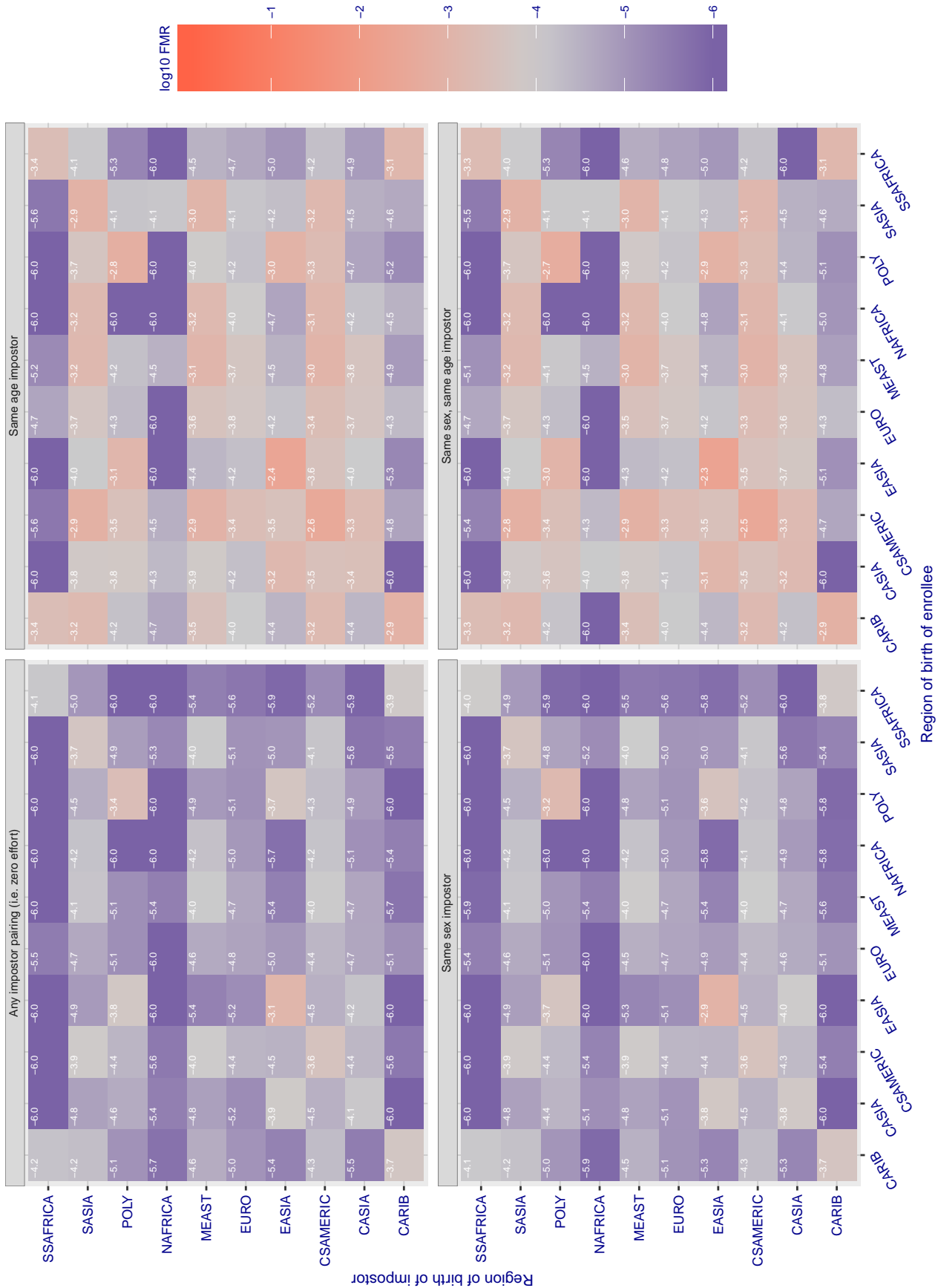


Figure 324: For algorithm yisheng-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold  $T = 37.698$  for algorithm yitu\_003, giving  $FMR(T) = 0.0001$  globally.

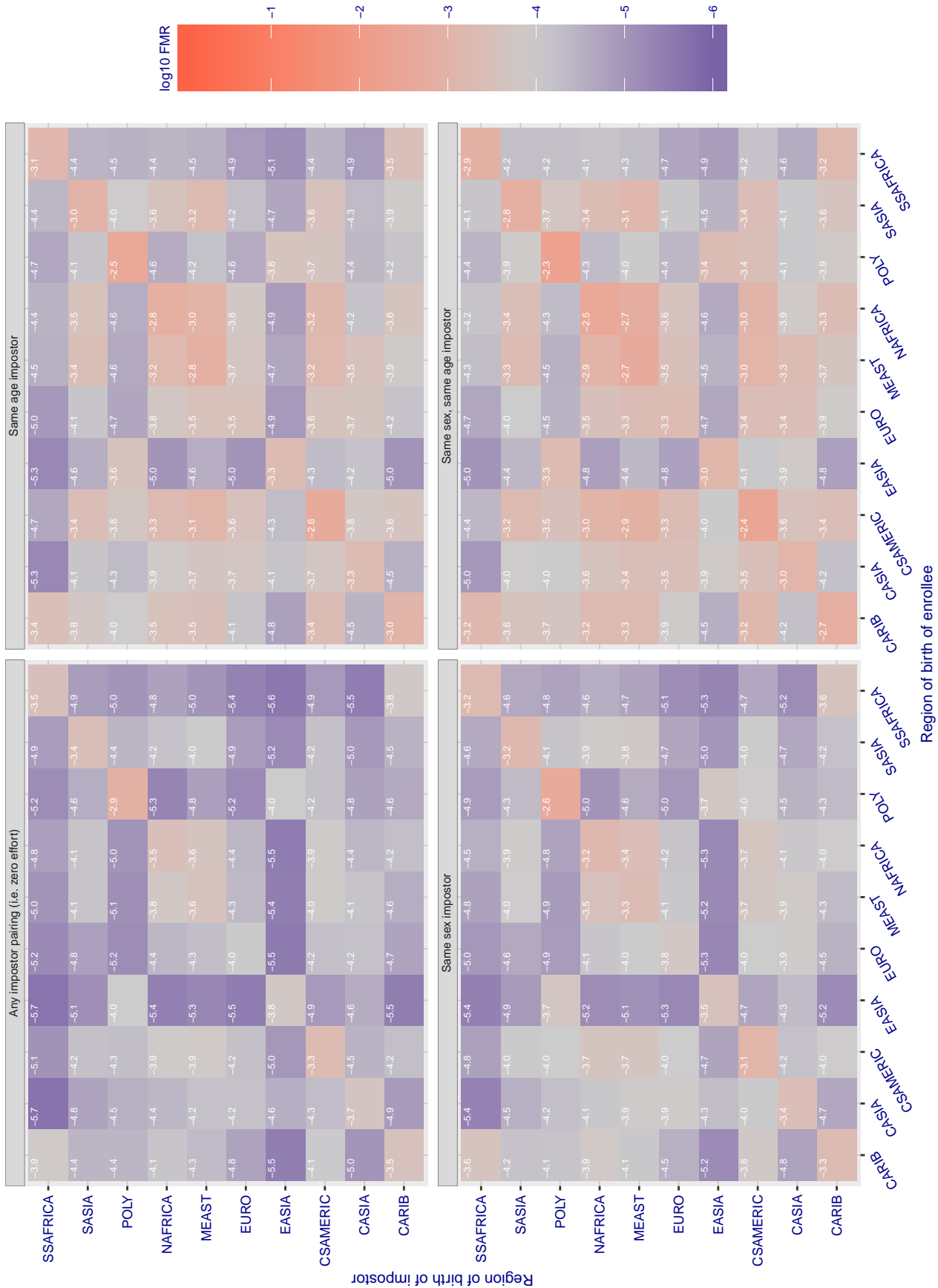


Figure 325: For algorithm yitu-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 2.575$  for algorithm 3divi\_003, giving  $FMR(T) = 0.001$  globally.

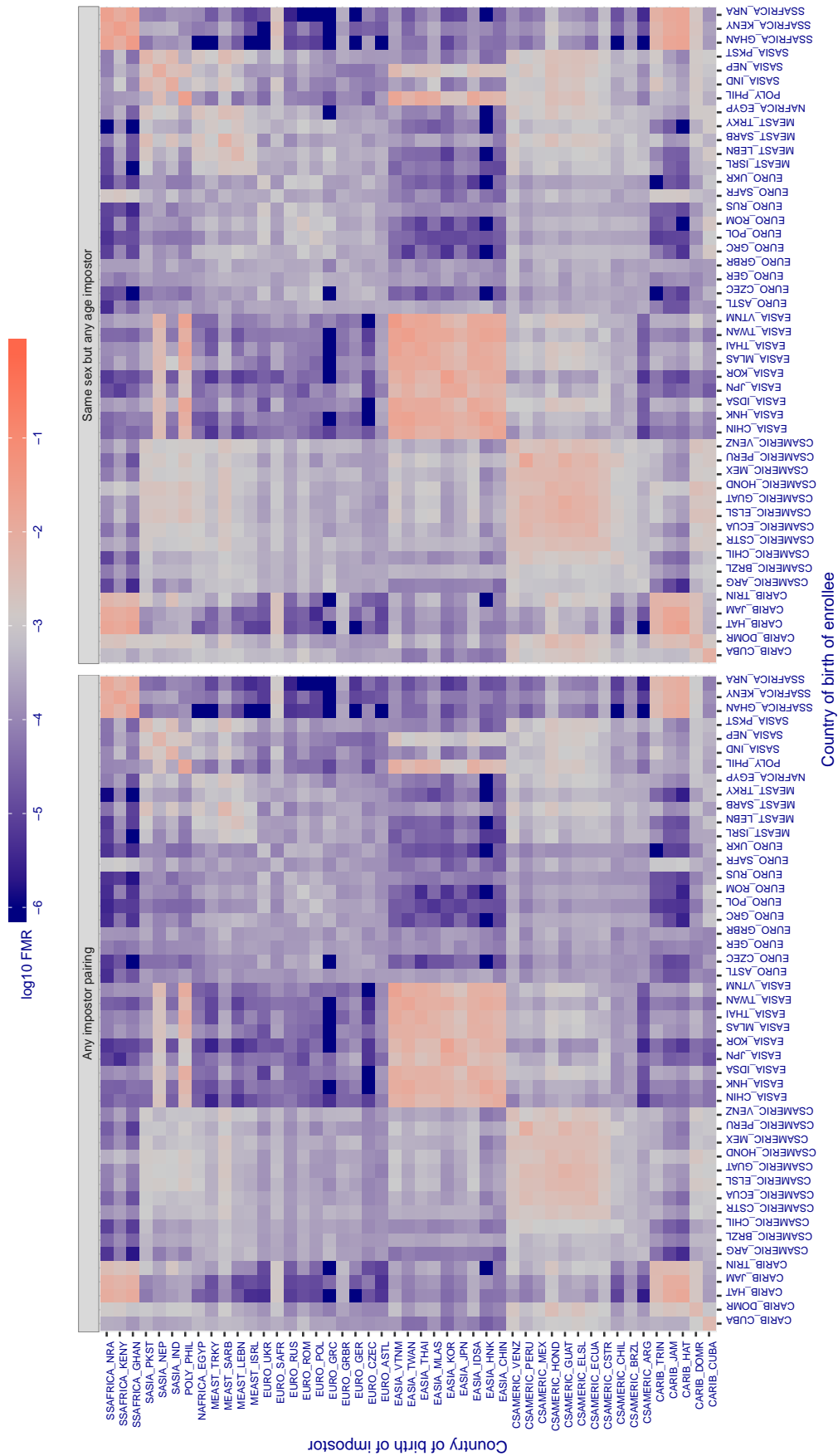


Figure 326: For algorithm 3divi-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 2.692$  for algorithm 3divi\_004, giving  $FMR(T) = 0.001$  globally.

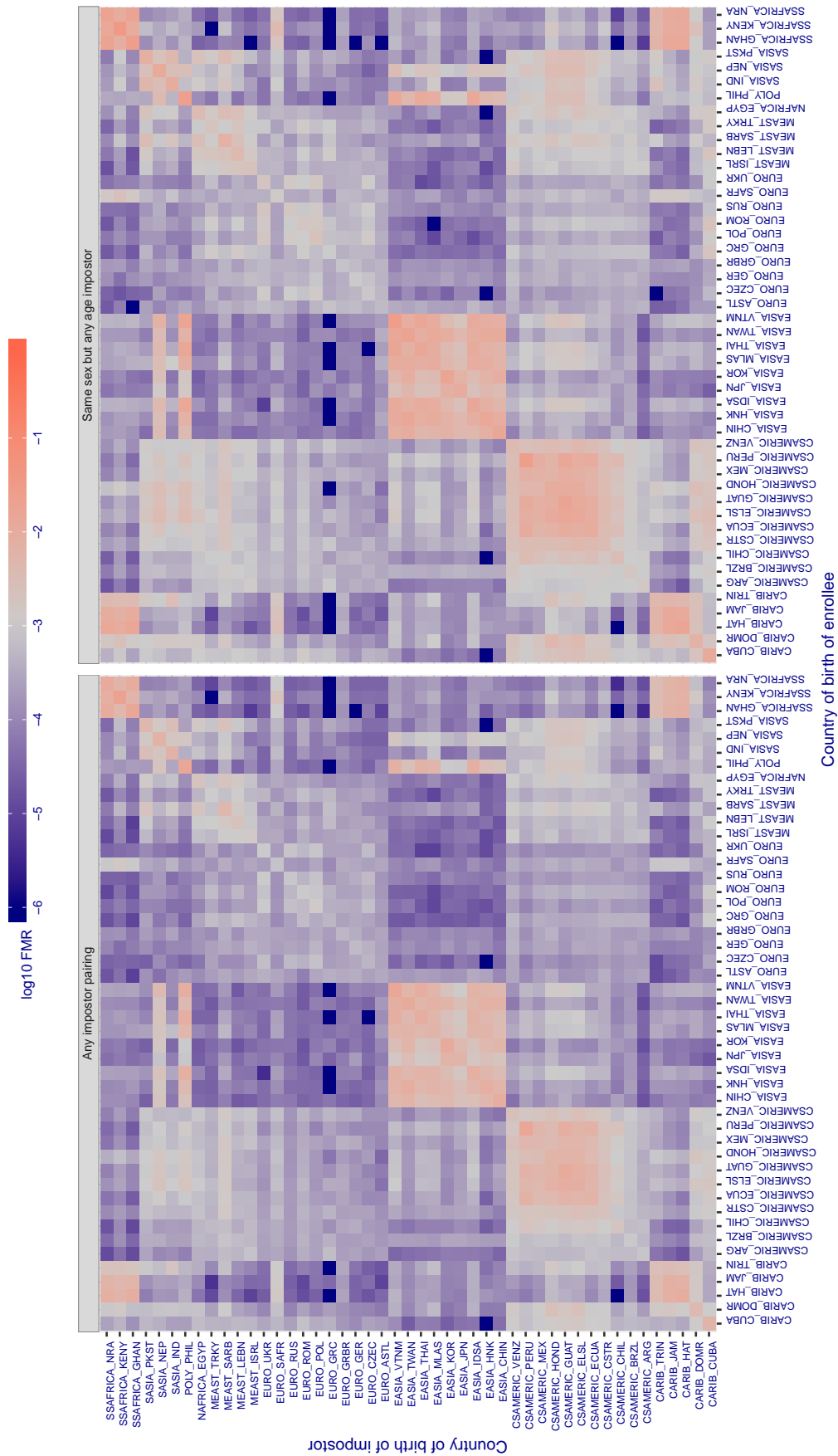


Figure 327: For algorithm 3divi-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.632$  for algorithm `adera_001`, giving  $FMR(T) = 0.001$  globally.

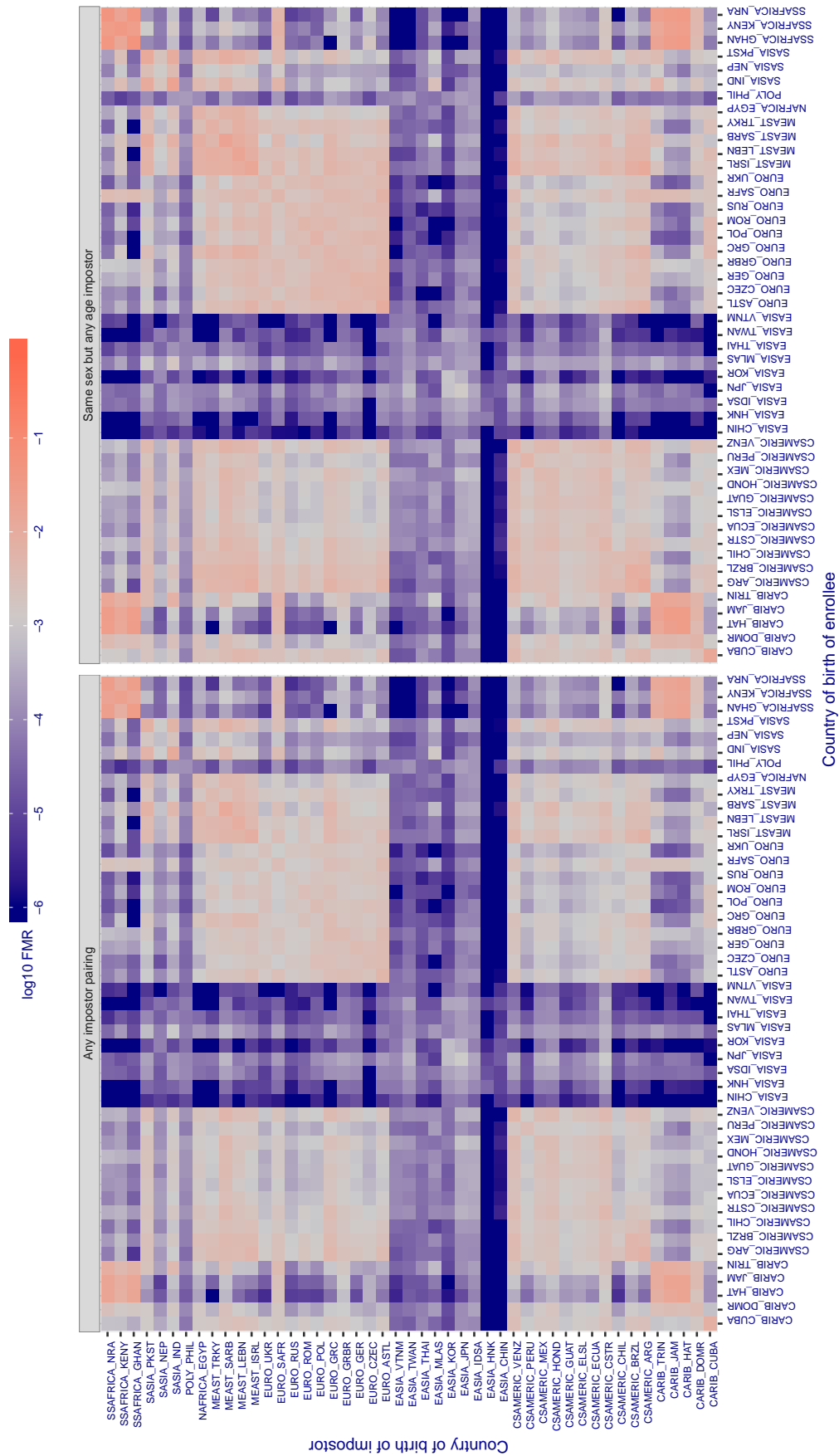


Figure 328: For algorithm `adera-001` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each  $+1$  increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 0.469$  for algorithm aimall\_001, giving  $FMR(T) = 0.001$  globally.

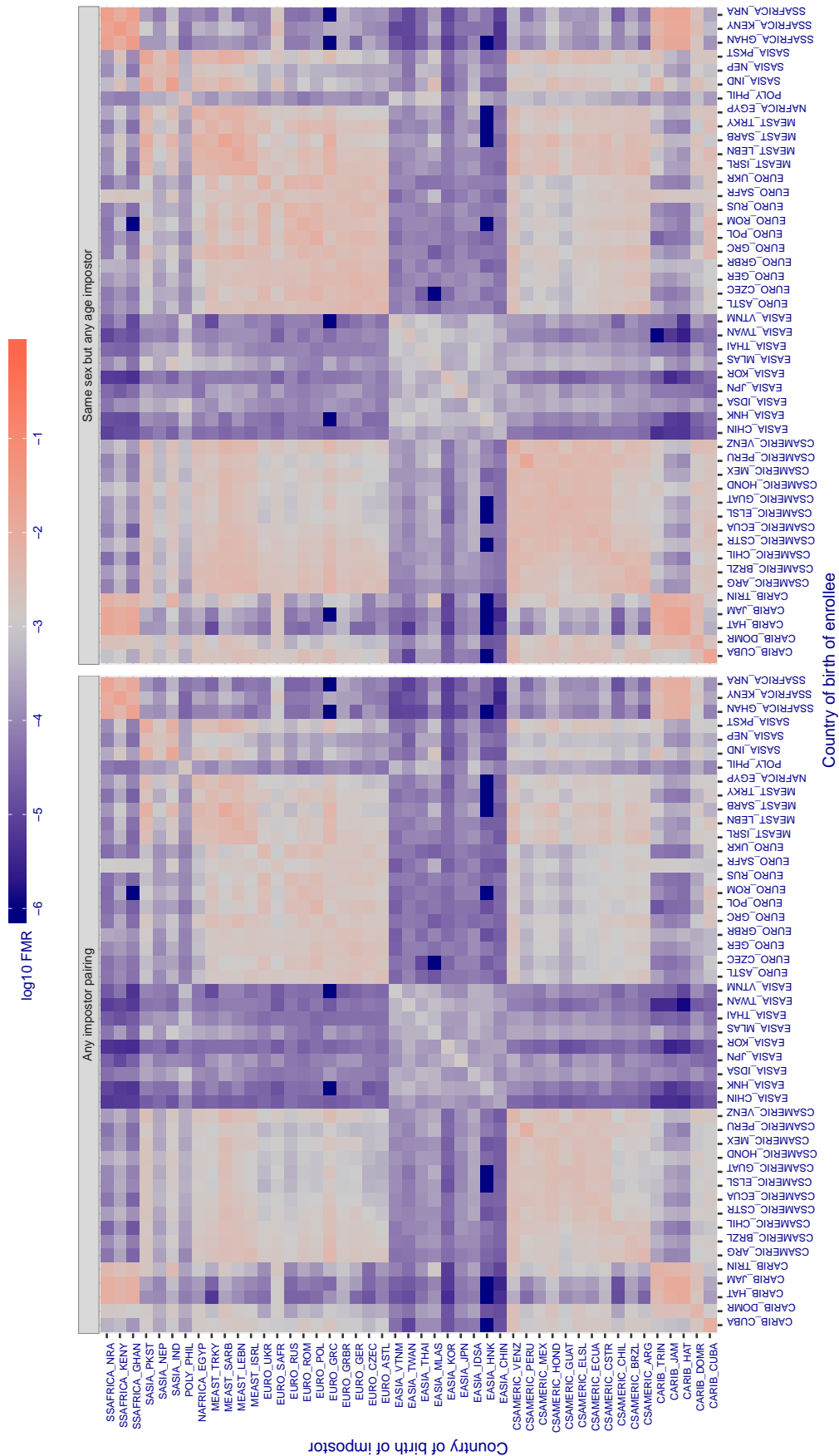


Figure 329: For algorithm aimall-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.659$  for algorithm aiunionface\_000, giving  $FMR(T) = 0.001$  globally.

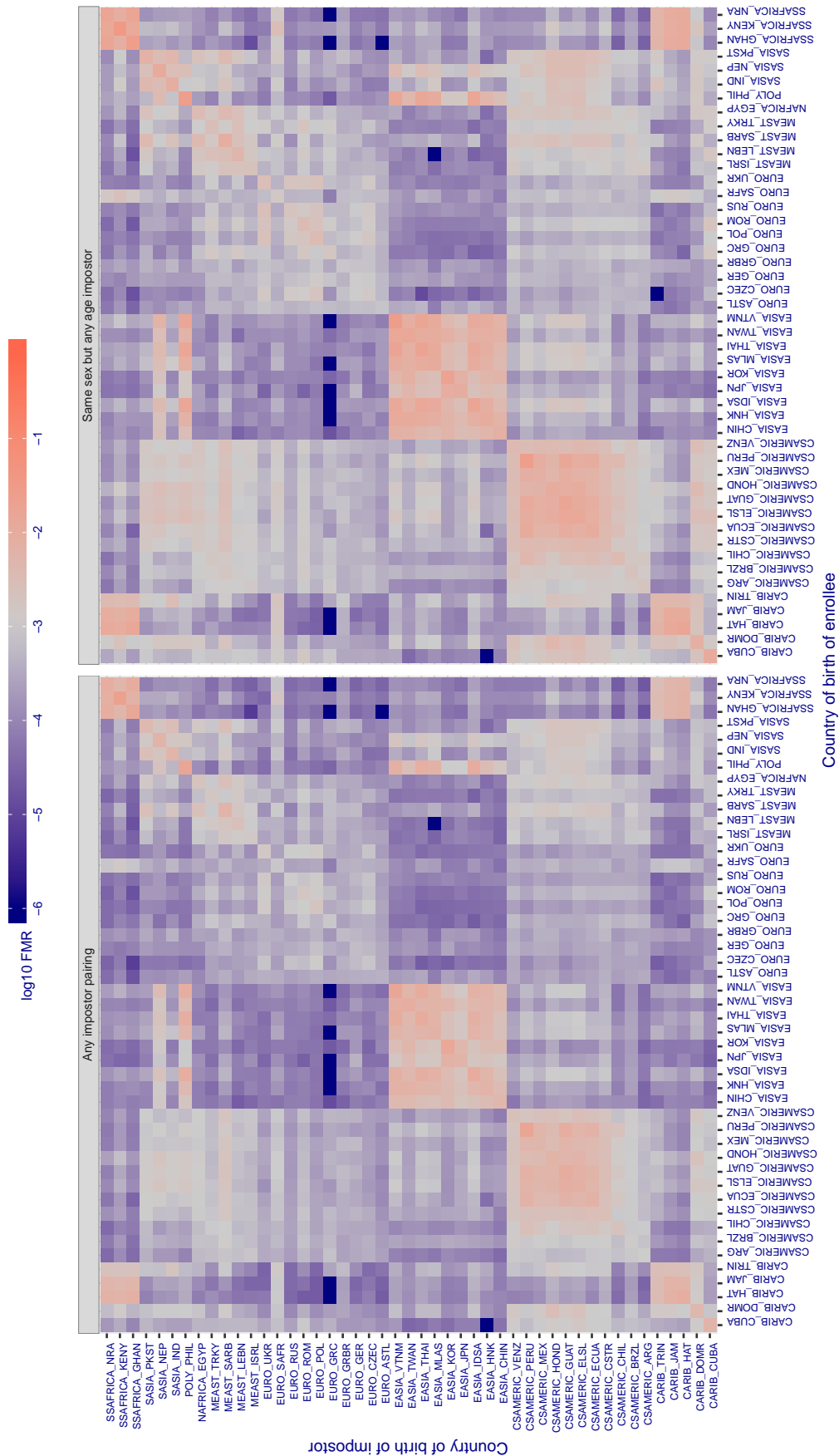


Figure 330: For algorithm aiunionface-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.662$  for algorithm alchera\_000, giving  $FMR(T) = 0.001$  globally.

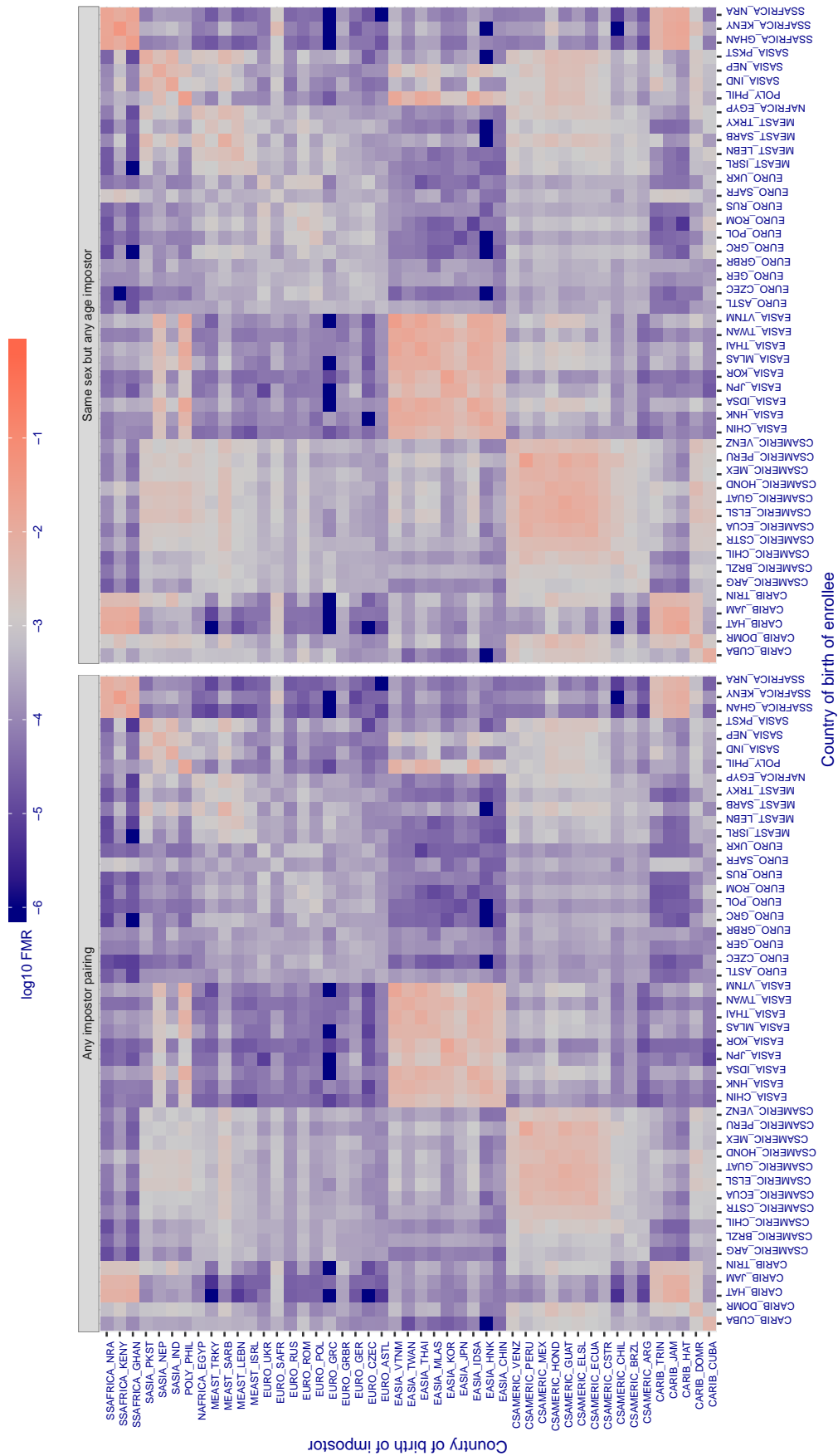


Figure 331: For algorithm alchera-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.667$  for algorithm alchera\_001, giving  $FMR(T) = 0.001$  globally.

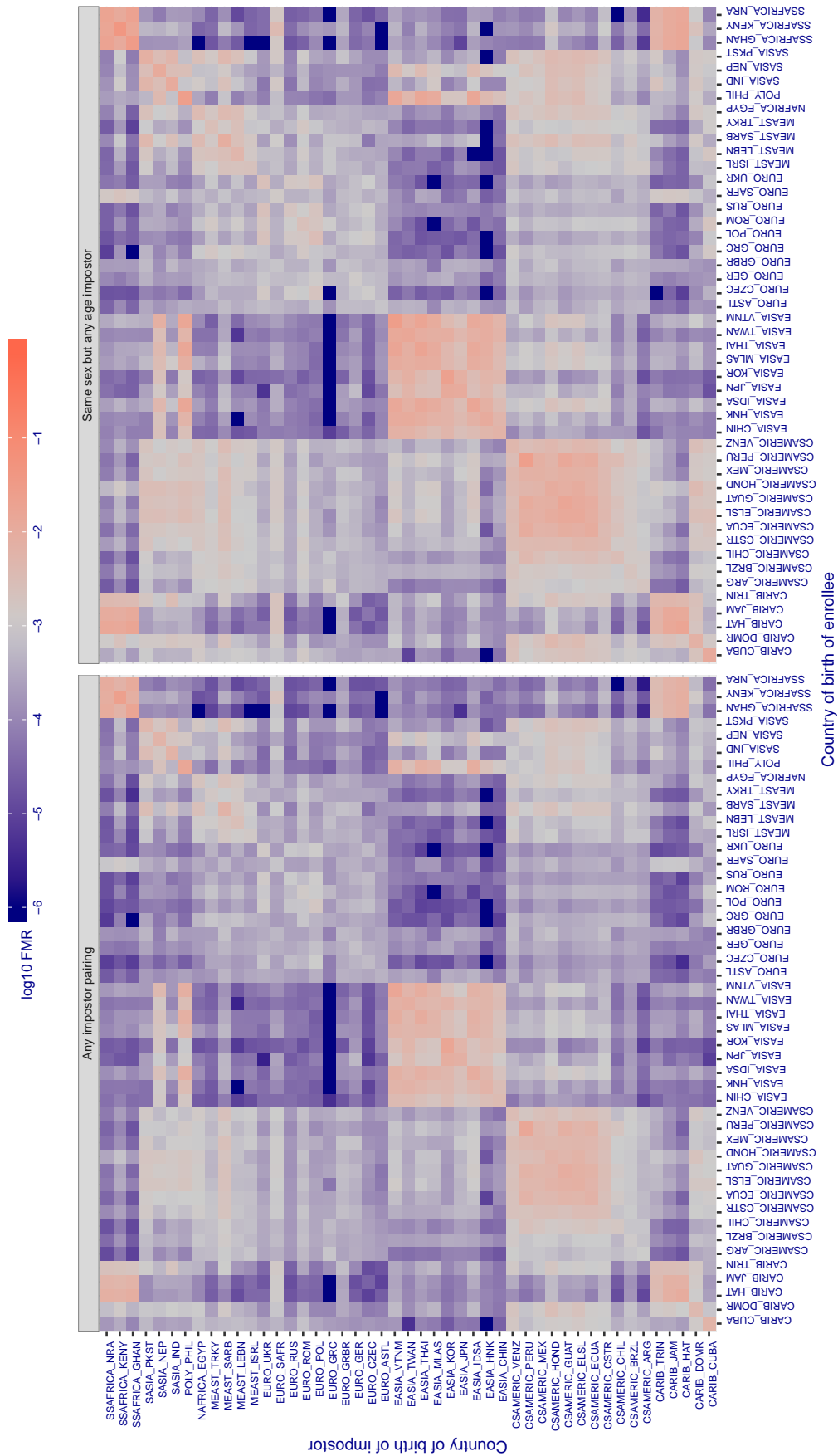


Figure 332: For algorithm alchera-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.339$  for algorithm `allgovision_000`, giving  $FMR(T) = 0.001$  globally.

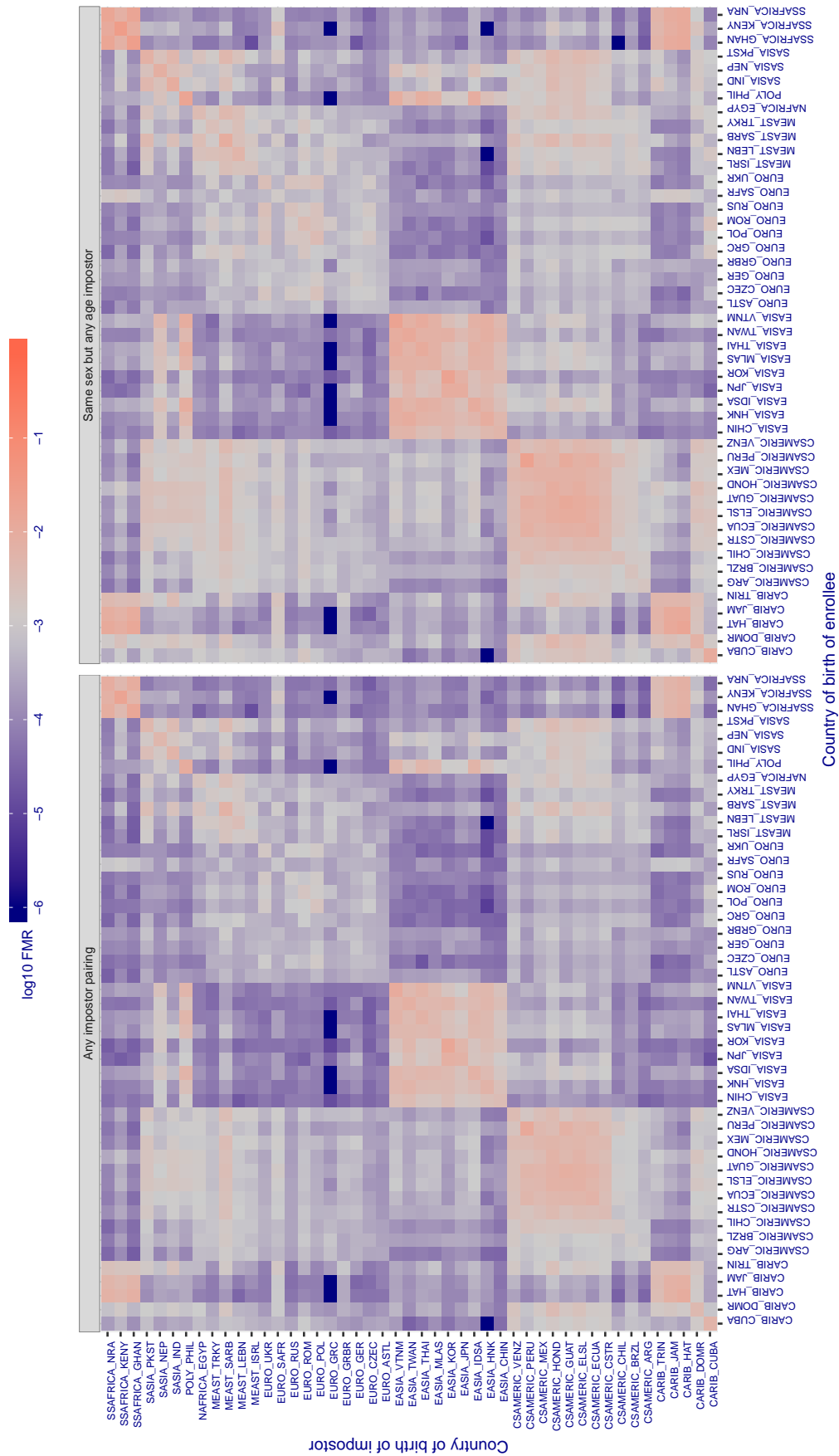


Figure 333: For algorithm `allgovision-000` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.313$  for algorithm  $\alpha\text{face}_{001}$ , giving  $\text{FMR}(T) = 0.001$  globally.

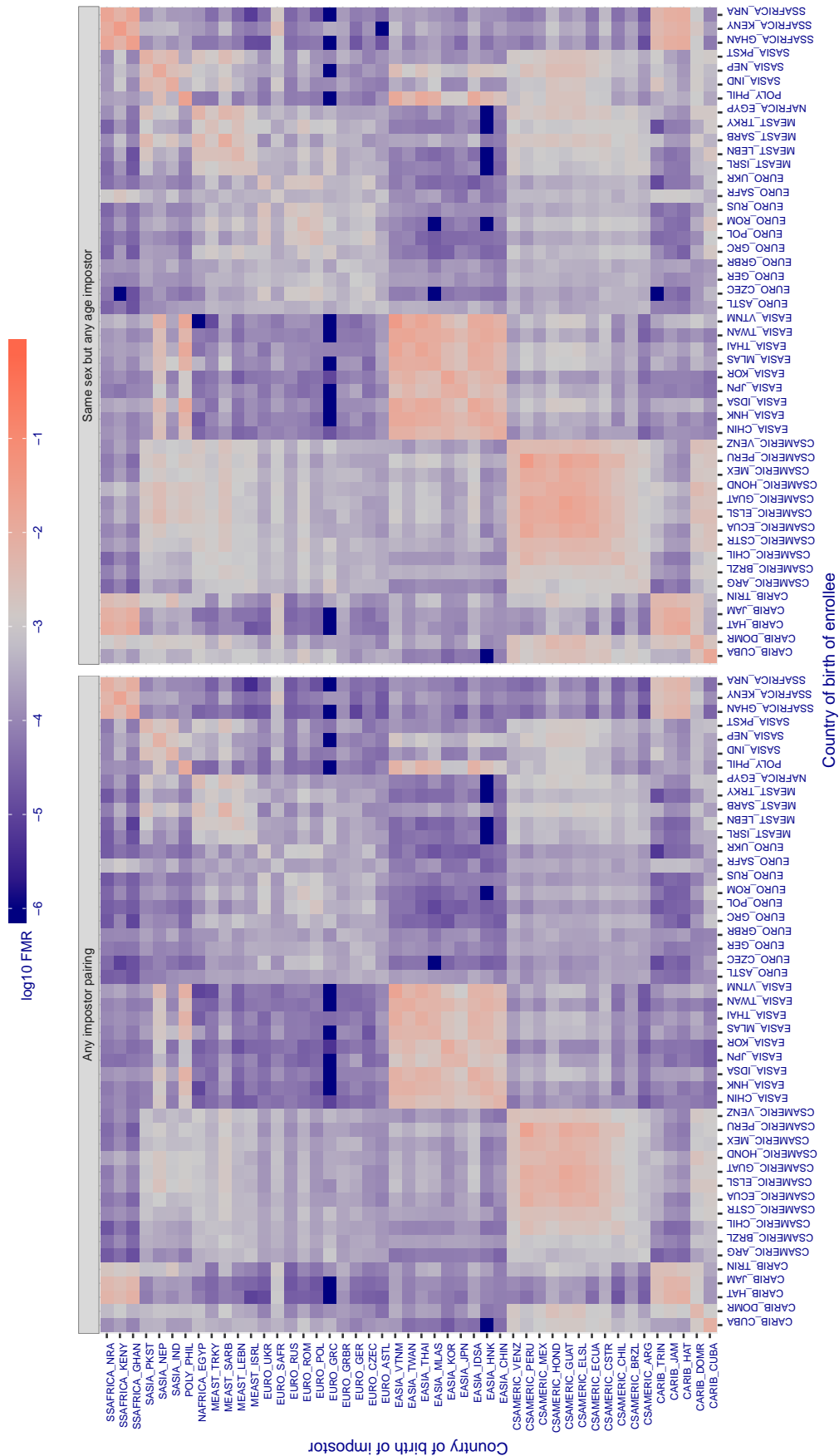


Figure 334: For algorithm  $\alpha\text{face}_{001}$  operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} \text{FMR}$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 3.524$  for algorithm amplifiedgroup\_001, giving  $FMR(T) = 0.001$  globally.

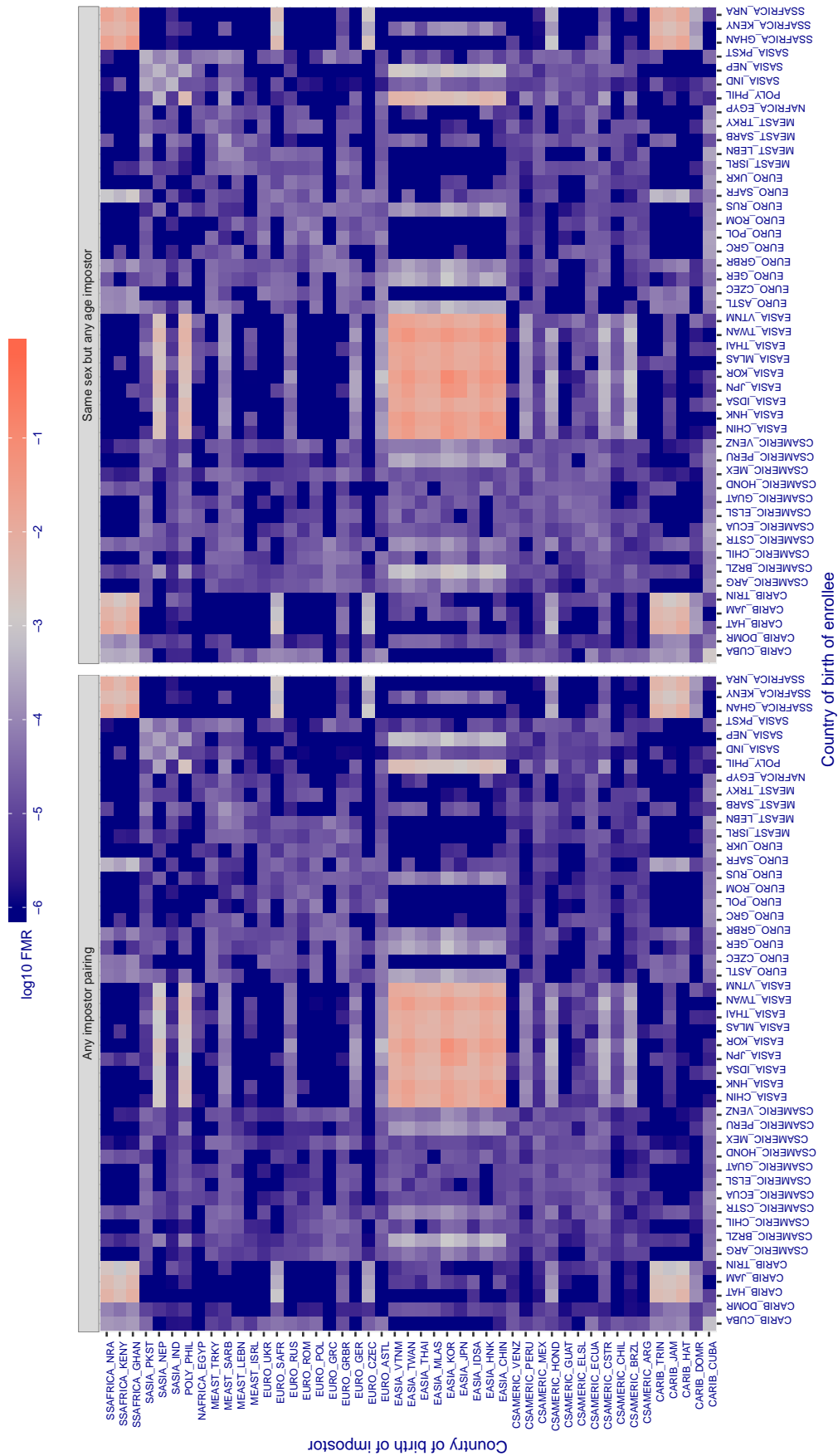


Figure 335: For algorithm amplifiedgroup-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 0.313$  for algorithm anke\_003, giving  $FMR(T) = 0.001$  globally.

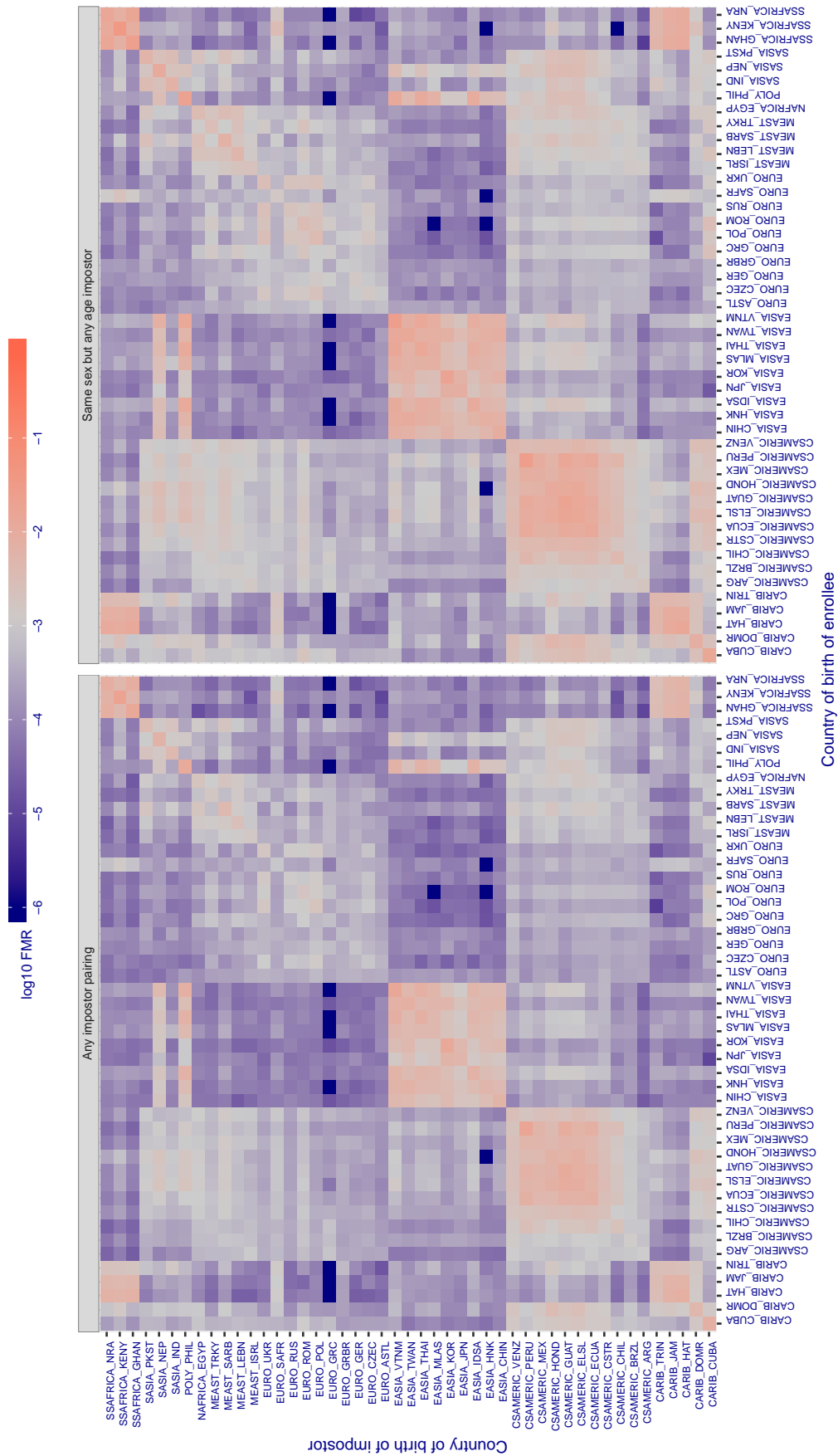


Figure 336: For algorithm anke-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 0.309$  for algorithm anke\_004, giving  $FMR(T) = 0.001$  globally.

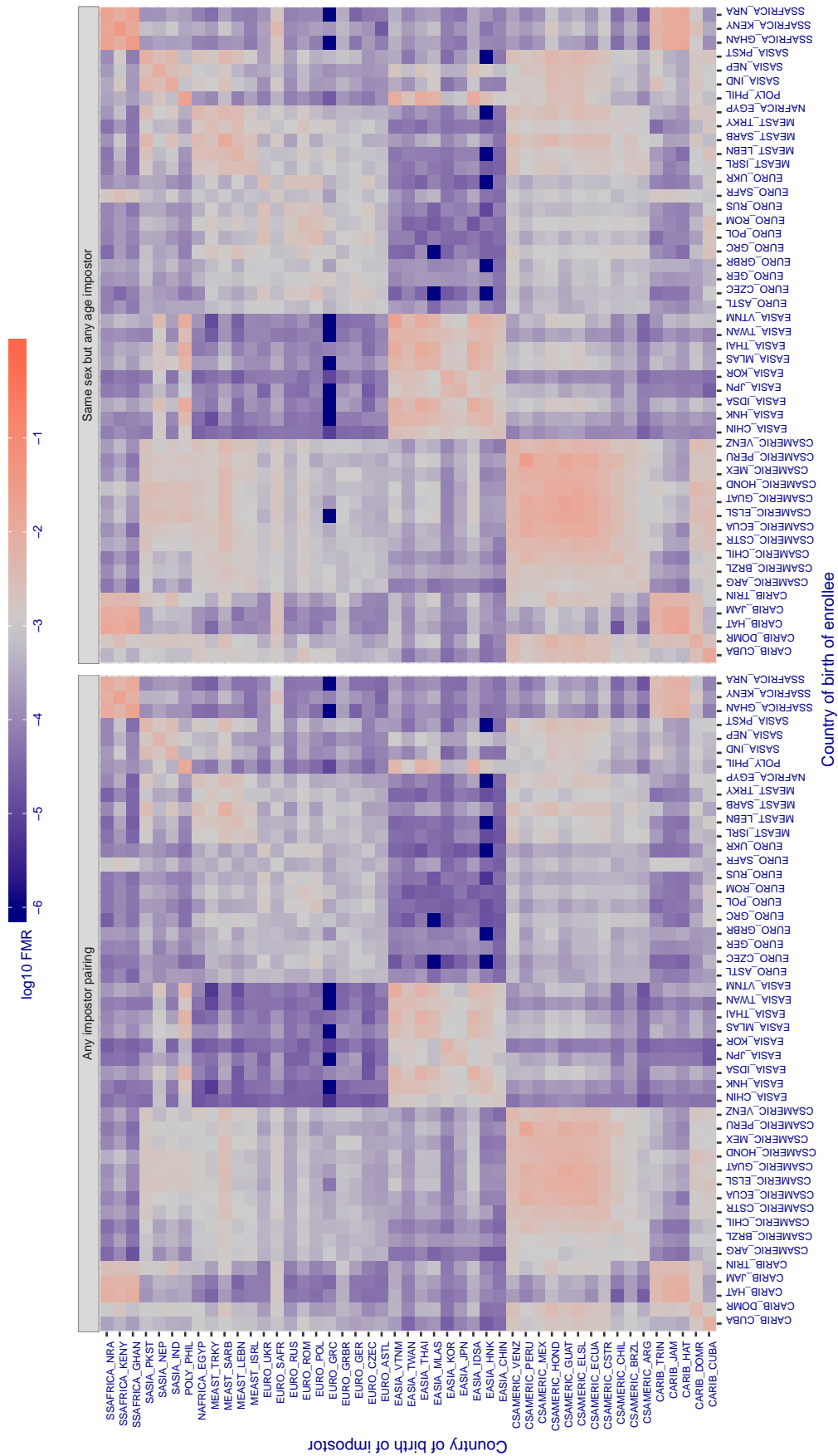


Figure 337: For algorithm anke-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 1.431$  for algorithm anyvision\_002, giving  $FMR(T) = 0.001$  globally.

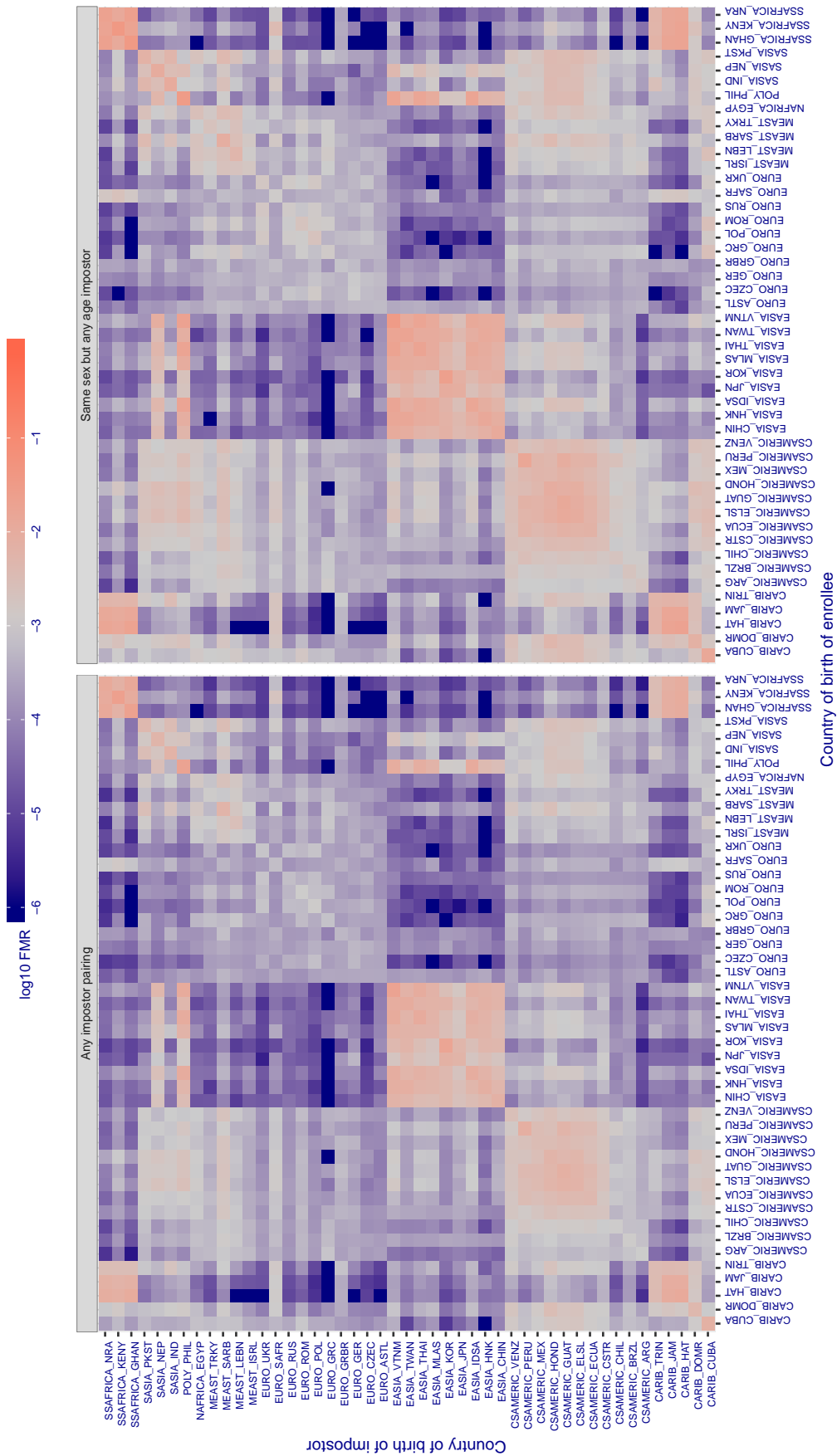


Figure 338: For algorithm anyvision-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 1.297$  for algorithm anyvision\_004, giving  $FMR(T) = 0.001$  globally.

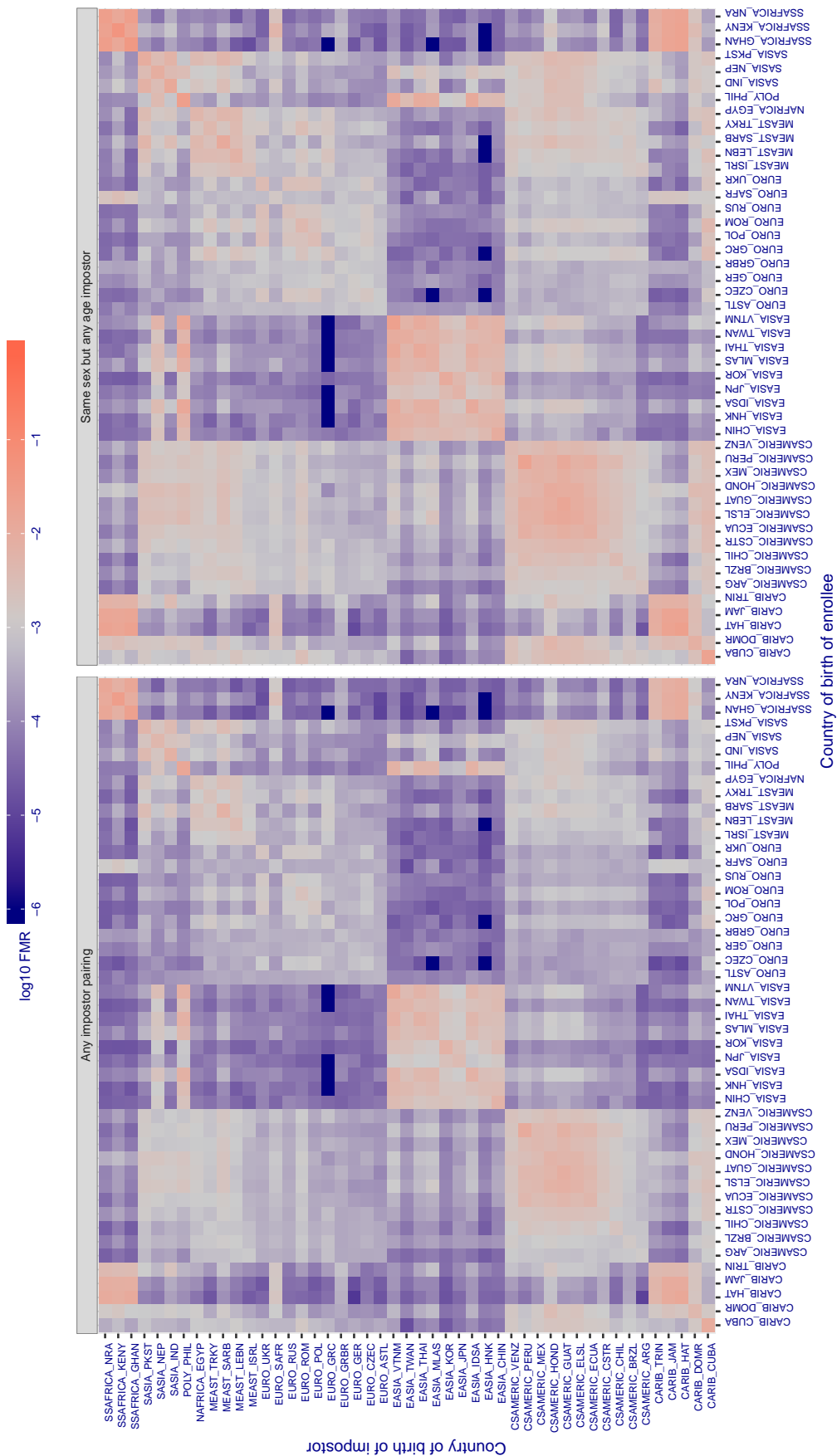


Figure 339: For algorithm anyvision-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 1.299$  for algorithm asusaics\_000, giving  $FMR(T) = 0.001$  globally.

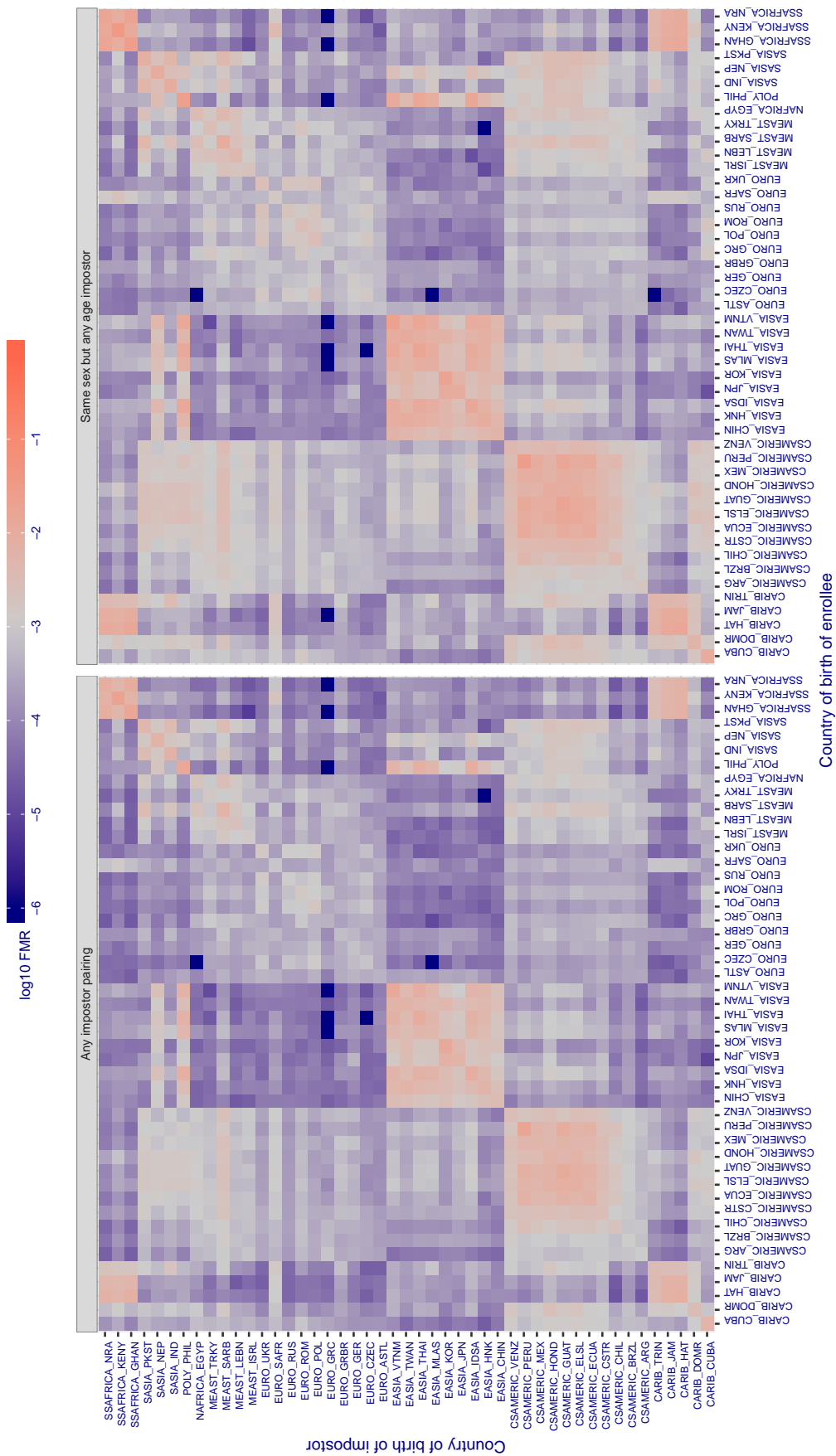


Figure 340: For algorithm asusaics-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 2.758$  for algorithm aware\_003, giving  $FMR(T) = 0.001$  globally.

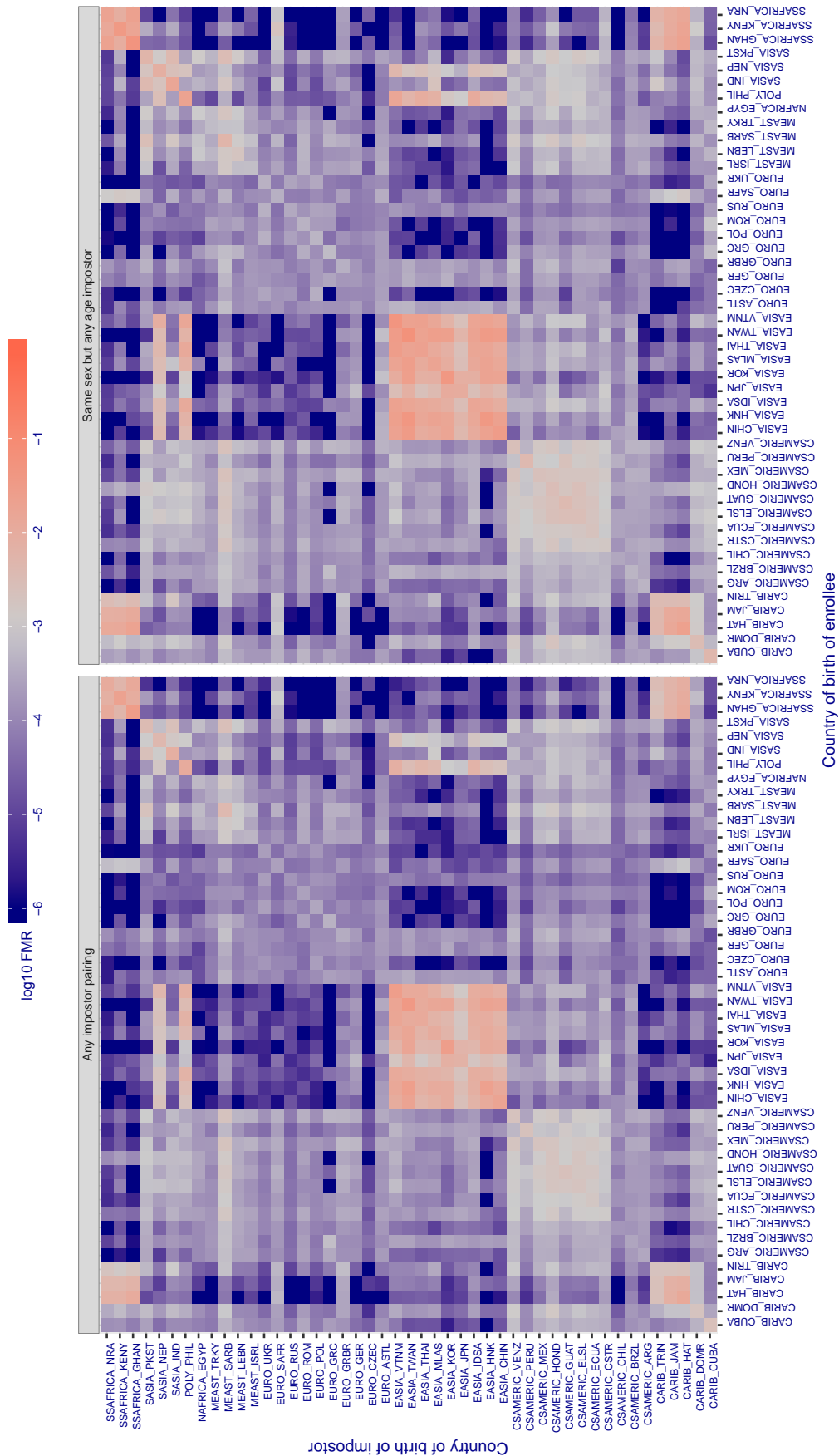


Figure 341: For algorithm aware-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 3.681$  for algorithm aware\_004, giving  $FMR(T) = 0.001$  globally.

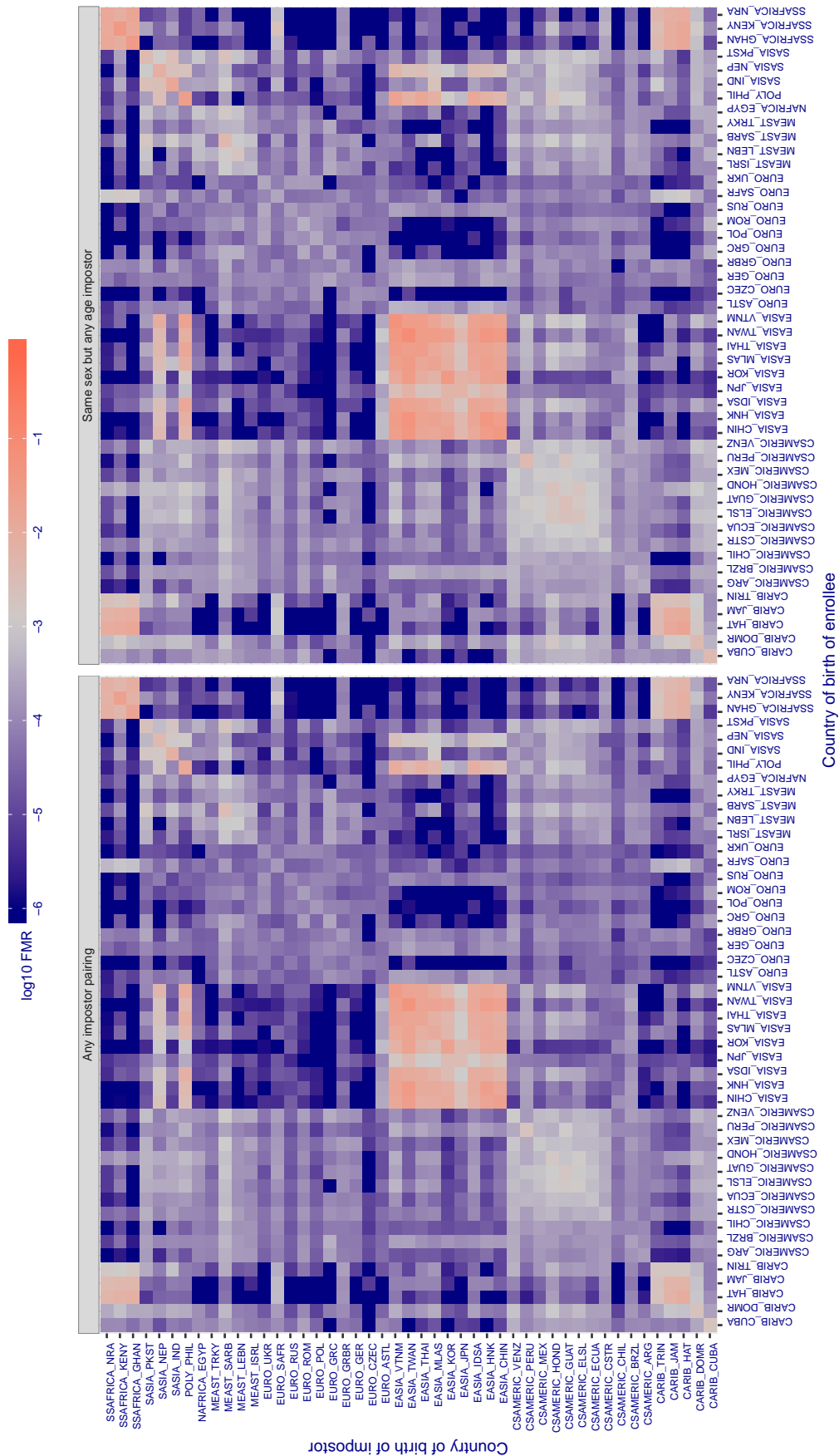


Figure 342: For algorithm aware-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.790$  for algorithm awiros\_001, giving  $FMR(T) = 0.001$  globally.

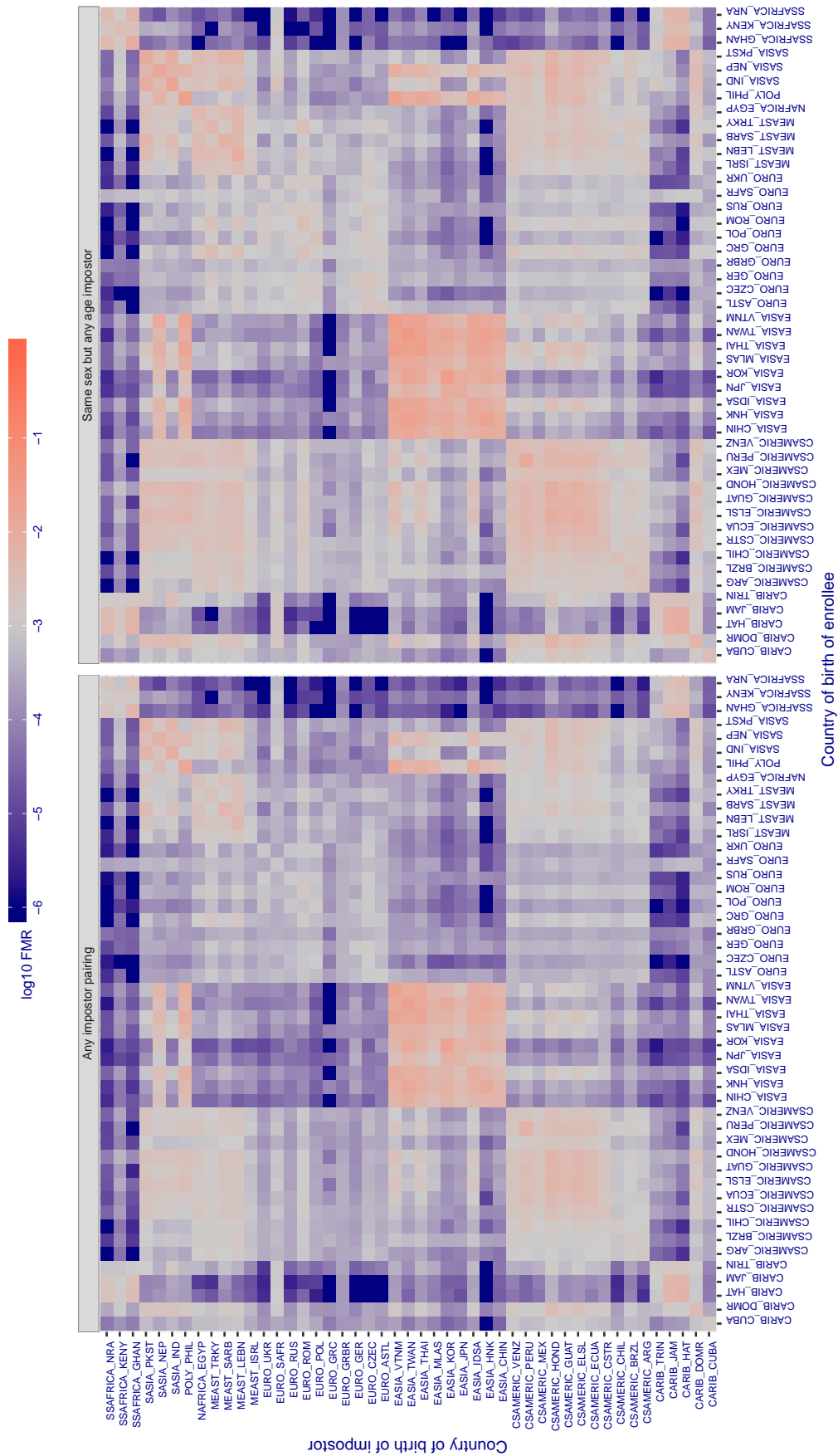


Figure 343: For algorithm awiros-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 0.800$  for algorithm ayonix\_000, giving  $FMR(T) = 0.001$  globally.

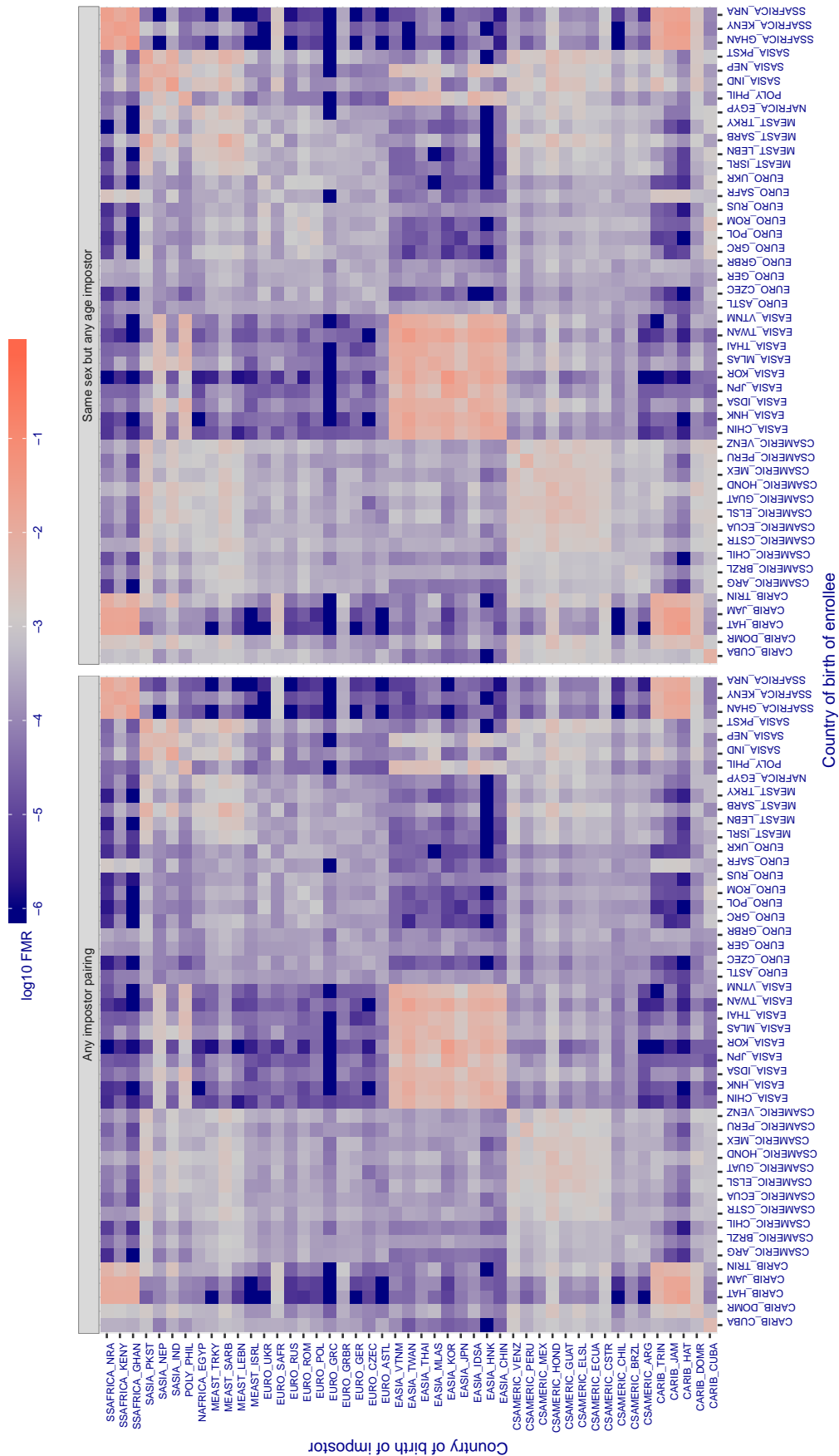


Figure 344: For algorithm ayonix-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 0.649$  for algorithm `bm_001`, giving  $FMR(T) = 0.001$  globally.

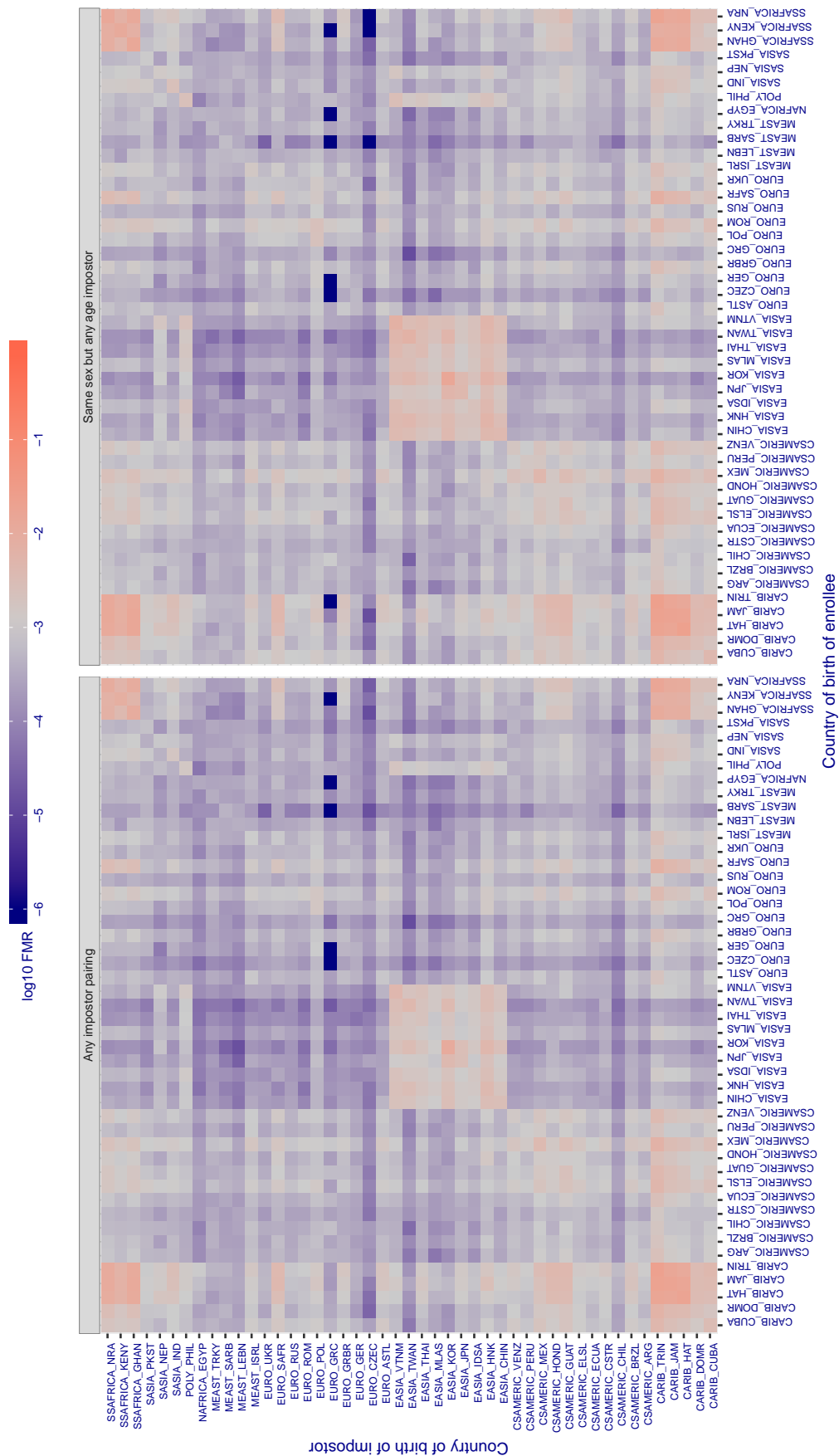


Figure 345: For algorithm `bm-001` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each  $+1$  increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.306$  for algorithm camvi\_002, giving  $FMR(T) = 0.001$  globally.

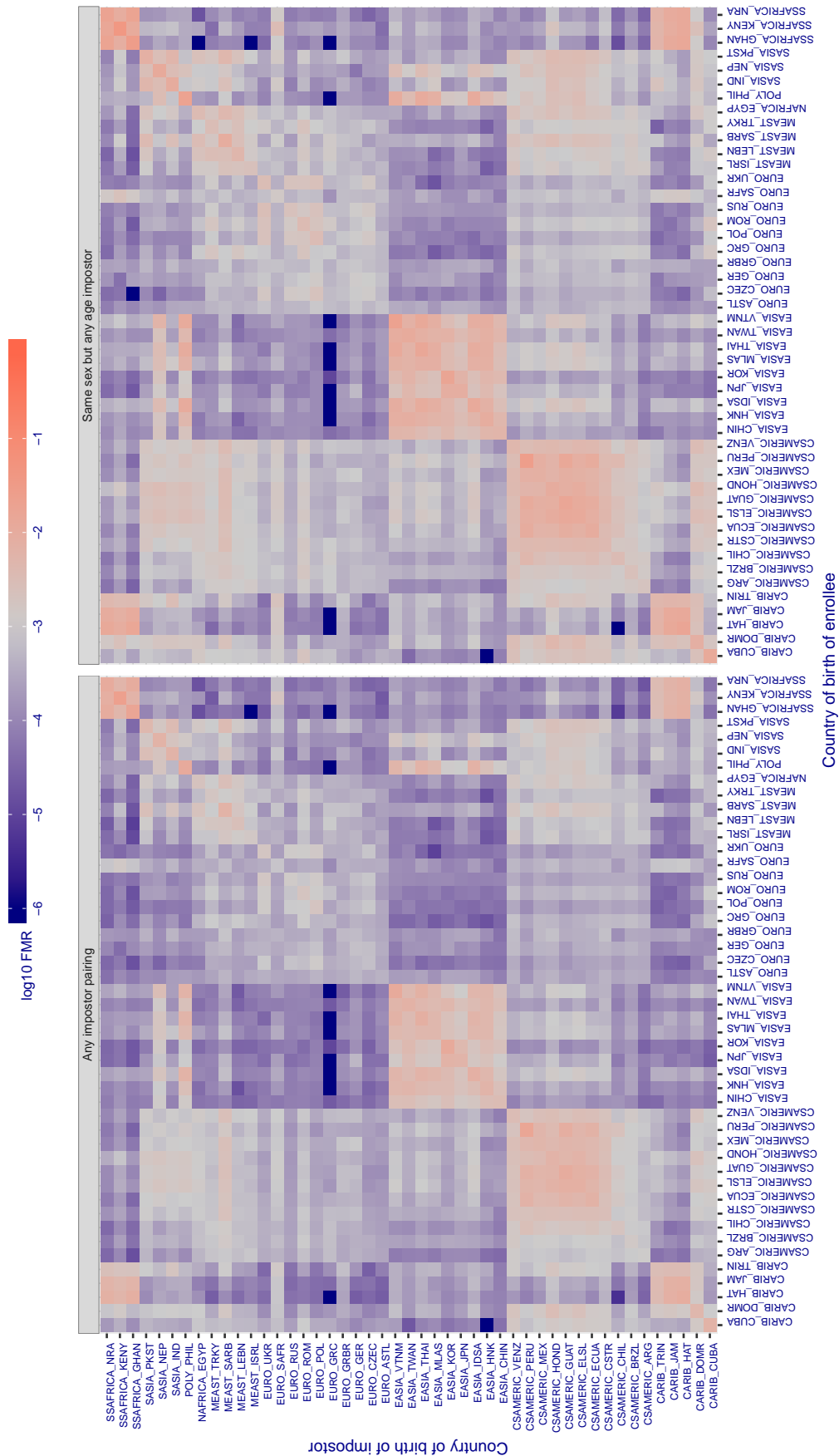


Figure 346: For algorithm camvi-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.272$  for algorithm camvi\_004, giving  $FMR(T) = 0.001$  globally.

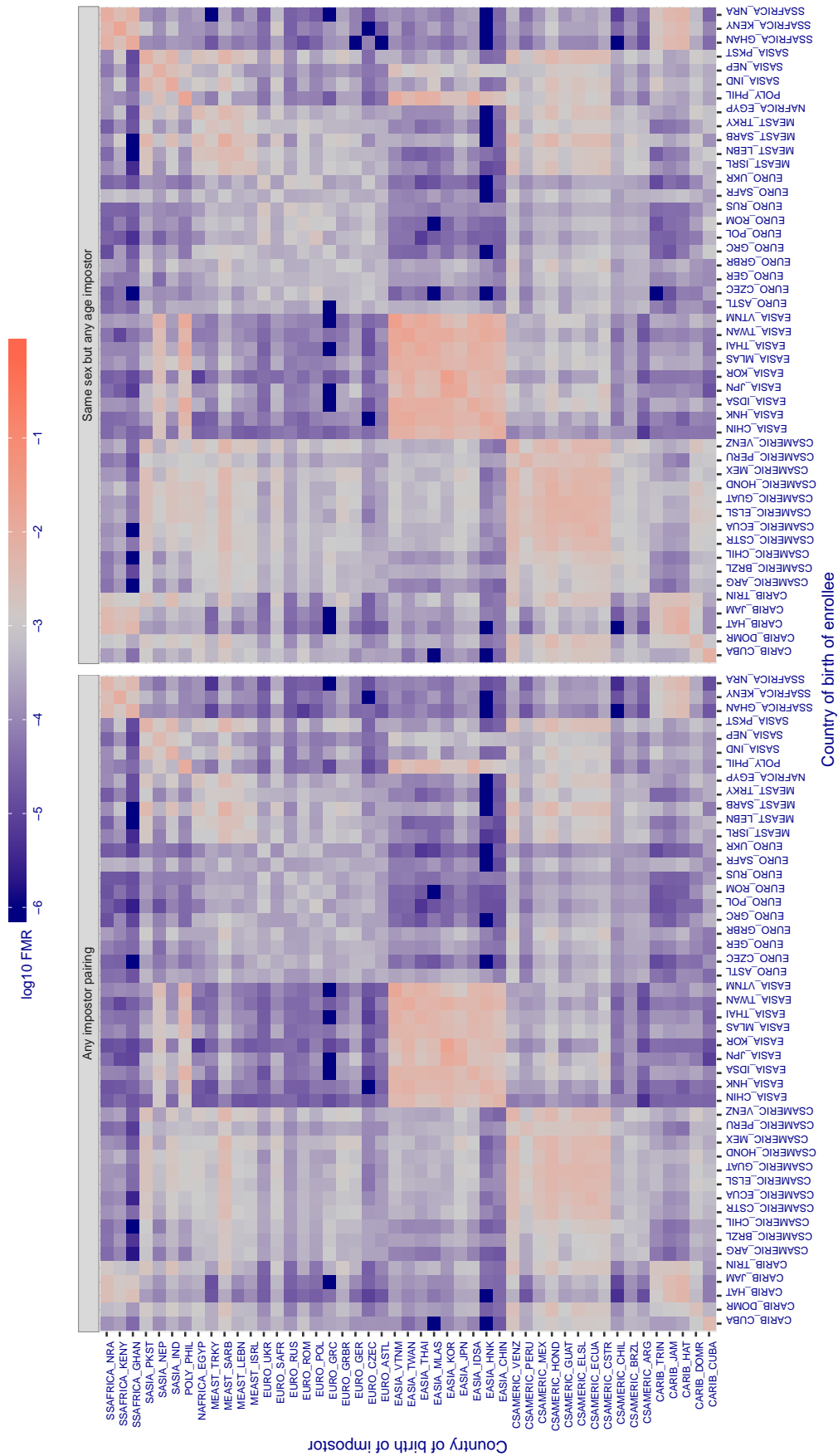


Figure 347: For algorithm camvi-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.346$  for algorithm ceiec\_001, giving  $FMR(T) = 0.001$  globally.

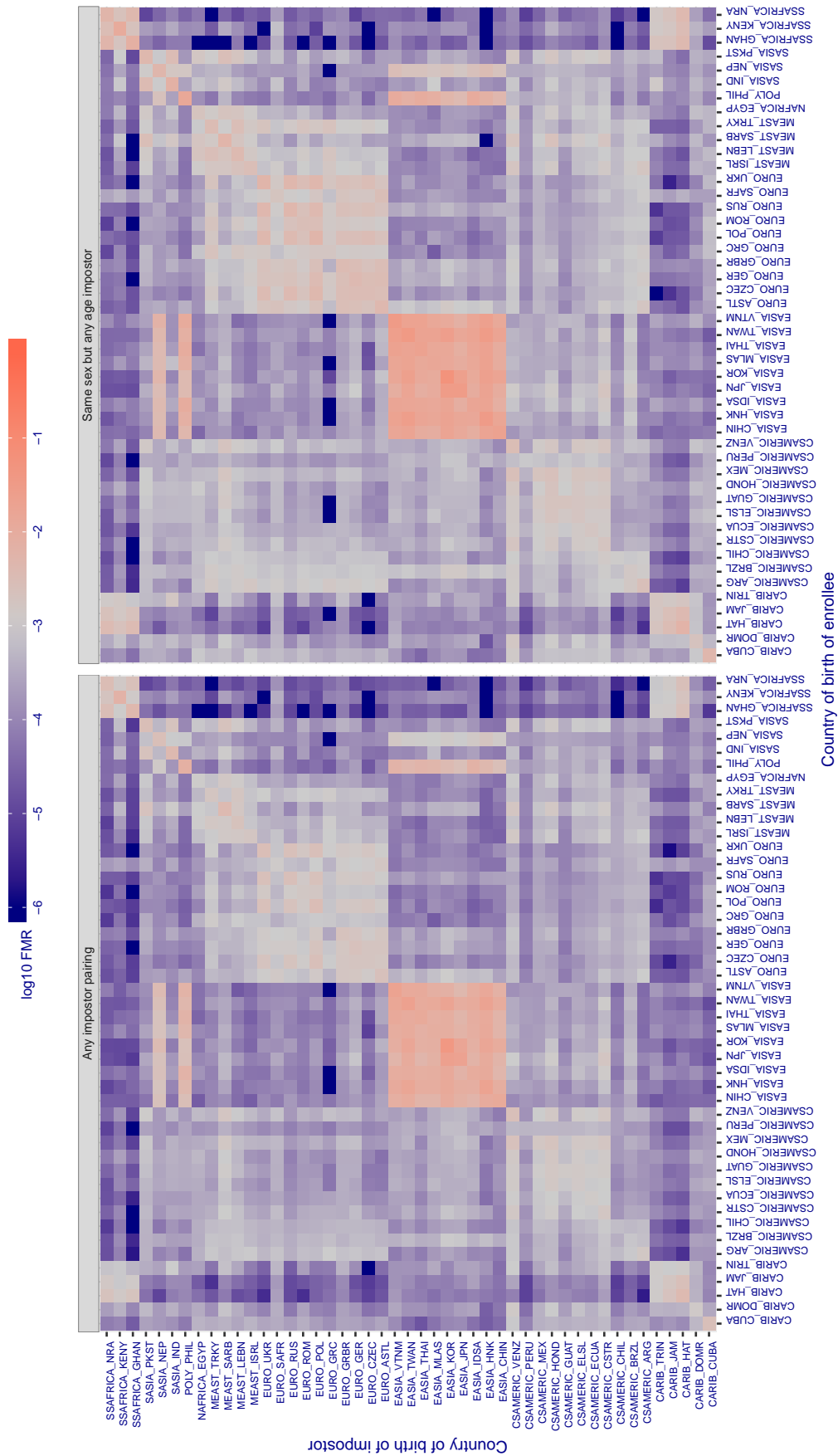


Figure 348: For algorithm ceiec-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.247$  for algorithm ceiec\_002, giving  $FMR(T) = 0.001$  globally.

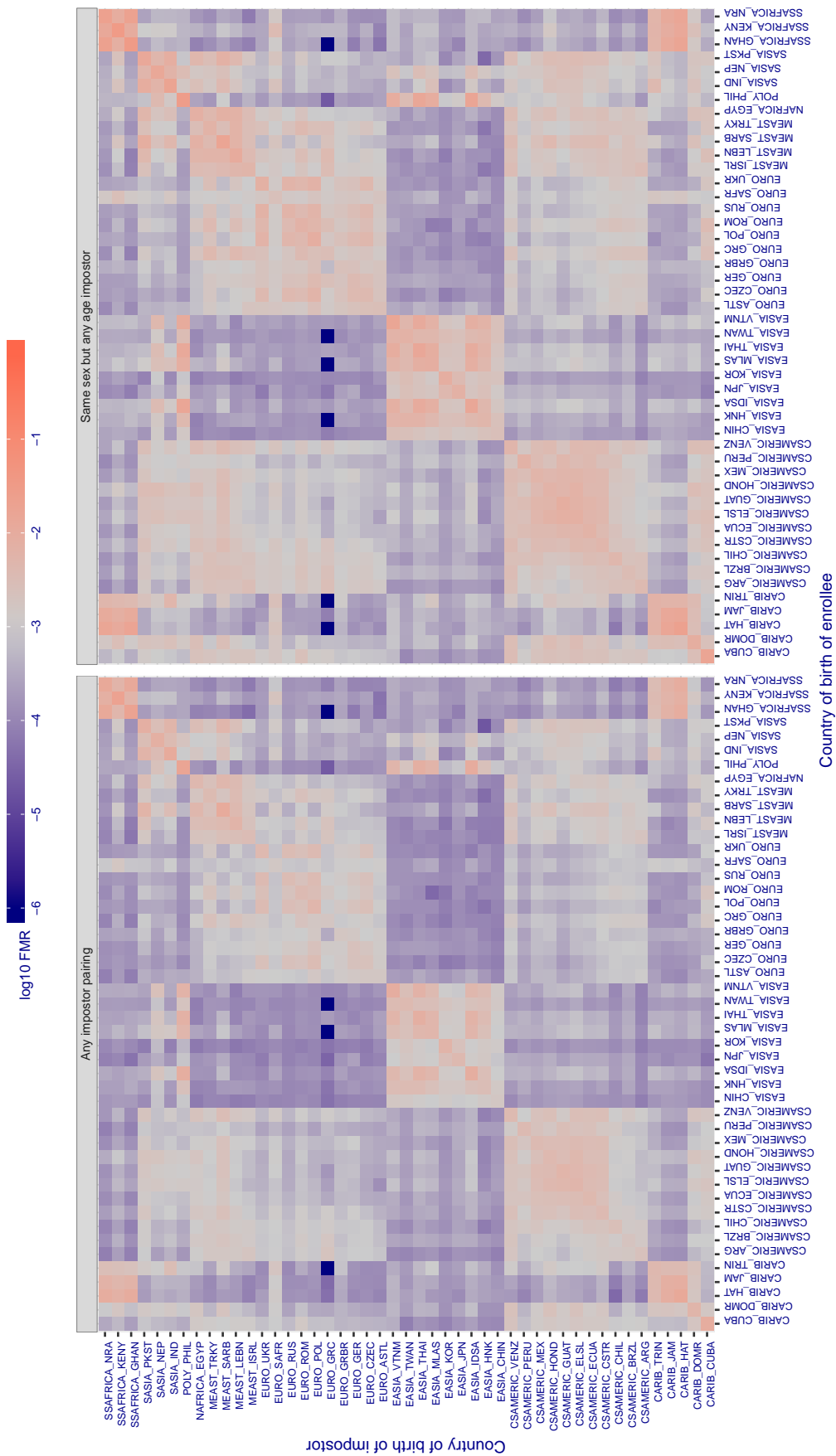


Figure 349: For algorithm ceiec-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.365$  for algorithm `chtface_001`, giving  $FMR(T) = 0.001$  globally.

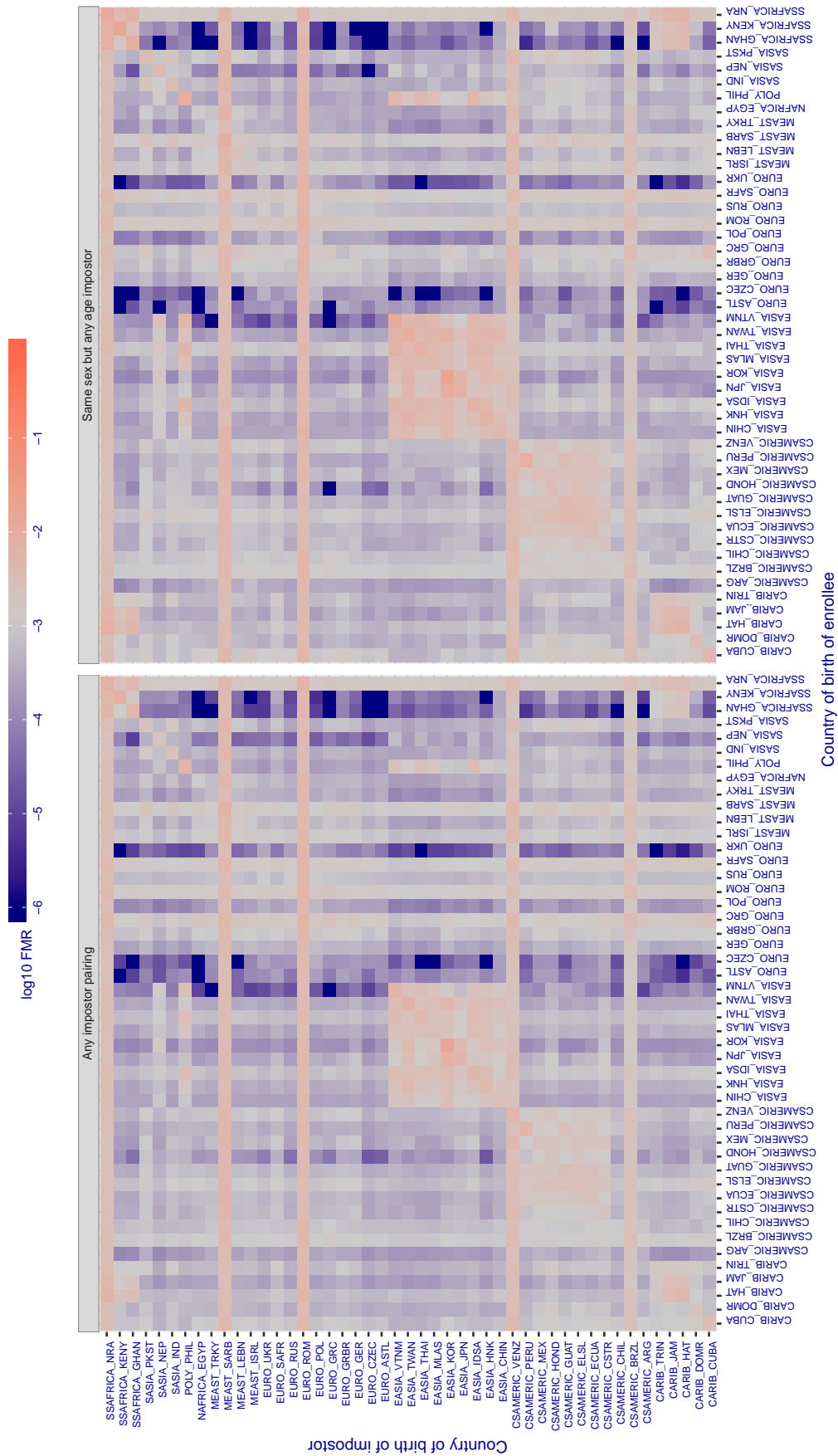


Figure 350: For algorithm `chtface-001` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 2845.000$  for algorithm cogent\_003, giving  $FMR(T) = 0.001$  globally.

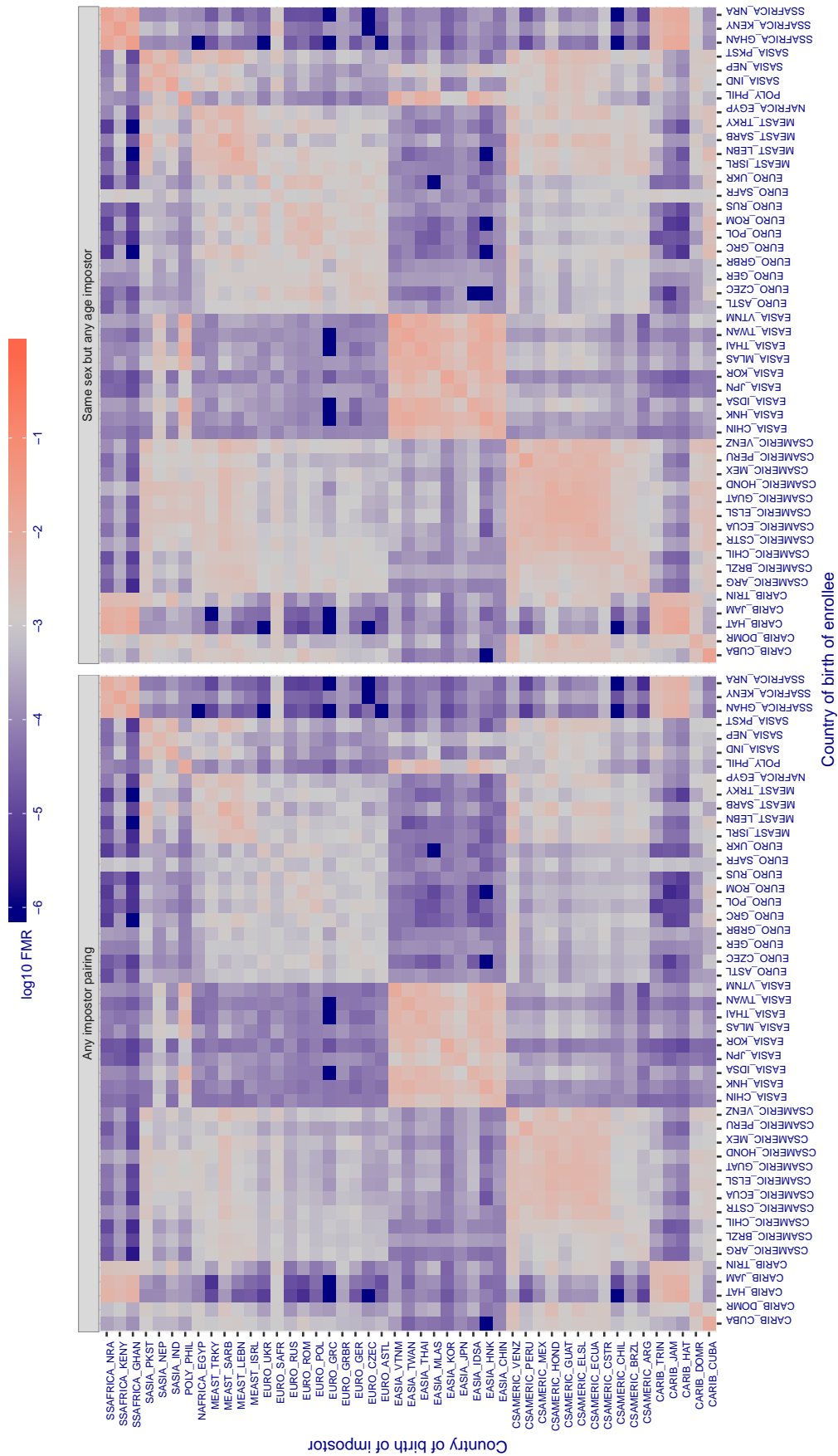


Figure 351: For algorithm cogent-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 2939.000$  for algorithm cogent\_004, giving  $FMR(T) = 0.001$  globally.

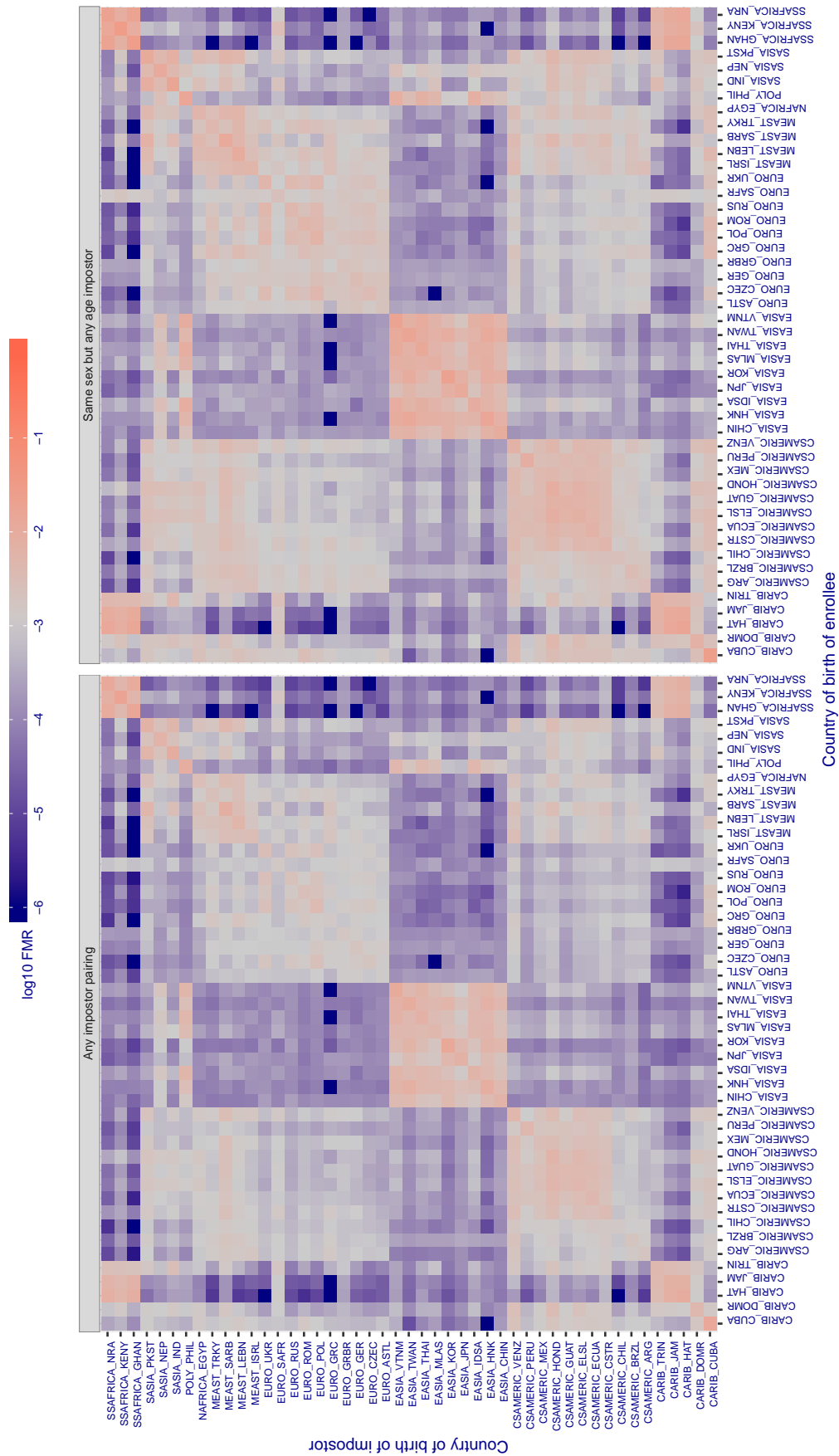


Figure 352: For algorithm cogent-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



**Cross country FMR at threshold  $T = 0.522$  for algorithm `cognitec_000`, giving  $FMR(T) = 0.001$  globally.**

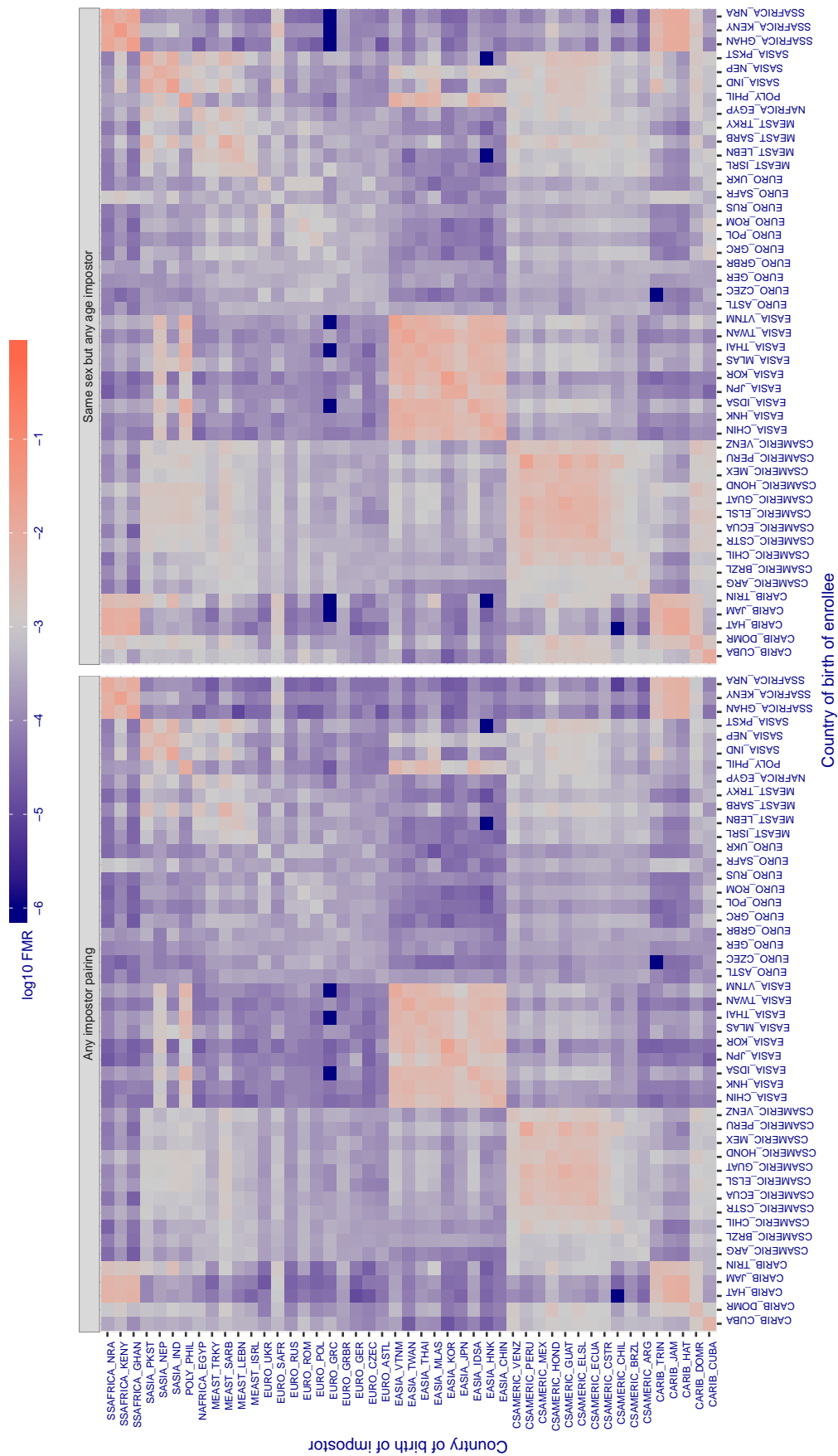


Figure 353: For algorithm `cognitec-000` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.522$  for algorithm `cognitec_001`, giving  $FMR(T) = 0.001$  globally.

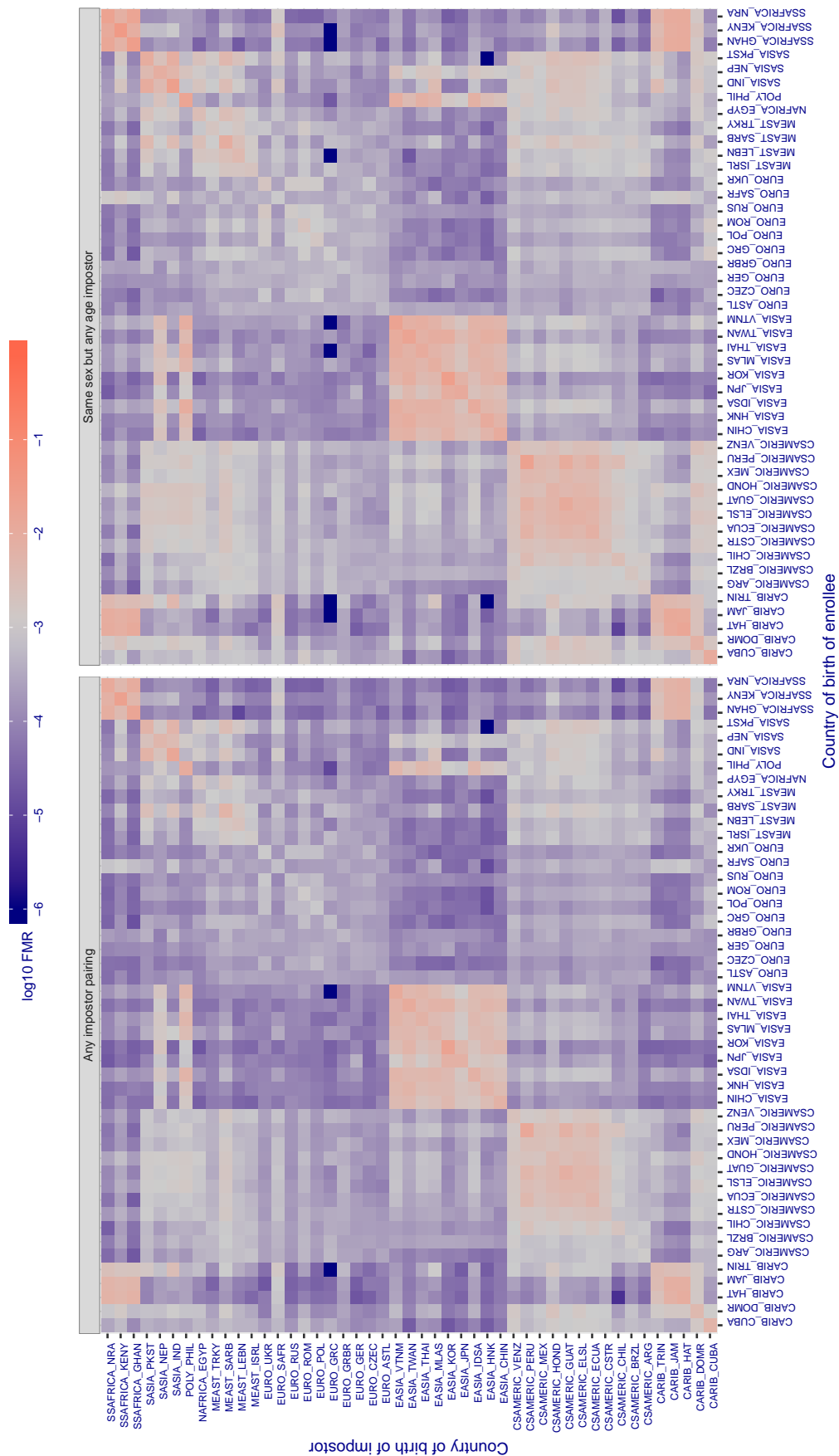


Figure 354: For algorithm `cognitec-001` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each  $+1$  increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 3.572$  for algorithm `ctcbank_000`, giving  $FMR(T) = 0.001$  globally.

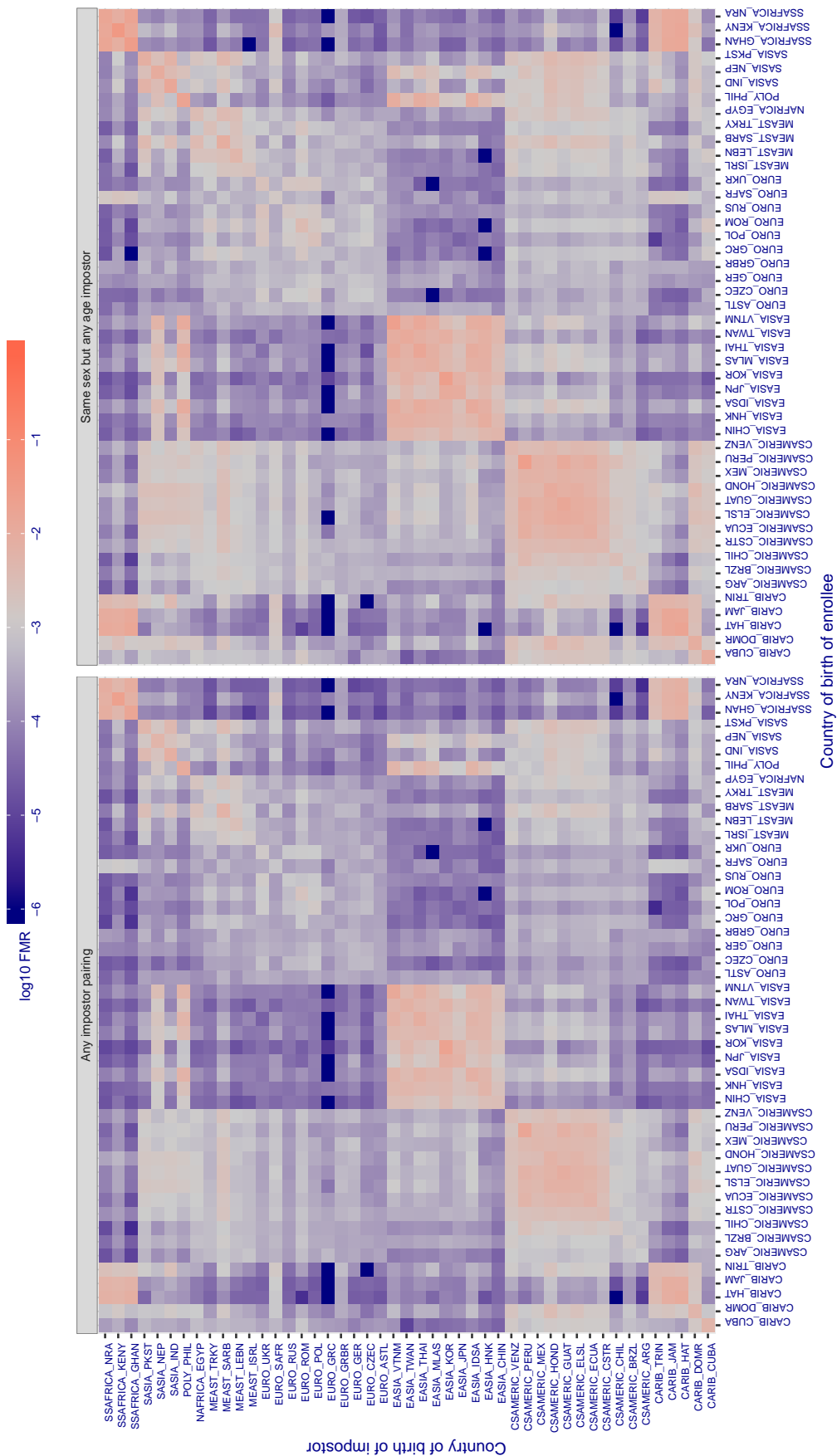


Figure 355: For algorithm `ctcbank-000` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 3.600$  for algorithm `ctcbank_001`, giving  $FMR(T) = 0.001$  globally.

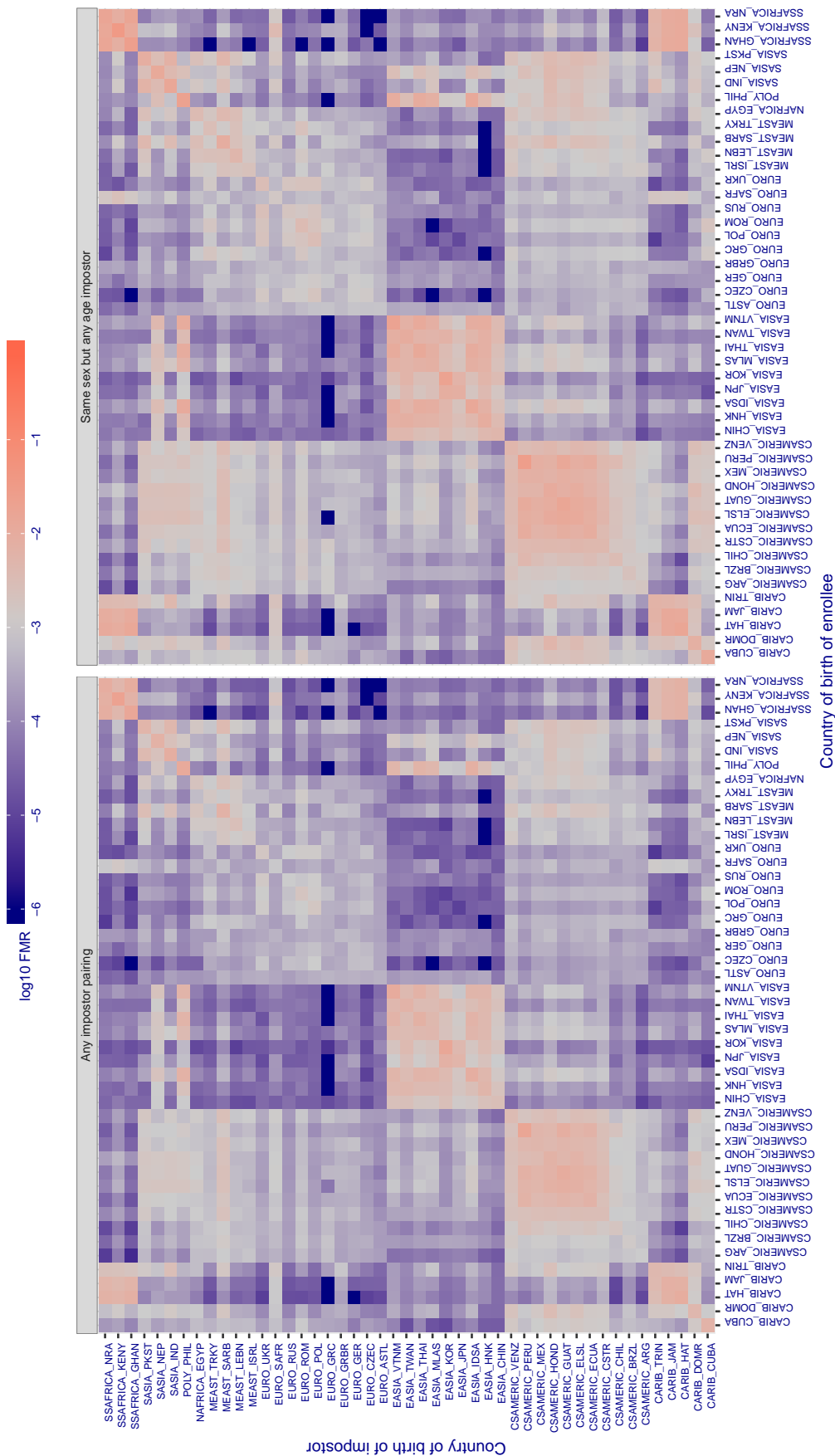


Figure 356: For algorithm `ctcbank-001` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each  $+1$  increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.702$  for algorithm cyberextruder\_001, giving  $FMR(T) = 0.001$  globally.

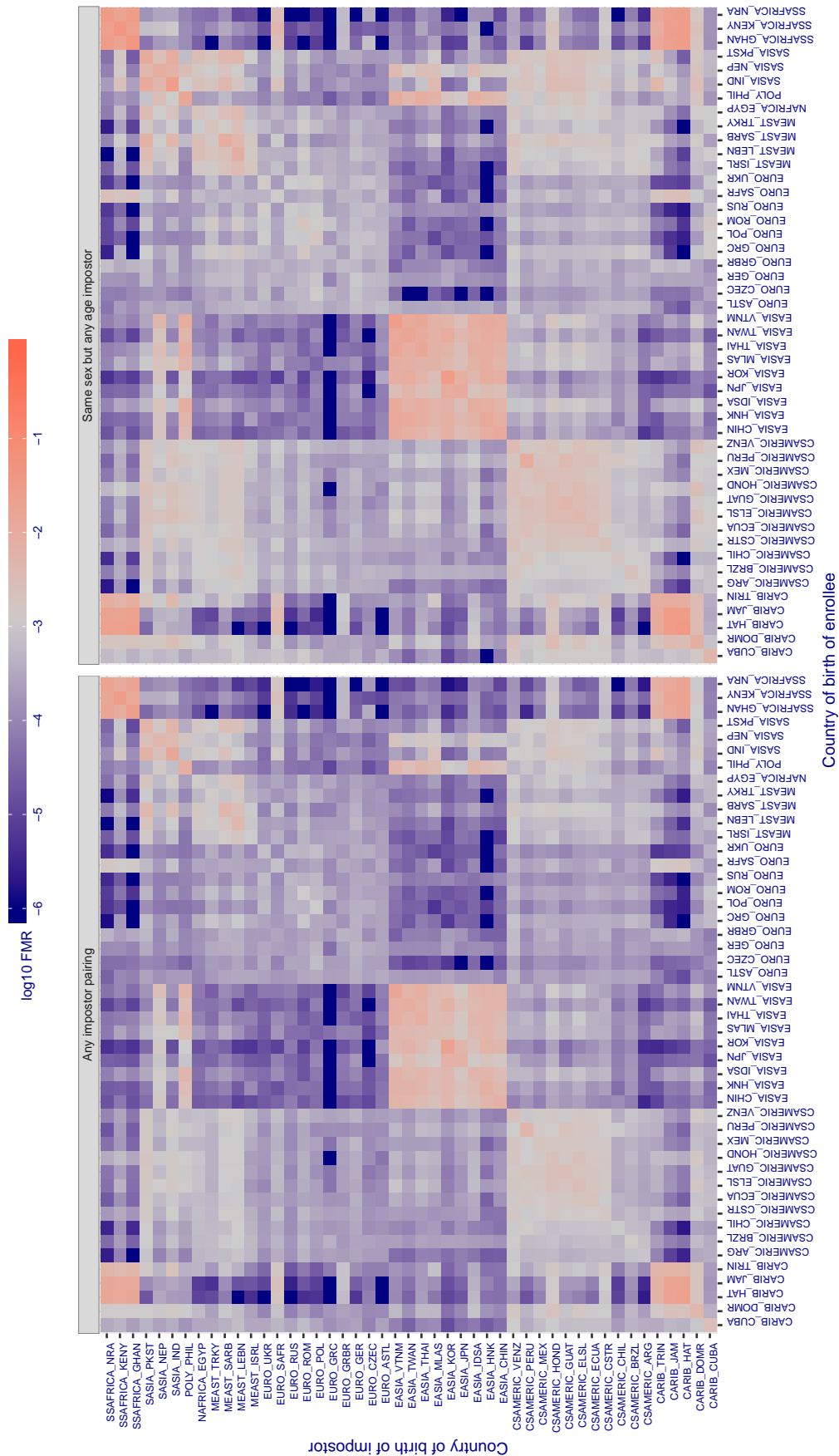


Figure 357: For algorithm cyberextruder-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.408$  for algorithm cyberextruder\_002, giving  $FMR(T) = 0.001$  globally.

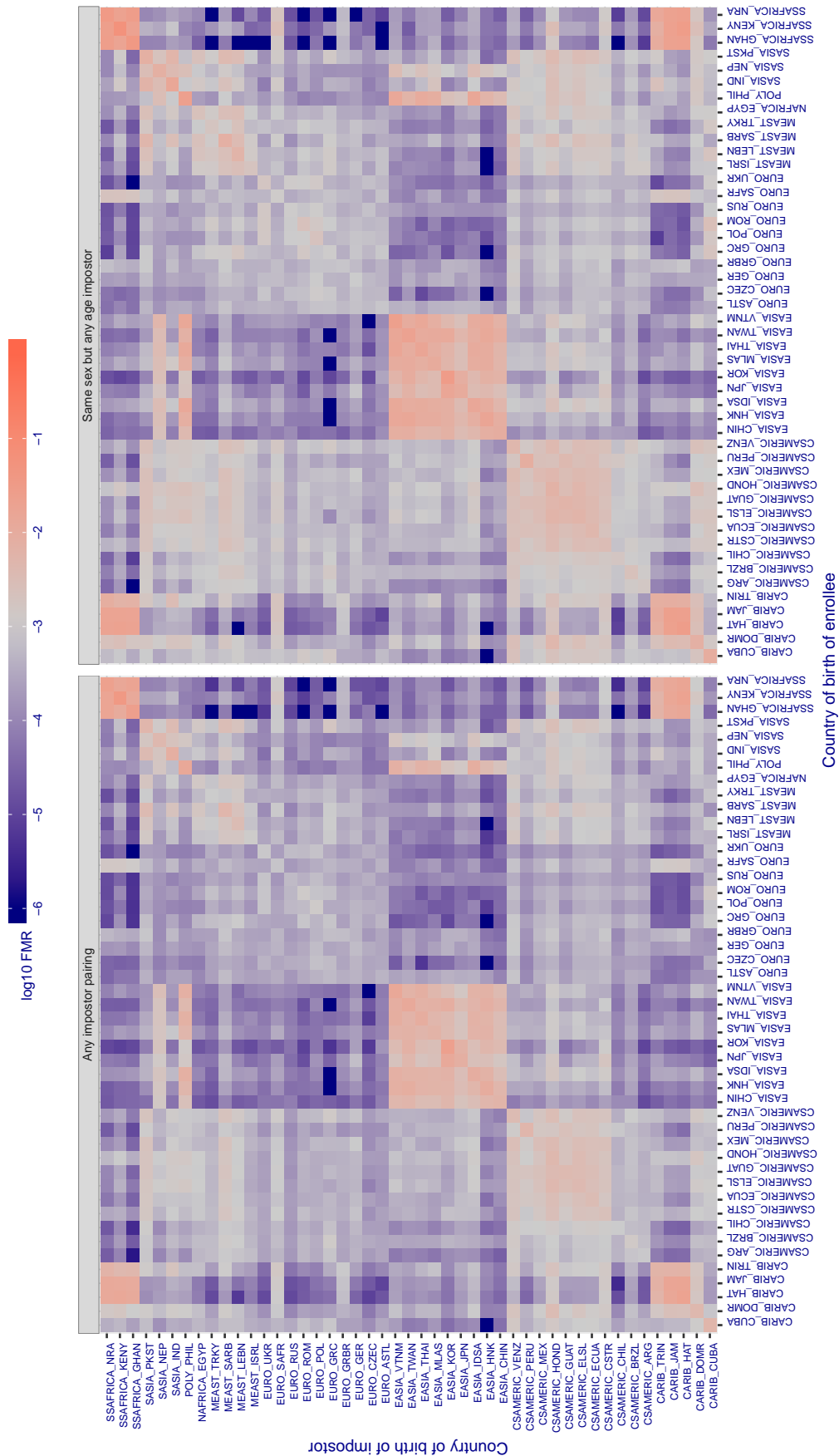


Figure 358: For algorithm cyberextruder-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 1.322$  for algorithm cyberlink\_002, giving  $FMR(T) = 0.001$  globally.

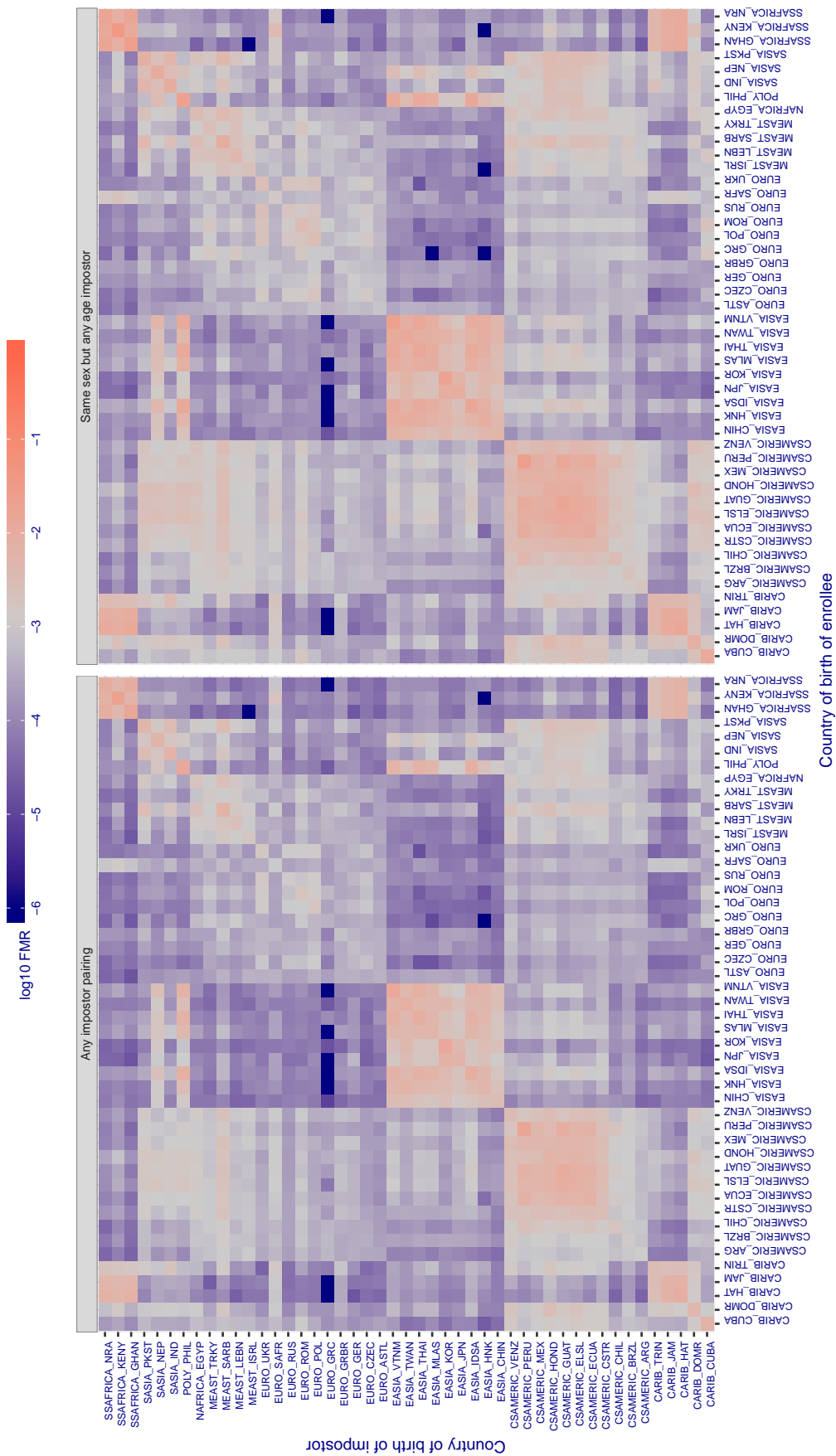


Figure 359: For algorithm cyberlink-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 5958.000$  for algorithm dahua\_002, giving  $FMR(T) = 0.001$  globally.

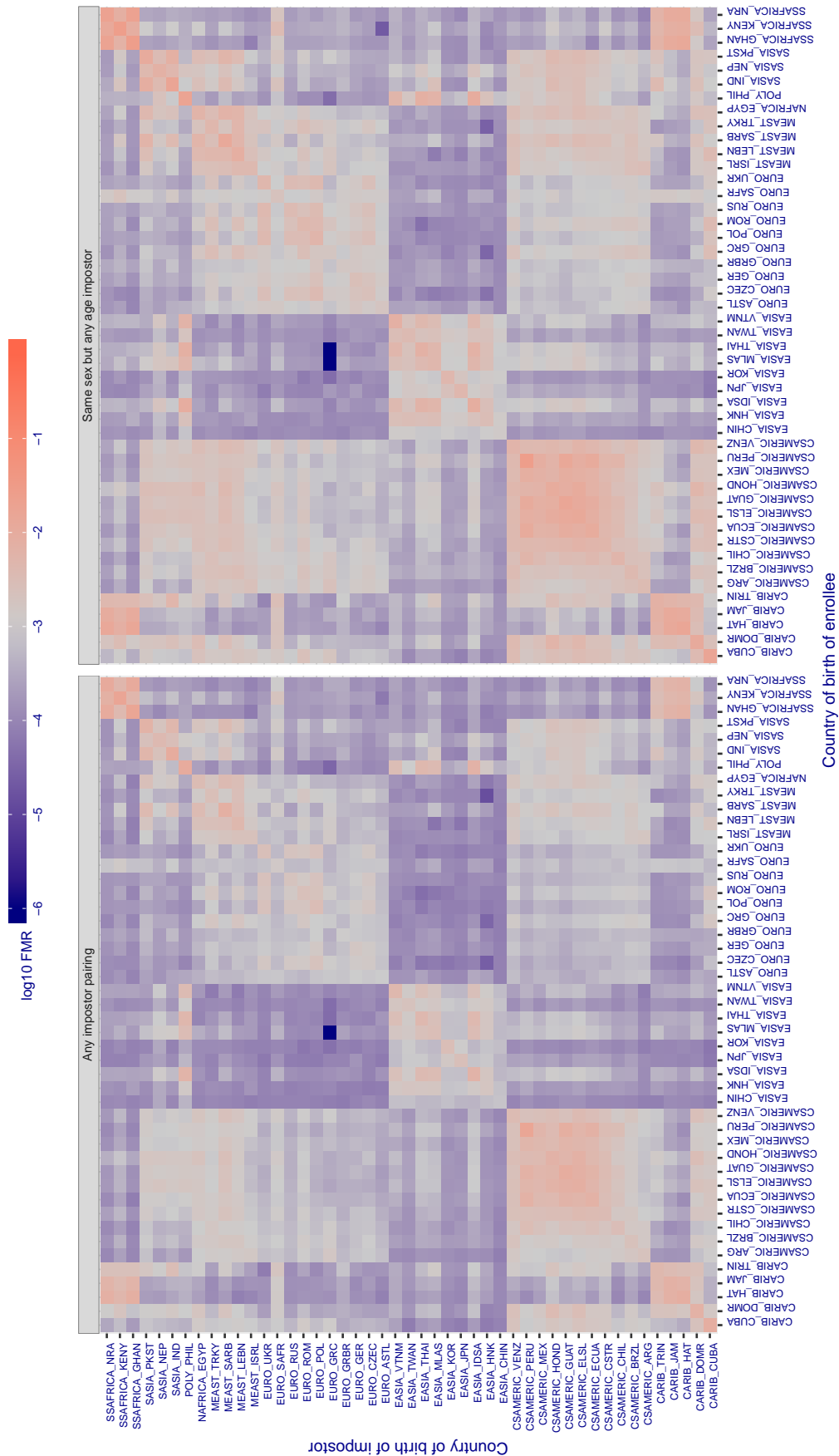


Figure 360: For algorithm dahua-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 5392.000$  for algorithm dahua\_003, giving  $FMR(T) = 0.001$  globally.

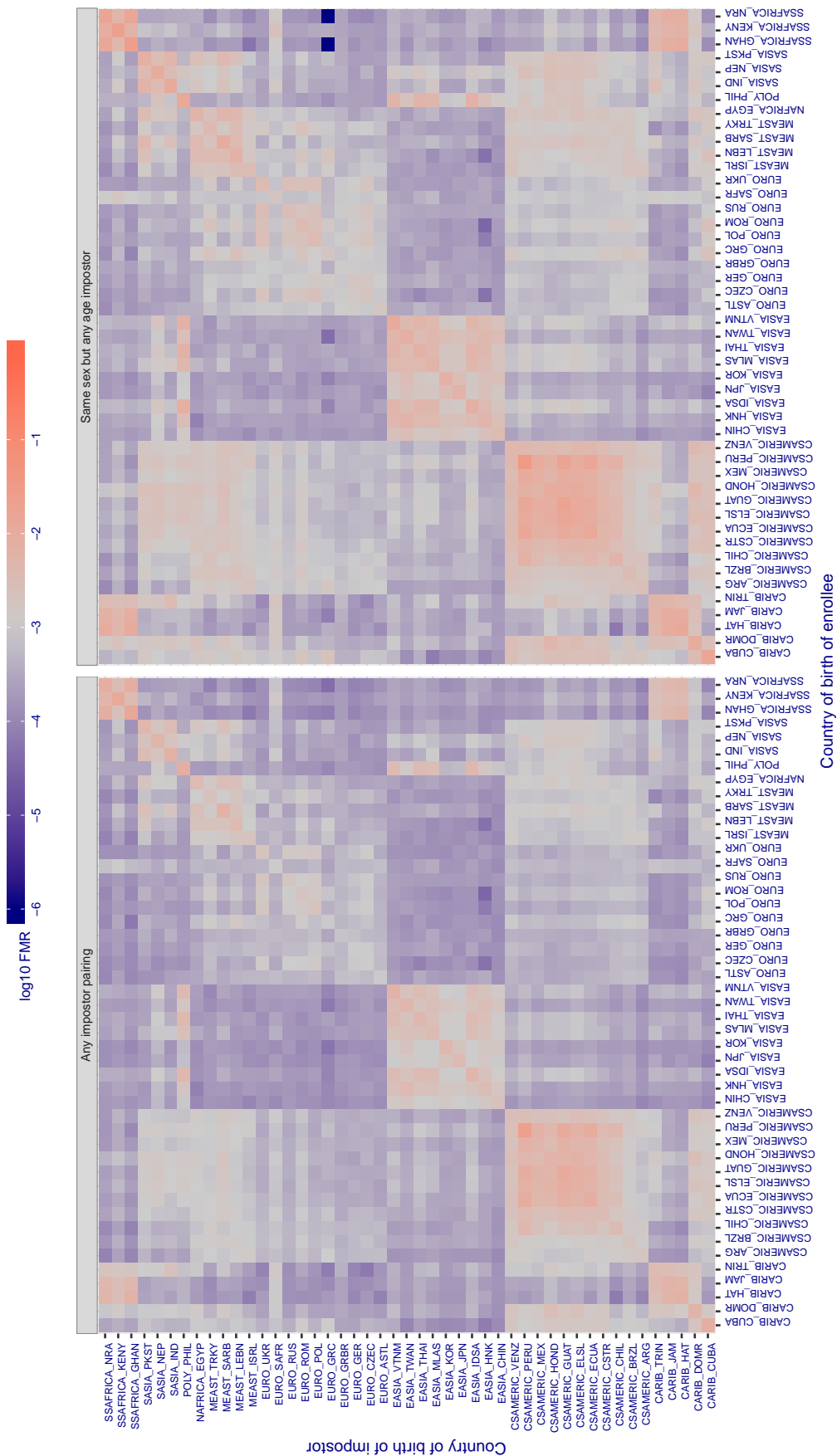


Figure 361: For algorithm dahua-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 1.293$  for algorithm deepglint\_001, giving  $FMR(T) = 0.001$  globally.

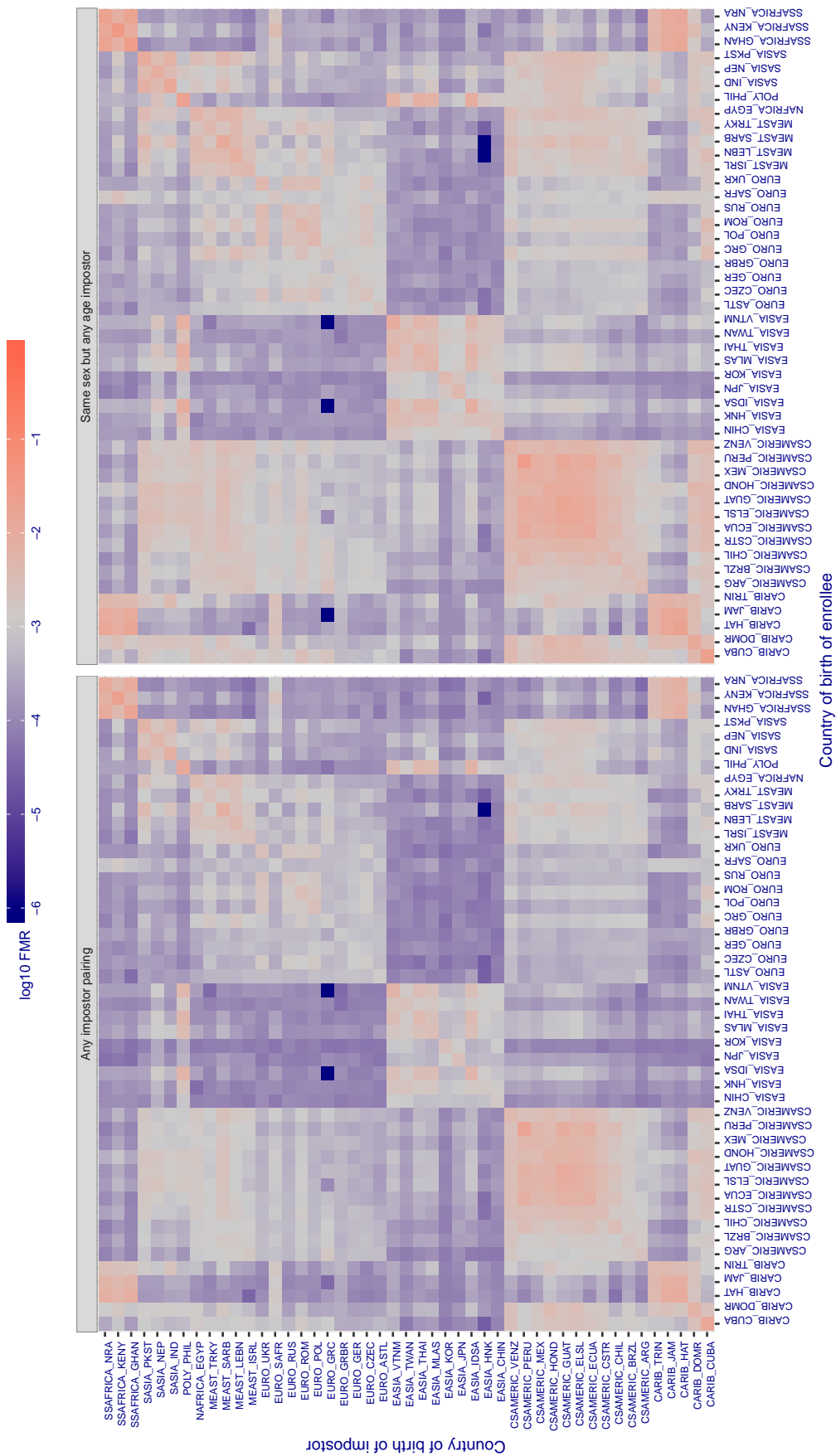


Figure 362: For algorithm deepglint-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 1.300$  for algorithm deepsea\_001, giving  $FMR(T) = 0.001$  globally.

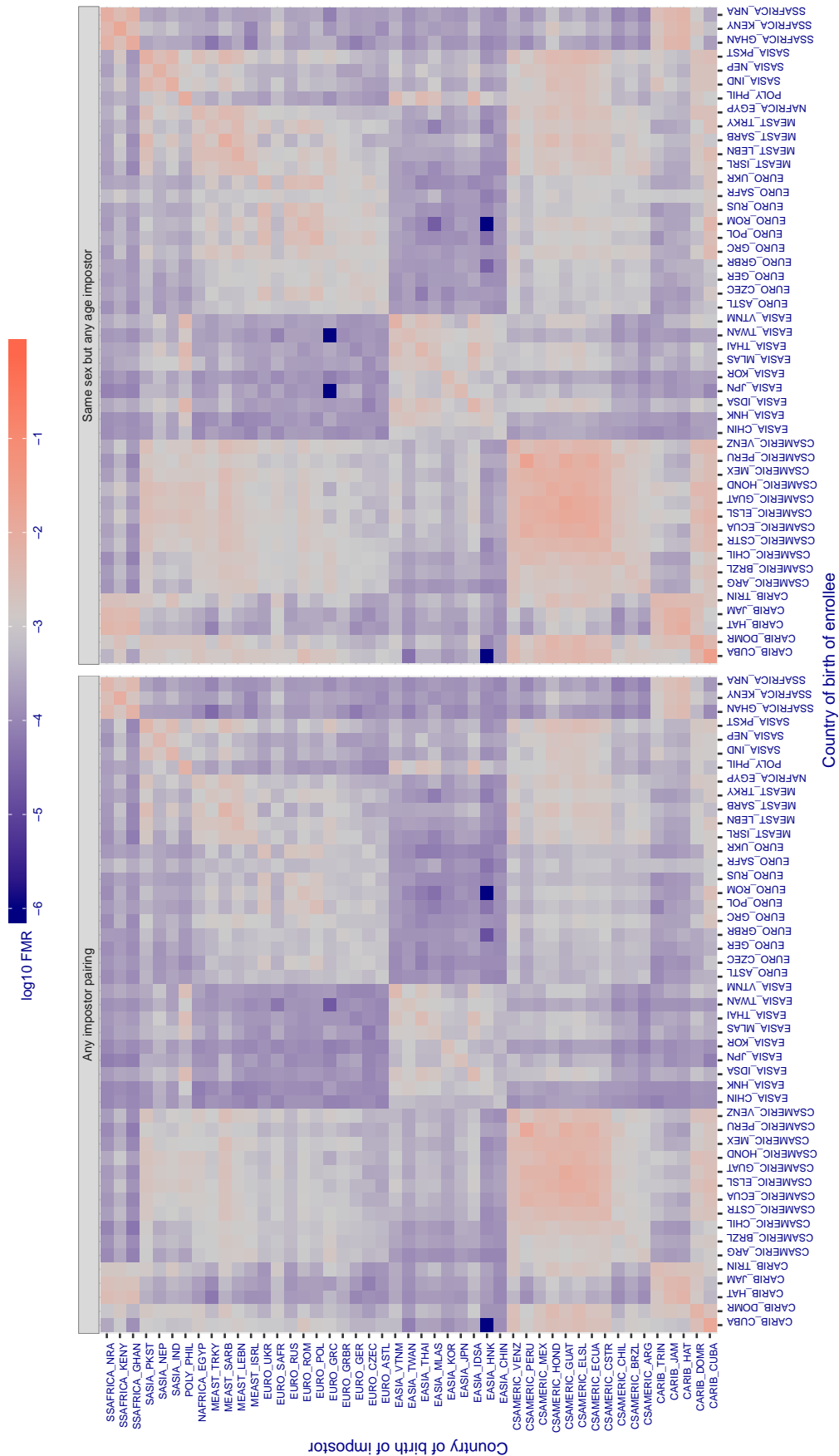


Figure 363: For algorithm deepsea-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 75.231$  for algorithm dermalog\_005, giving  $FMR(T) = 0.001$  globally.

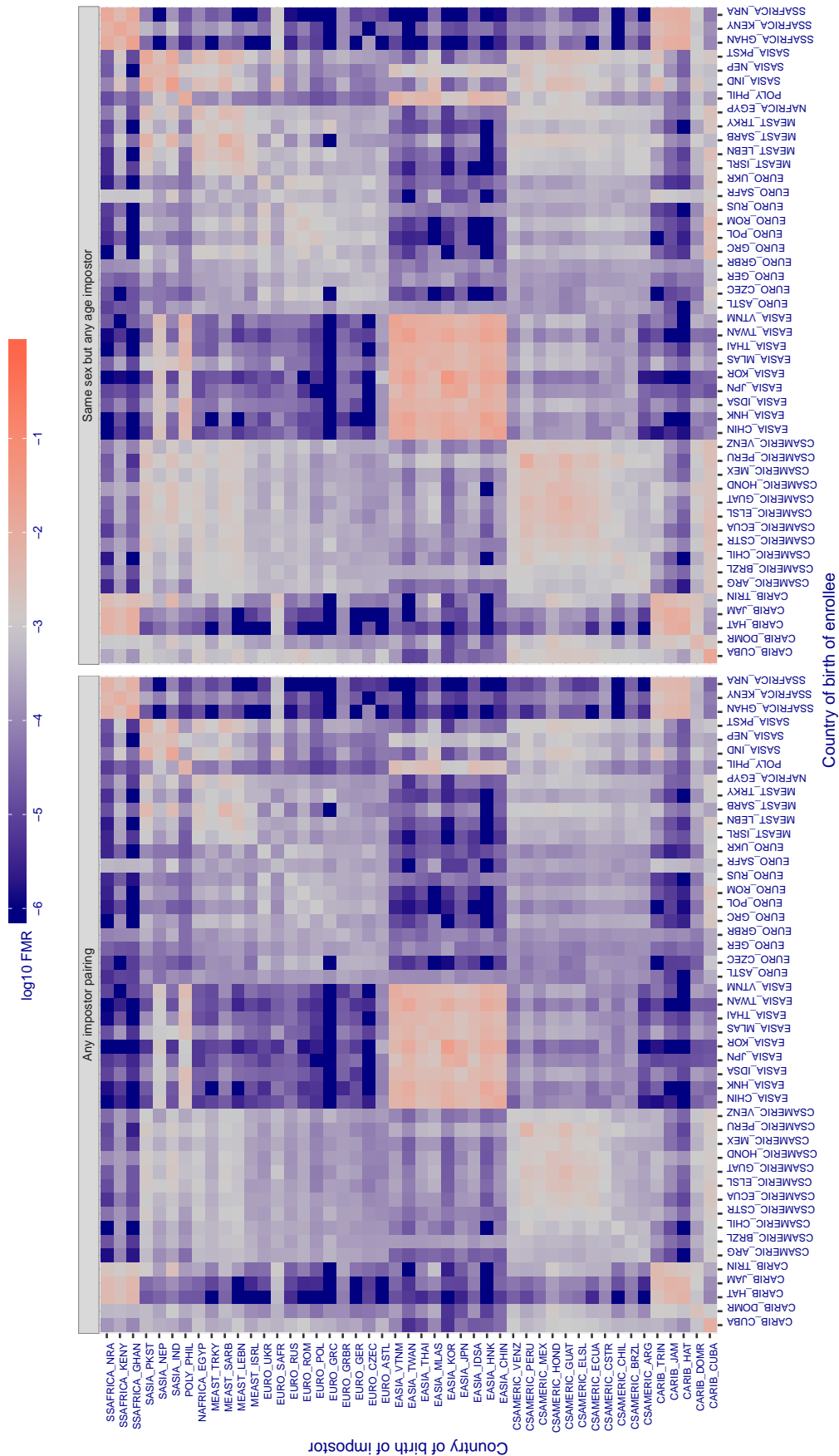


Figure 364: For algorithm dermalog-005 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 76.496$  for algorithm dermalog\_006, giving  $FMR(T) = 0.001$  globally.

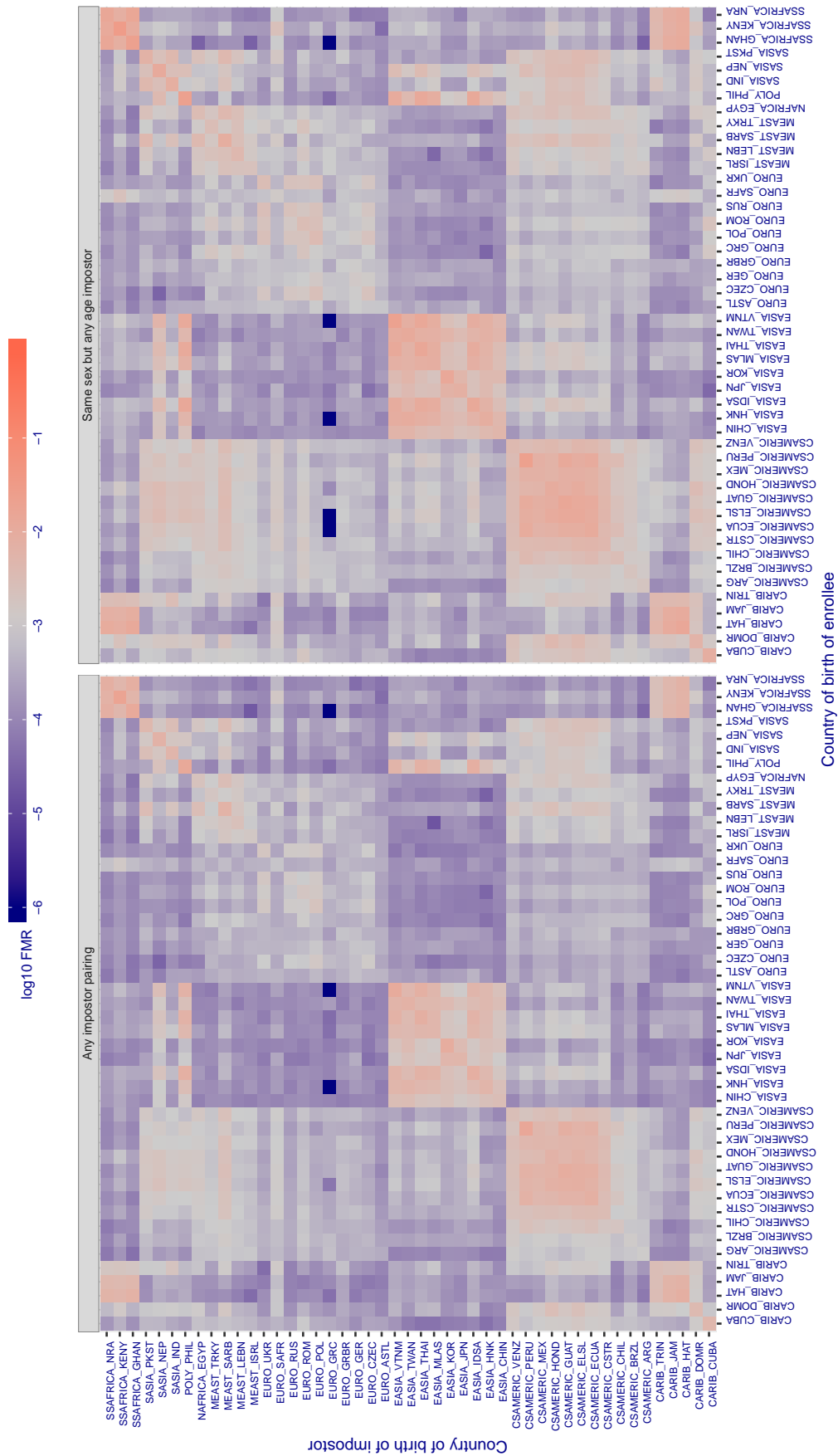


Figure 365: For algorithm dermalog-006 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.250$  for algorithm didiglobalface\_001, giving  $FMR(T) = 0.001$  globally.

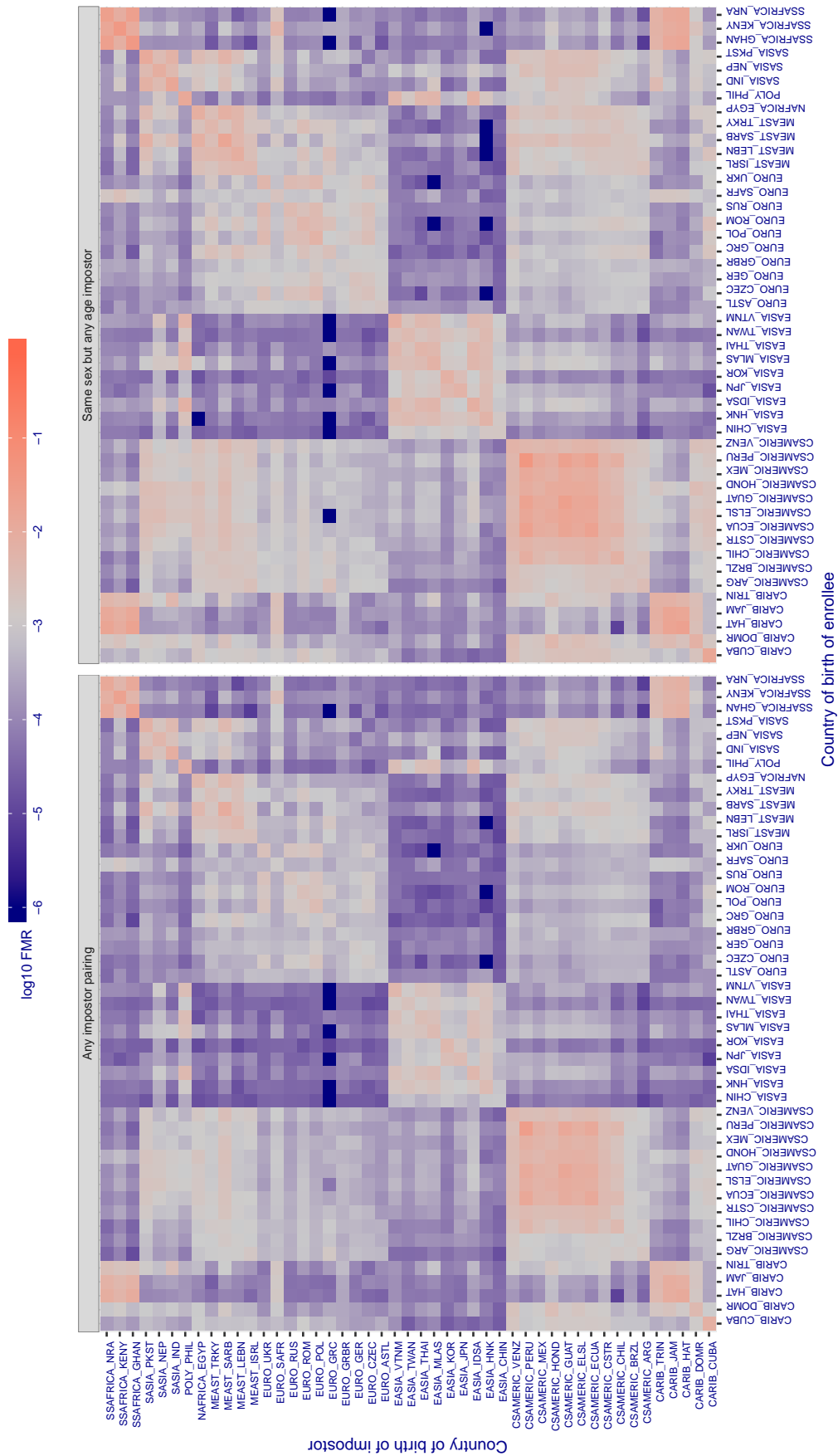


Figure 366: For algorithm didiglobalface-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.547$  for algorithm digitalbarriers\_002, giving  $FMR(T) = 0.001$  globally.

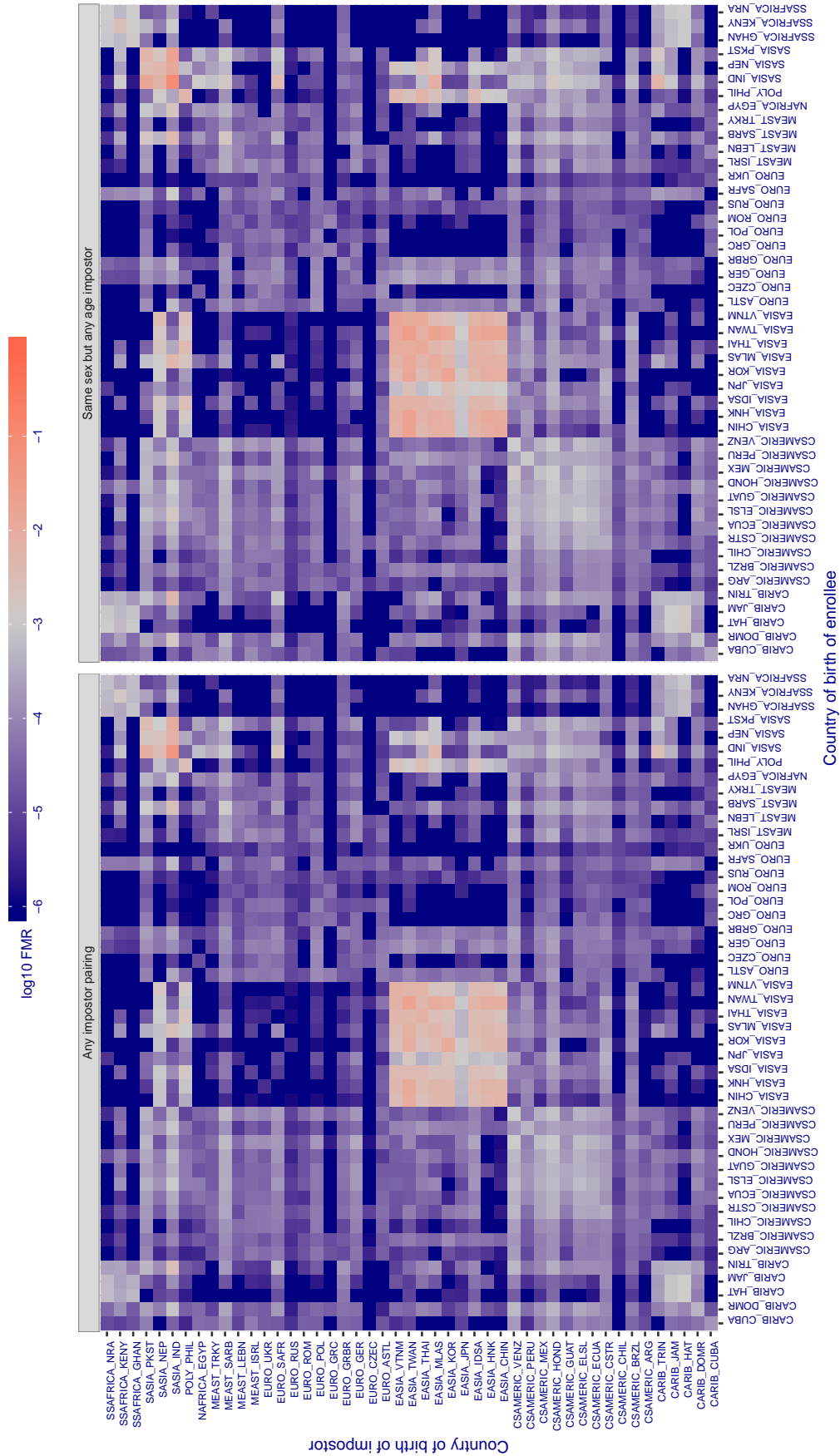


Figure 367: For algorithm digitalbarriers-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 0.974$  for algorithm `dsk_000`, giving  $FMR(T) = 0.001$  globally.

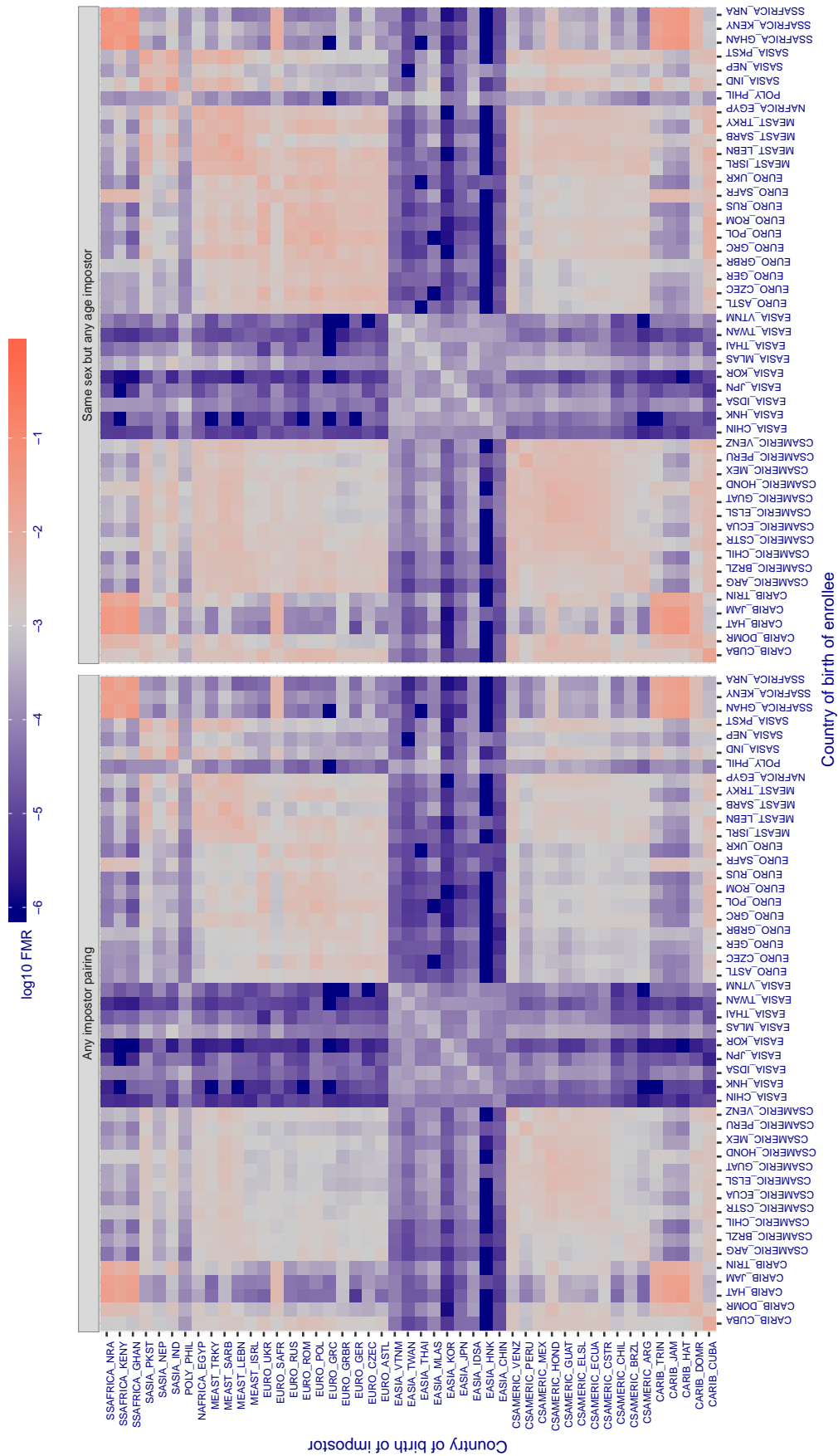


Figure 368: For algorithm `dsk-000` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each  $+1$  increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 48.749$  for algorithm einetworks\_000, giving  $FMR(T) = 0.001$  globally.

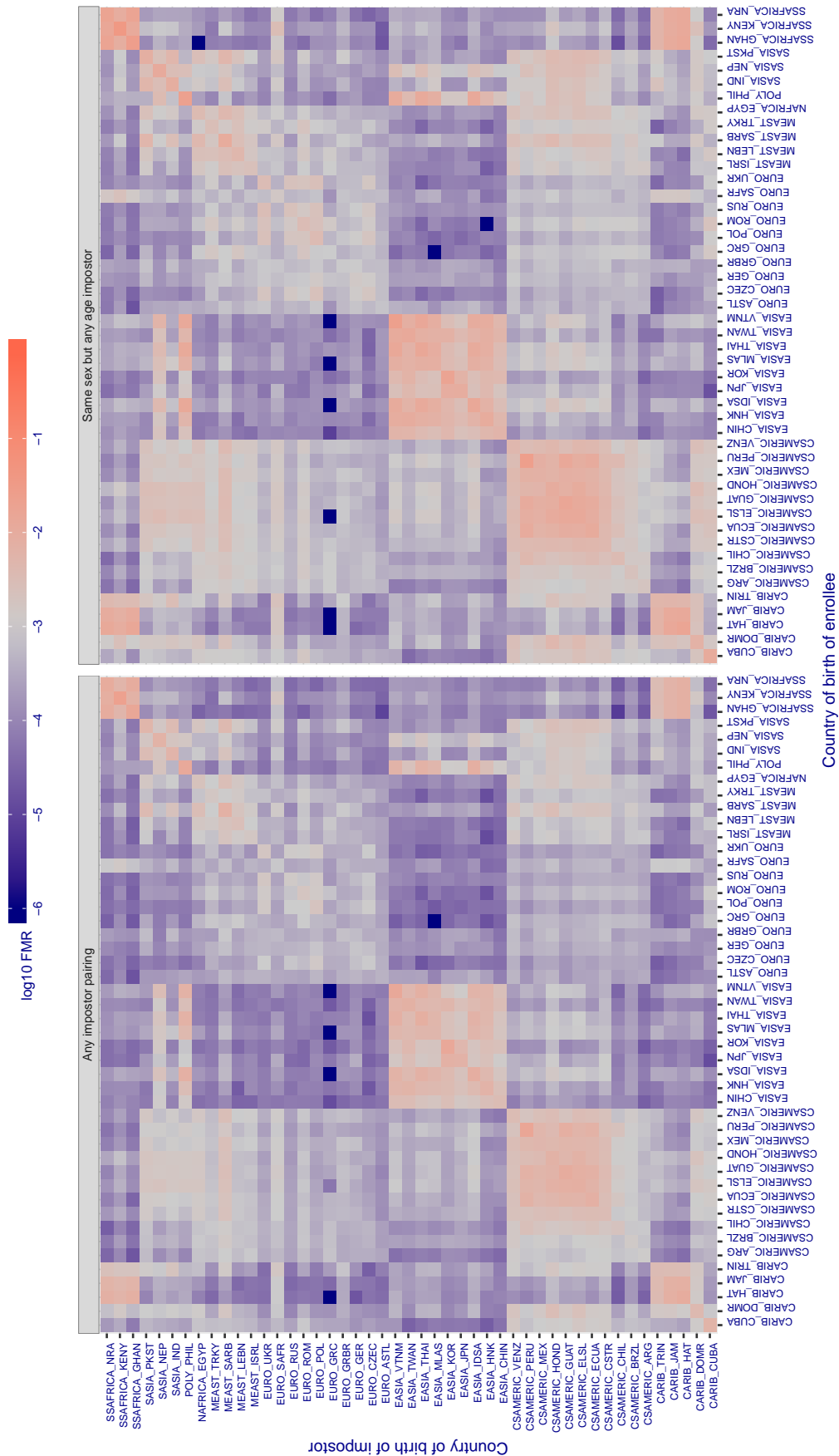


Figure 369: For algorithm einetworks-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 2.426$  for algorithm everai\_002, giving  $FMR(T) = 0.001$  globally.

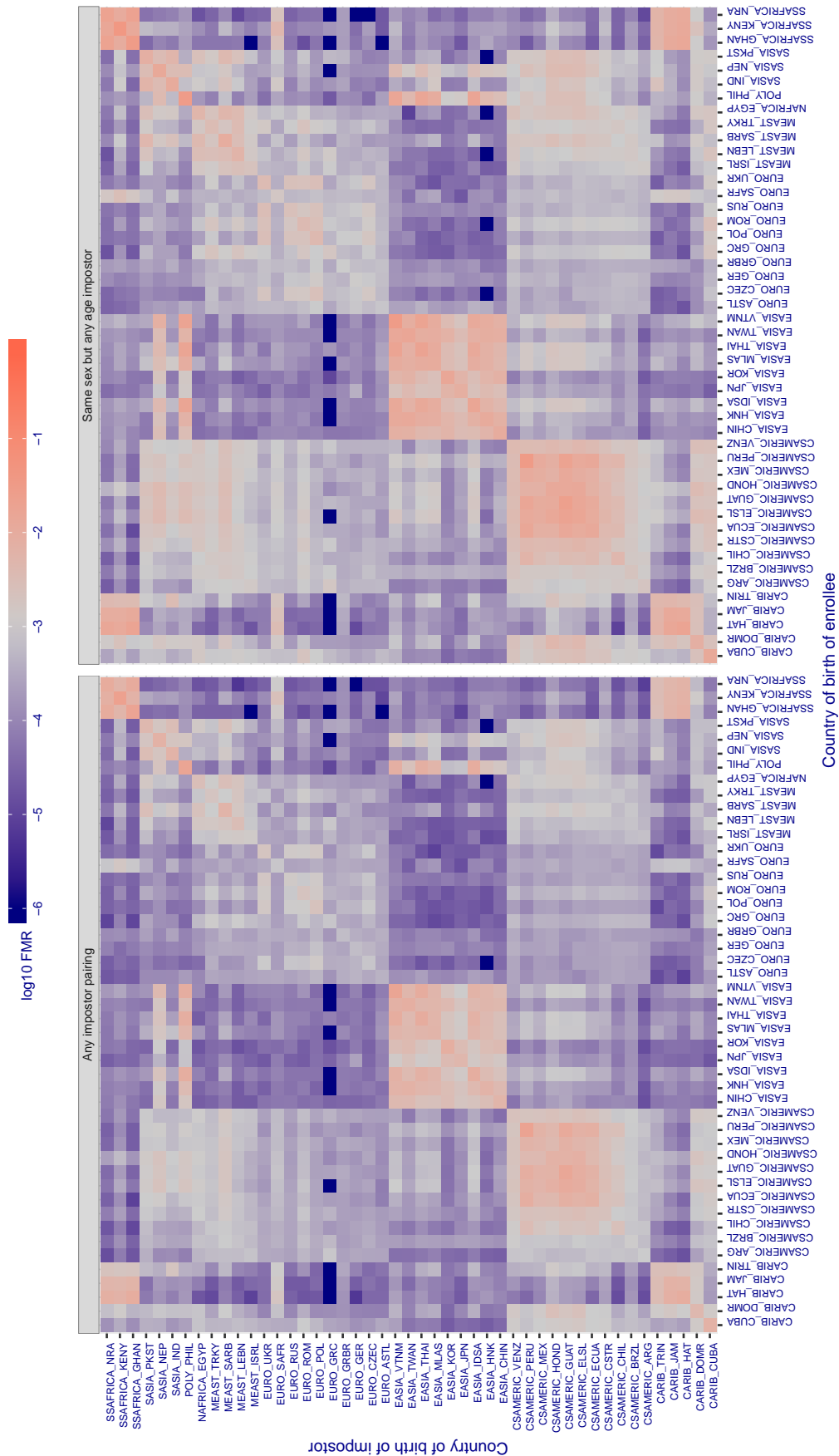


Figure 370: For algorithm everai-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.311$  for algorithm  $f8\_001$ , giving  $FMR(T) = 0.001$  globally.

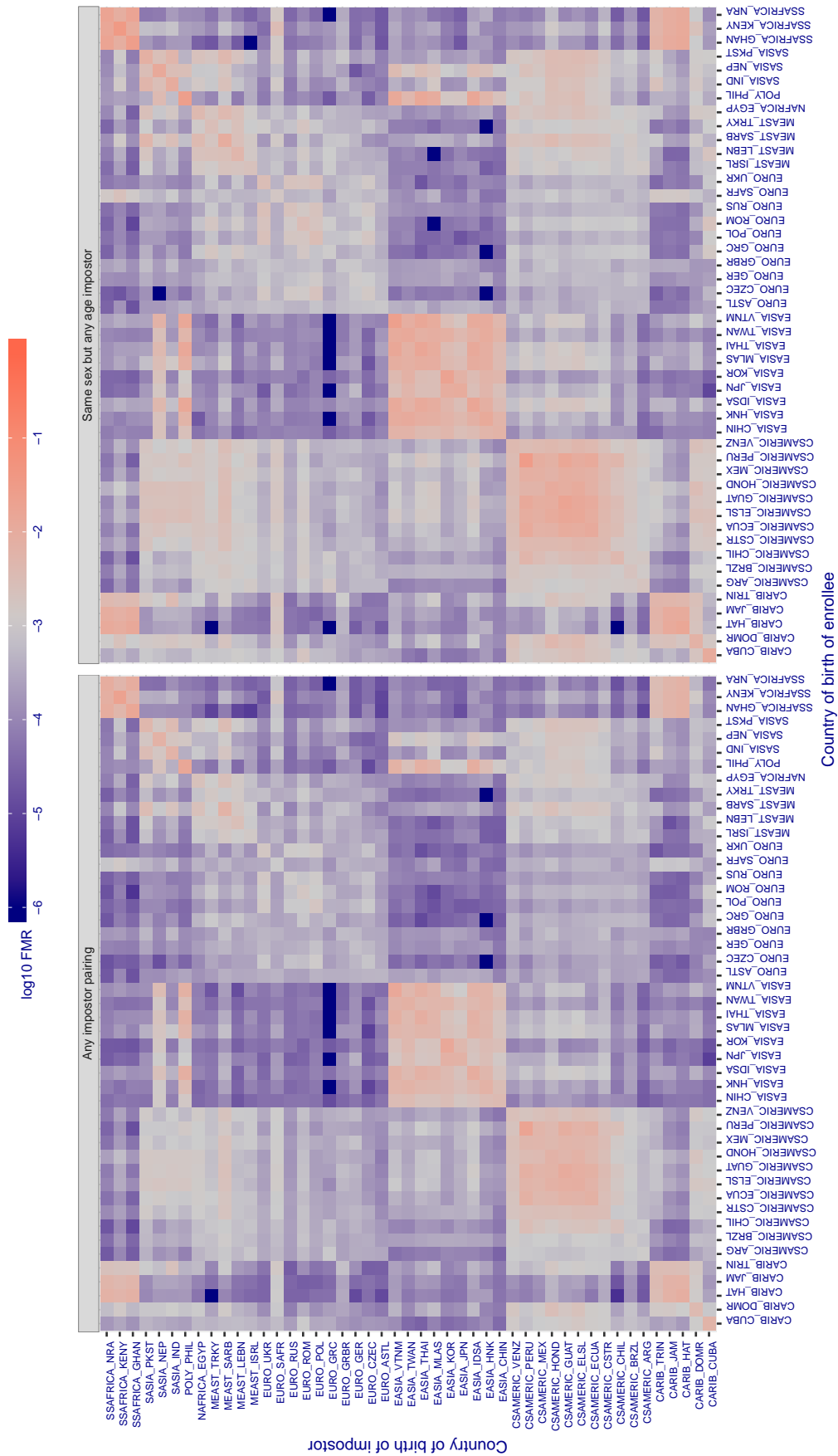


Figure 371: For algorithm  $f8-001$  operating on *visa* images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 1.300$  for algorithm facesoft\_000, giving  $FMR(T) = 0.001$  globally.

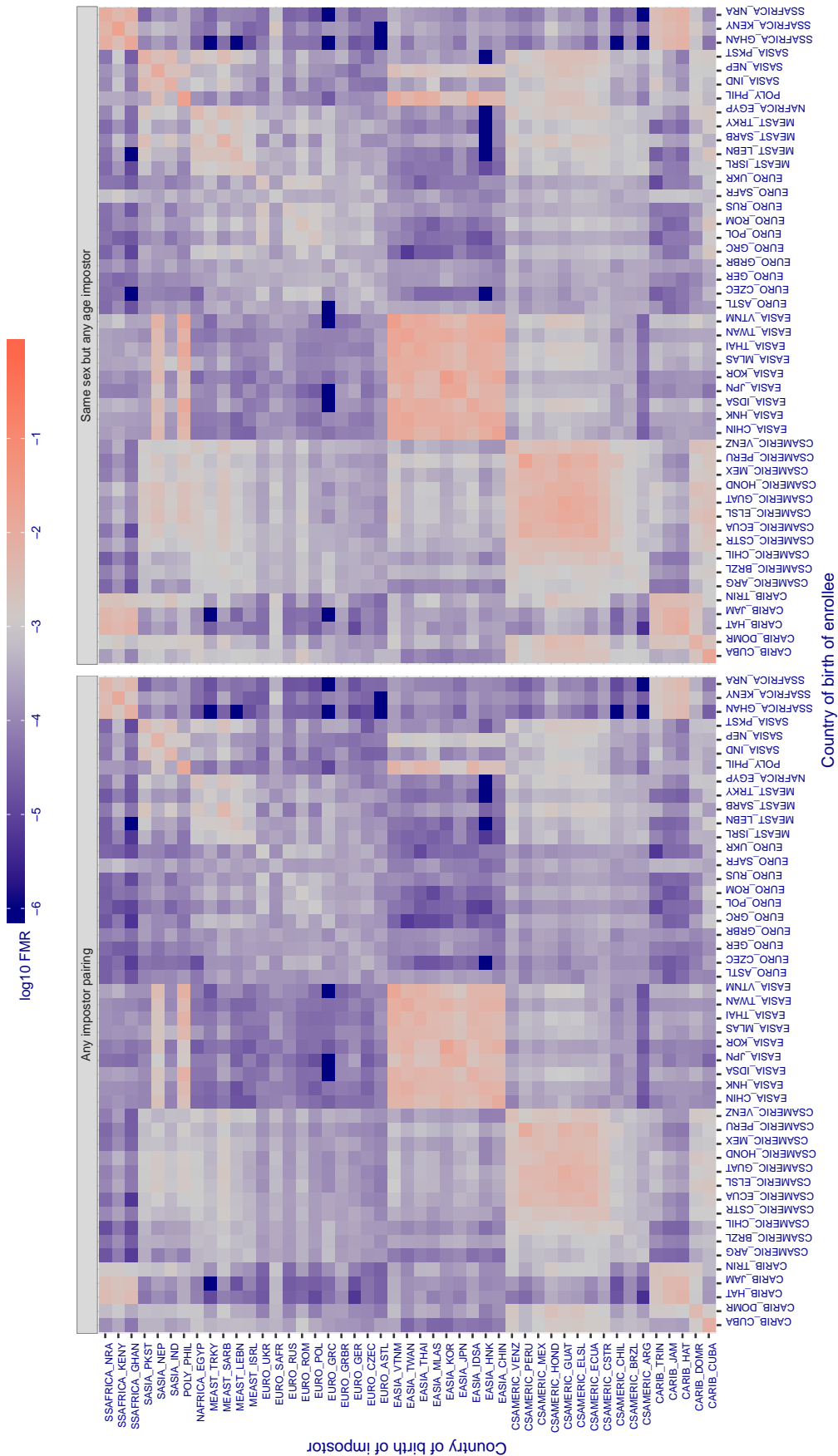


Figure 372: For algorithm facesoft-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.596$  for algorithm glory\_001, giving  $FMR(T) = 0.001$  globally.

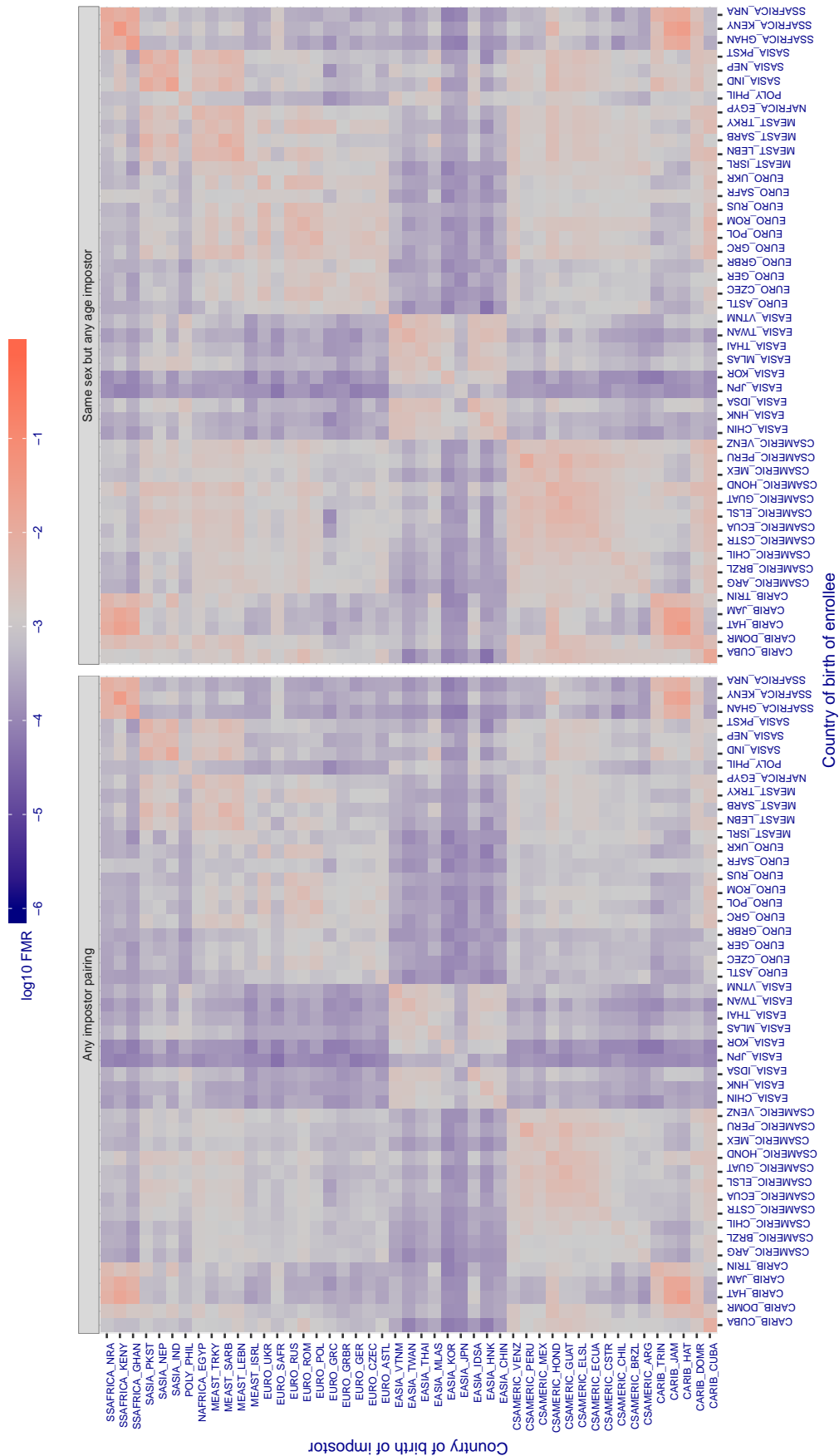


Figure 373: For algorithm glory-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.572$  for algorithm glory\_002, giving  $FMR(T) = 0.001$  globally.

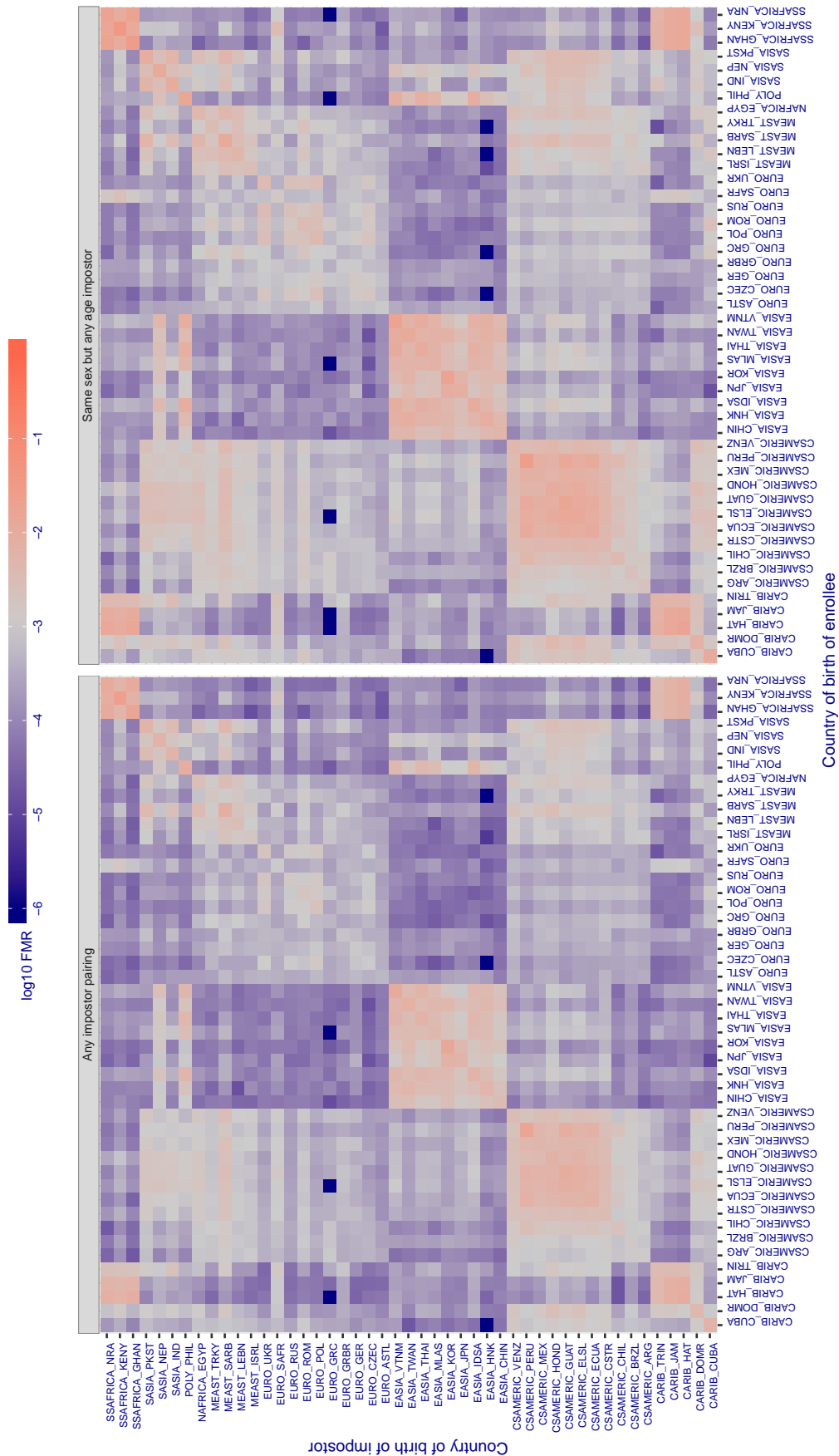


Figure 374: For algorithm glory-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.357$  for algorithm gorilla\_003, giving  $FMR(T) = 0.001$  globally.

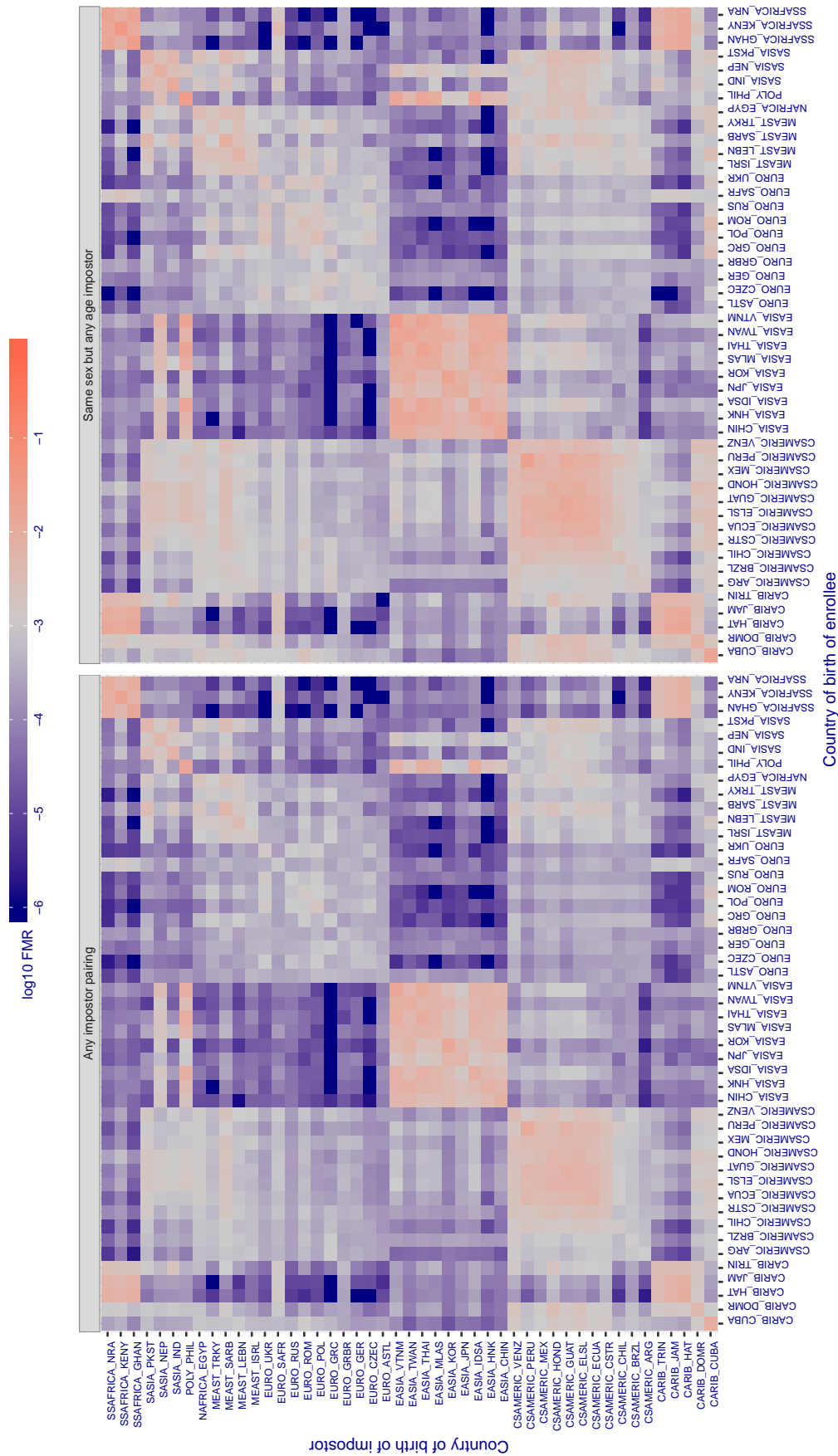


Figure 375: For algorithm gorilla-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 0.426$  for algorithm gorilla\_004, giving  $FMR(T) = 0.001$  globally.

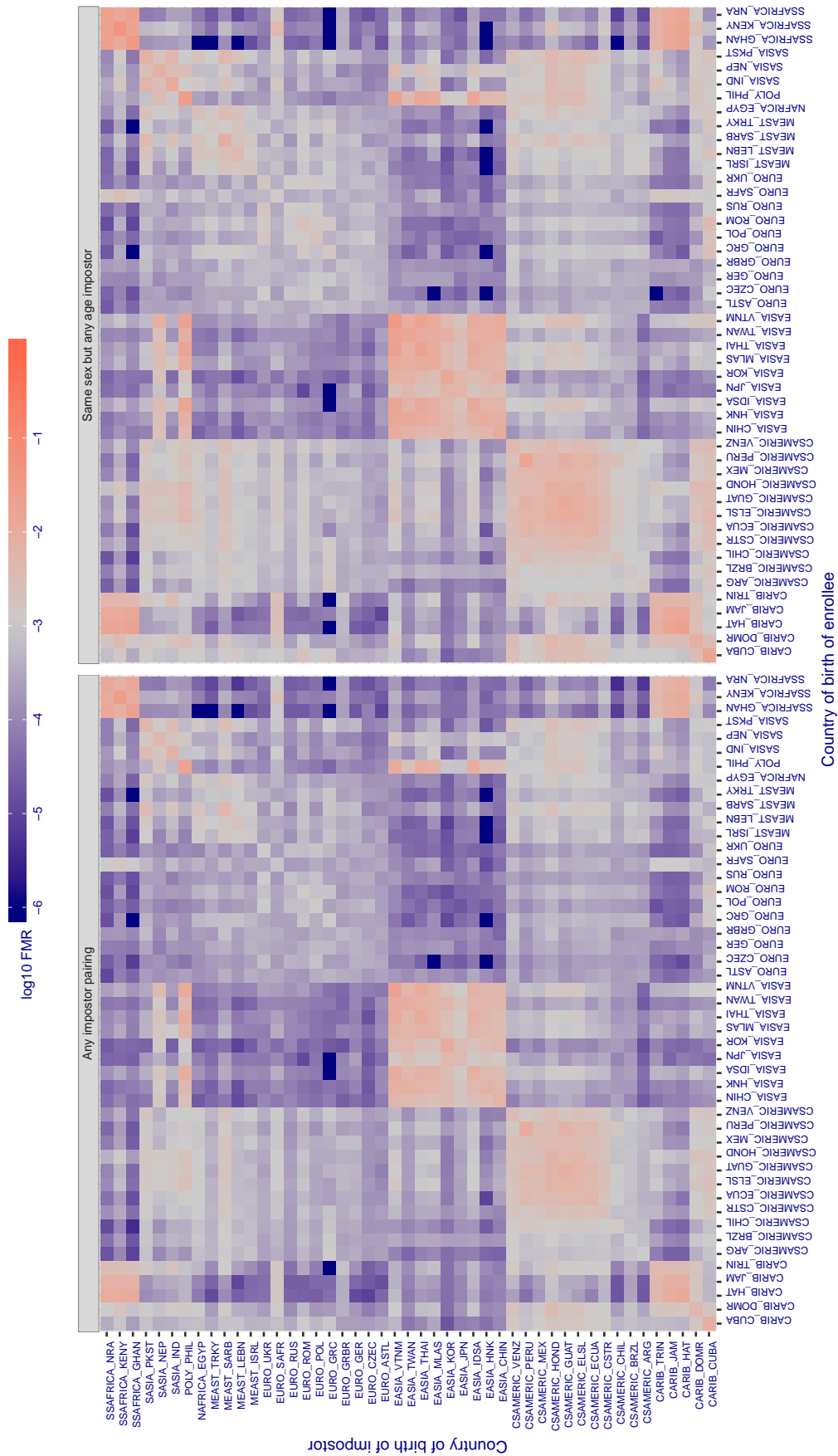


Figure 376: For algorithm gorilla-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 63.025$  for algorithm hik\_001, giving  $FMR(T) = 0.001$  globally.

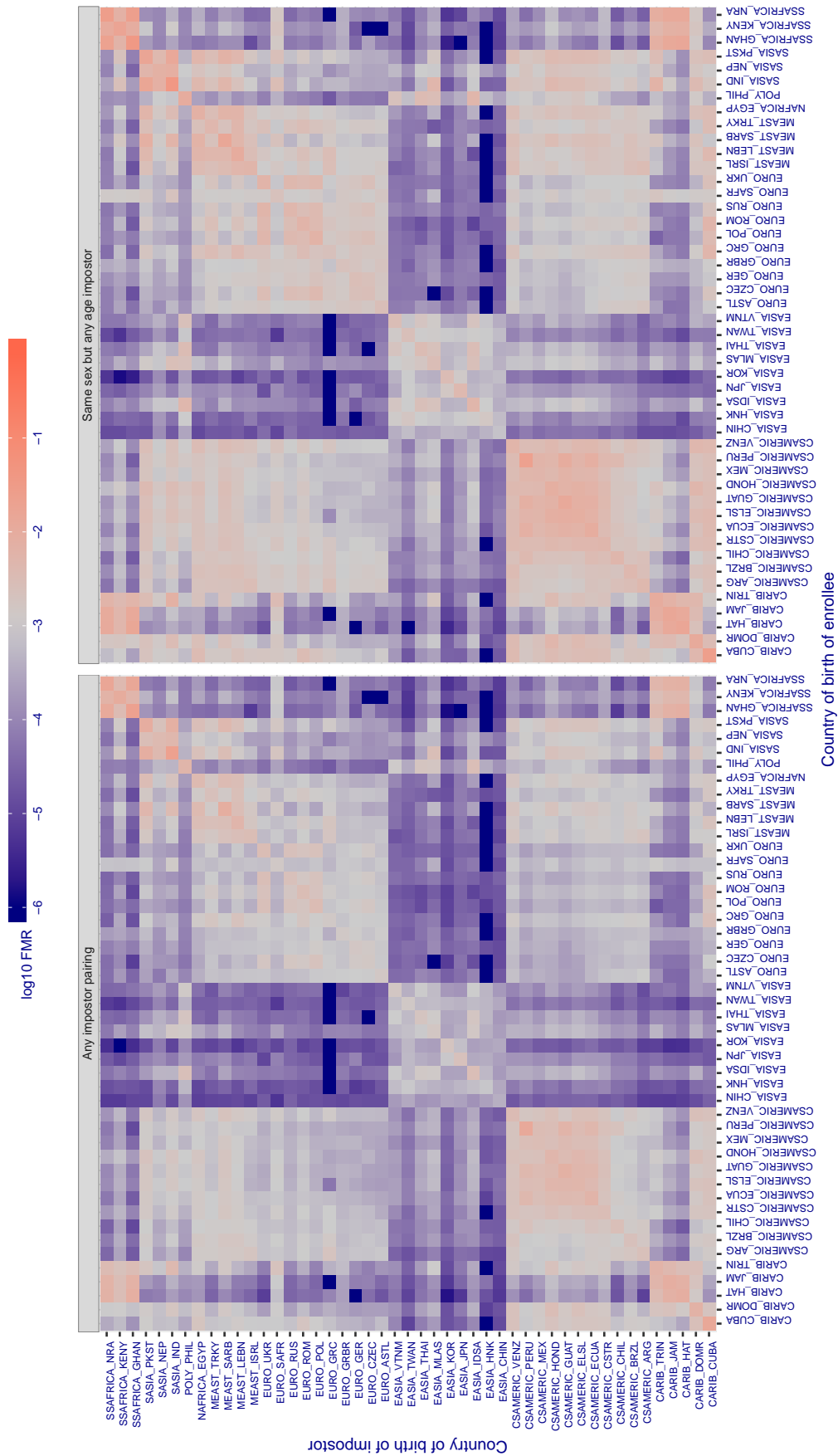


Figure 377: For algorithm hik-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.727$  for algorithm hr\_001, giving  $FMR(T) = 0.001$  globally.

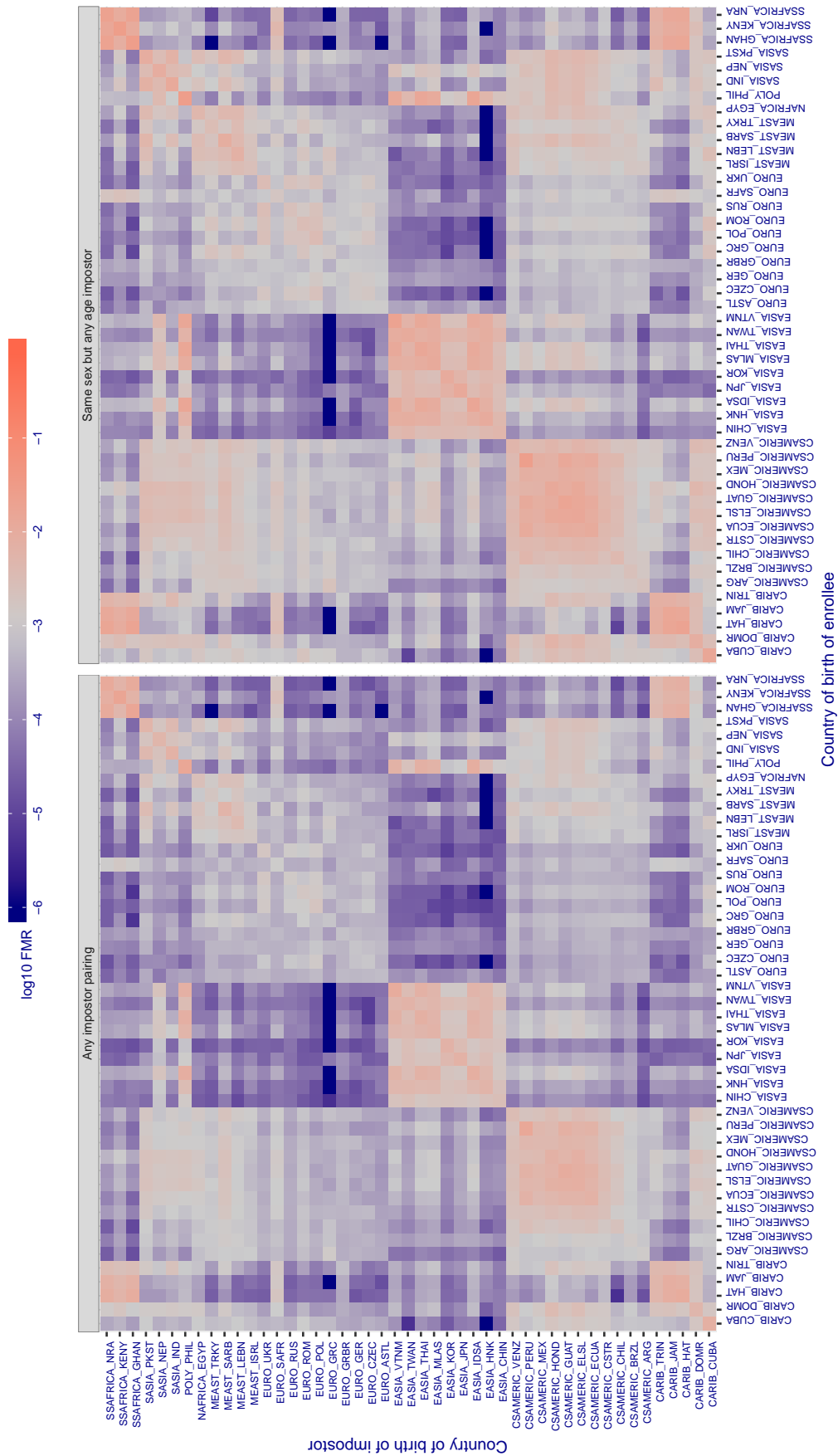


Figure 378: For algorithm hr-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log<sub>10</sub> FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.109$  for algorithm hr\_002, giving  $FMR(T) = 0.001$  globally.

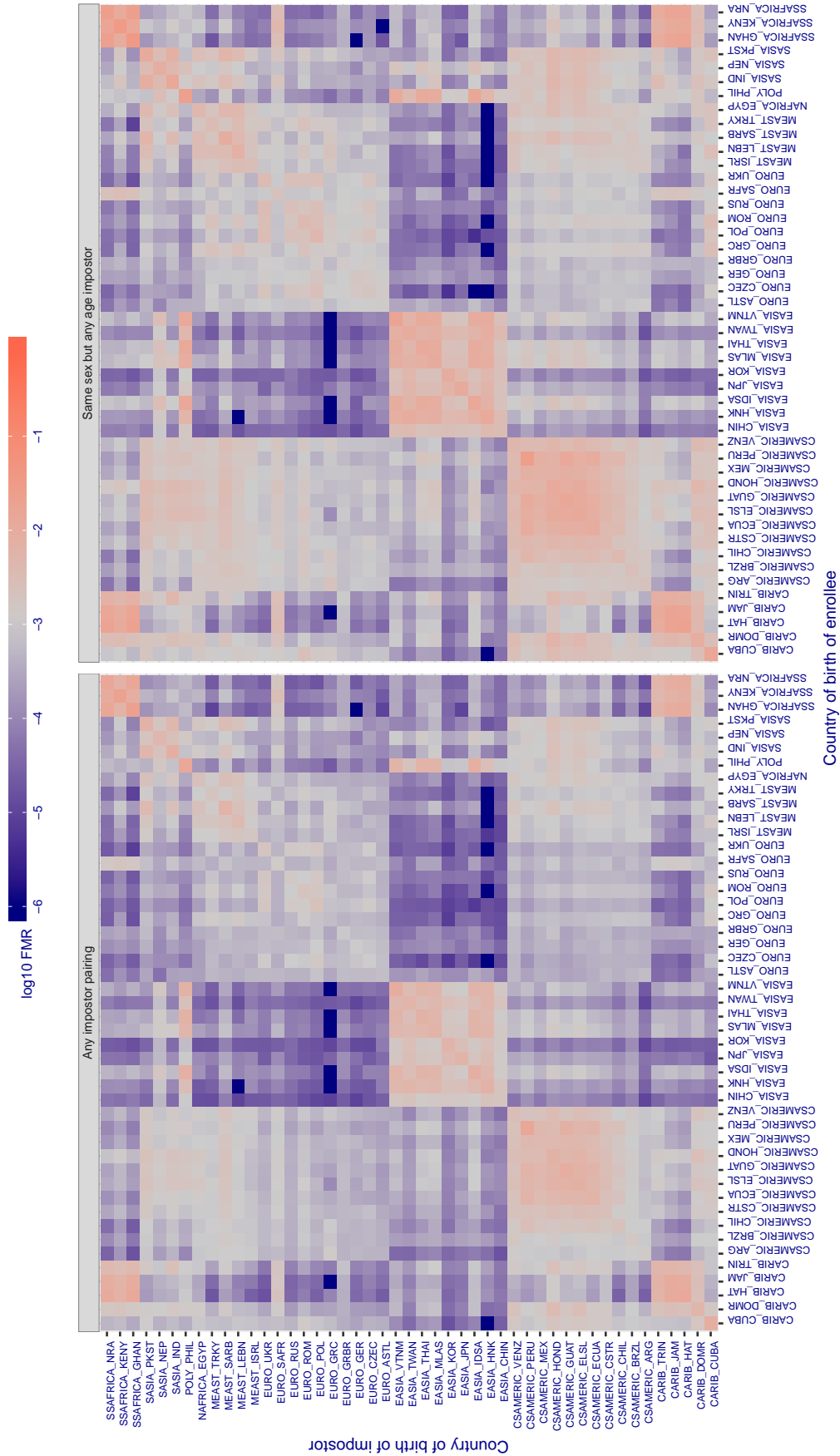


Figure 379: For algorithm hr-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 36641.000$  for algorithm `id3_003`, giving  $FMR(T) = 0.001$  globally.

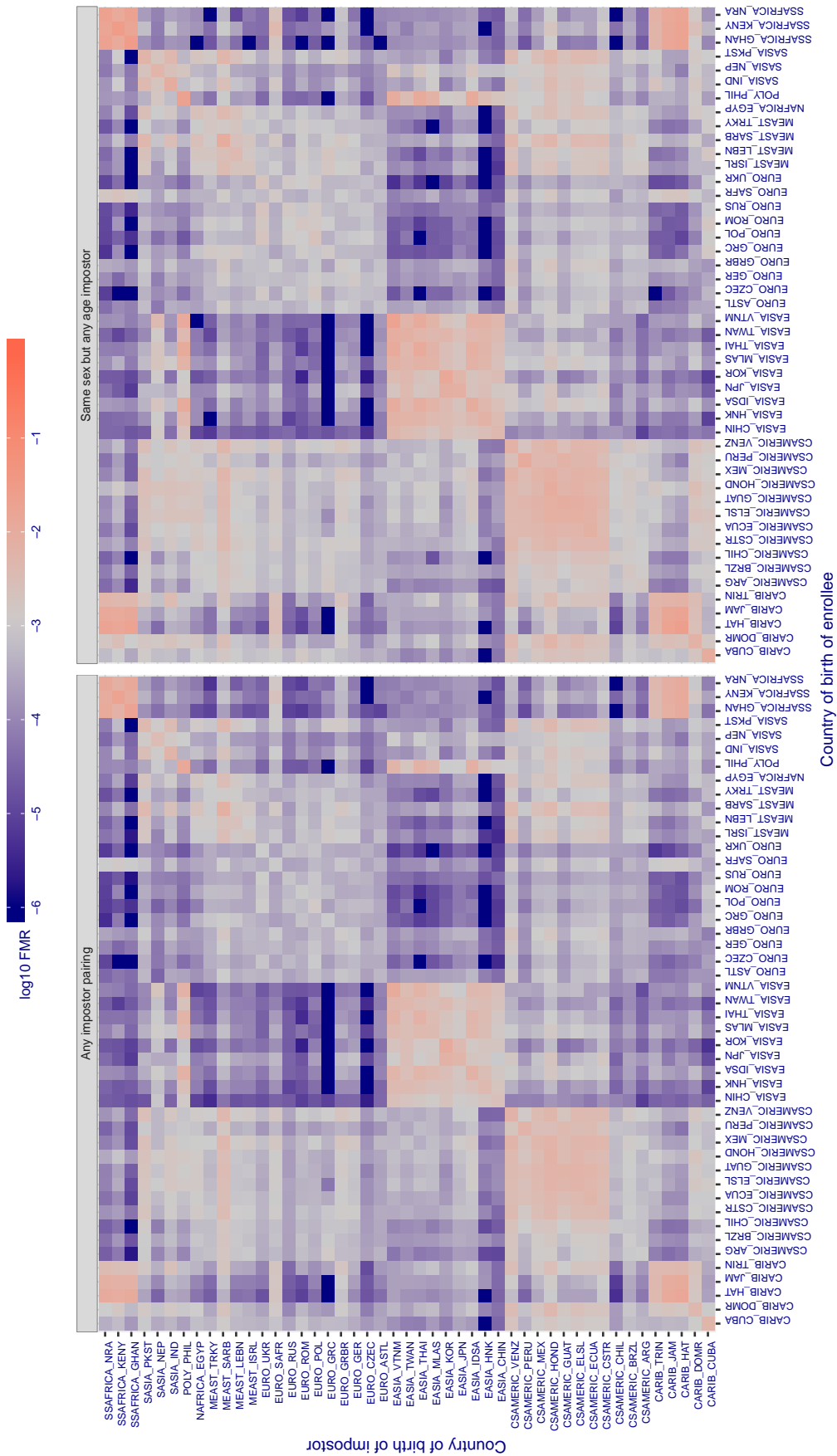


Figure 380: For algorithm `id3-003` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each  $+1$  increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 36163.000$  for algorithm `id3_004`, giving  $FMR(T) = 0.001$  globally.

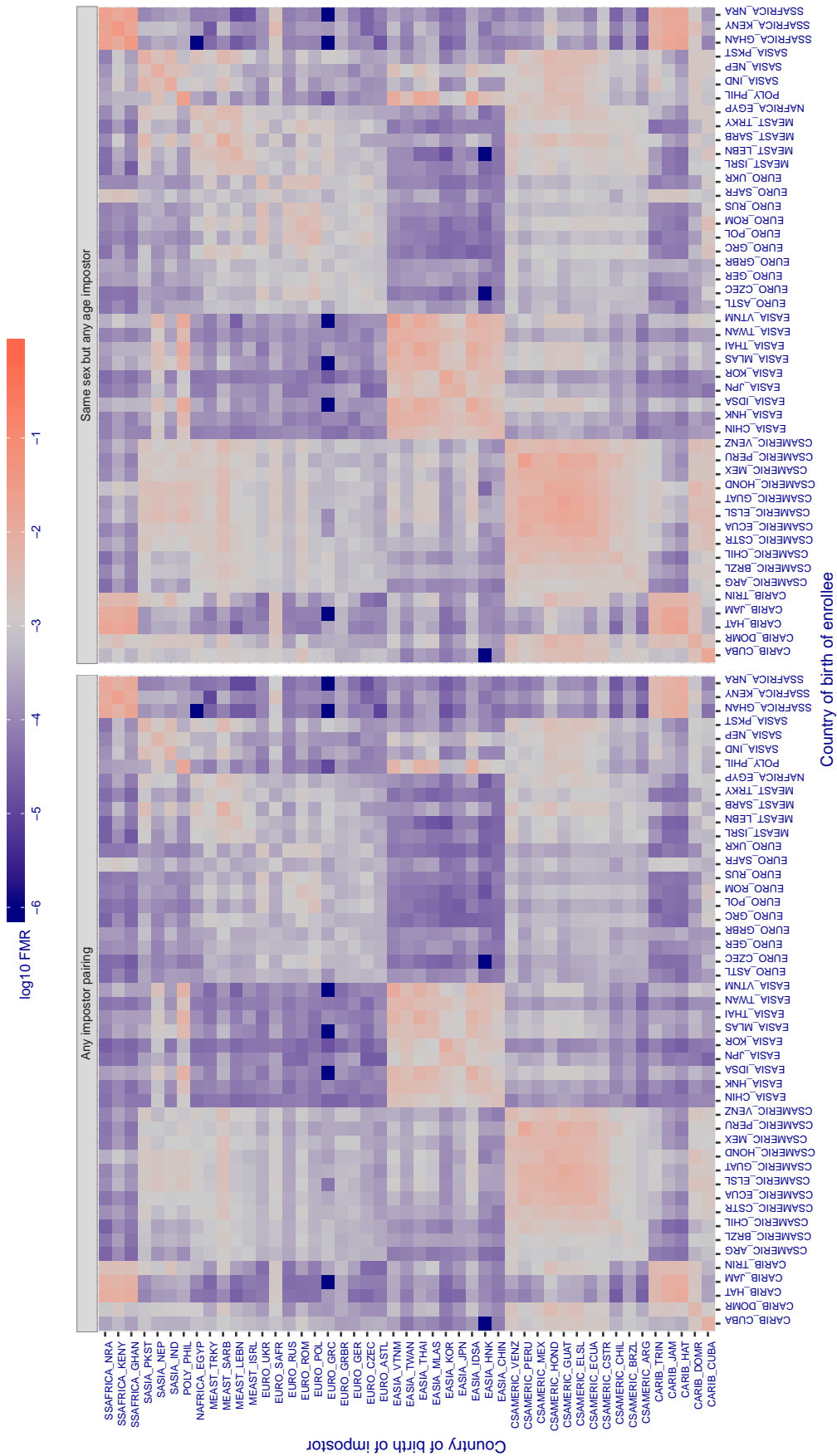


Figure 381: For algorithm `id3-004` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each  $+1$  increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 3261.090$  for algorithm idemia\_004, giving  $FMR(T) = 0.001$  globally.

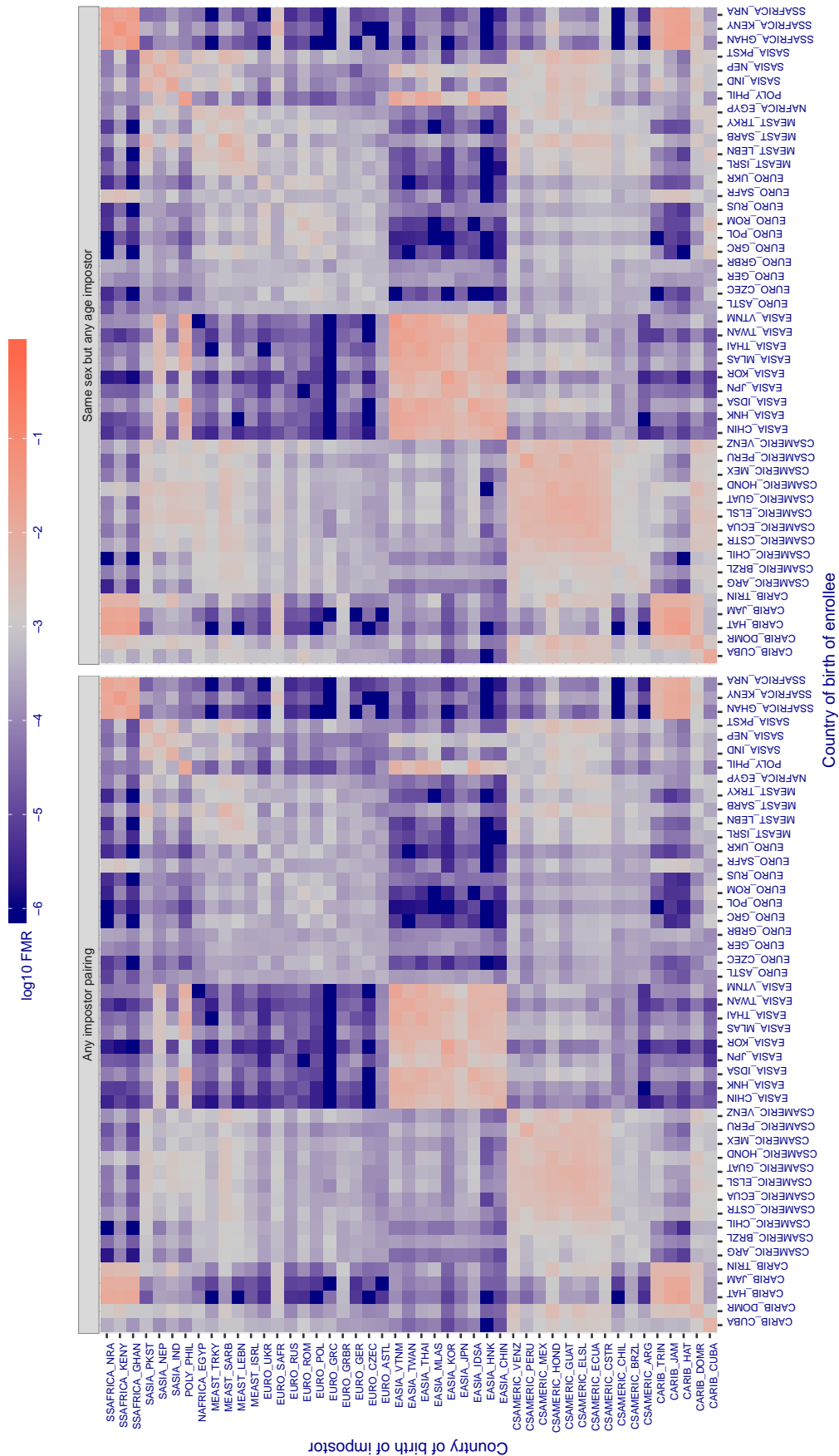


Figure 382: For algorithm idemia-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 3178.151$  for algorithm `idemia_005`, giving  $FMR(T) = 0.001$  globally.

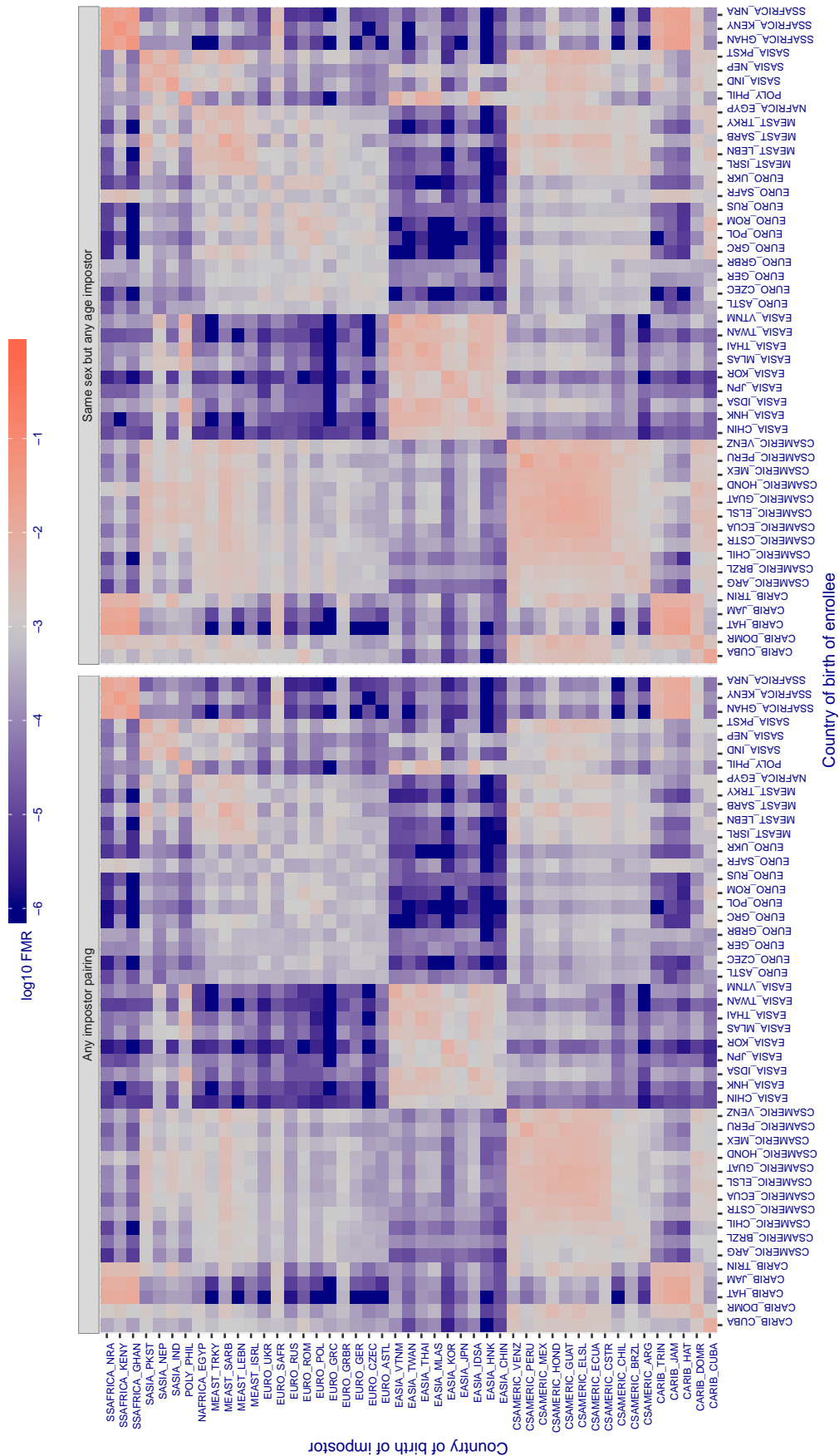


Figure 383: For algorithm `idemia-005` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 0.721$  for algorithm `it_000`, giving  $FMR(T) = 0.001$  globally.

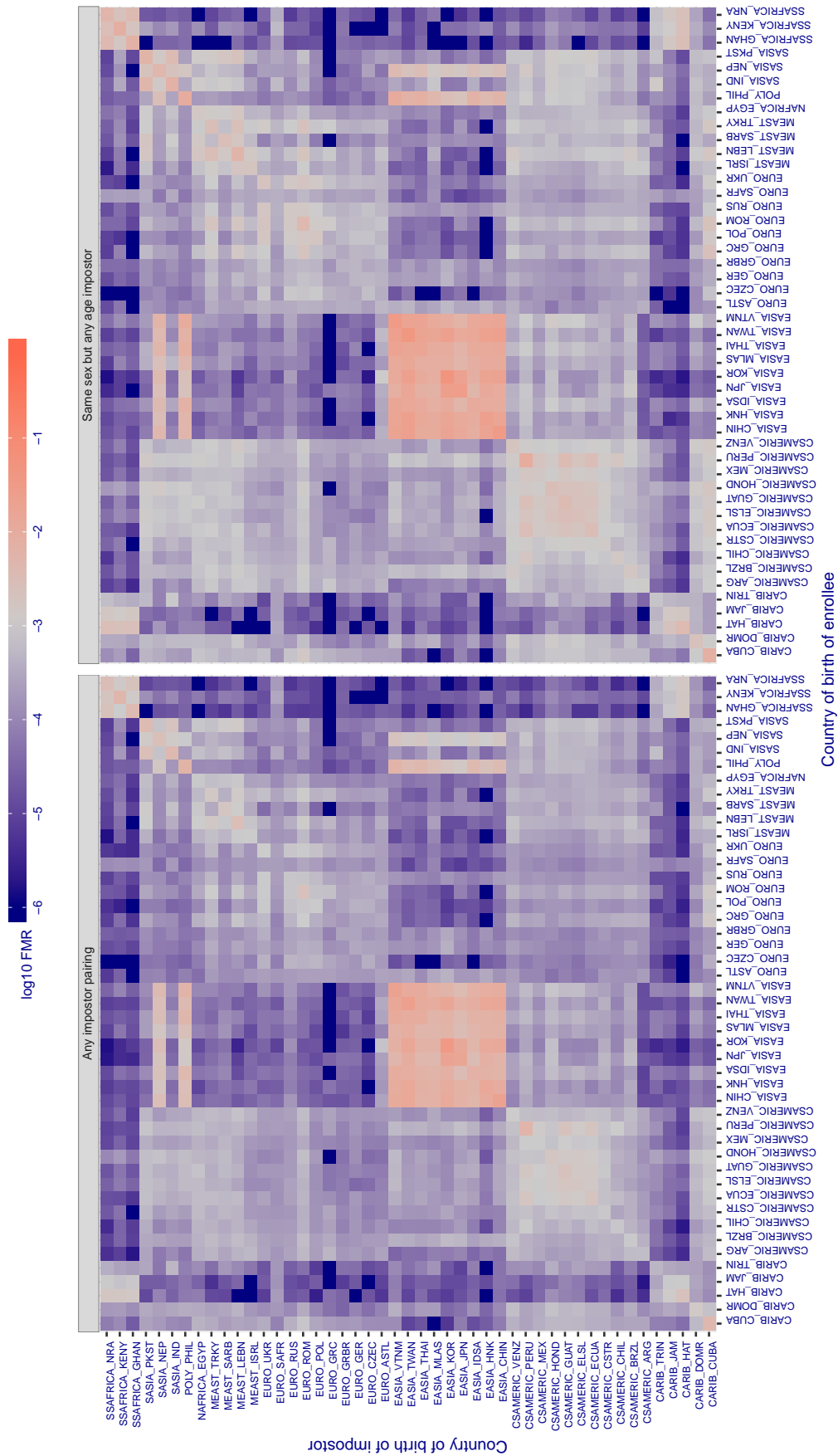


Figure 384: For algorithm `it-000` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each  $+1$  increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 0.647$  for algorithm `it_001`, giving  $FMR(T) = 0.001$  globally.

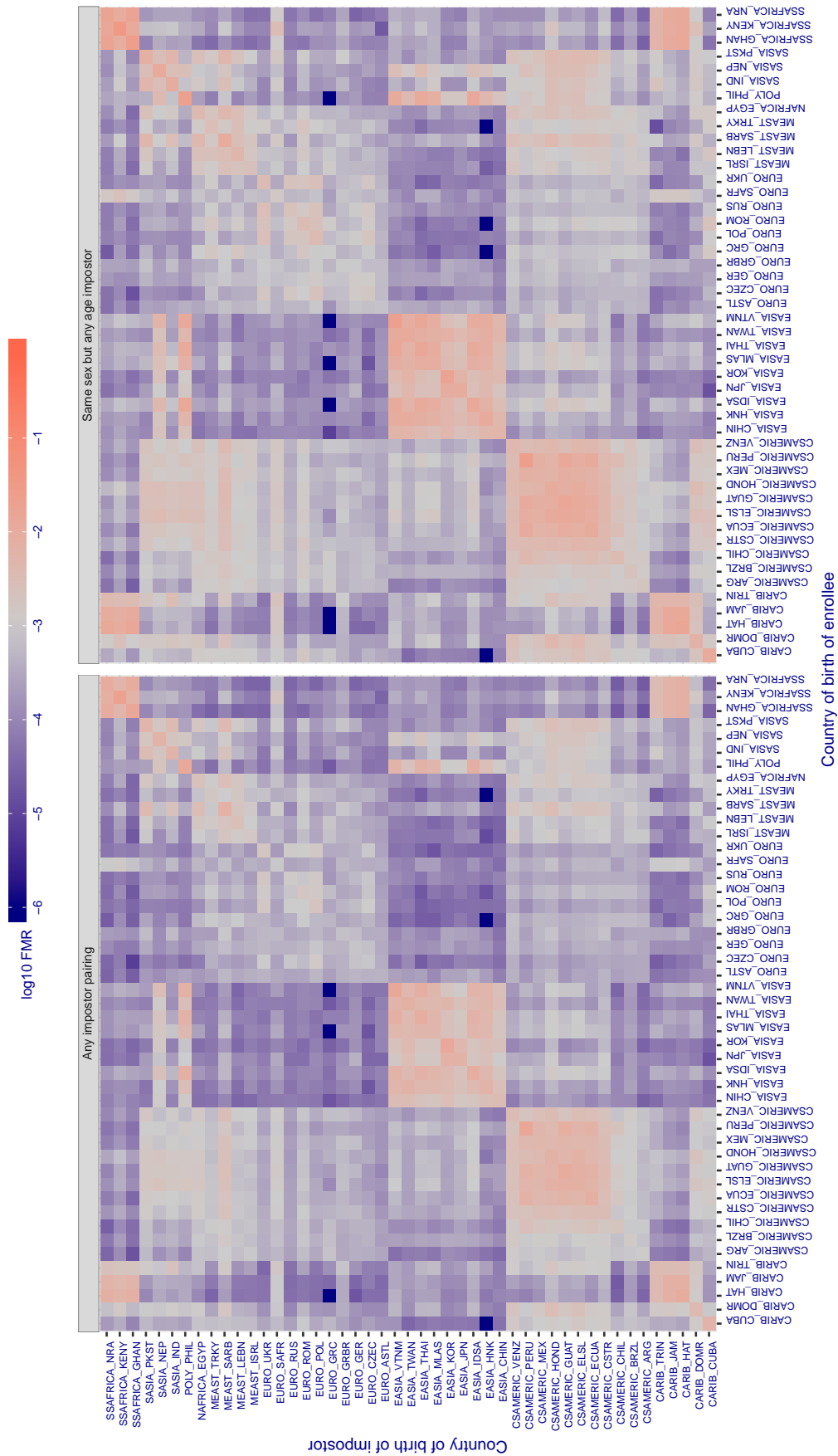


Figure 385: For algorithm `it-001` operating on *visa* images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each  $+1$  increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.809$  for algorithm `imagus_000`, giving  $FMR(T) = 0.001$  globally.

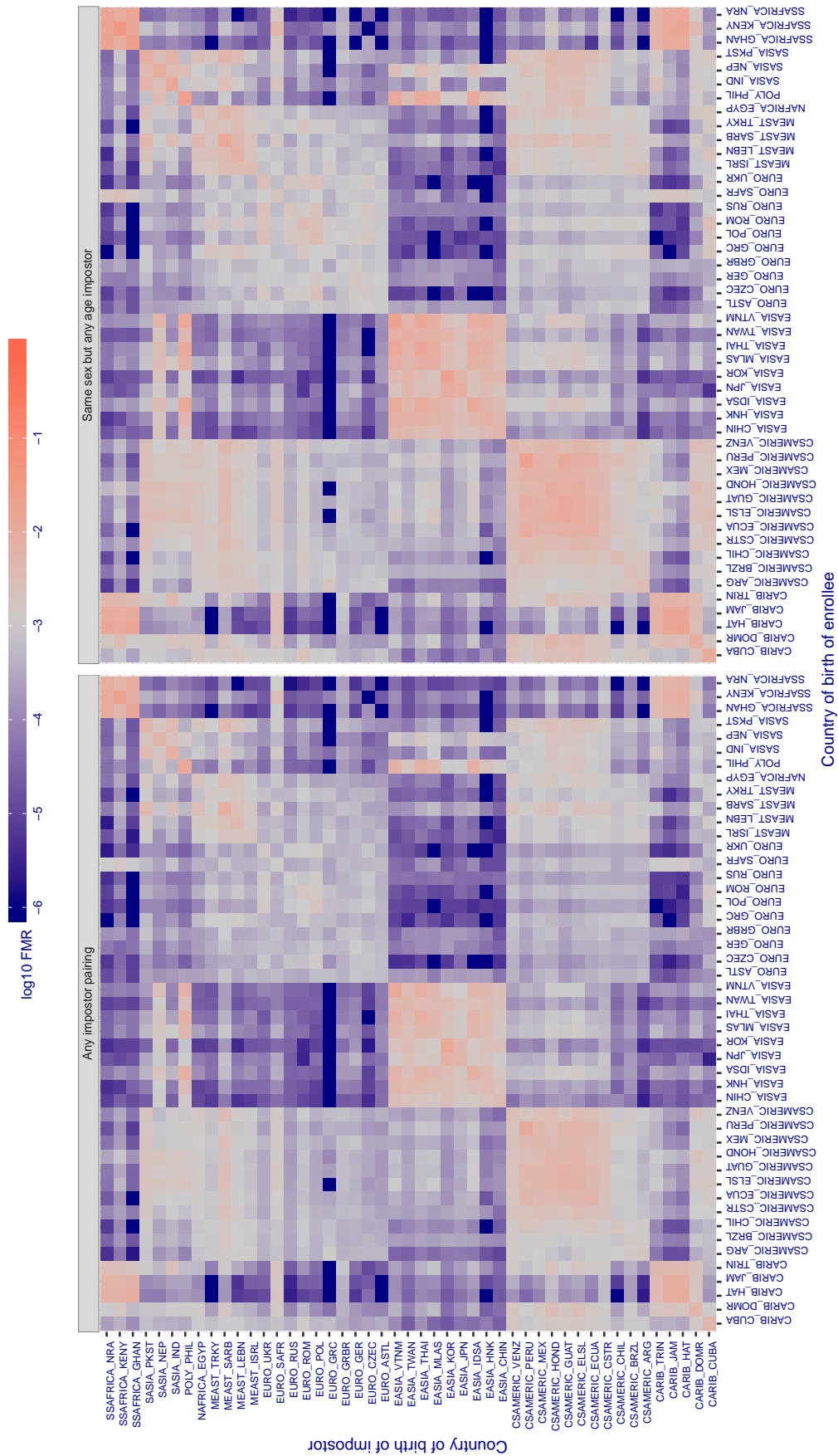


Figure 386: For algorithm `imagus-000` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each  $+1$  increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.308$  for algorithm `imagus_001`, giving  $FMR(T) = 0.001$  globally.

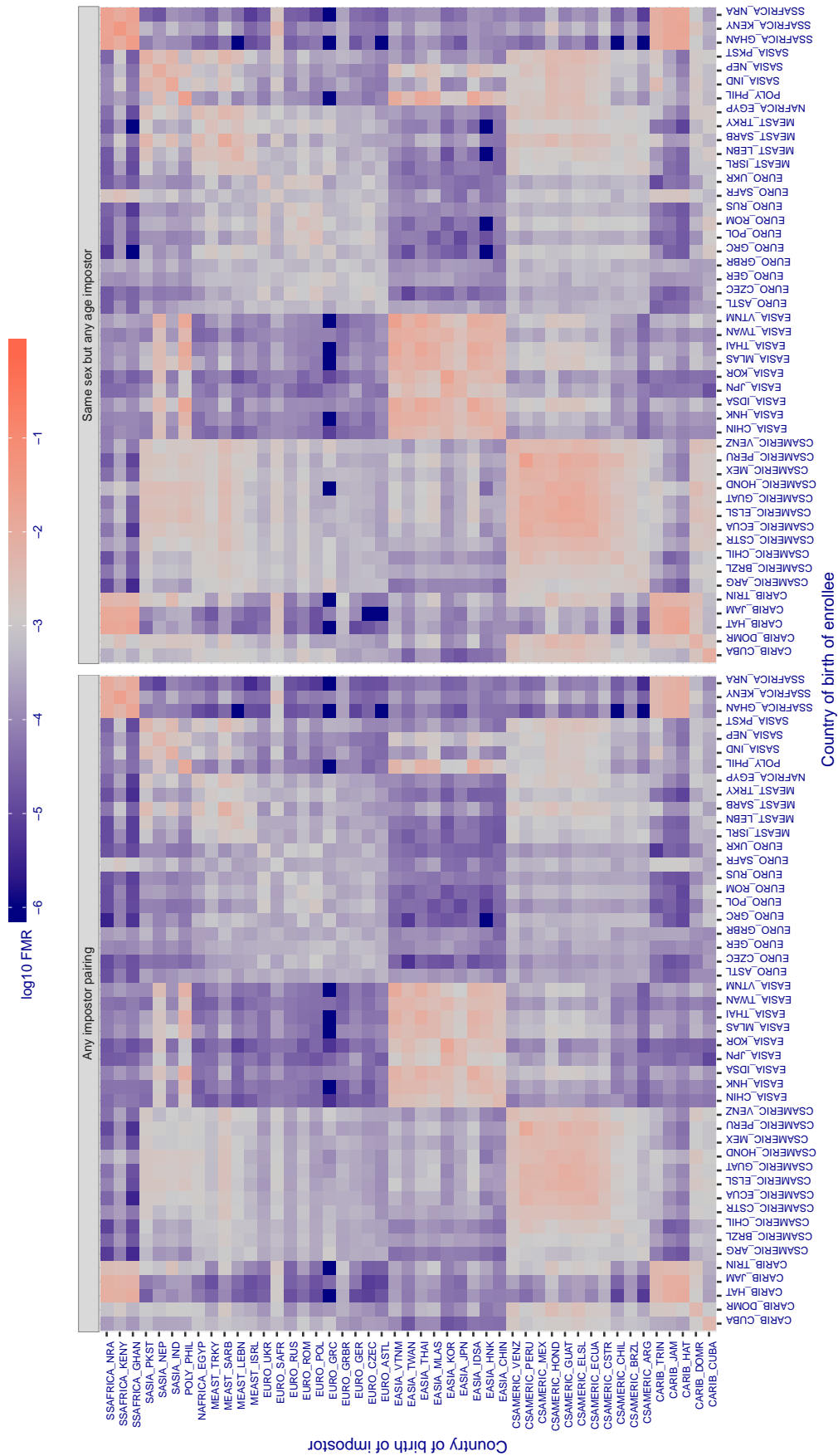


Figure 387: For algorithm `imagus-001` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each  $+1$  increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 1.302$  for algorithm imperial\_000, giving  $FMR(T) = 0.001$  globally.

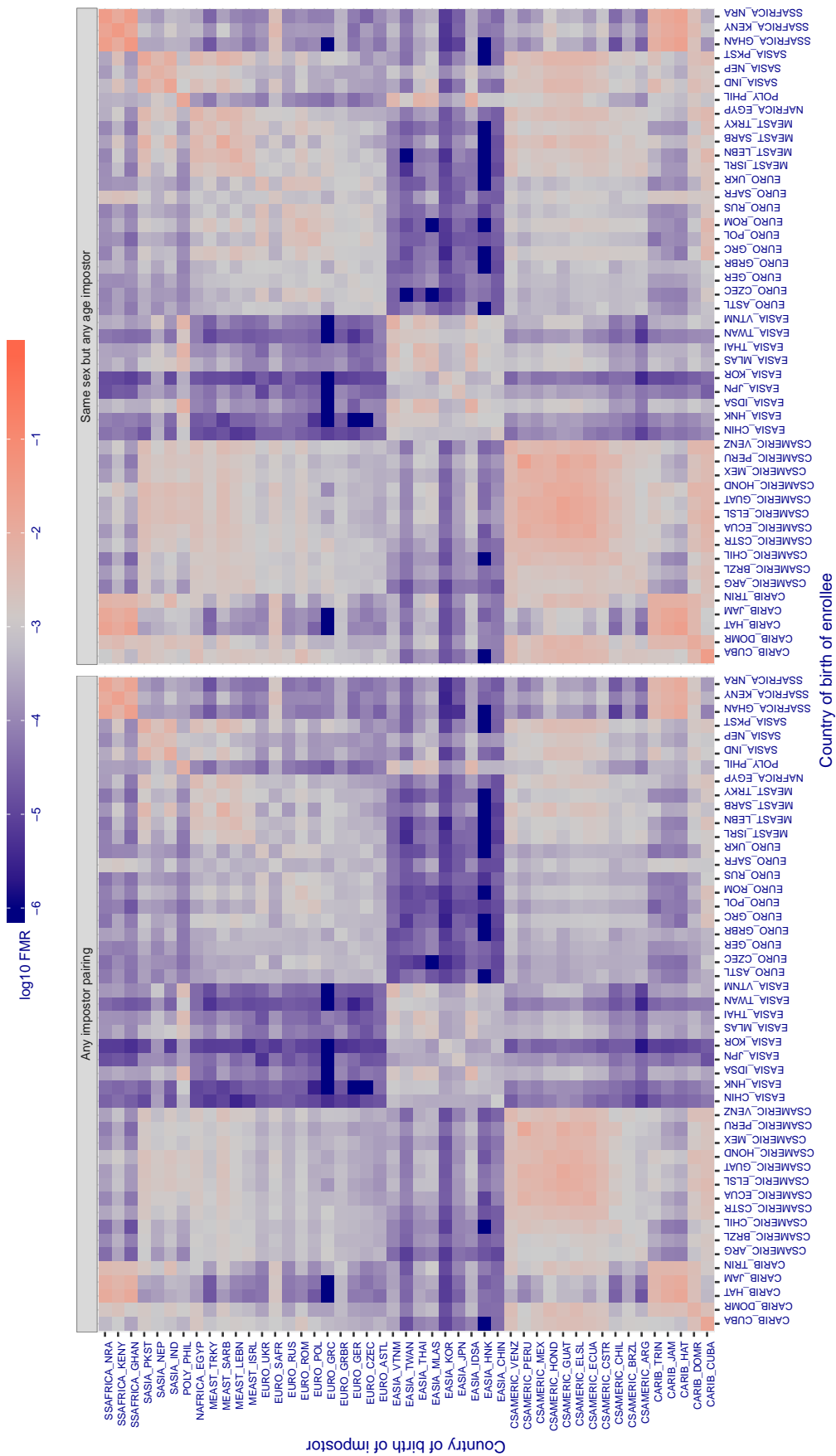


Figure 388: For algorithm imperial-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 1.285$  for algorithm imperial\_002, giving  $FMR(T) = 0.001$  globally.

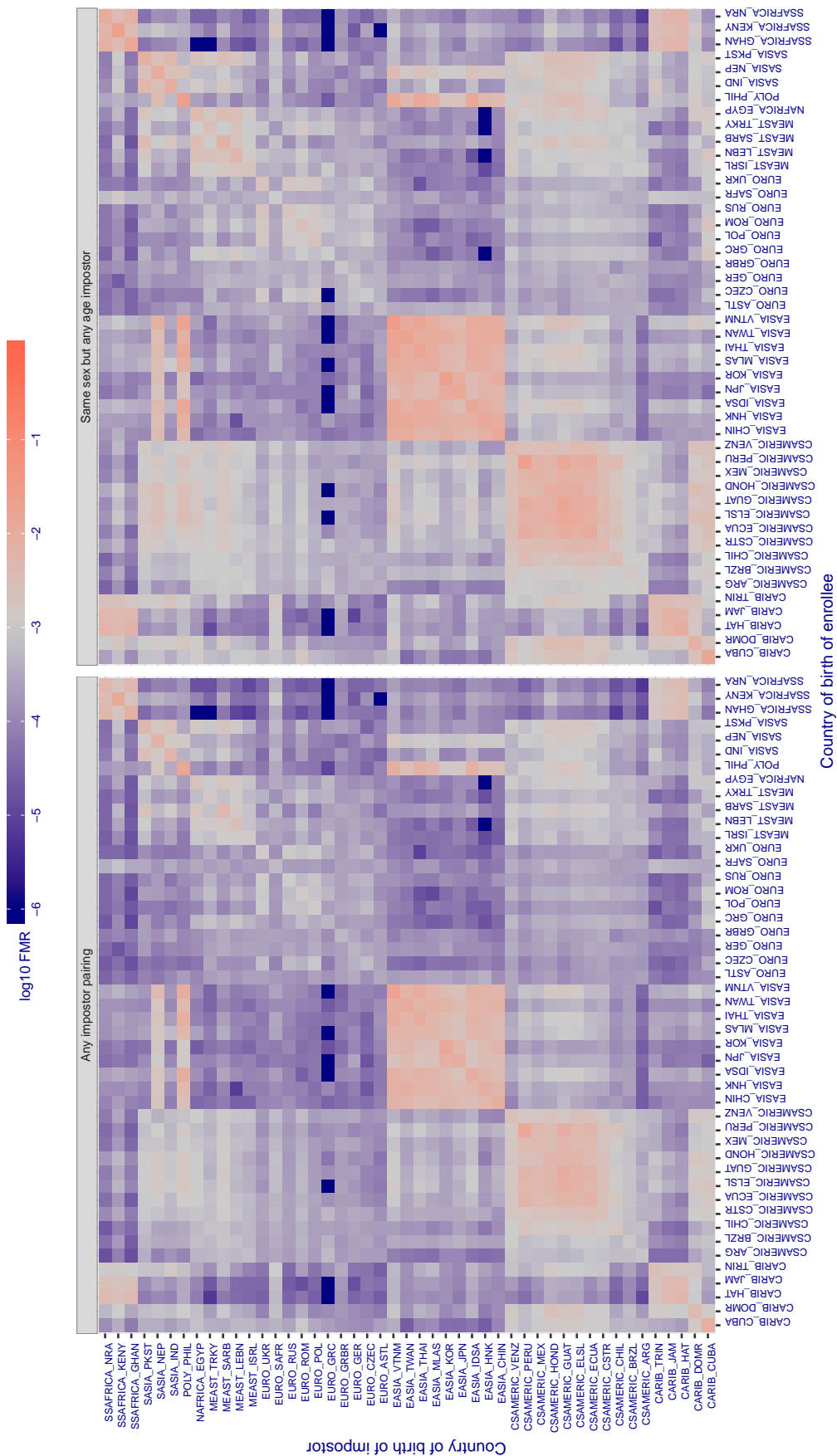


Figure 389: For algorithm imperial-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 1.314$  for algorithm incode\_004, giving  $FMR(T) = 0.001$  globally.

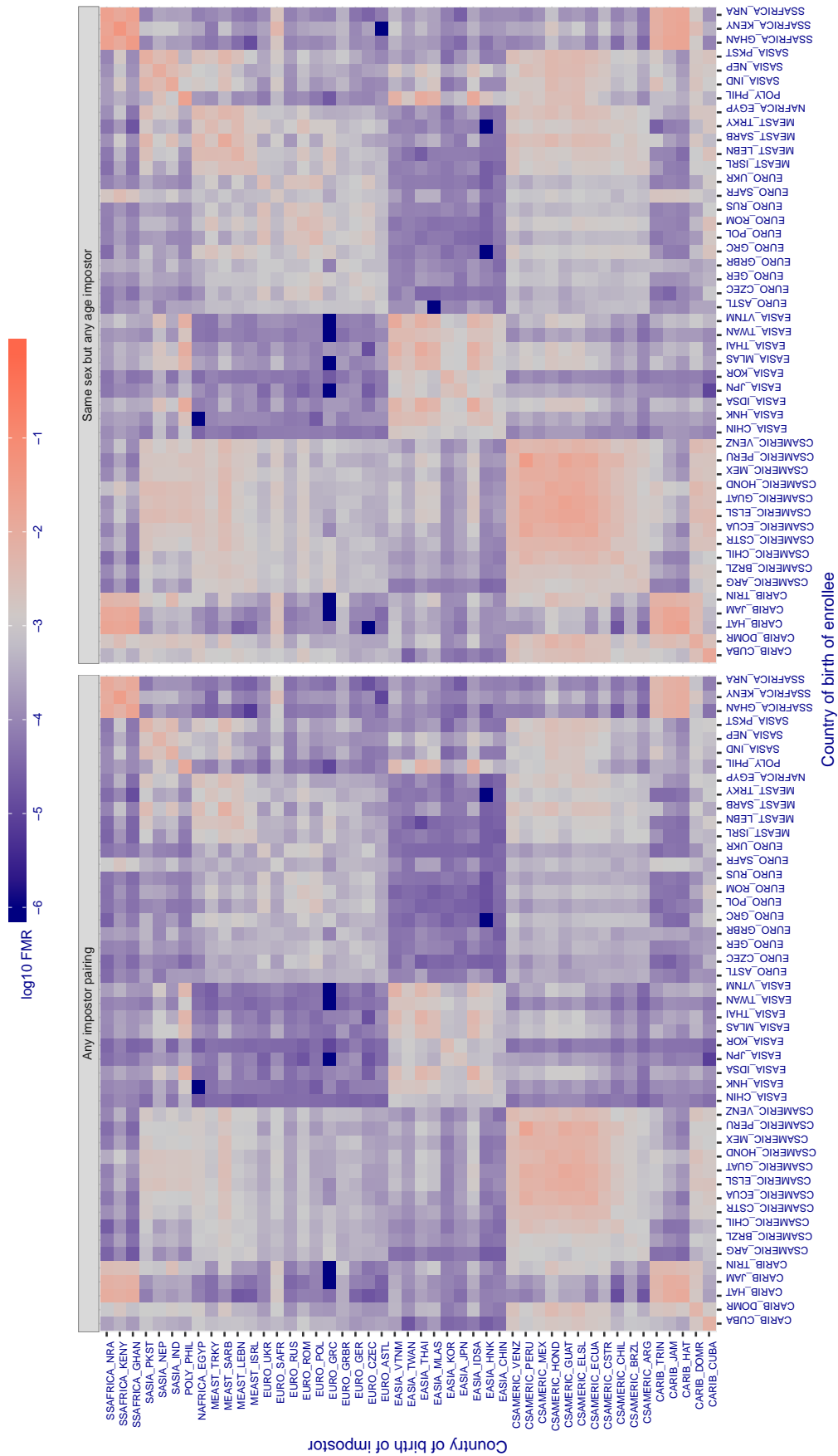


Figure 390: For algorithm incode-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.336$  for algorithm innovativetechnologytd\_001, giving  $FMR(T) = 0.001$  globally.

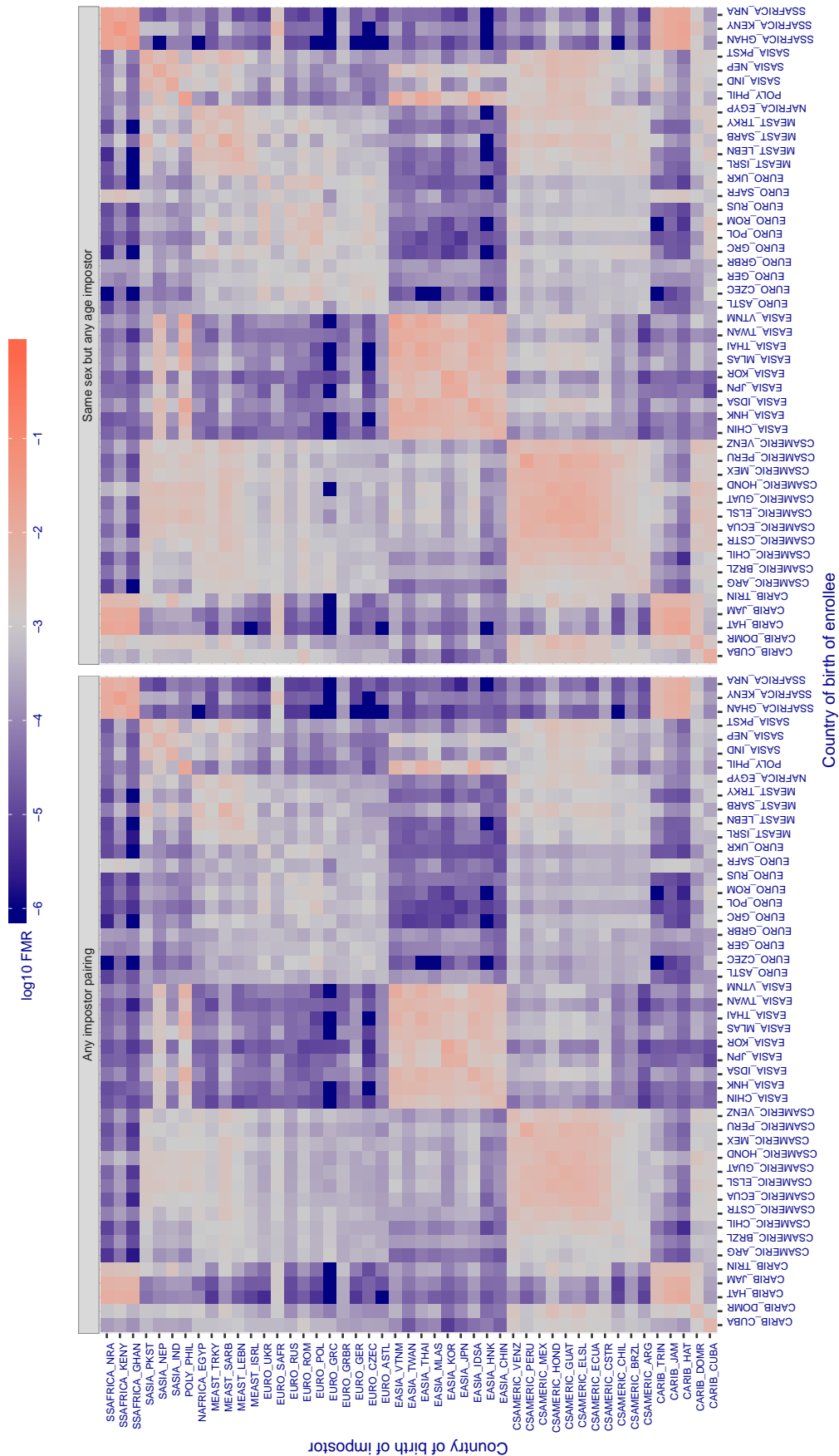


Figure 391: For algorithm innovativetechnologytd-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 21.422$  for algorithm innovatrics\_004, giving  $FMR(T) = 0.001$  globally.

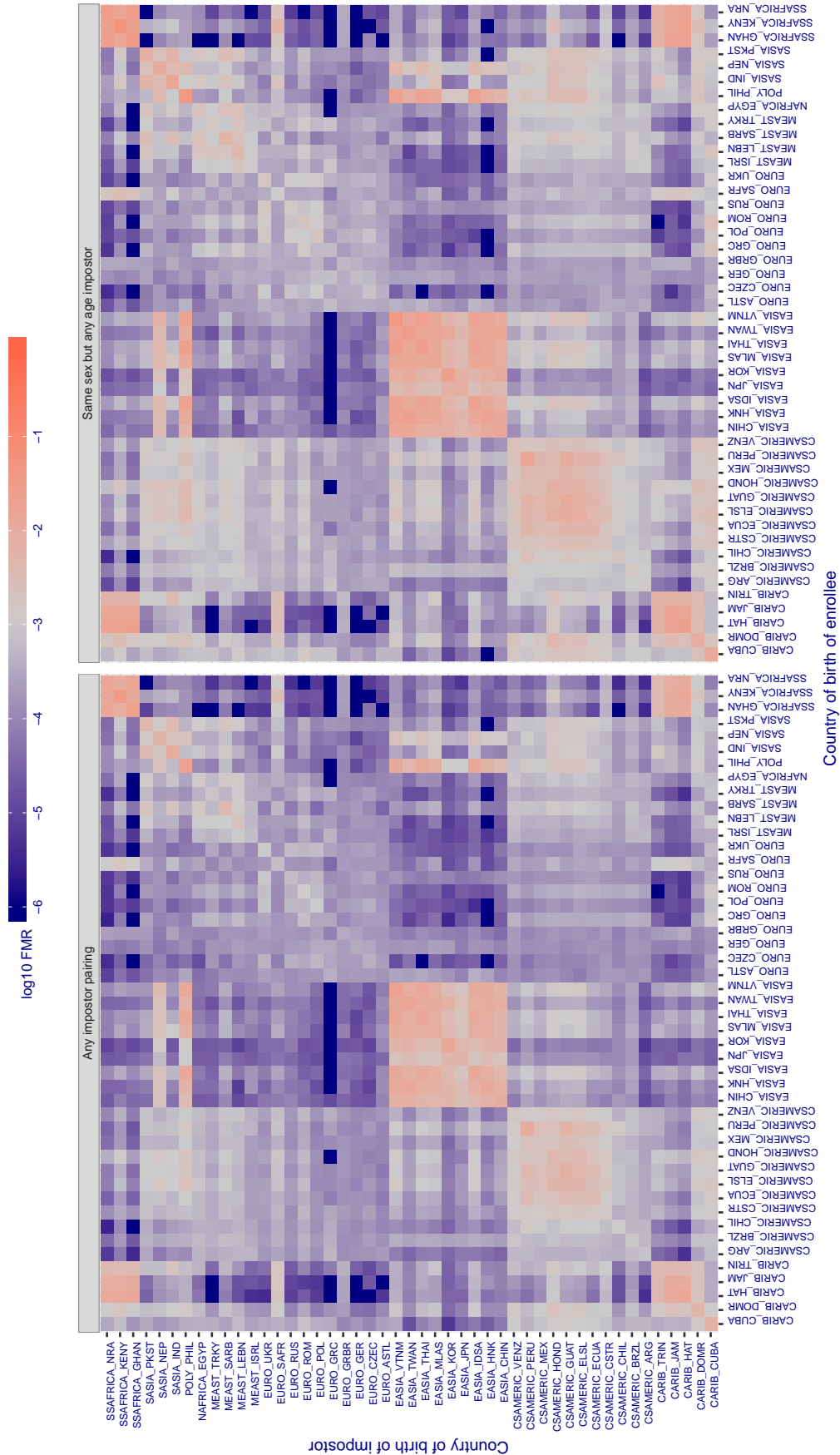


Figure 392: For algorithm innovatrics-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 20.505$  for algorithm innovatrics\_006, giving  $FMR(T) = 0.001$  globally.

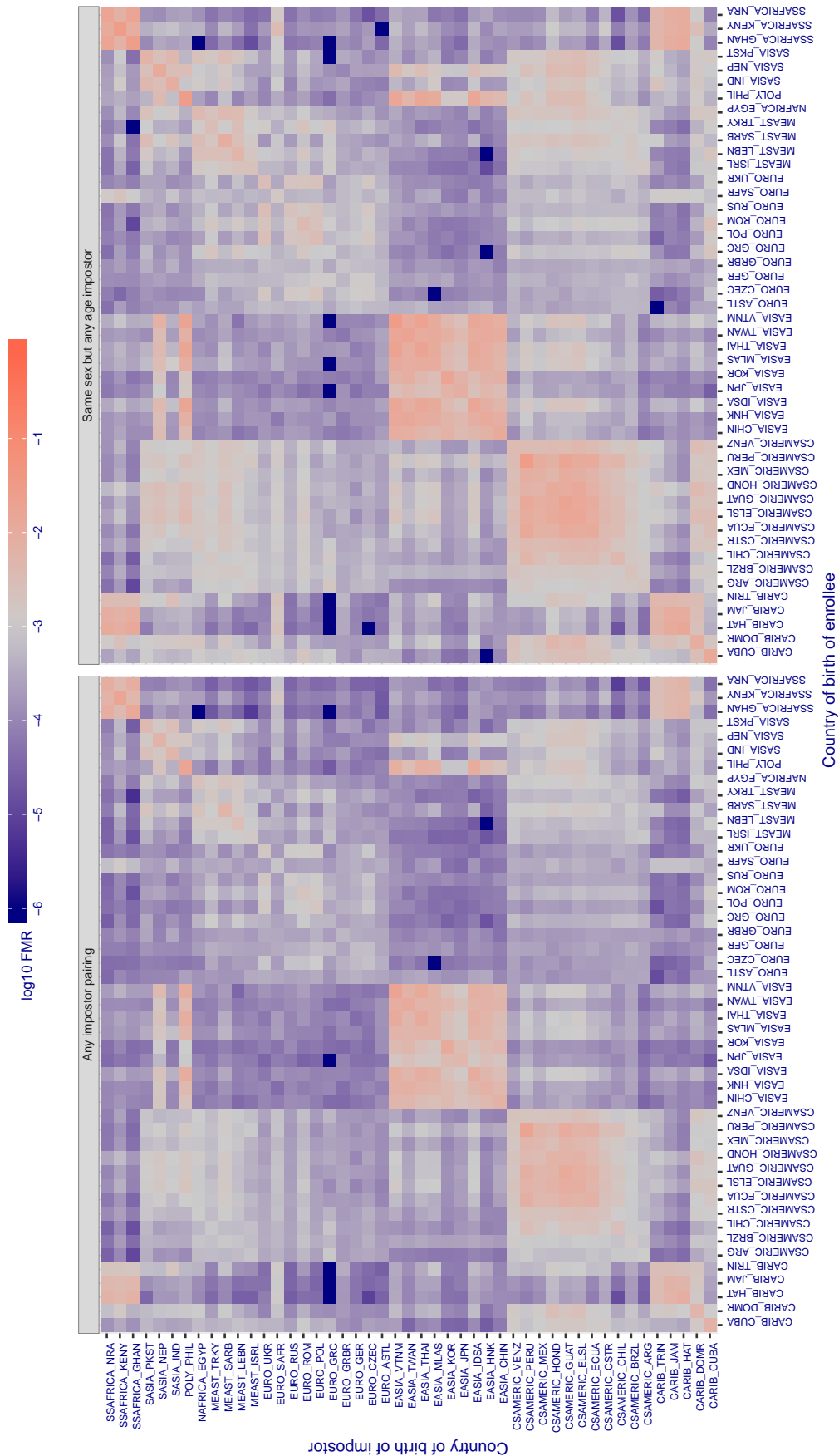


Figure 393: For algorithm innovatrics-006 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.662$  for algorithm `intellcloudai_001`, giving  $FMR(T) = 0.001$  globally.

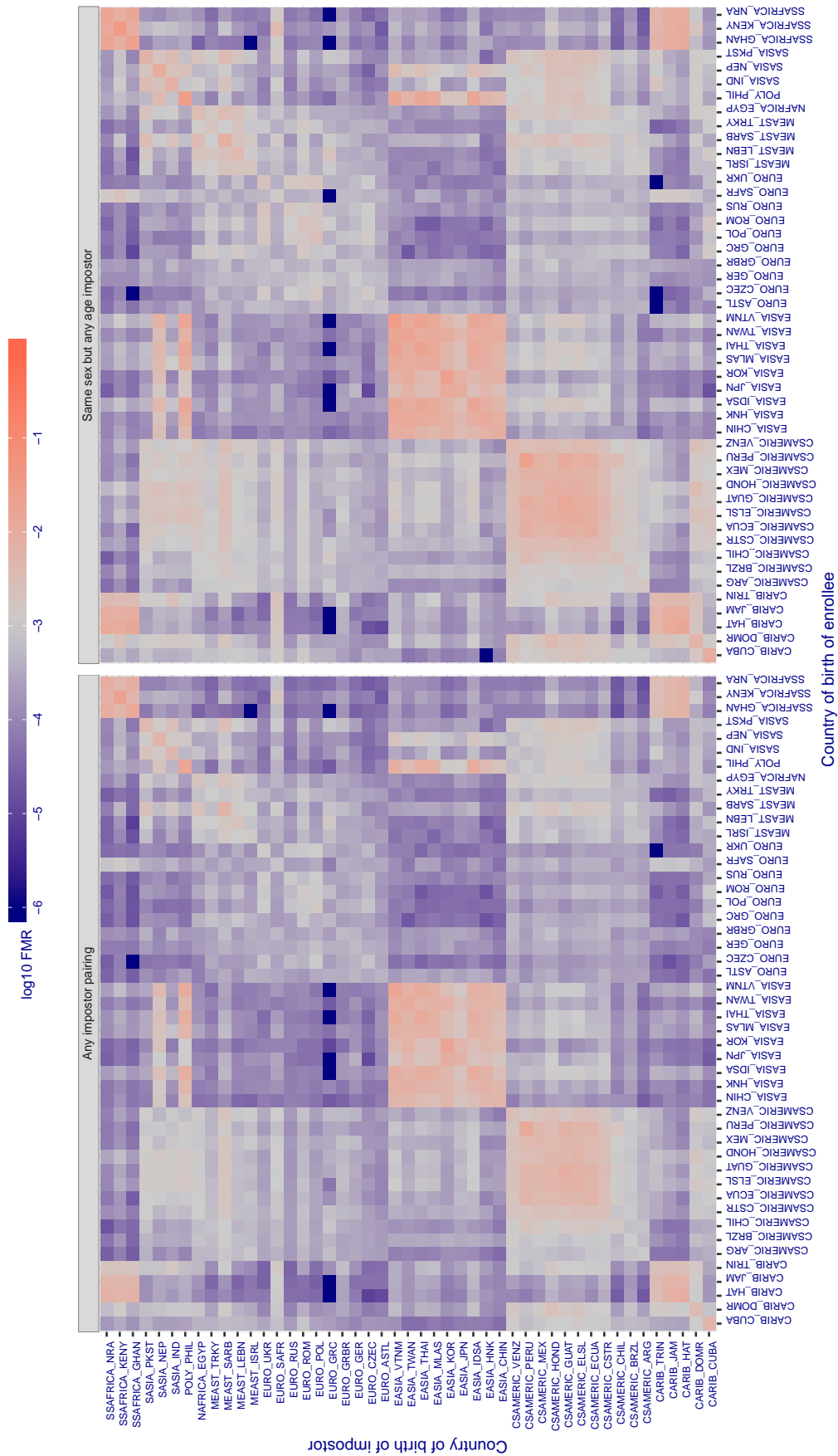


Figure 394: For algorithm `intellcloudai-001` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.240$  for algorithm intellifusion\_001, giving  $FMR(T) = 0.001$  globally.

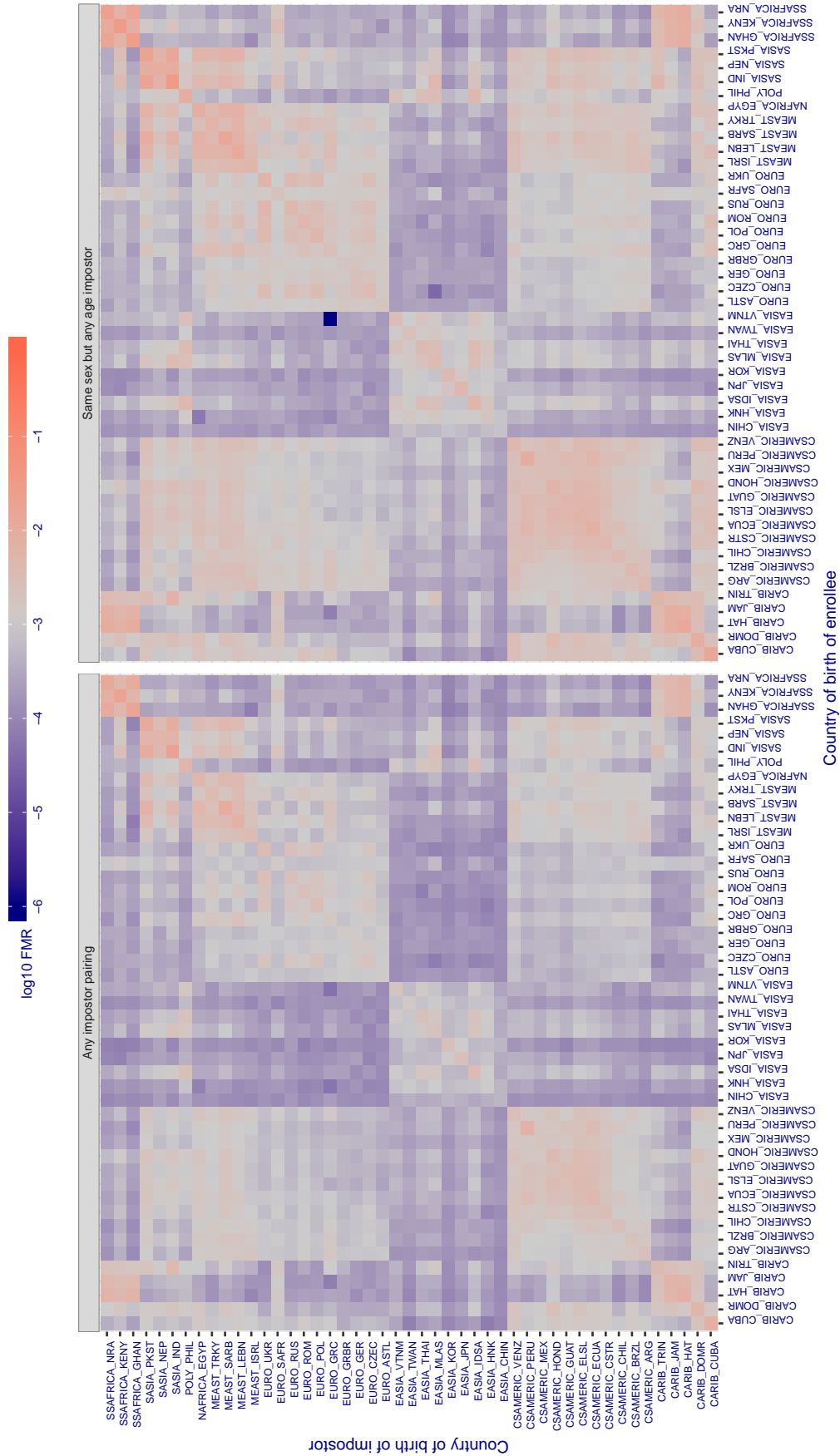


Figure 395: For algorithm intellifusion-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 37.554$  for algorithm intellivision\_001, giving  $FMR(T) = 0.001$  globally.

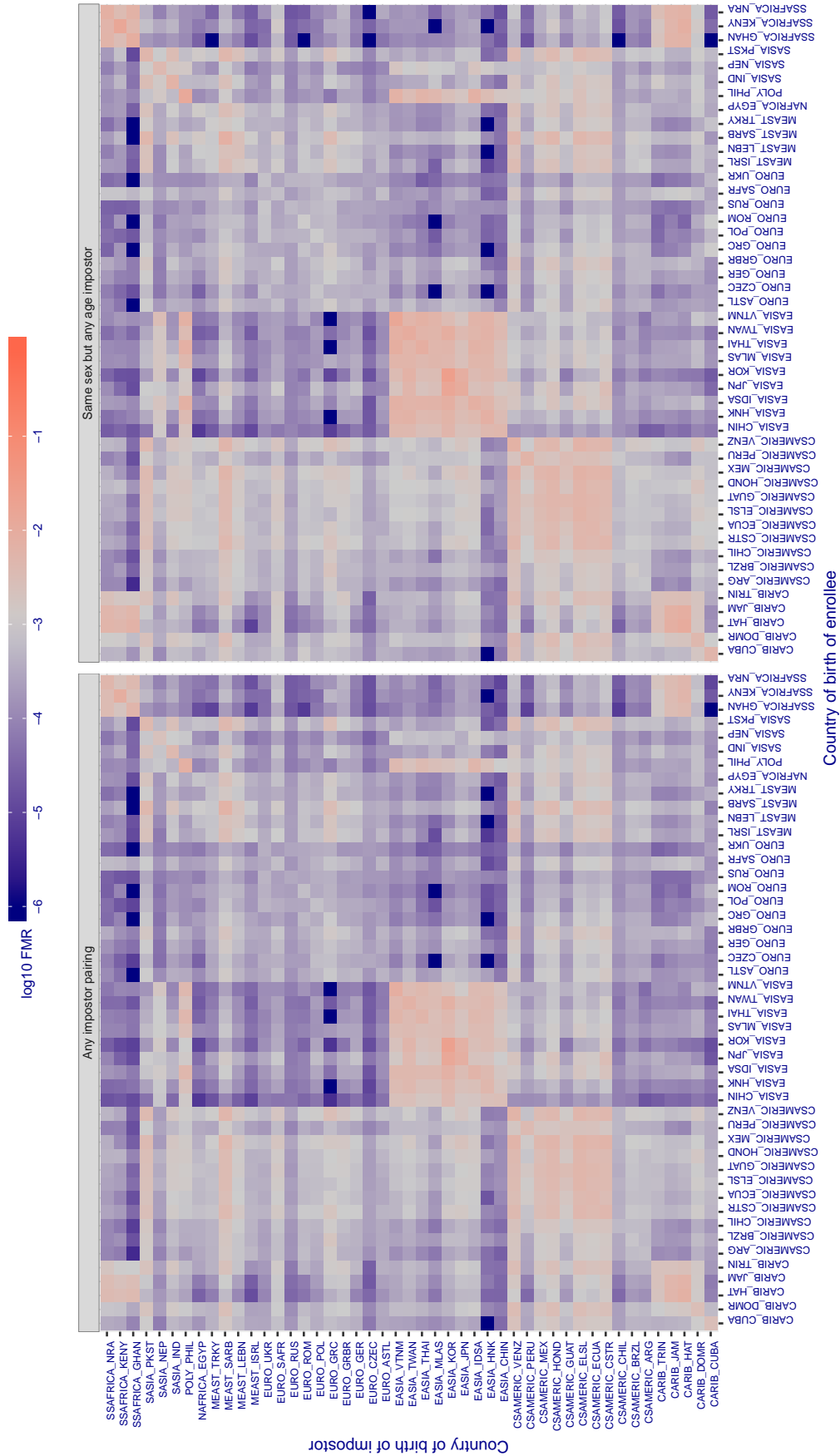


Figure 396: For algorithm intellivision-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 31.547$  for algorithm intellivision\_002, giving  $FMR(T) = 0.001$  globally.

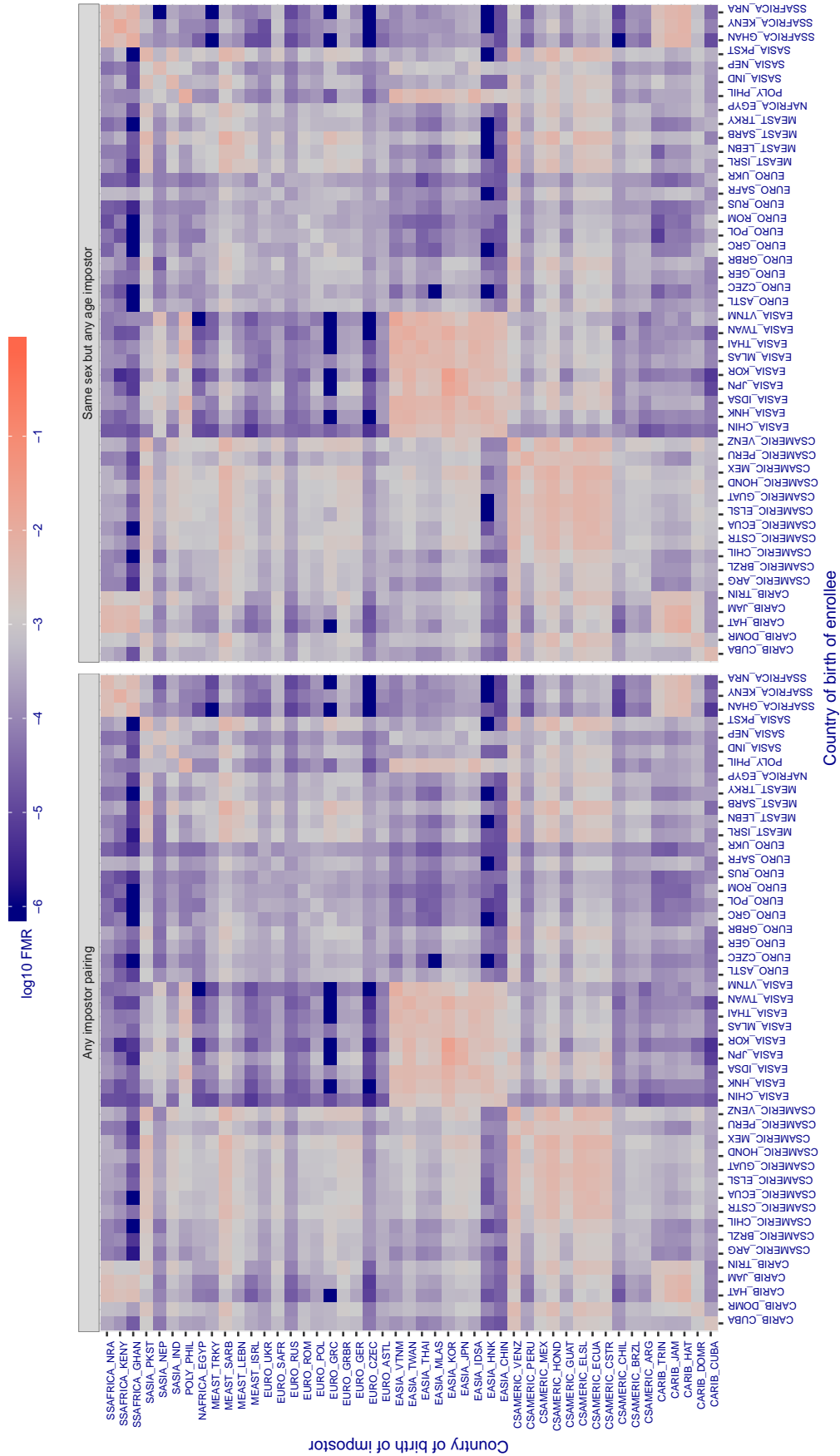


Figure 397: For algorithm intellivision-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 1.306$  for algorithm intsysmsu\_000, giving  $FMR(T) = 0.001$  globally.

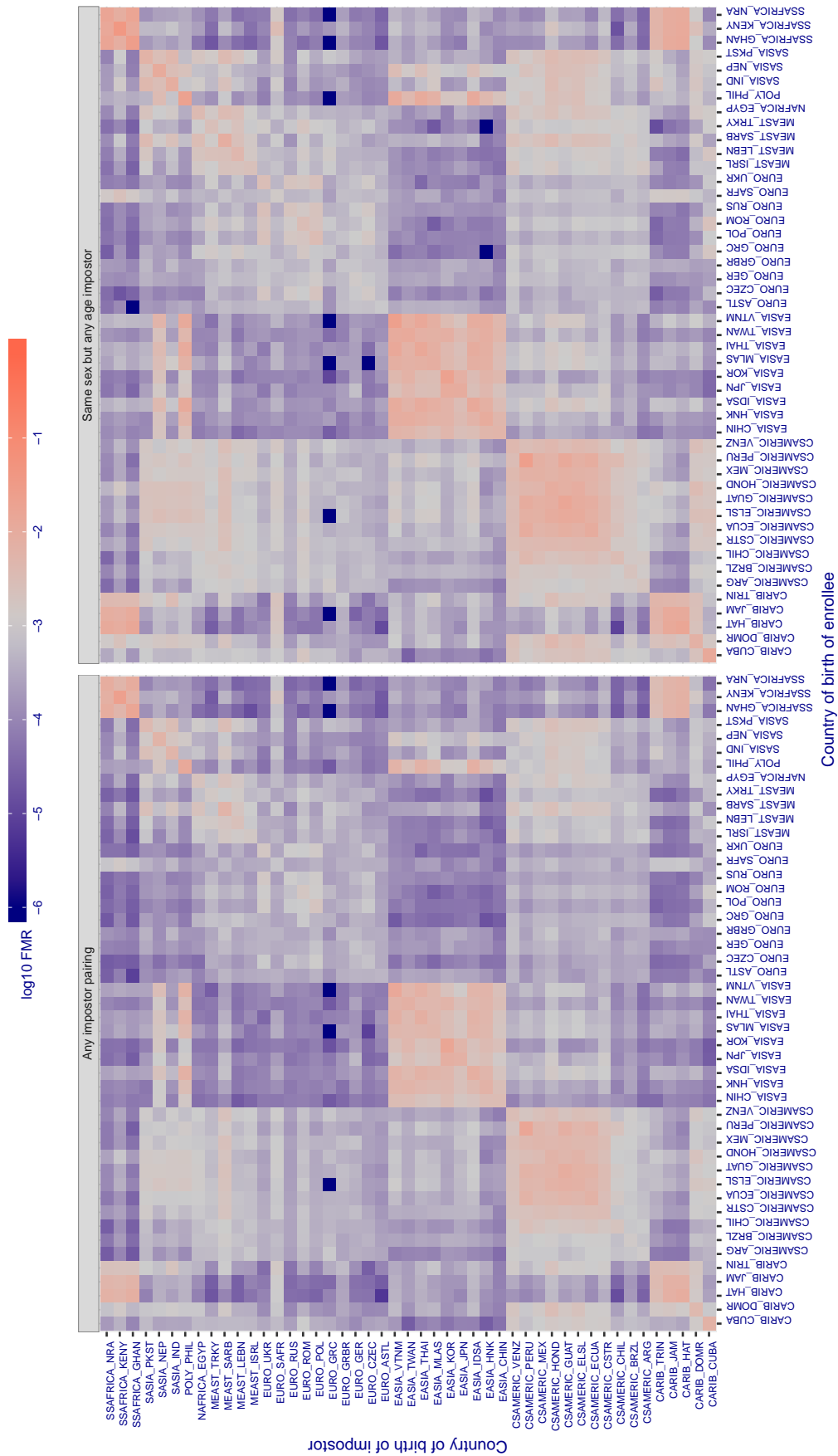


Figure 399: For algorithm intsysmsu-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 1.924$  for algorithm intsysmsu\_001, giving  $FMR(T) = 0.001$  globally.

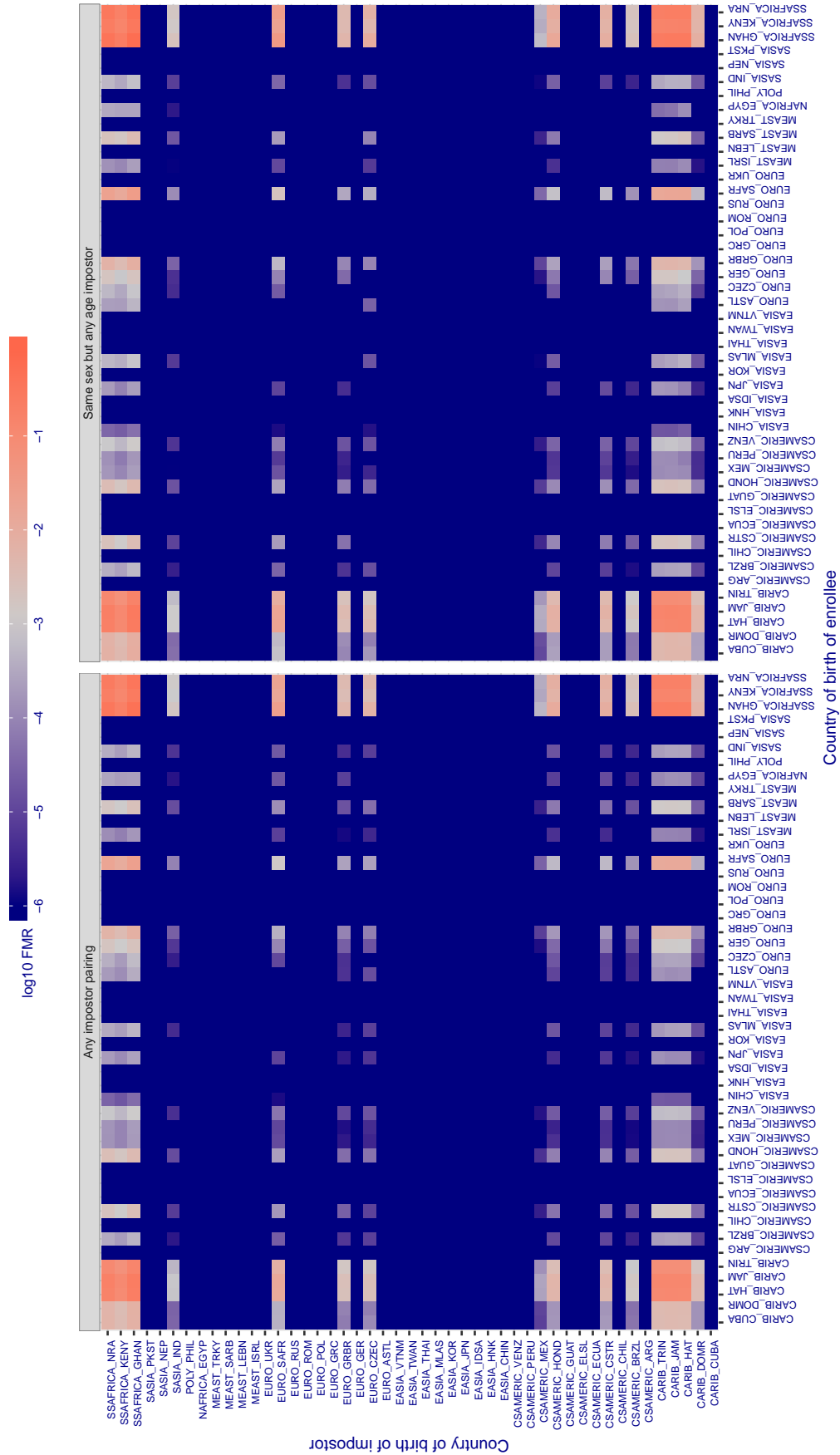


Figure 400: For algorithm intsysmsu-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 1.280$  for algorithm `iqface_000`, giving  $FMR(T) = 0.001$  globally.

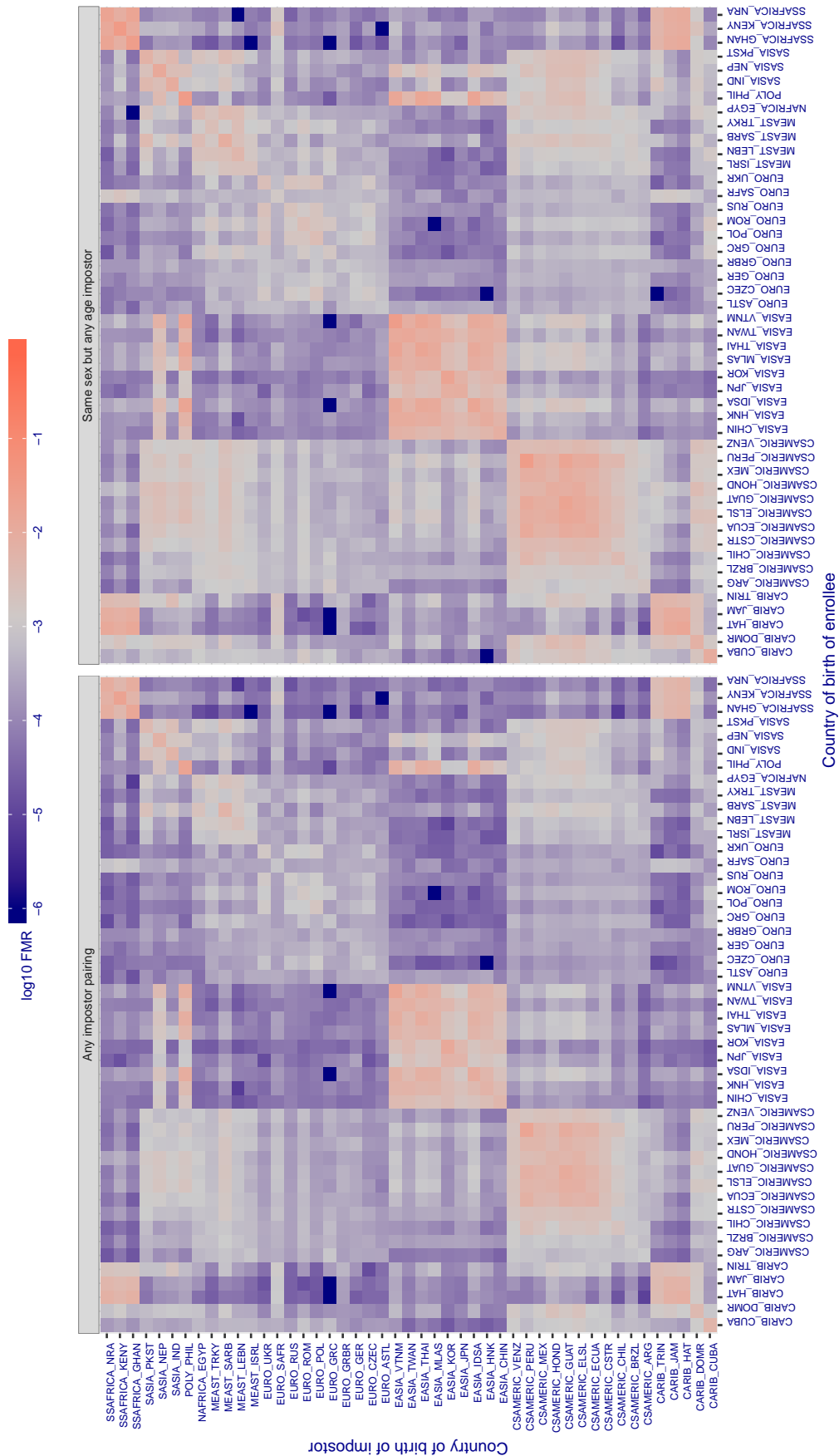


Figure 401: For algorithm `iqface-000` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each  $+1$  increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.982$  for algorithm isap\_001, giving  $FMR(T) = 0.001$  globally.

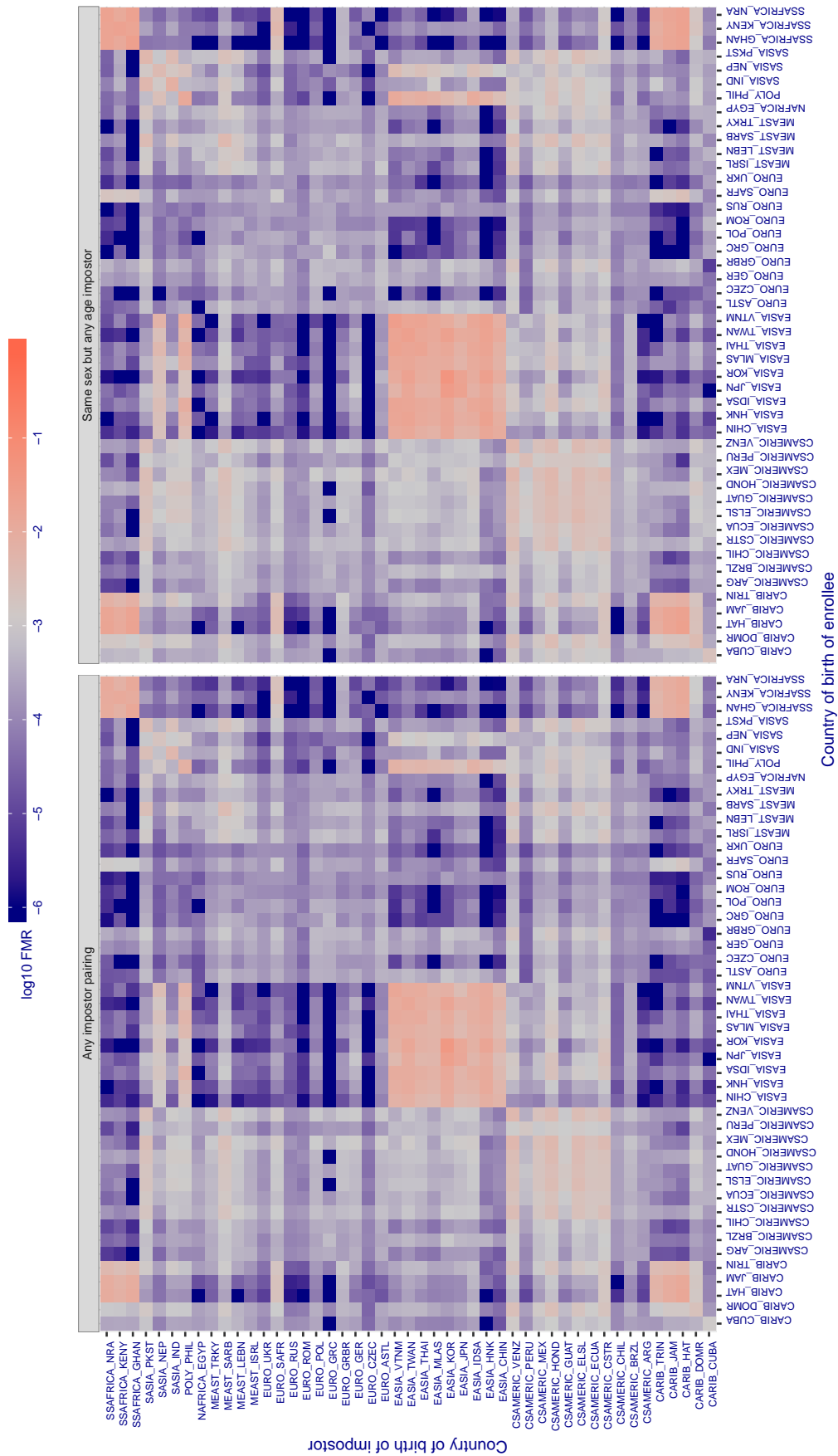


Figure 402: For algorithm isap-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 20.648$  for algorithm isityou\_000, giving  $FMR(T) = 0.001$  globally.

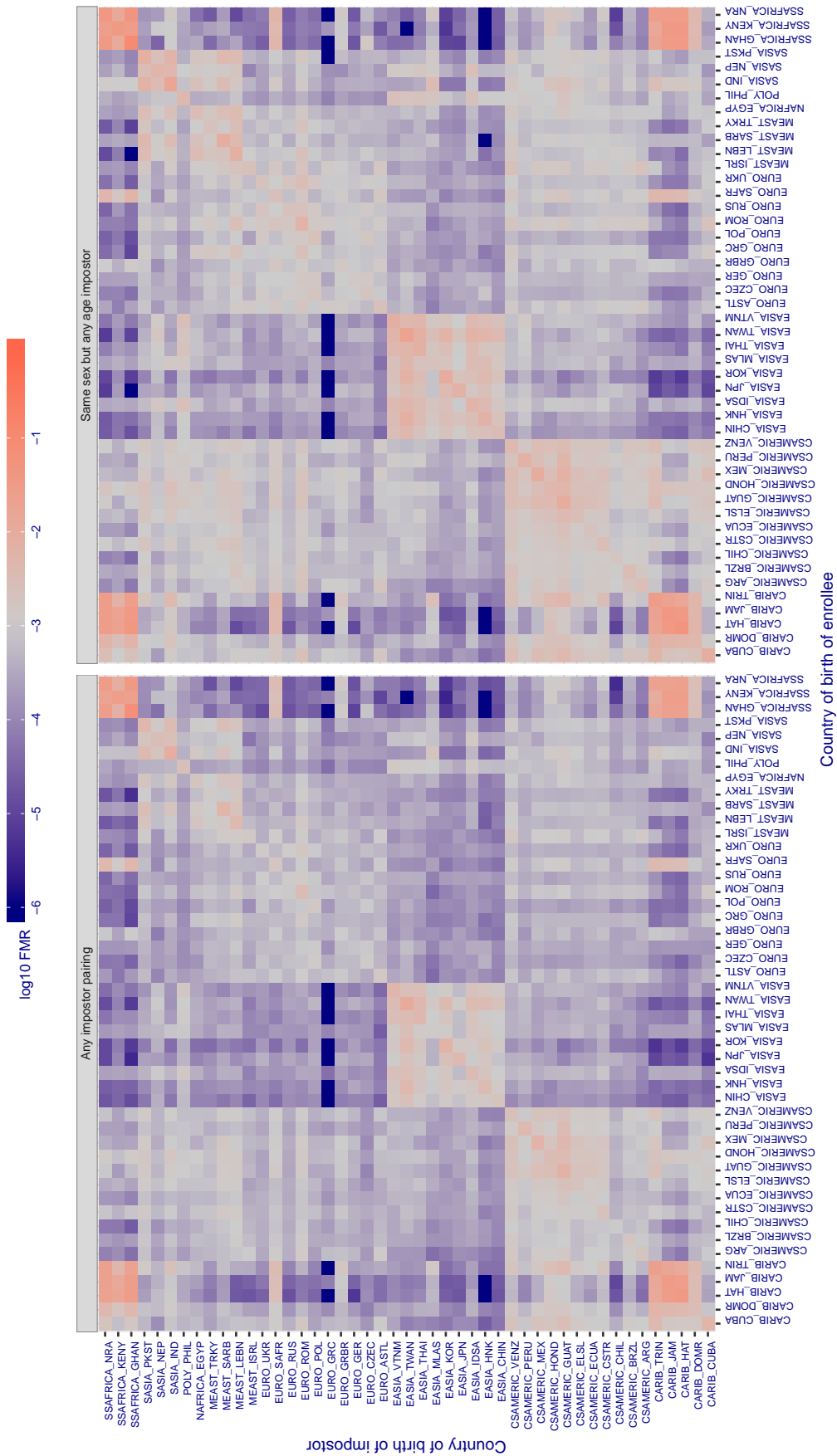


Figure 403: For algorithm isityou-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.649$  for algorithm isystems\_001, giving  $FMR(T) = 0.001$  globally.

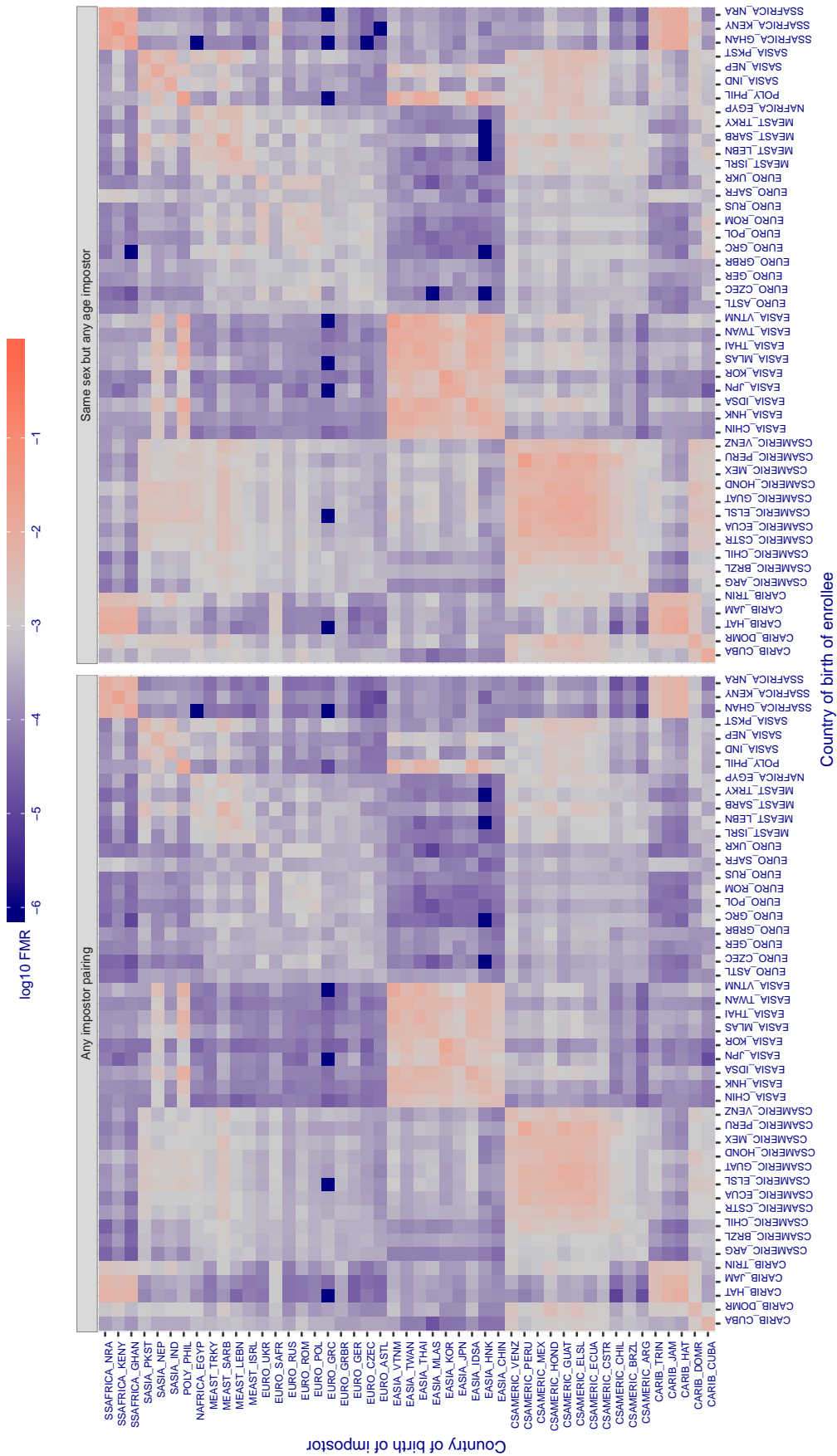


Figure 404: For algorithm isystems-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.647$  for algorithm isystems\_002, giving  $FMR(T) = 0.001$  globally.

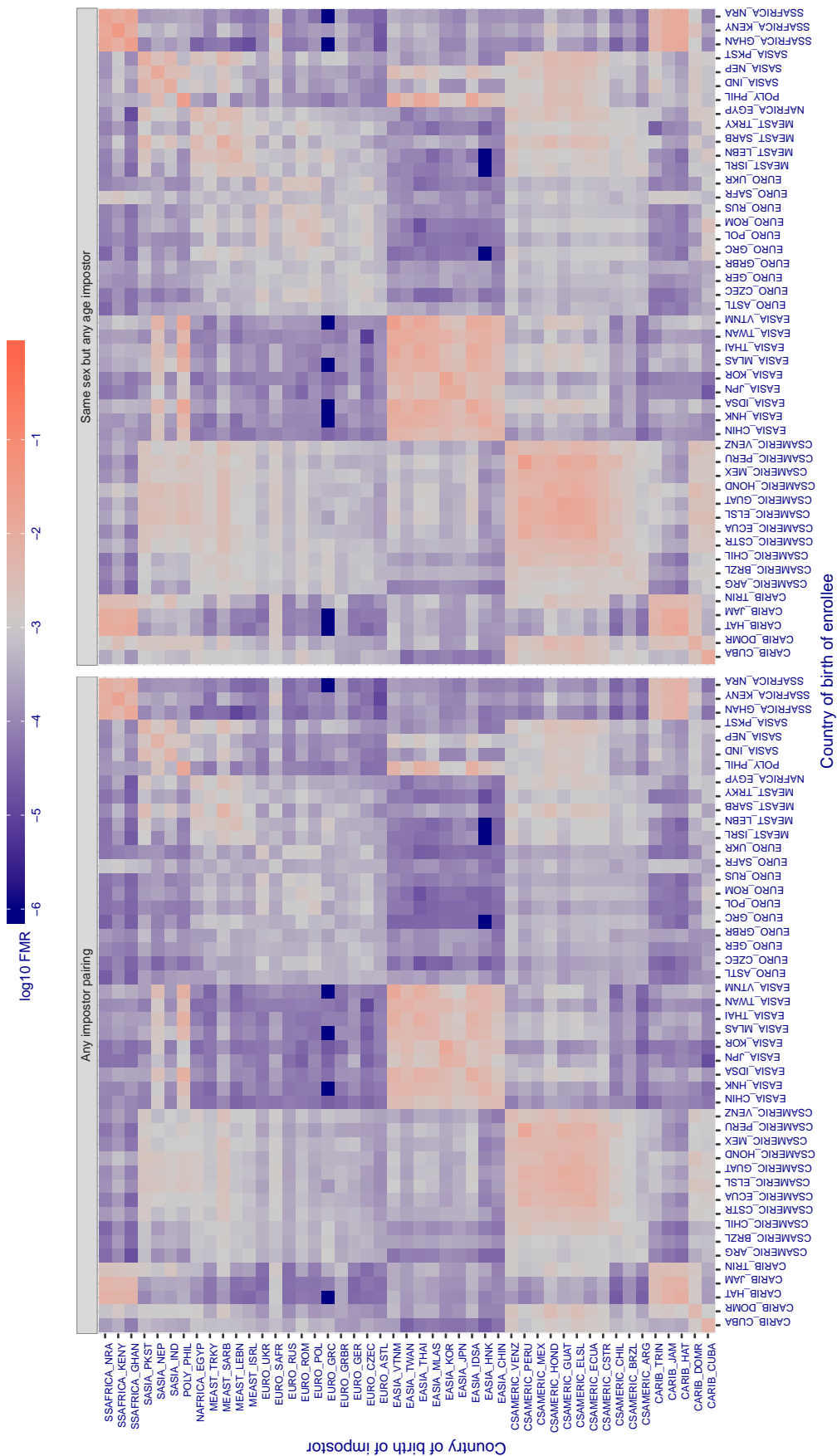


Figure 405: For algorithm isystems-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 10.316$  for algorithm itmo\_005, giving  $FMR(T) = 0.001$  globally.

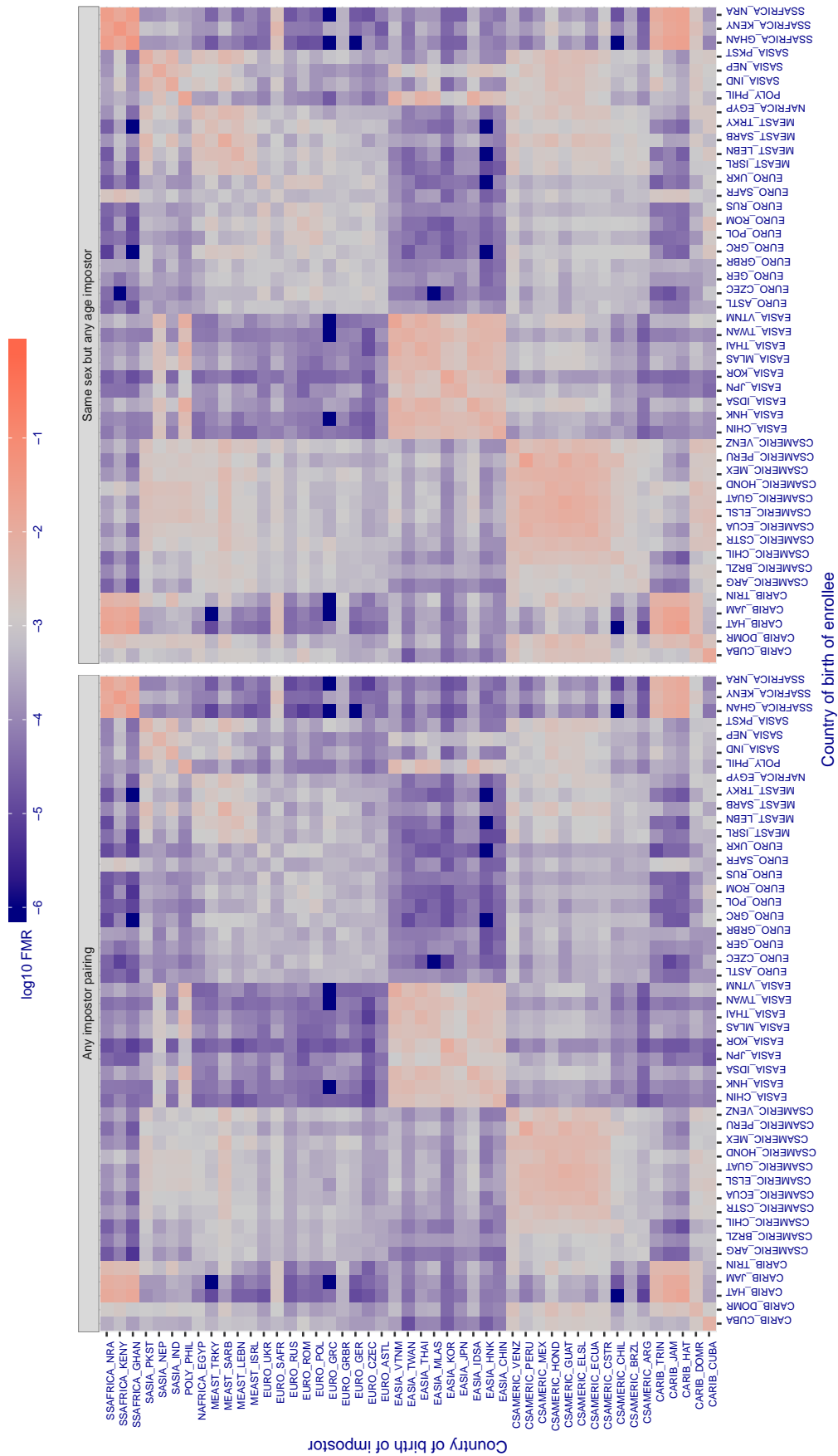


Figure 406: For algorithm itmo-005 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 12.030$  for algorithm itmo\_006, giving  $FMR(T) = 0.001$  globally.

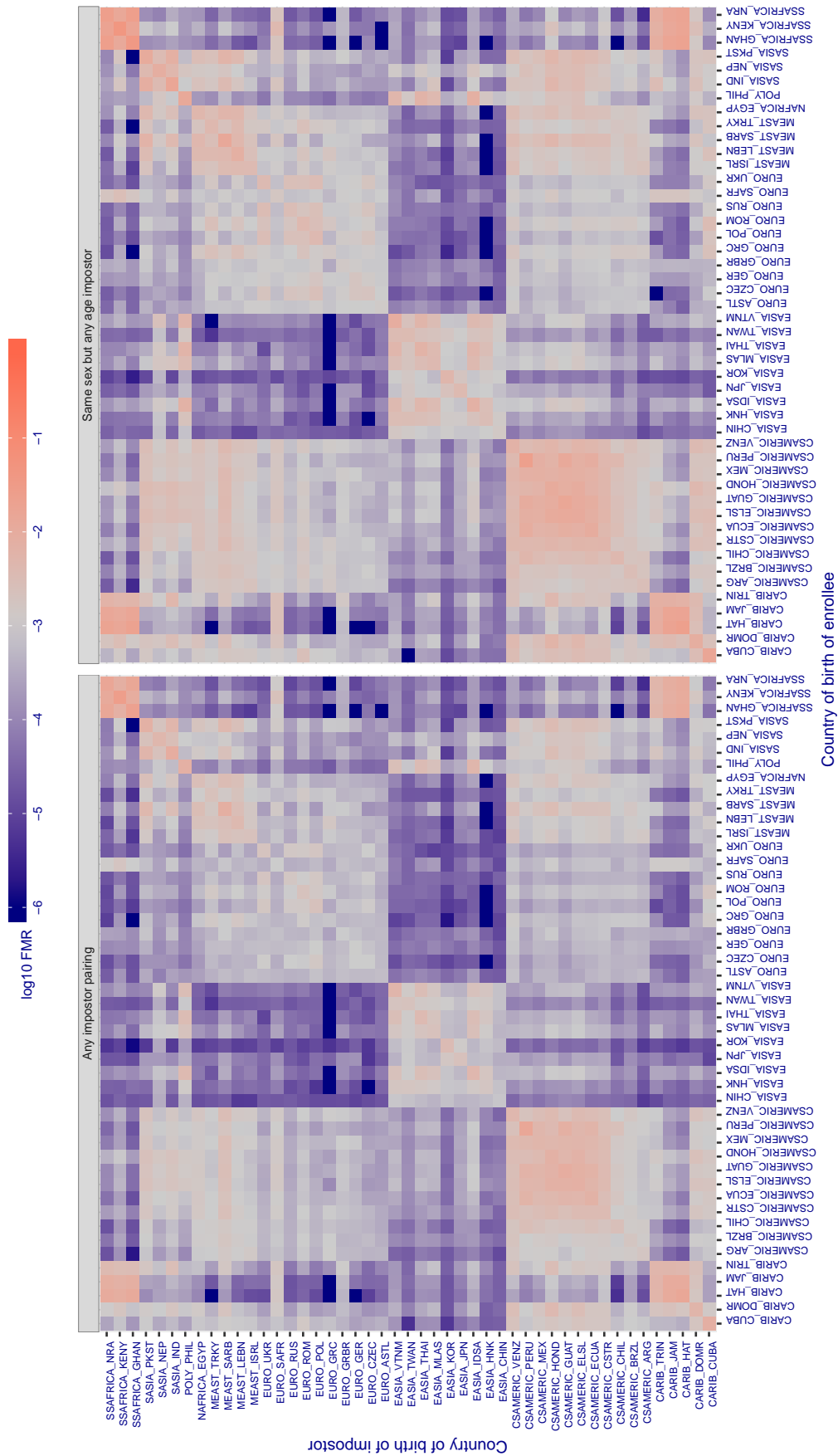


Figure 407: For algorithm itmo-006 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 1.192$  for algorithm kakao\_001, giving  $FMR(T) = 0.001$  globally.

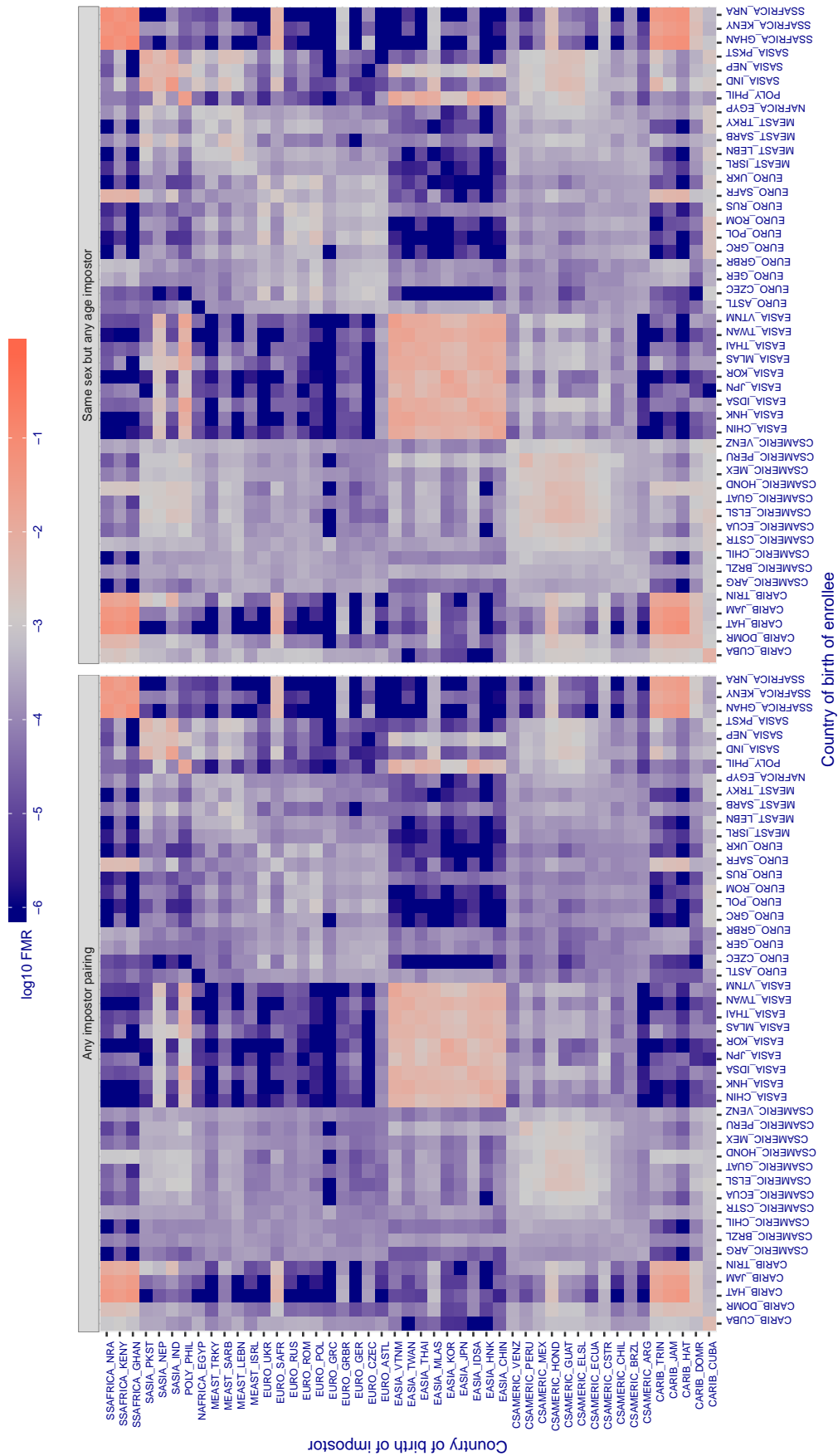


Figure 408: For algorithm kakao-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 0.854$  for algorithm kakao\_002, giving  $FMR(T) = 0.001$  globally.

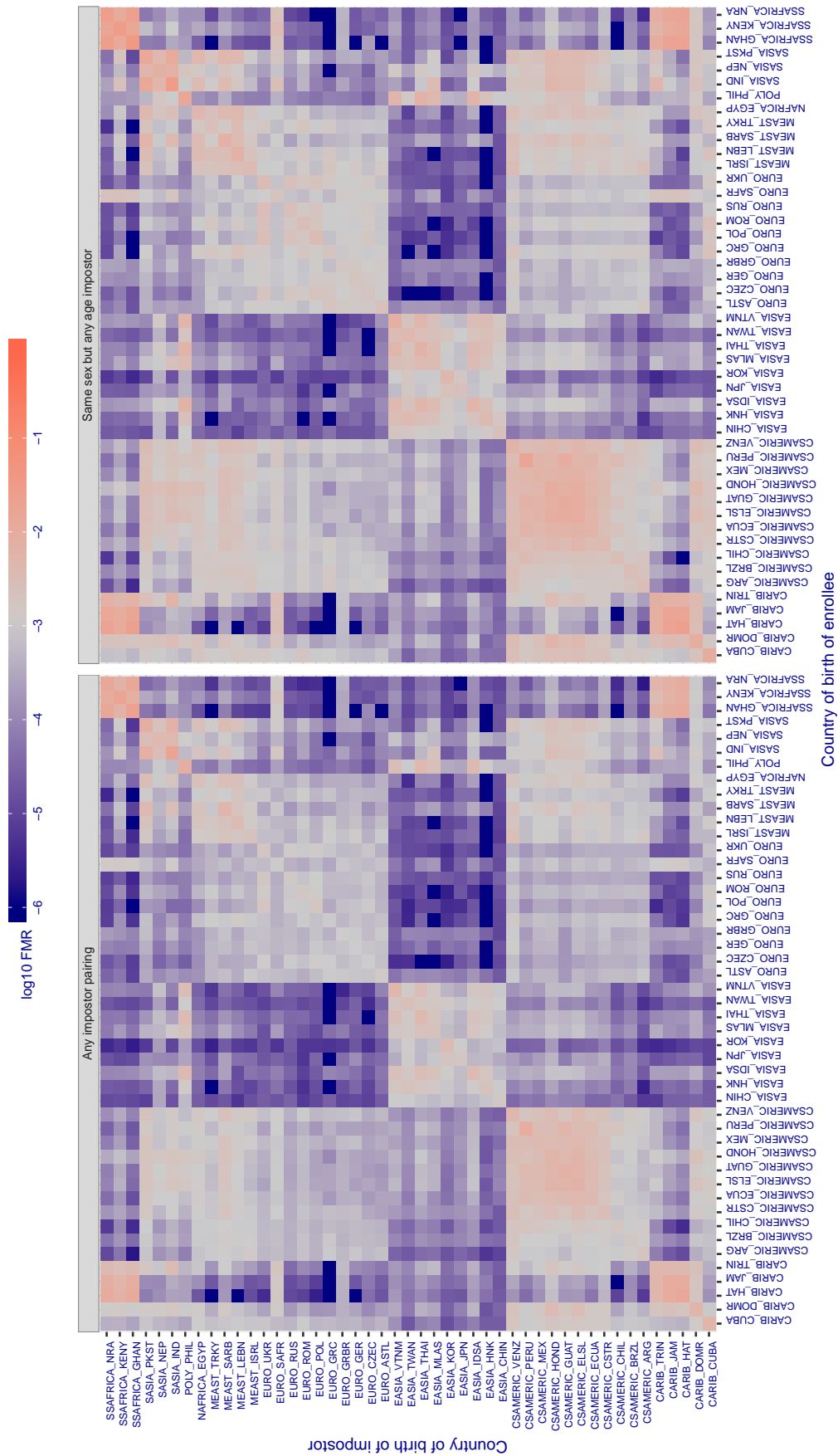


Figure 409: For algorithm kakao-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.650$  for algorithm `kedacom_000`, giving  $FMR(T) = 0.001$  globally.

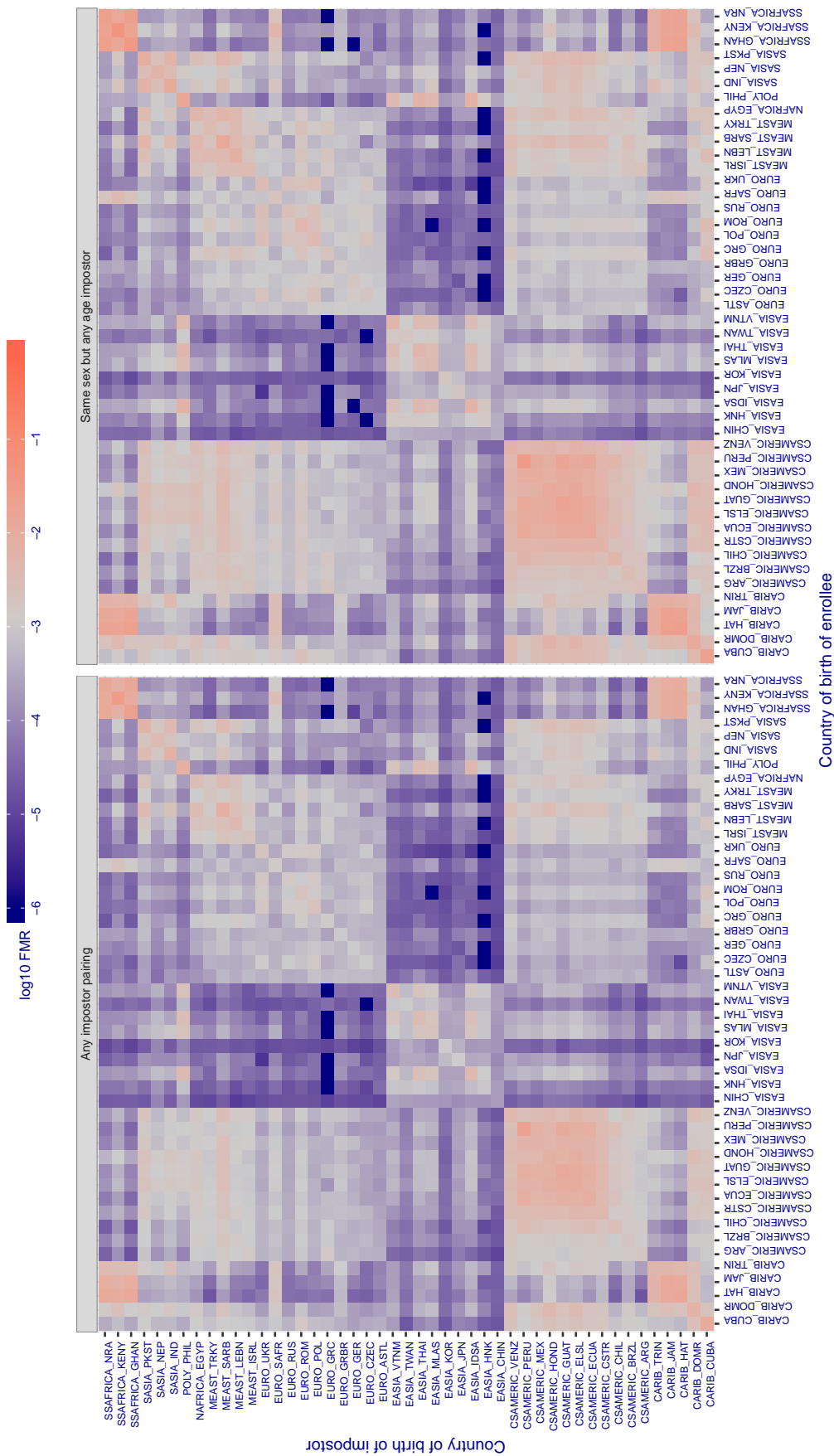


Figure 410: For algorithm `kedacom-000` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each  $+1$  increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.397$  for algorithm `kneron_003`, giving  $FMR(T) = 0.001$  globally.

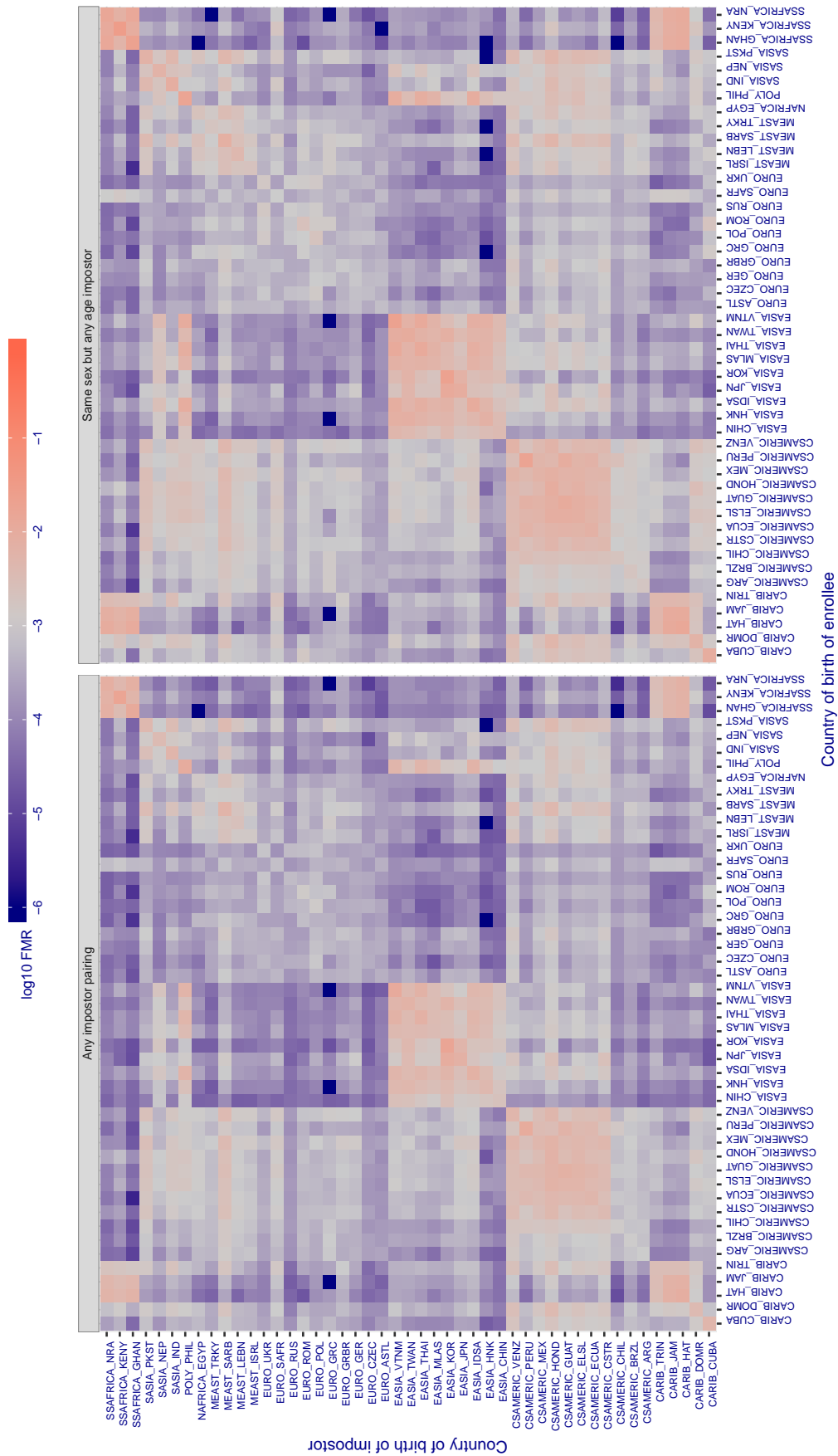


Figure 411: For algorithm `kneron-003` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.656$  for algorithm lookman\_002, giving  $FMR(T) = 0.001$  globally.

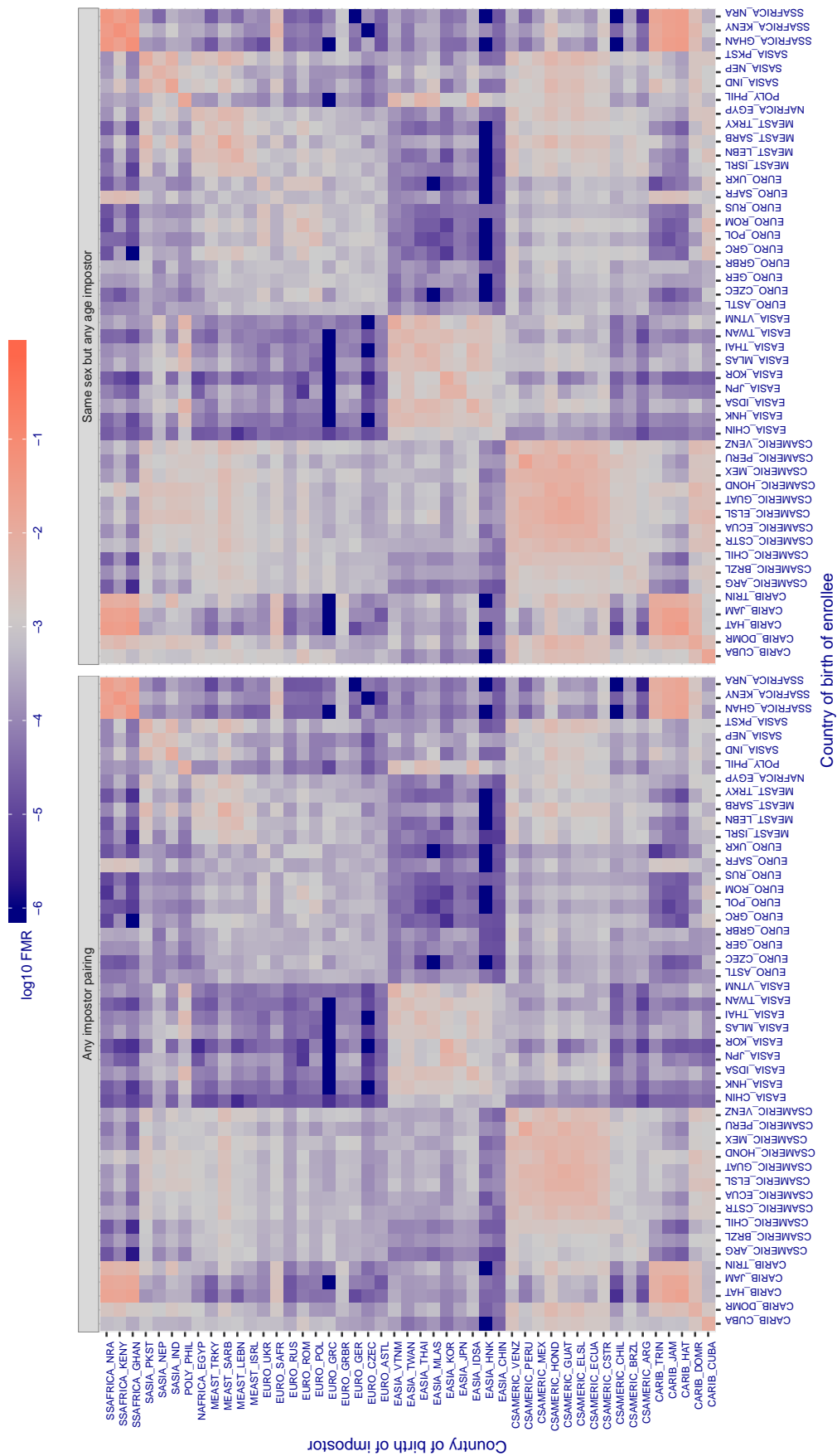


Figure 412: For algorithm lookman-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.703$  for algorithm lookman\_004, giving  $FMR(T) = 0.001$  globally.

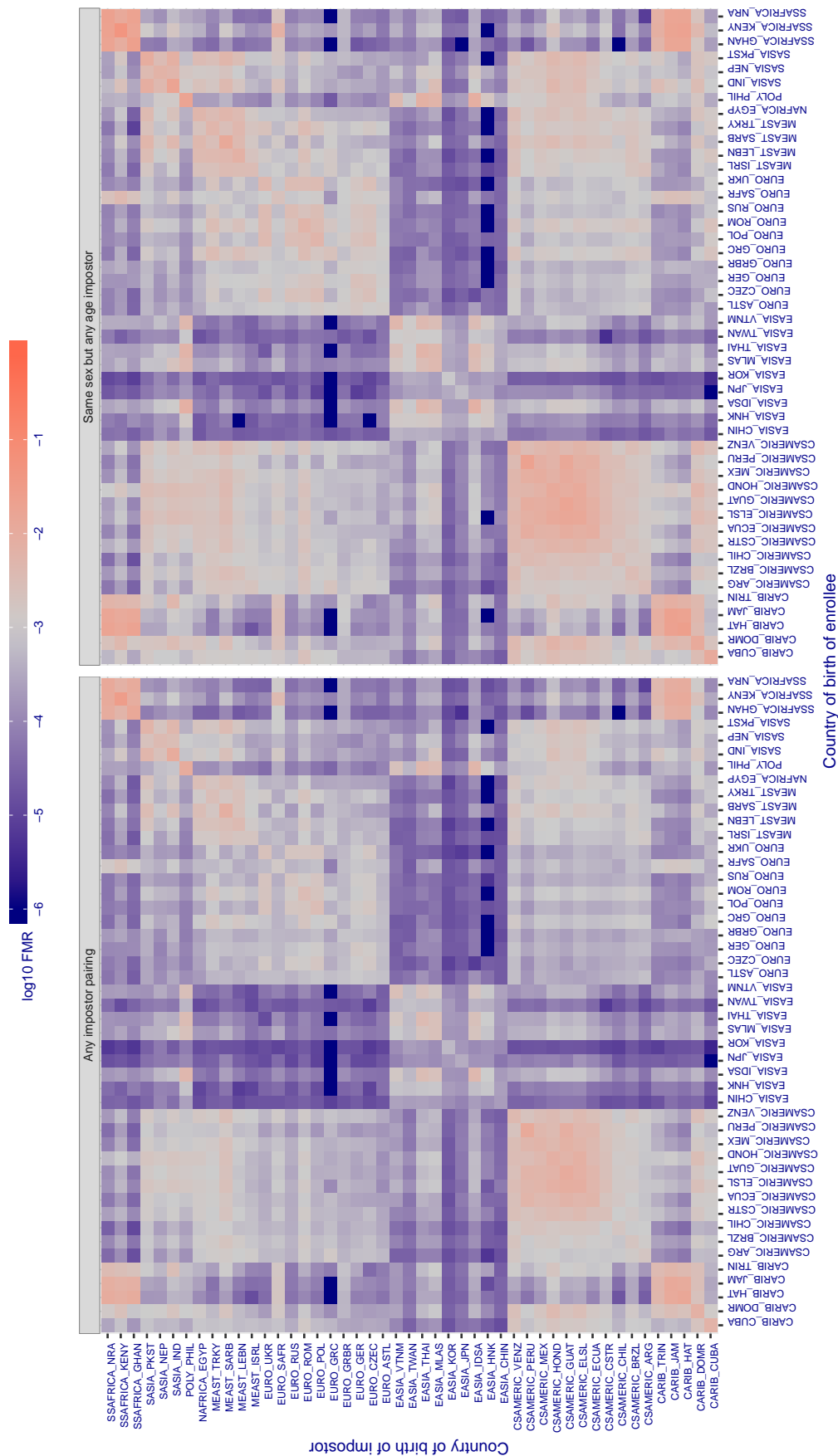


Figure 413: For algorithm lookman-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each  $+1$  increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 66.706$  for algorithm megvii\_001, giving  $FMR(T) = 0.001$  globally.

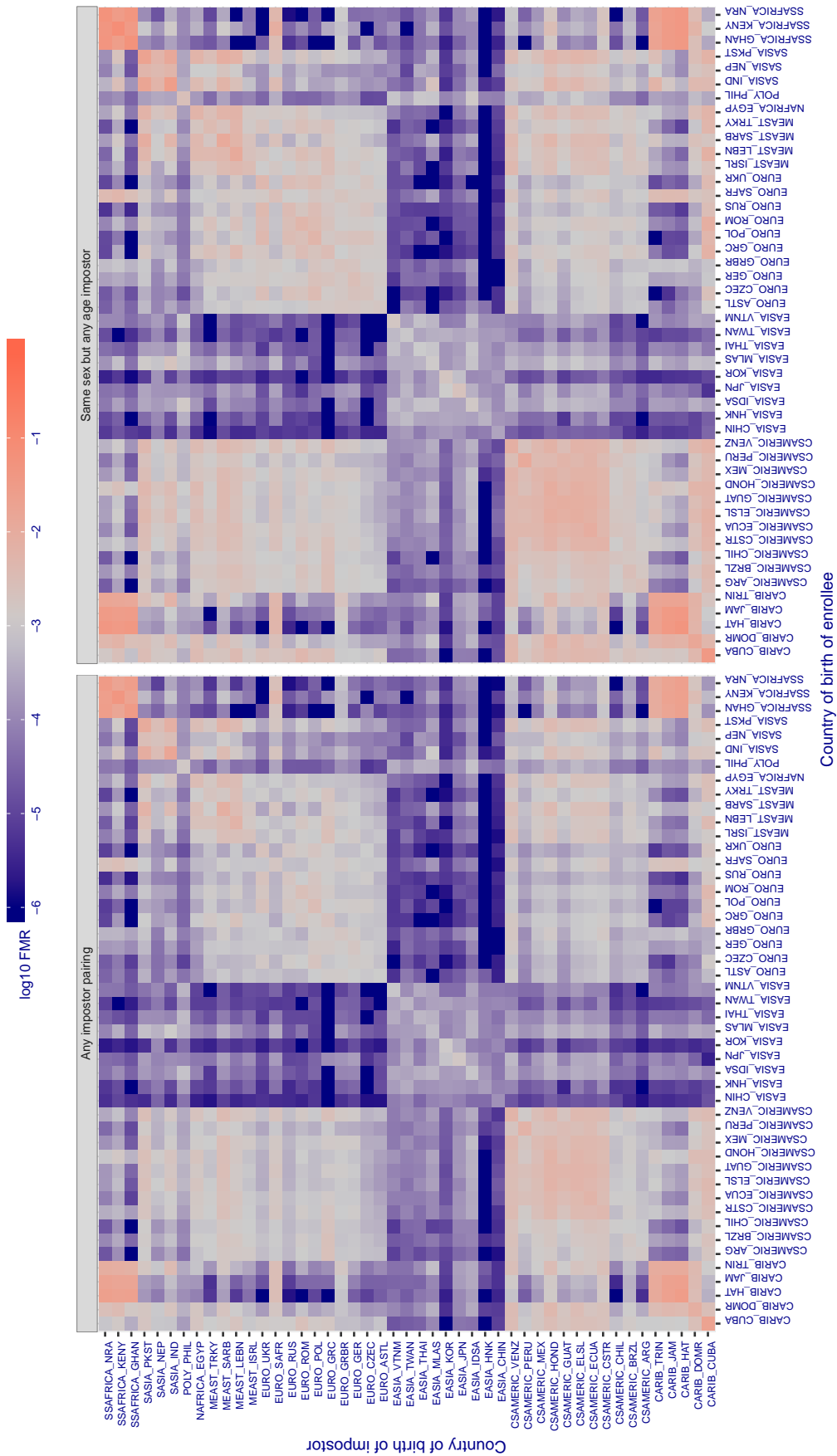


Figure 414: For algorithm megvii-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 58.026$  for algorithm megvii\_002, giving  $FMR(T) = 0.001$  globally.

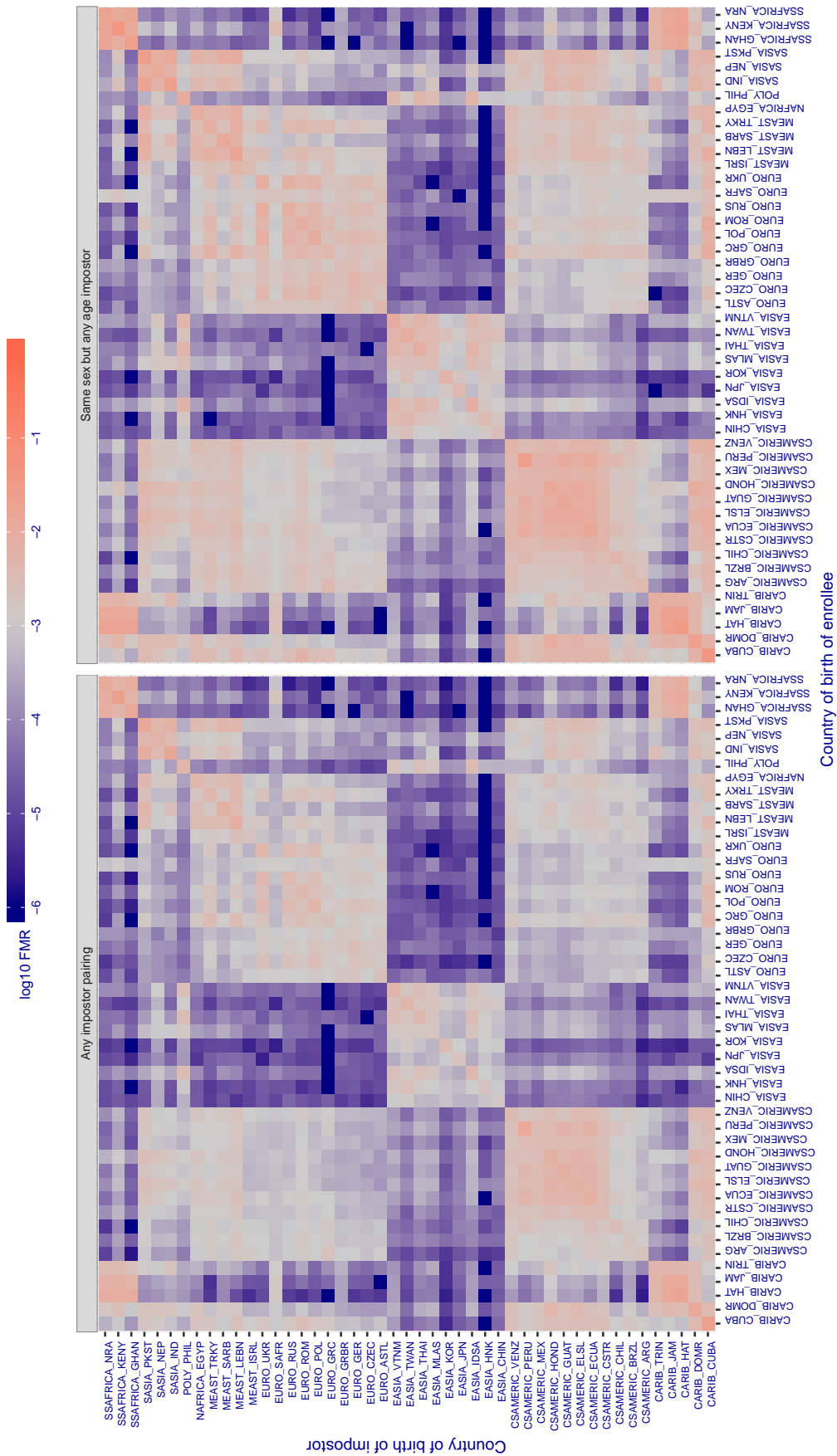


Figure 415: For algorithm megvii-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 0.345$  for algorithm meiya\_001, giving  $FMR(T) = 0.001$  globally.

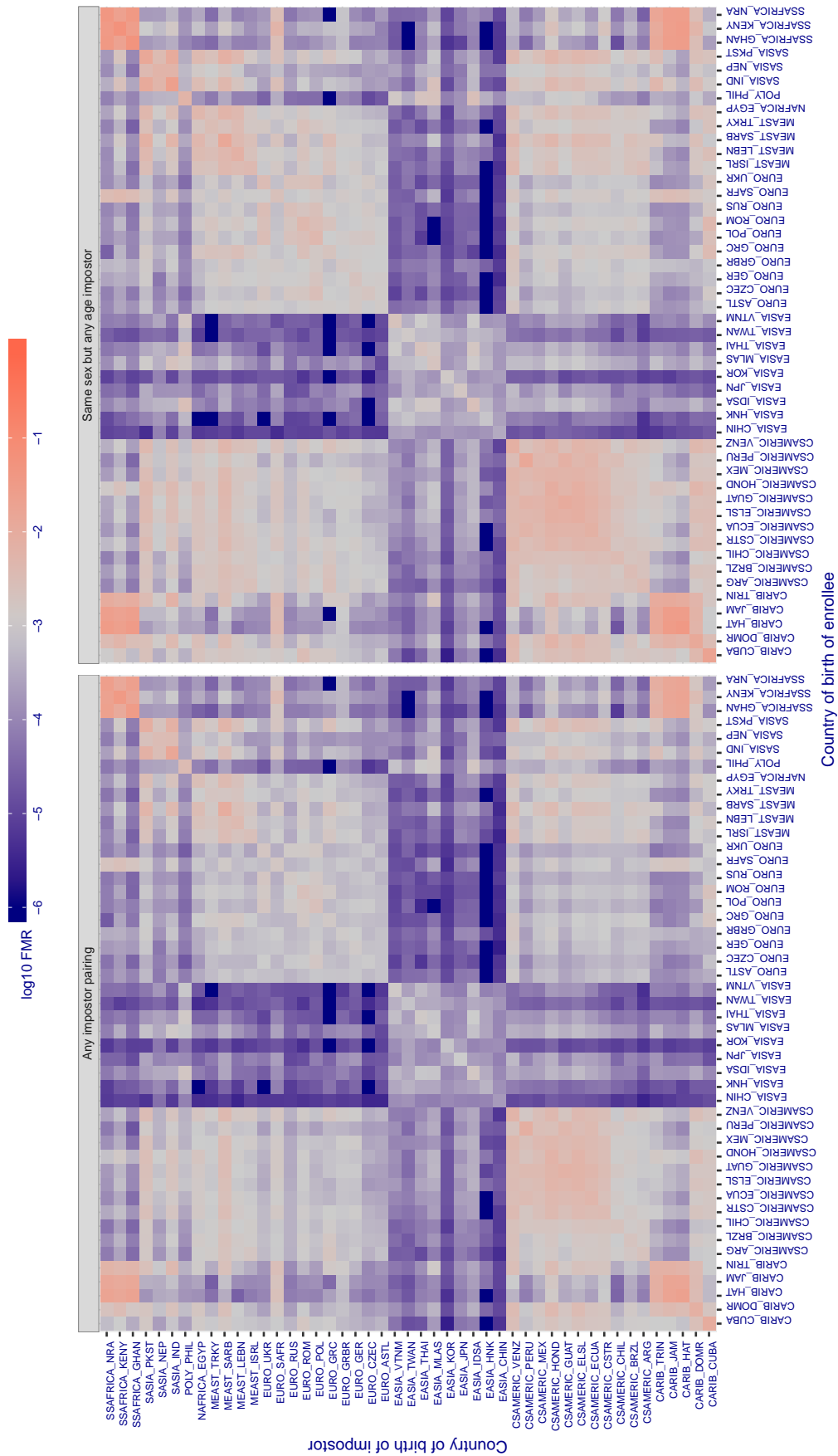


Figure 416: For algorithm meiya-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 0.624$  for algorithm microfocus\_001, giving  $FMR(T) = 0.001$  globally.

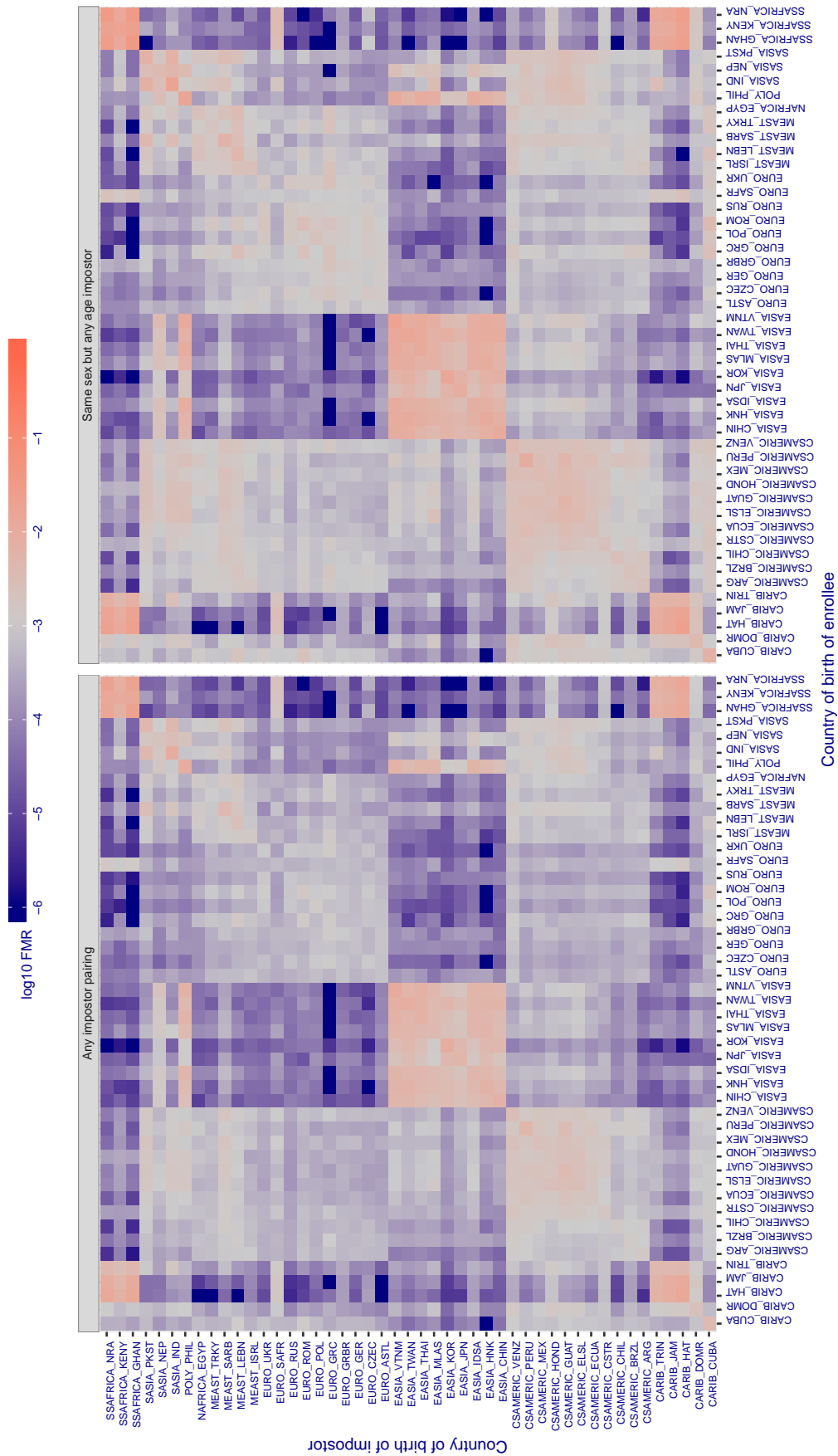


Figure 417: For algorithm microfocus-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.542$  for algorithm microfocus\_002, giving  $FMR(T) = 0.001$  globally.

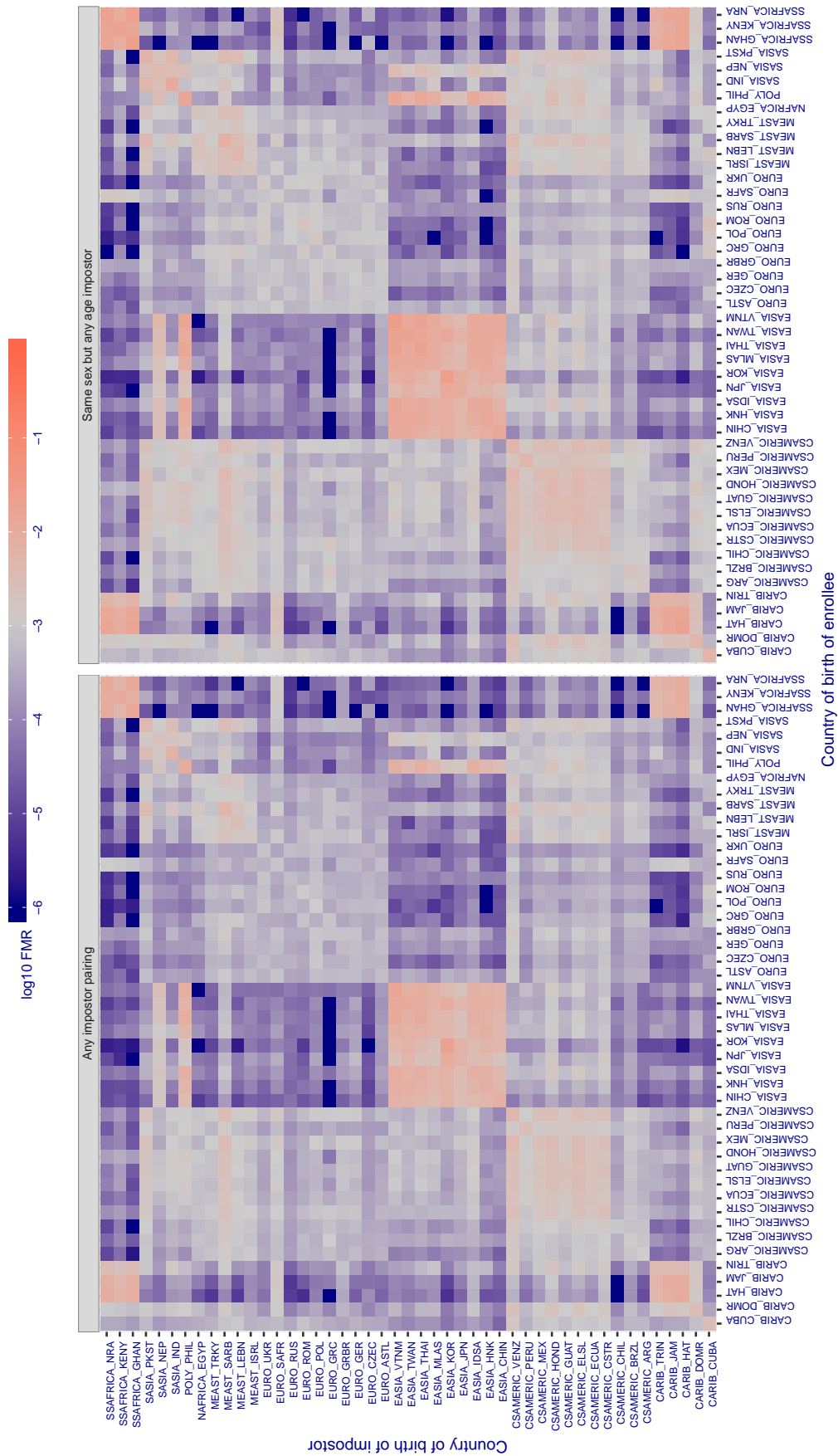


Figure 418: For algorithm microfocus-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 1.310$  for algorithm  $mt\_000$ , giving  $FMR(T) = 0.001$  globally.

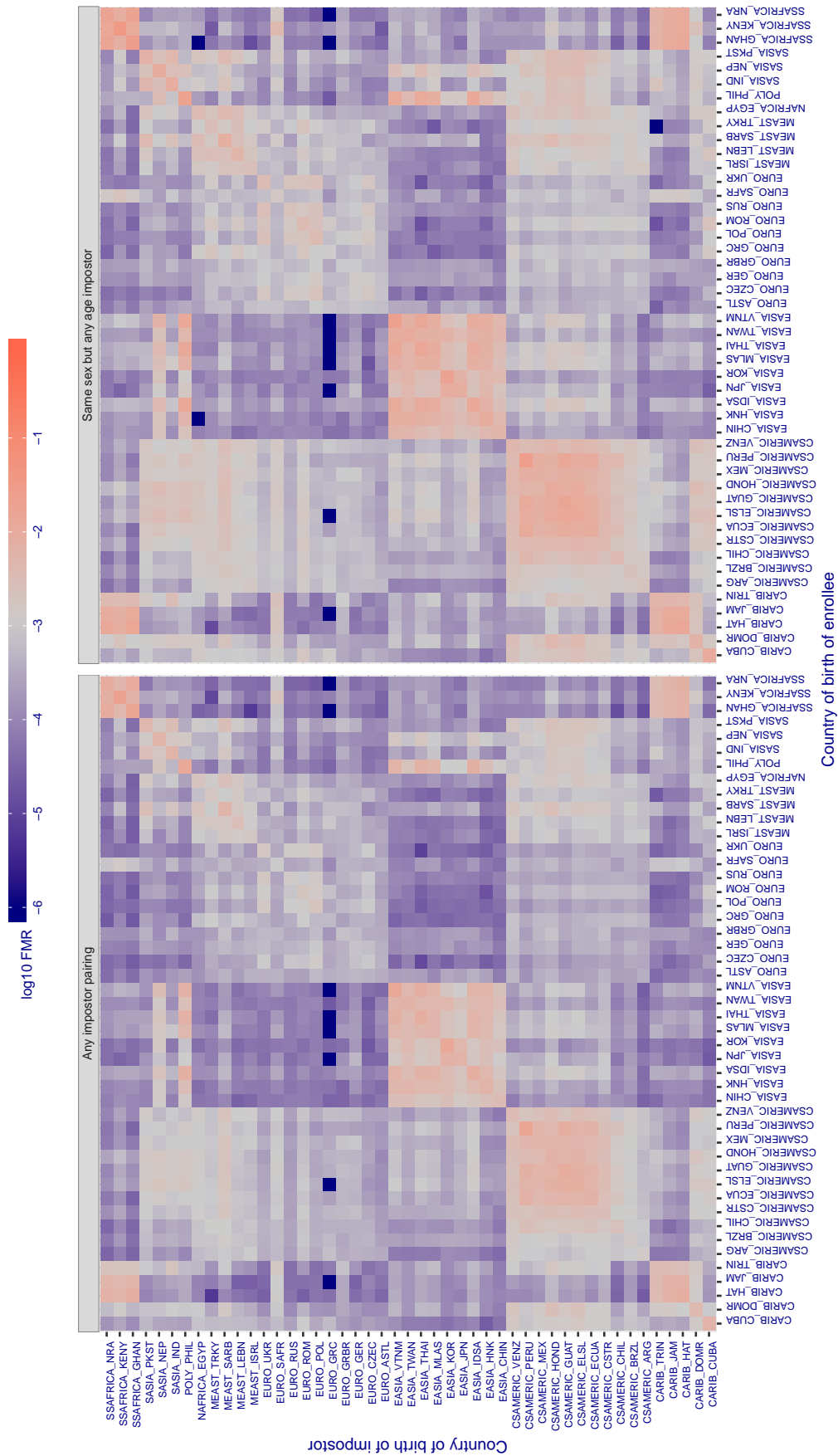


Figure 419: For algorithm  $mt-000$  operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each  $+1$  increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.679$  for algorithm `mvision_001`, giving  $FMR(T) = 0.001$  globally.

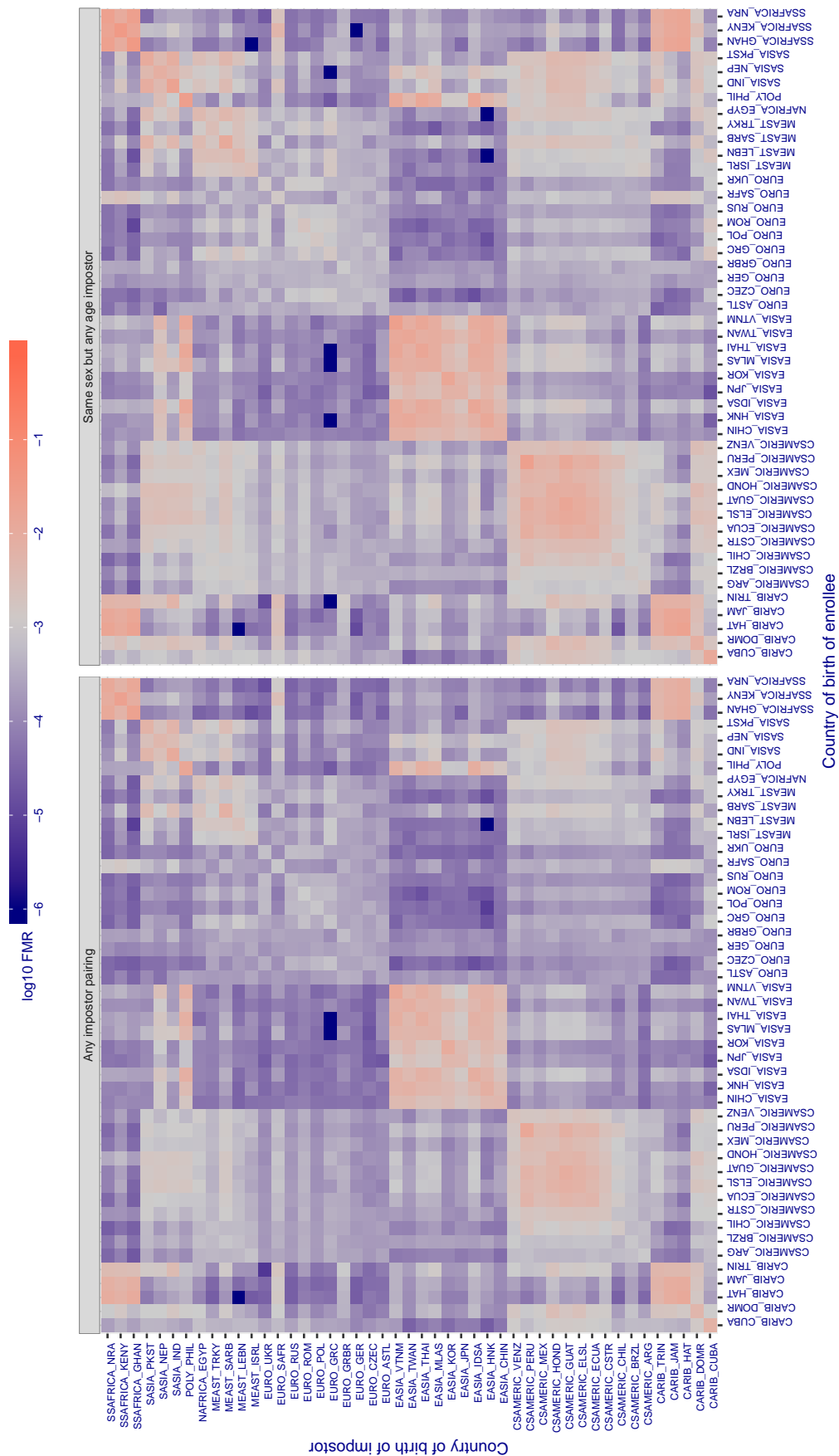


Figure 420: For algorithm `mvision-001` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each  $+1$  increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

**Cross country FMR at threshold  $T = 33.449$  for algorithm neurotechnology\_005, giving  $FMR(T) = 0.001$  globally.**

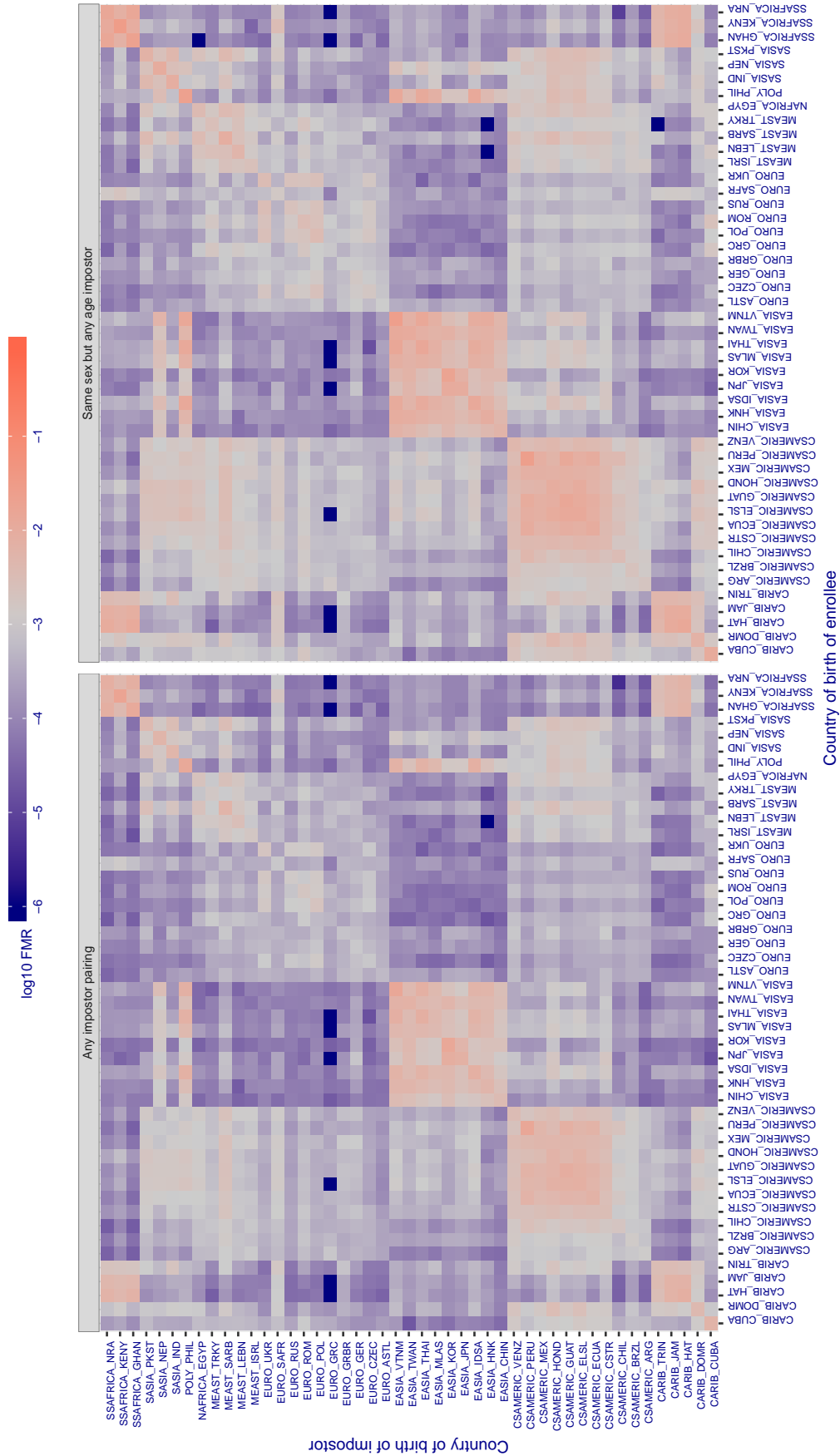


Figure 421: For algorithm neurotechnology-005 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 1686.000$  for algorithm neurotechnology\_006, giving  $FMR(T) = 0.001$  globally.

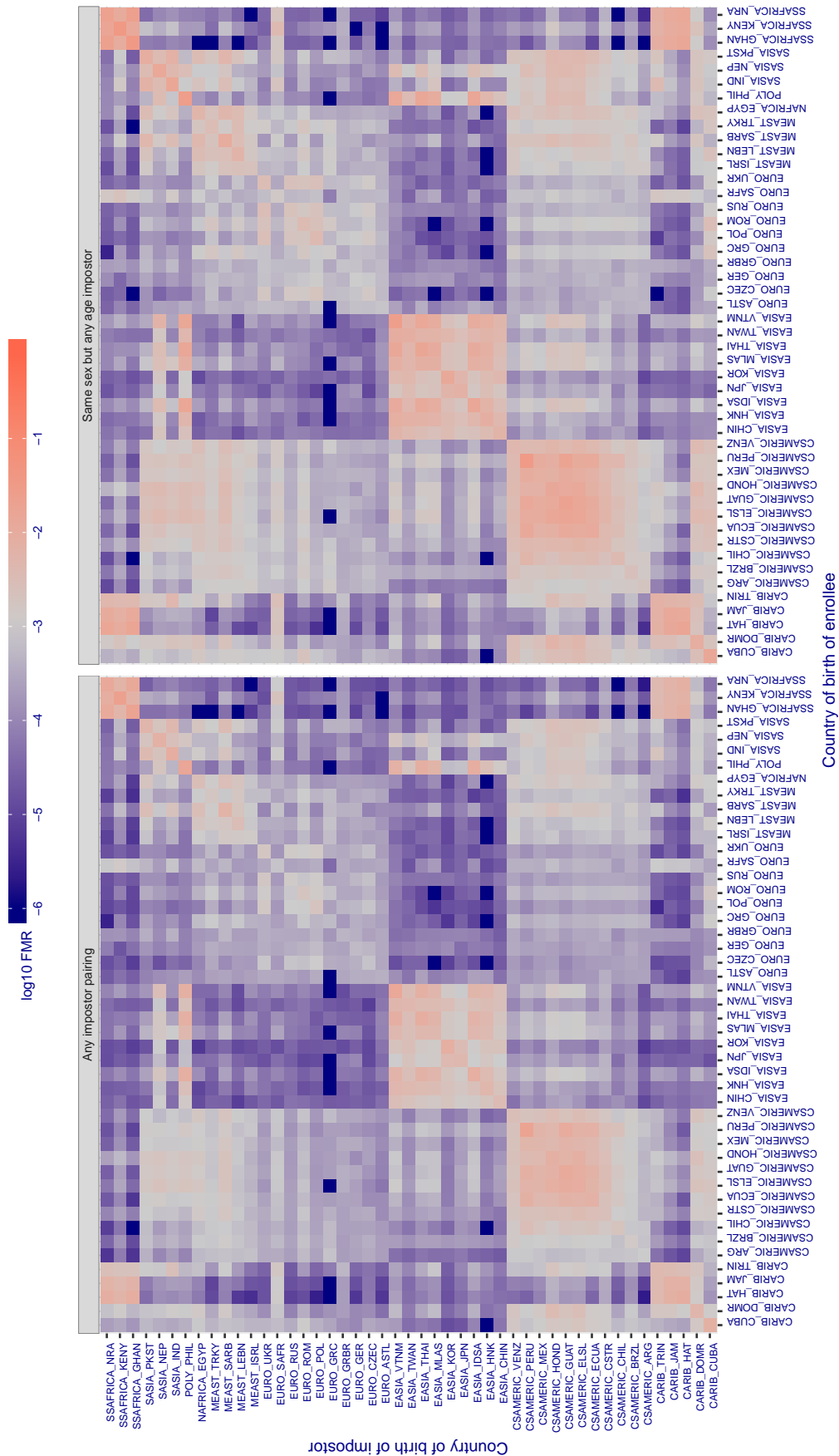


Figure 422: For algorithm neurotechnology-006 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.693$  for algorithm nodeflux\_001, giving  $FMR(T) = 0.001$  globally.

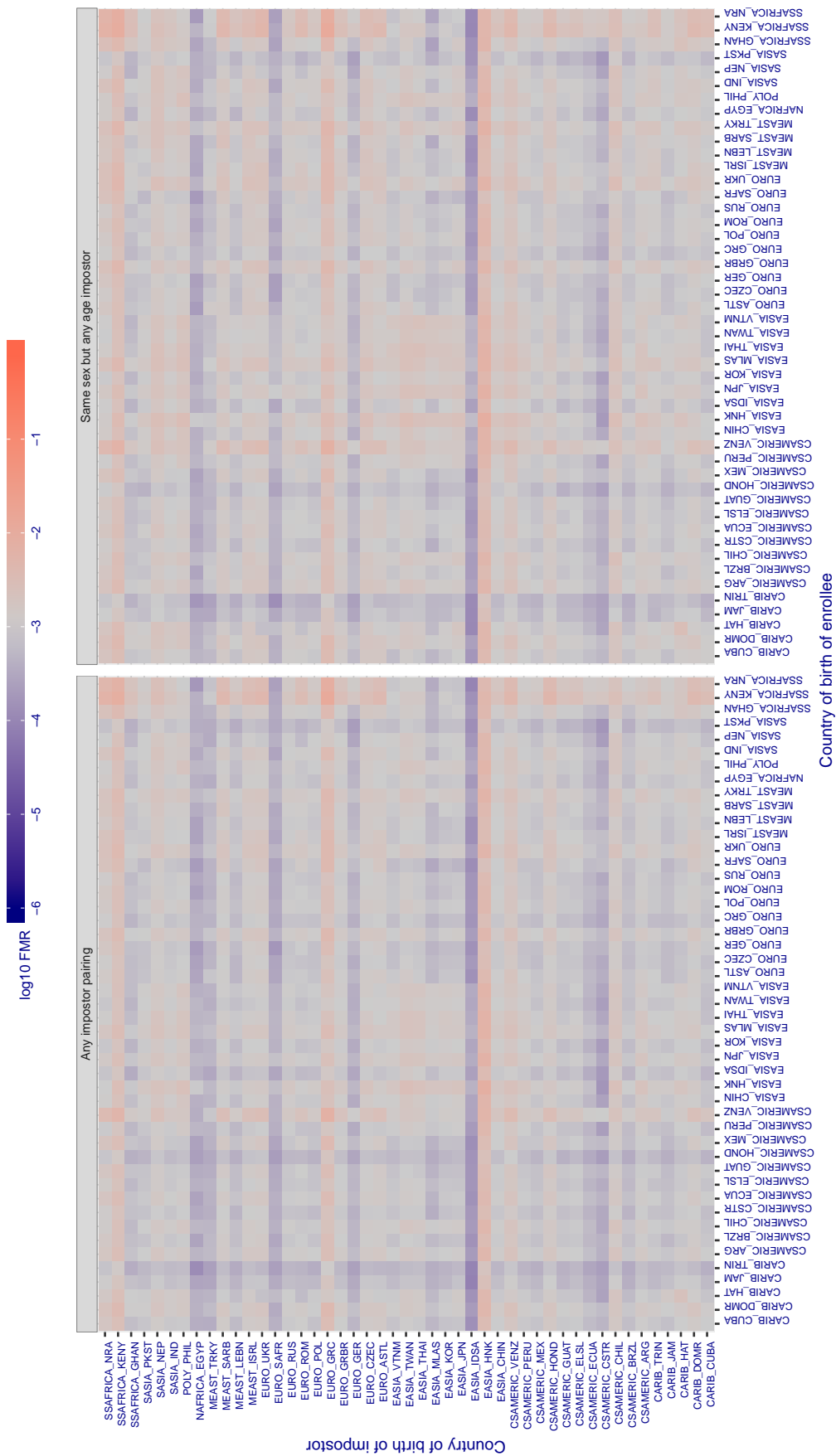


Figure 423: For algorithm nodeflux-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 0.420$  for algorithm nodeflux\_002, giving  $FMR(T) = 0.001$  globally.

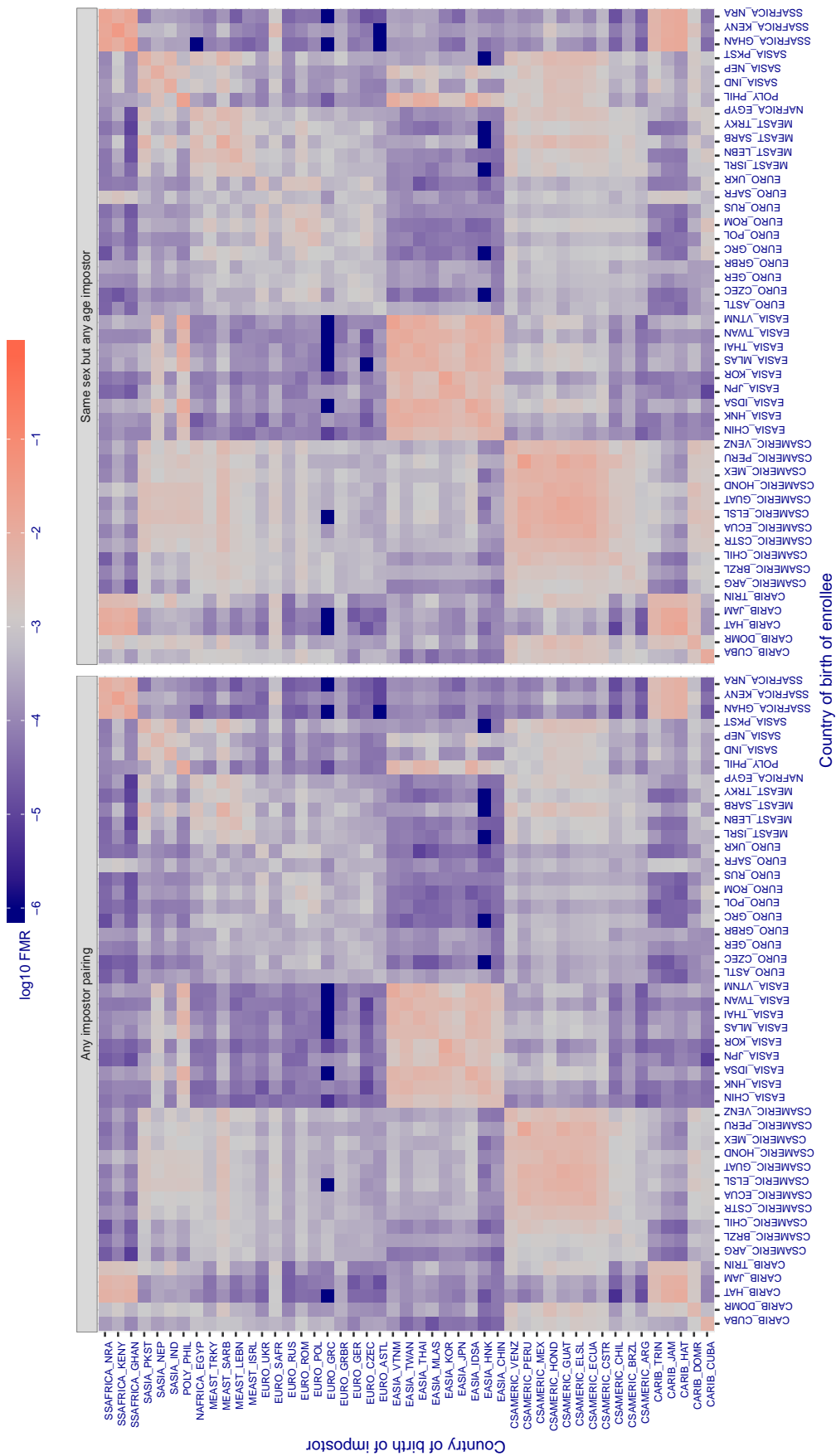


Figure 424: For algorithm nodeflux-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 133813914633823995430803299819739210886107349820666748131859178729416096534382565410687$

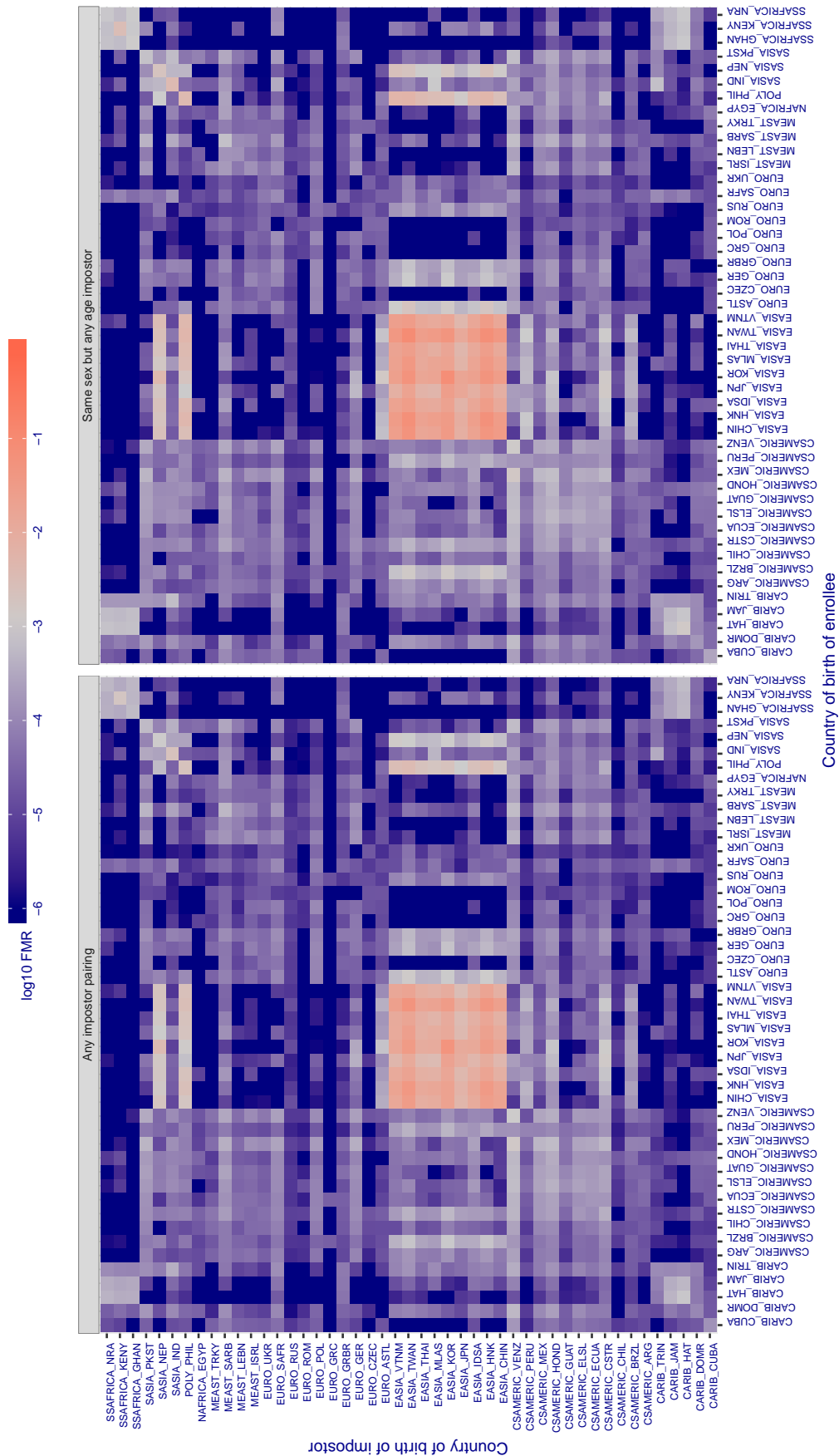


Figure 425: For algorithm notiontag-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 1.929$  for algorithm ntechlab\_006, giving  $FMR(T) = 0.001$  globally.

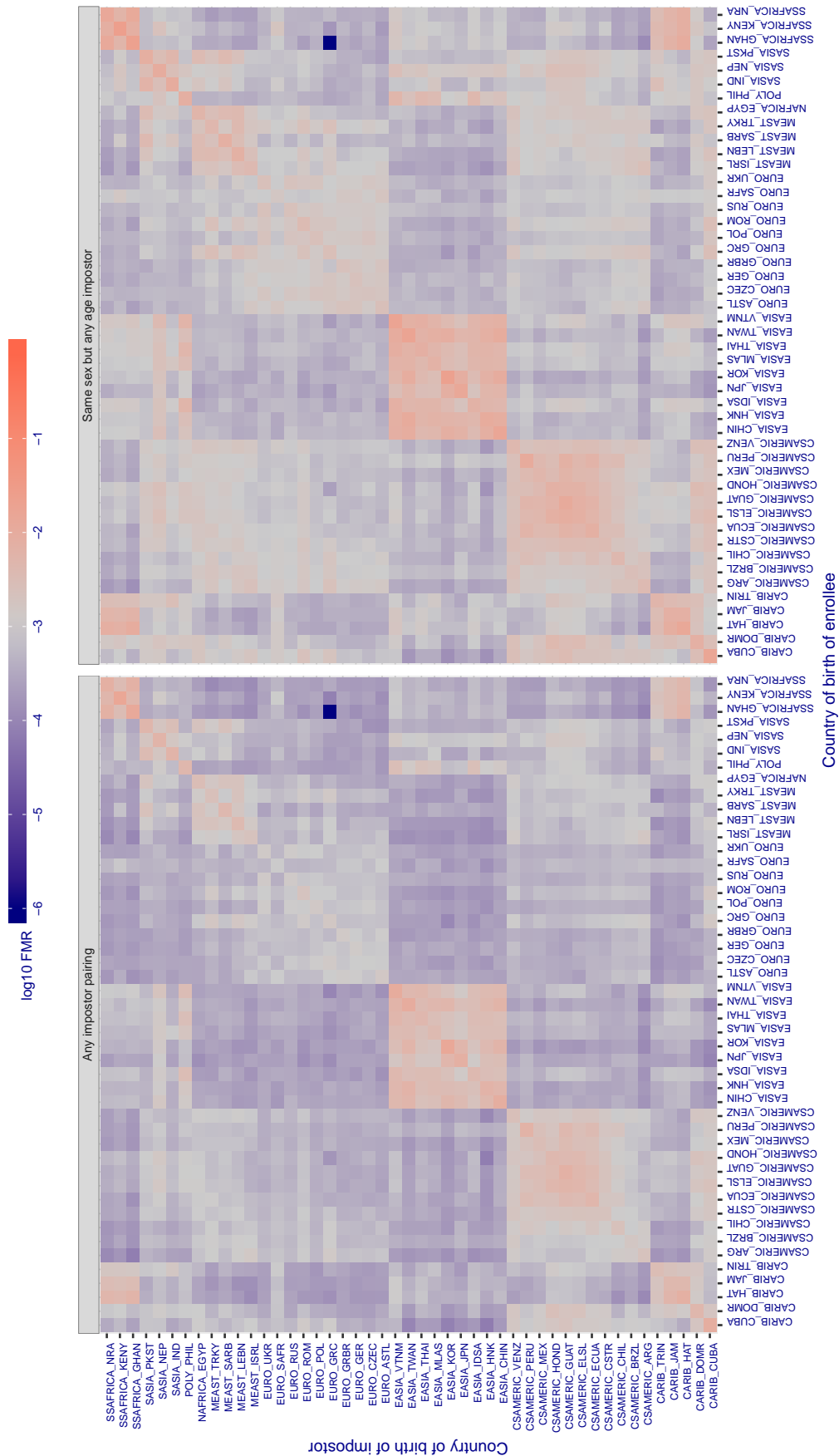


Figure 426: For algorithm ntechlab-006 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 1.319$  for algorithm ntechlab\_007, giving  $FMR(T) = 0.001$  globally.

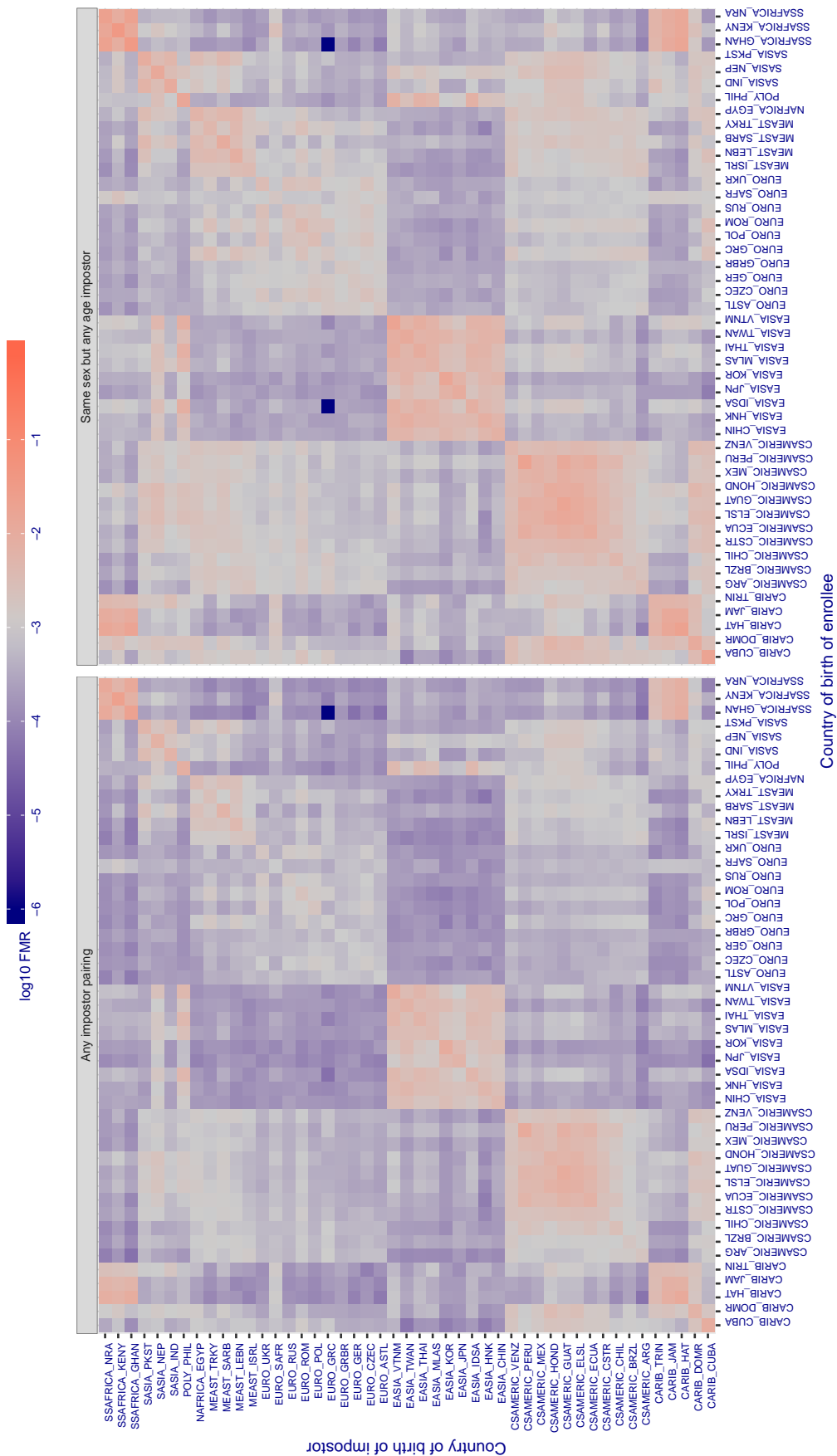


Figure 427: For algorithm ntechlab-007 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.334$  for algorithm pixelall\_002, giving  $FMR(T) = 0.001$  globally.

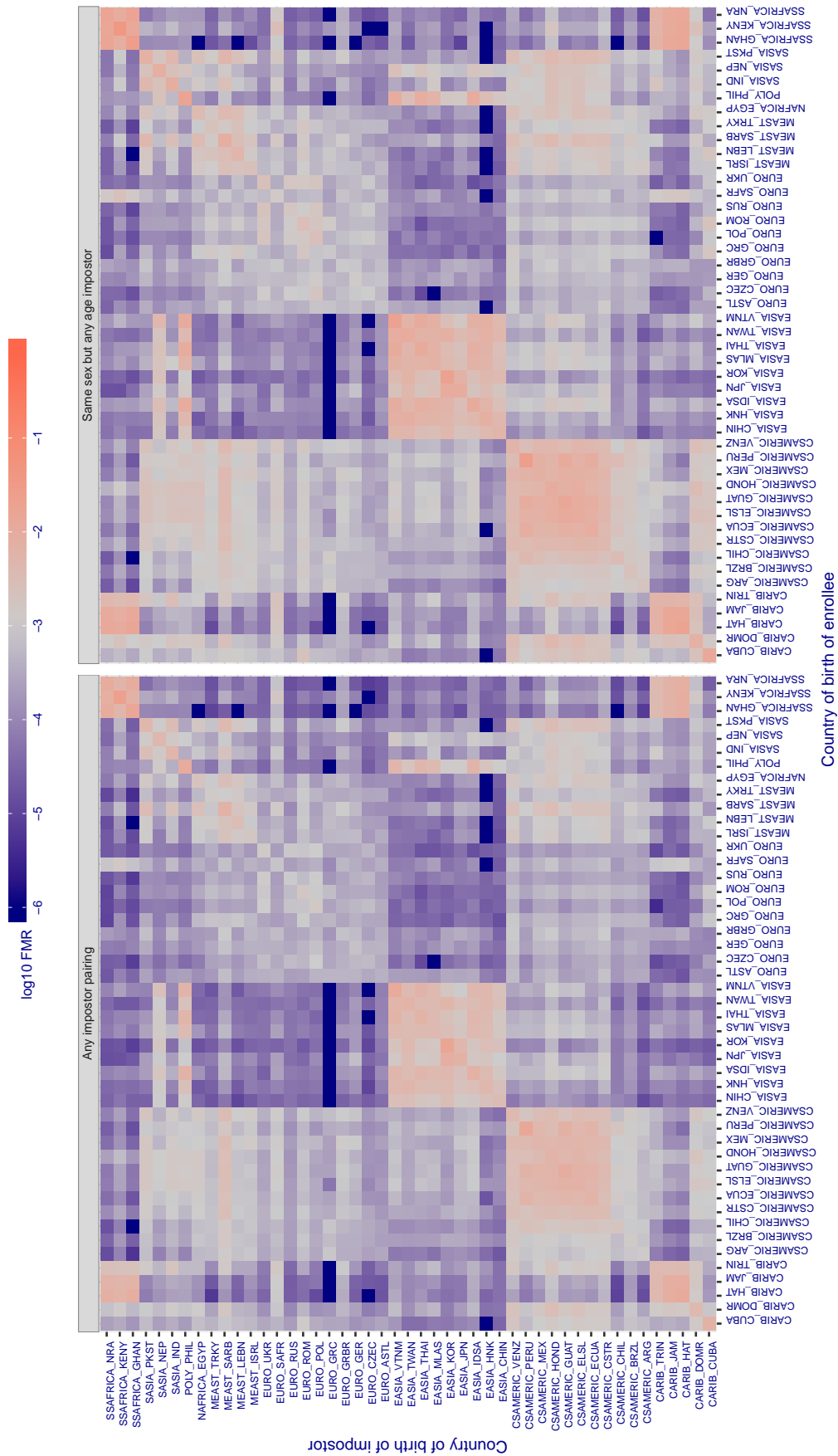


Figure 428: For algorithm pixelall-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.310$  for algorithm pixelall\_003, giving  $FMR(T) = 0.001$  globally.

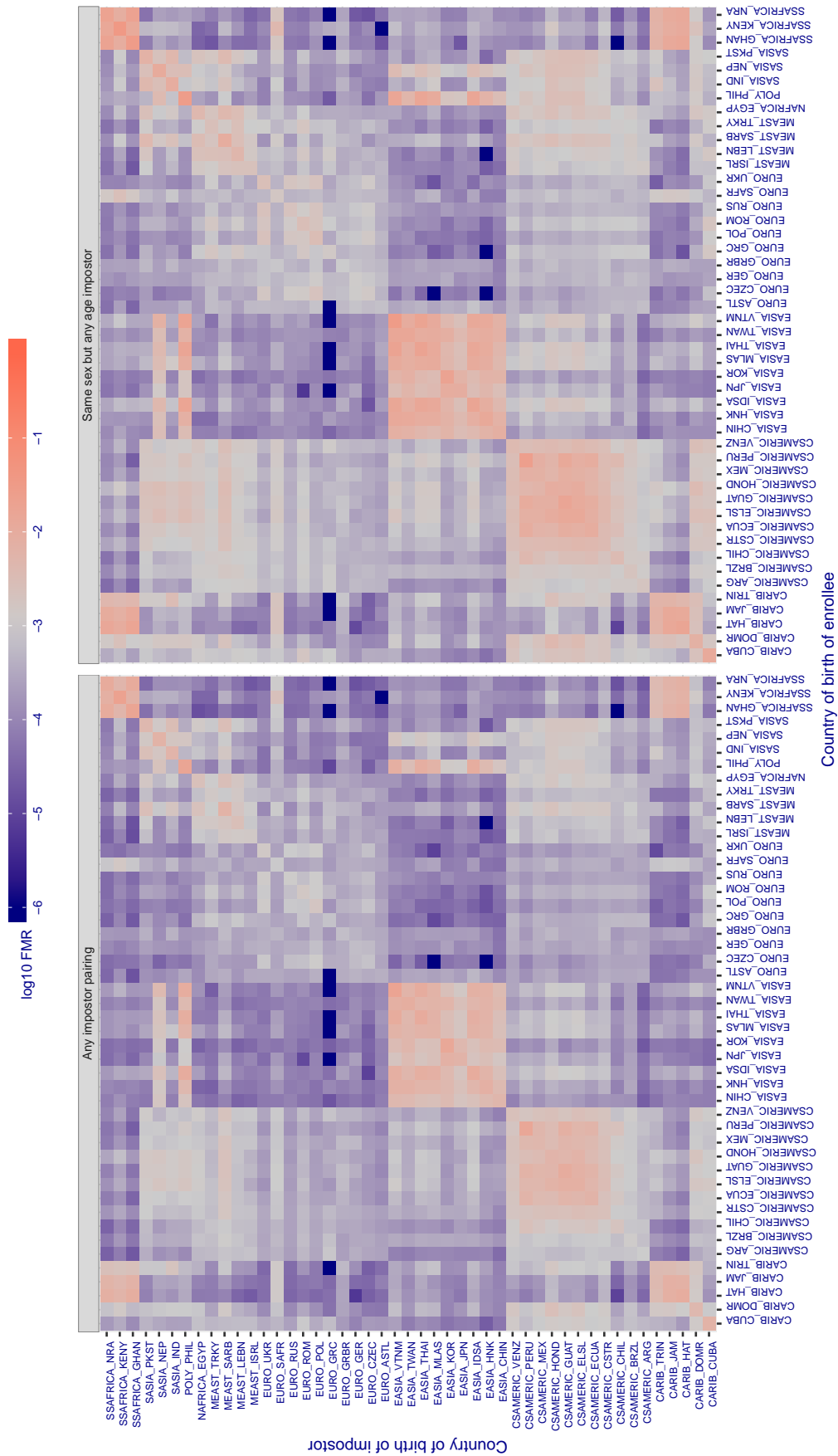


Figure 429: For algorithm pixelall-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.272$  for algorithm psl\_002, giving  $FMR(T) = 0.001$  globally.

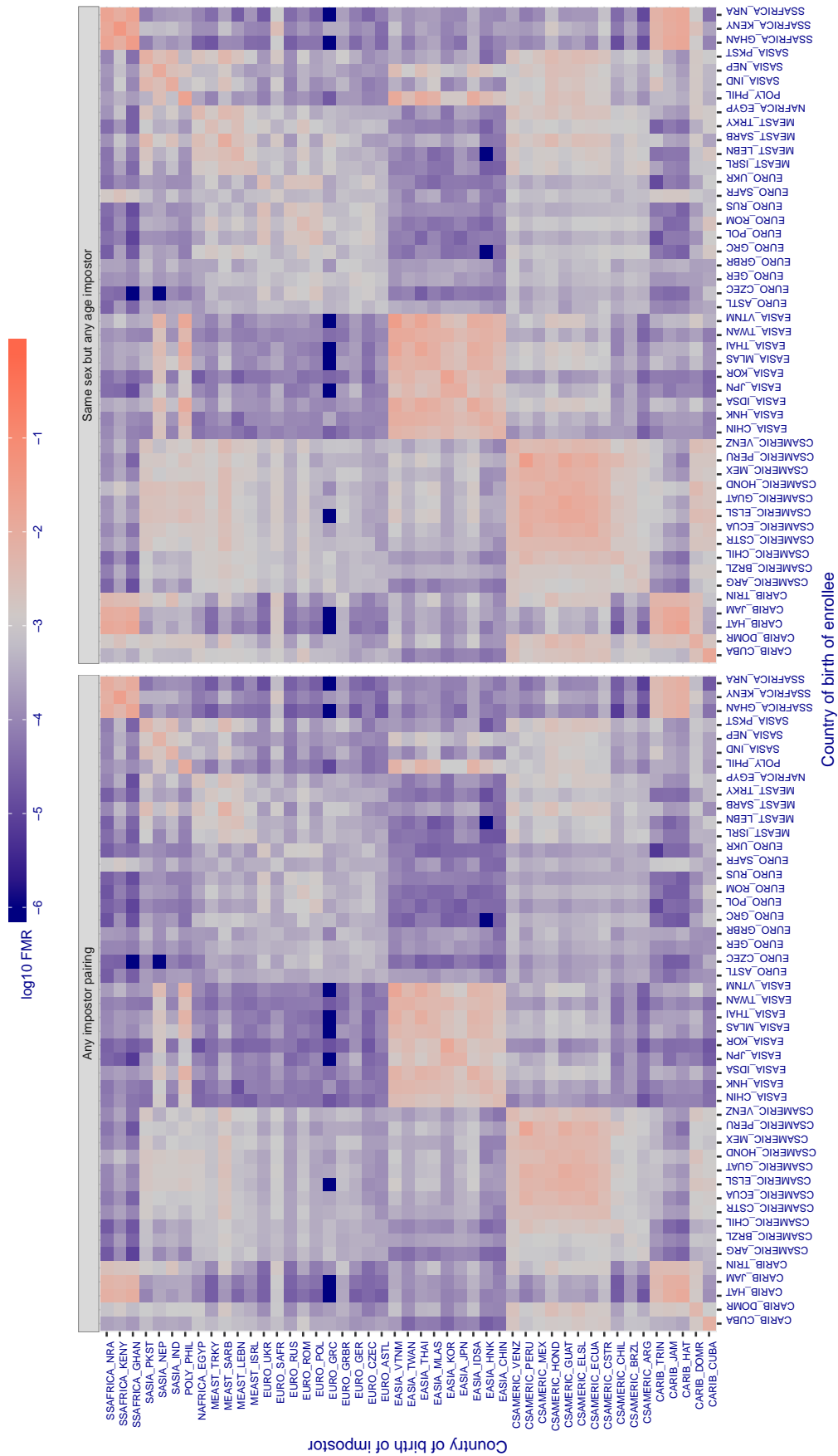


Figure 430: For algorithm psl-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 48.702$  for algorithm pyramid\_000, giving  $FMR(T) = 0.001$  globally.

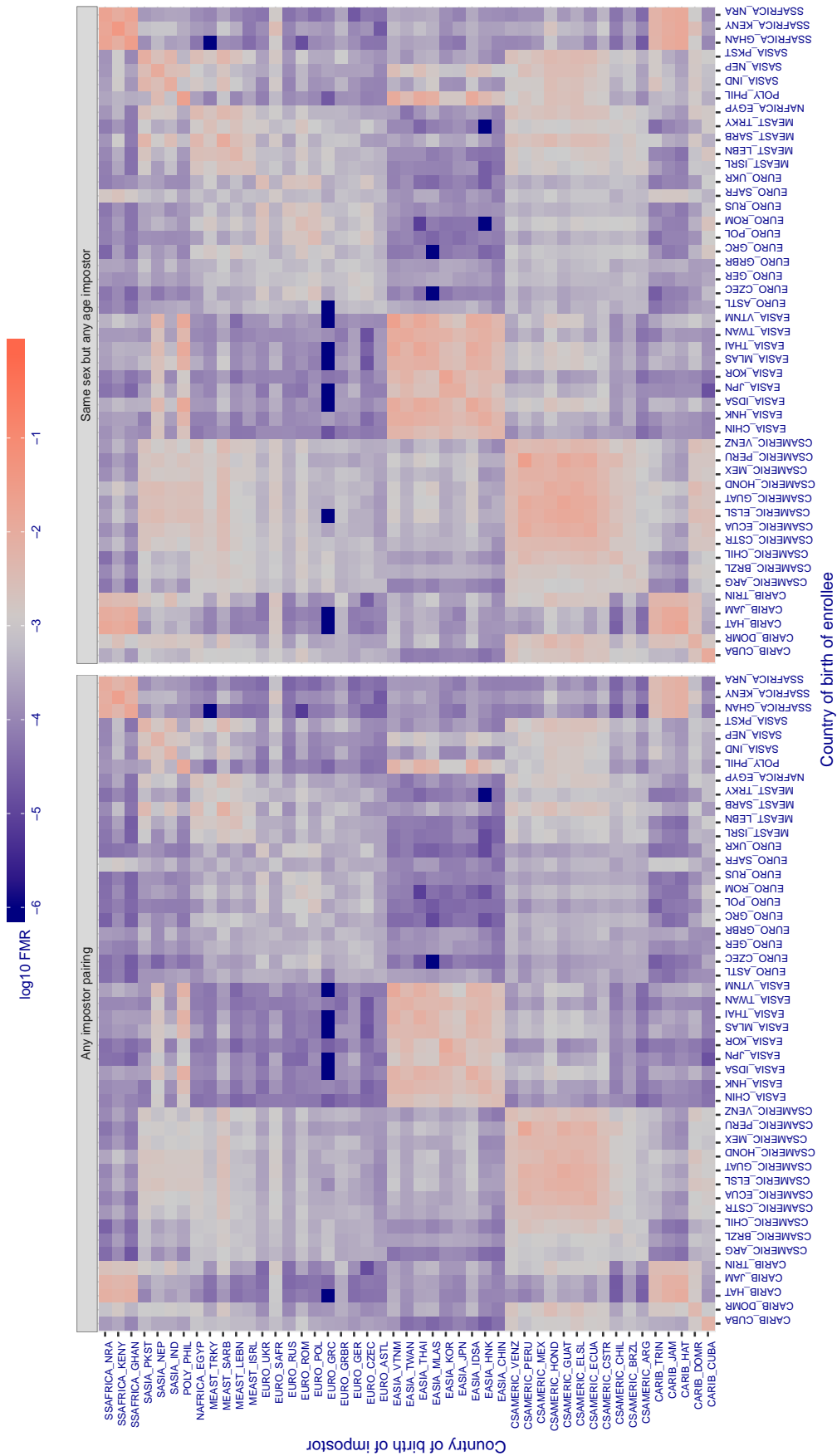


Figure 431: For algorithm pyramid-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 0.536$  for algorithm `rankone_007`, giving  $FMR(T) = 0.001$  globally.

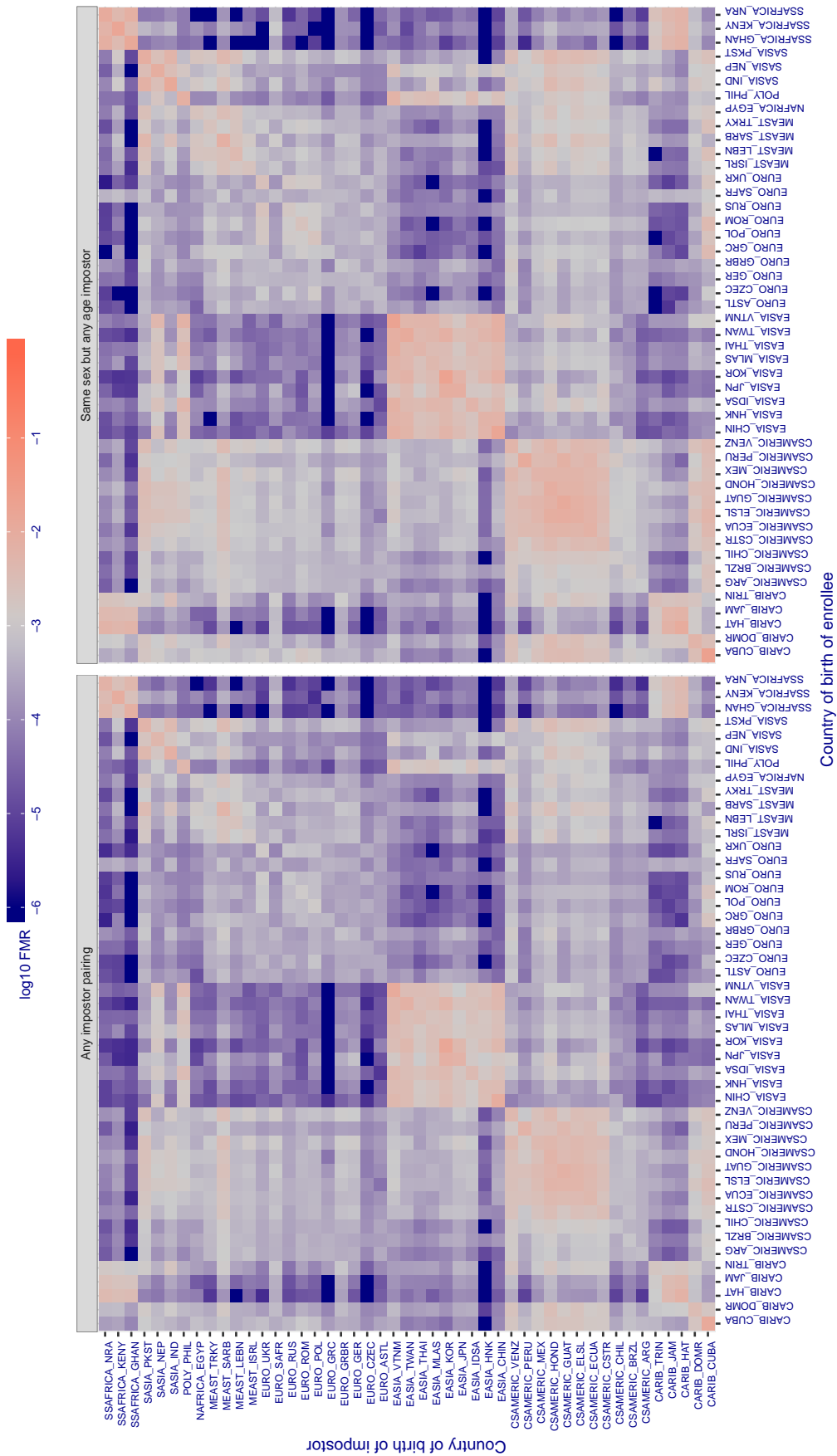


Figure 432: For algorithm `rankone-007` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 0.814$  for algorithm realnetworks\_002, giving  $FMR(T) = 0.001$  globally.

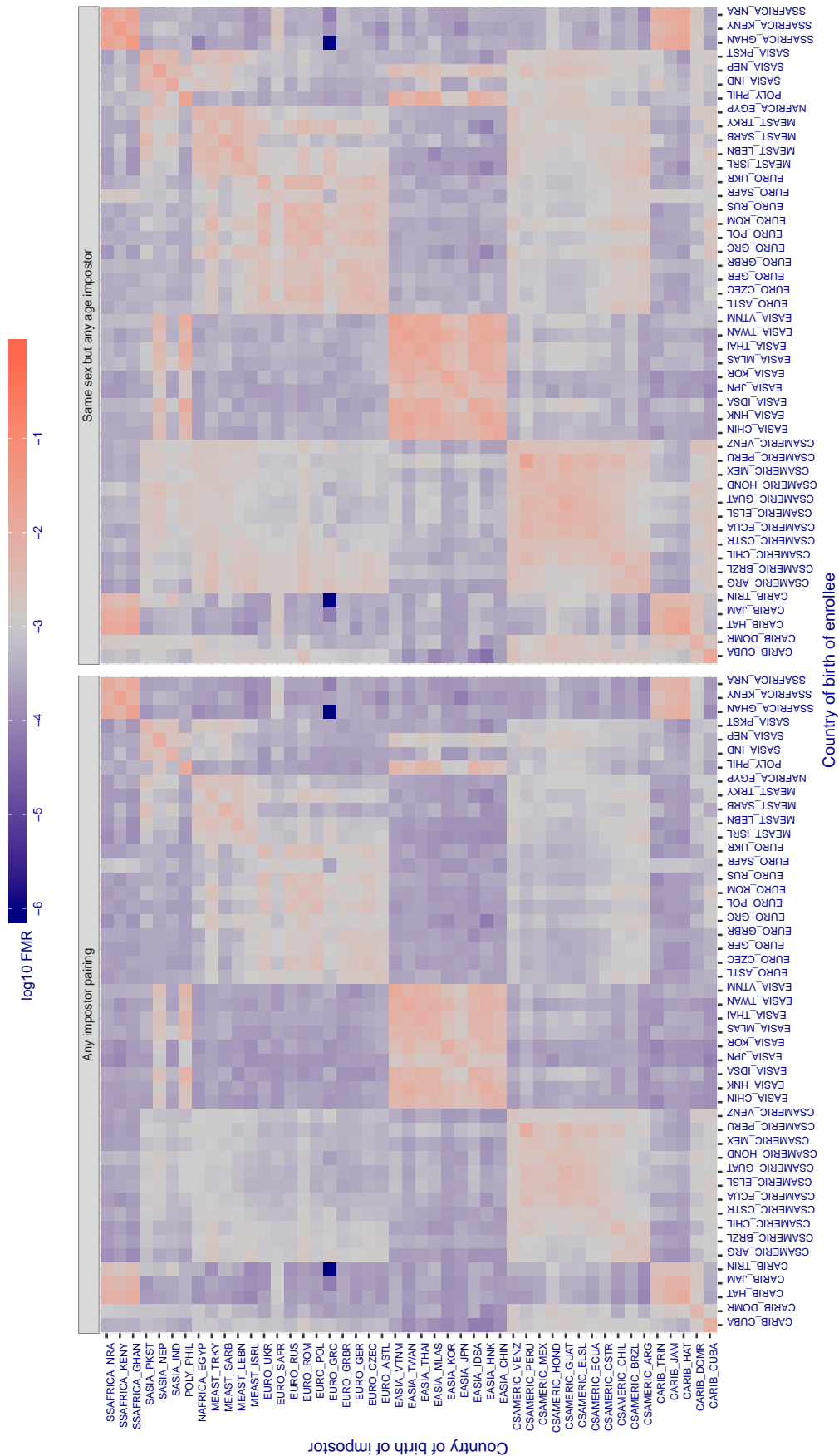


Figure 433: For algorithm realnetworks-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.817$  for algorithm realnetworks\_003, giving  $FMR(T) = 0.001$  globally.

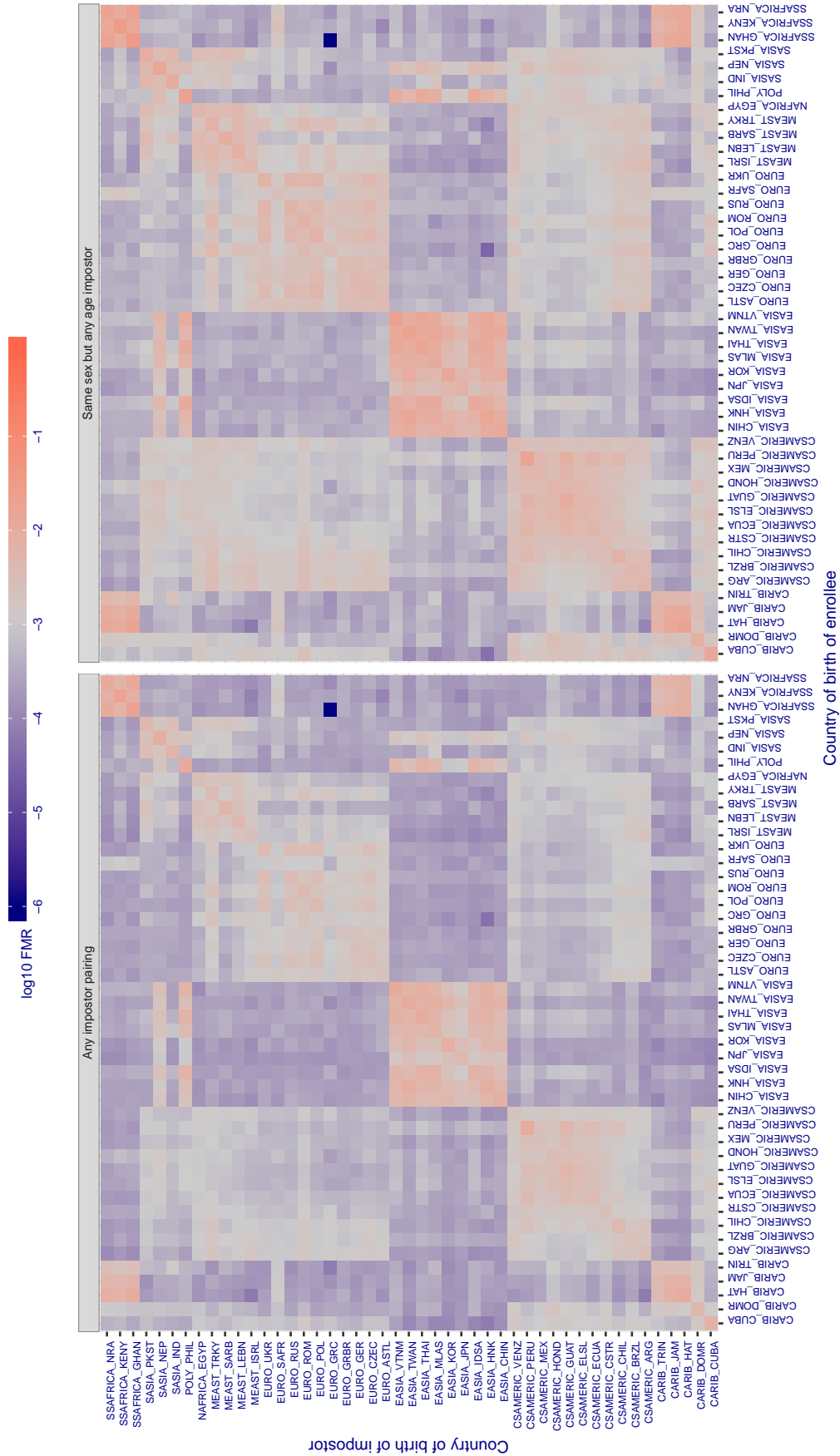


Figure 434: For algorithm realnetworks-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 65.920$  for algorithm remarkai\_000, giving  $FMR(T) = 0.001$  globally.

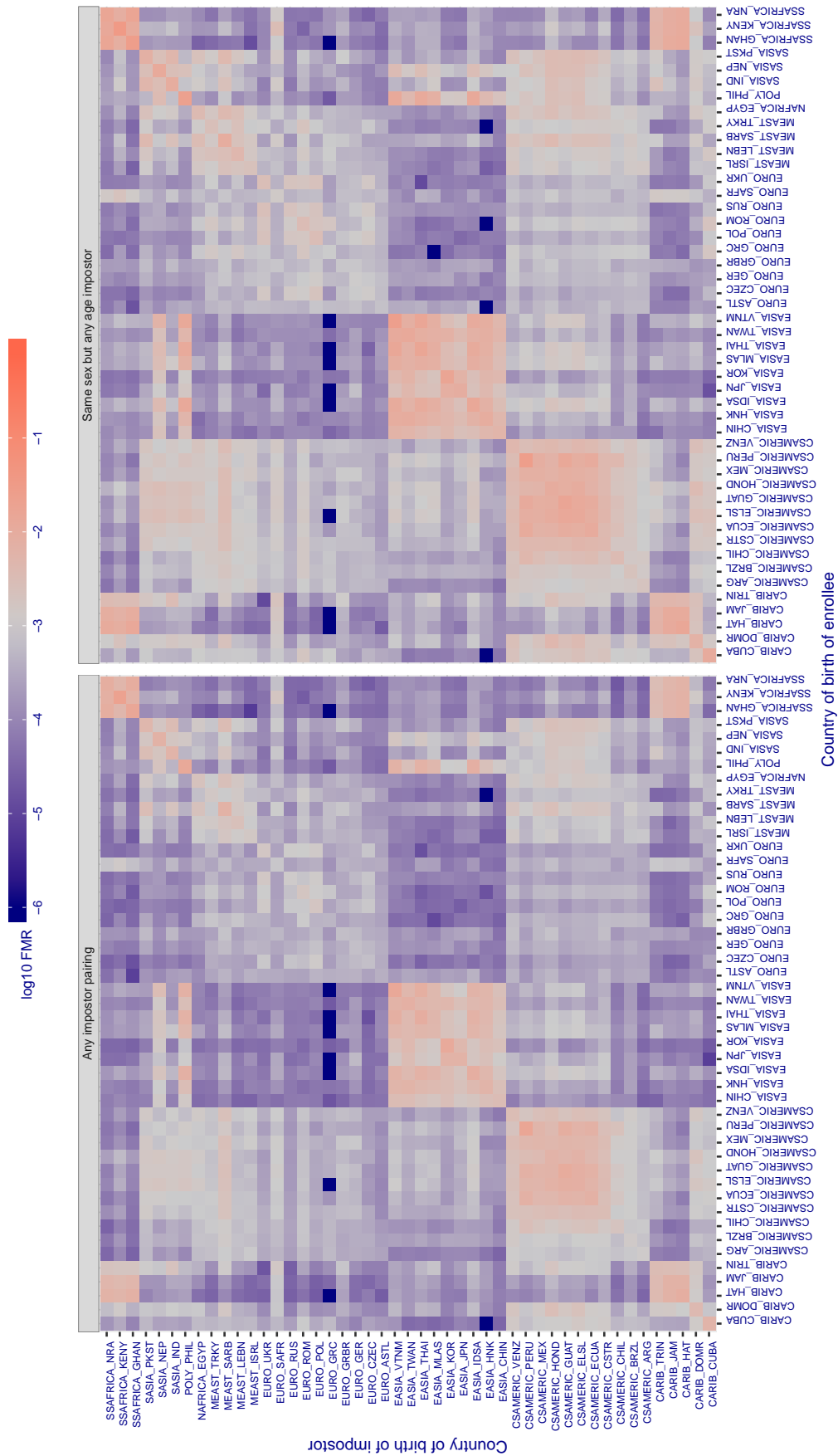


Figure 435: For algorithm remarkai-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 65.928$  for algorithm remarkai\_001, giving  $FMR(T) = 0.001$  globally.

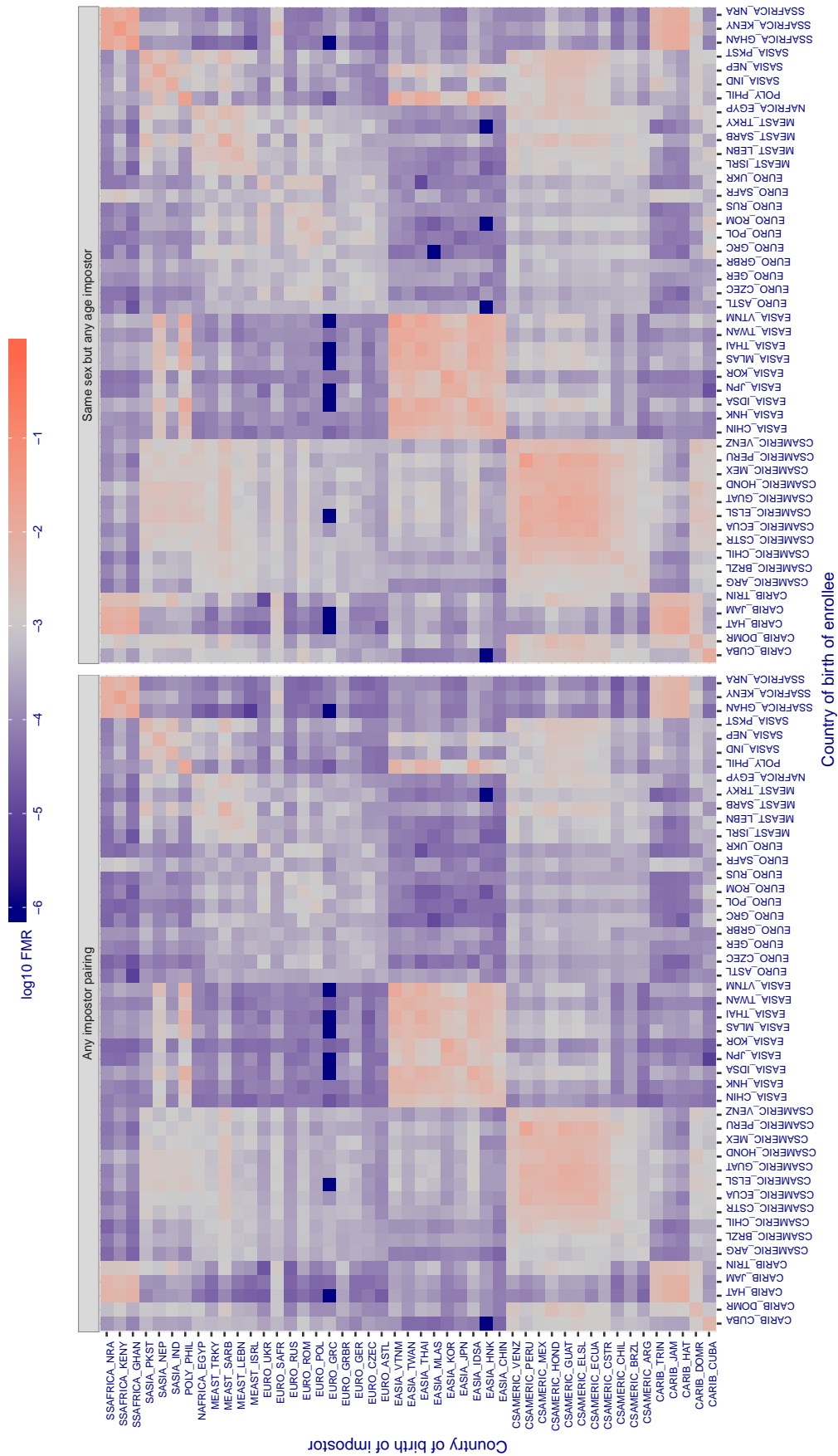


Figure 436: For algorithm remarkai-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.624$  for algorithm rokid\_000, giving  $FMR(T) = 0.001$  globally.

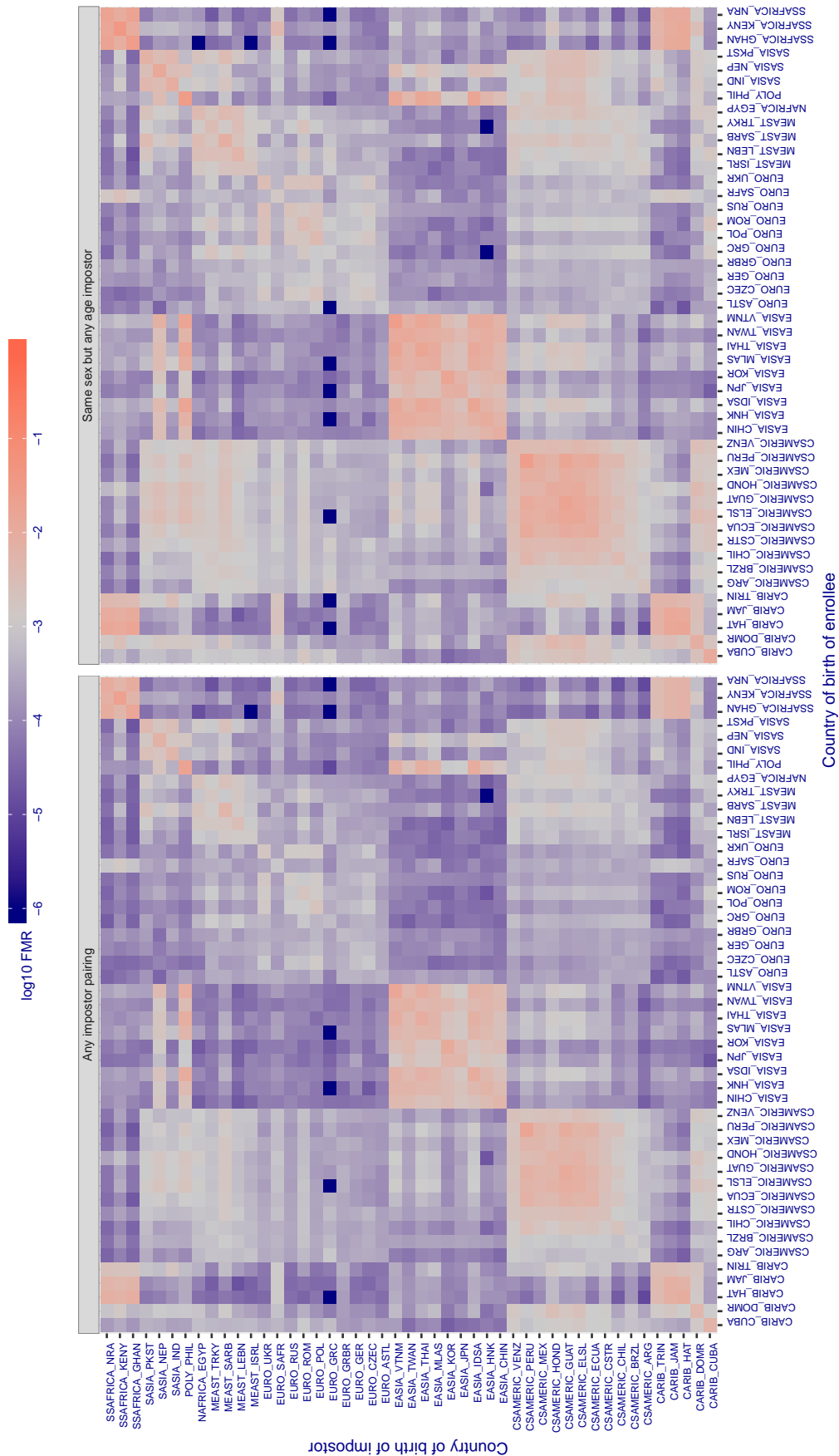


Figure 437: For algorithm rokid-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.609$  for algorithm saffe\_001, giving  $FMR(T) = 0.001$  globally.

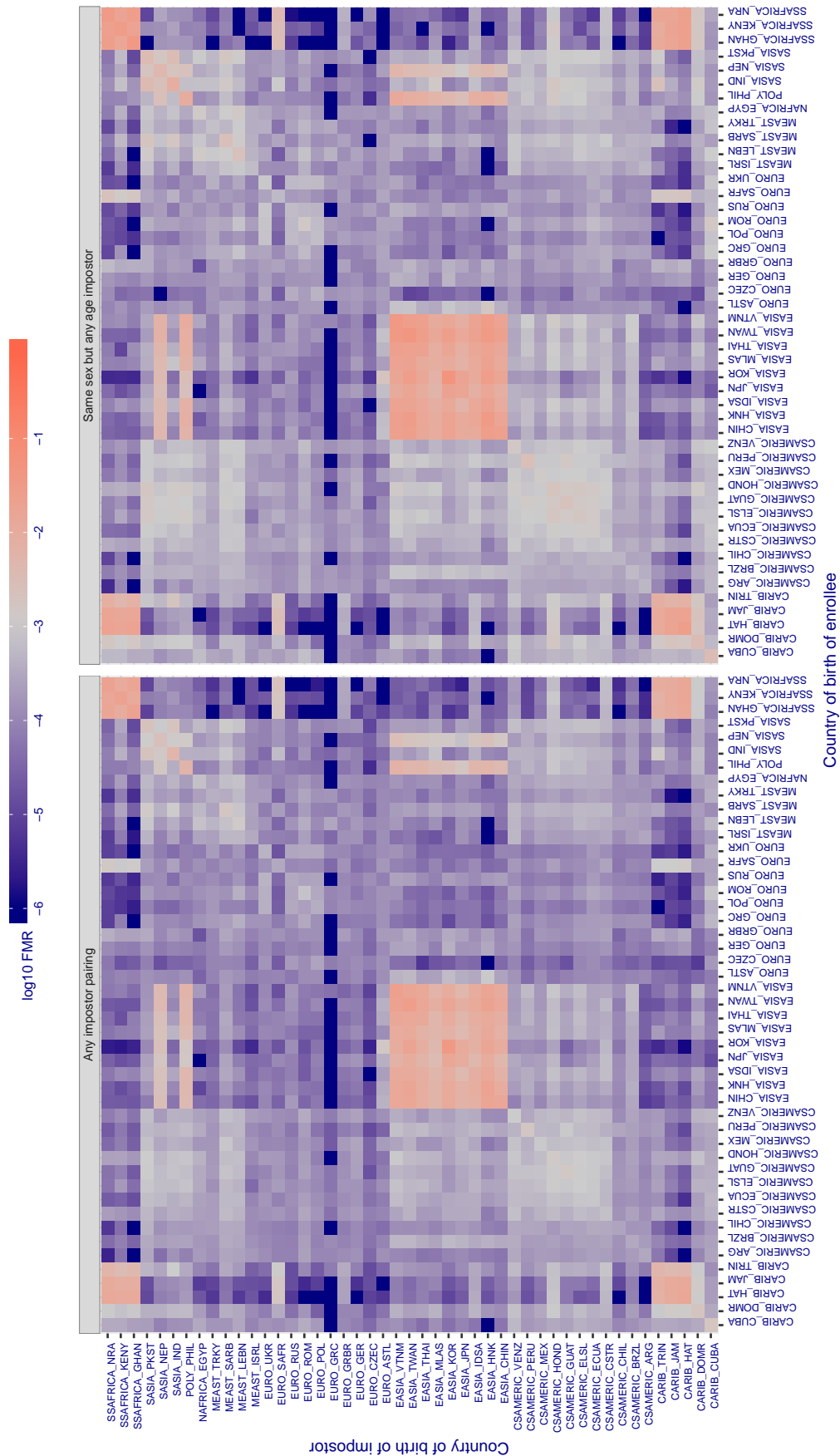


Figure 438: For algorithm saffe-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold T = 0.295 for algorithm saffe\_002, giving FMR(T) = 0.001 globally.

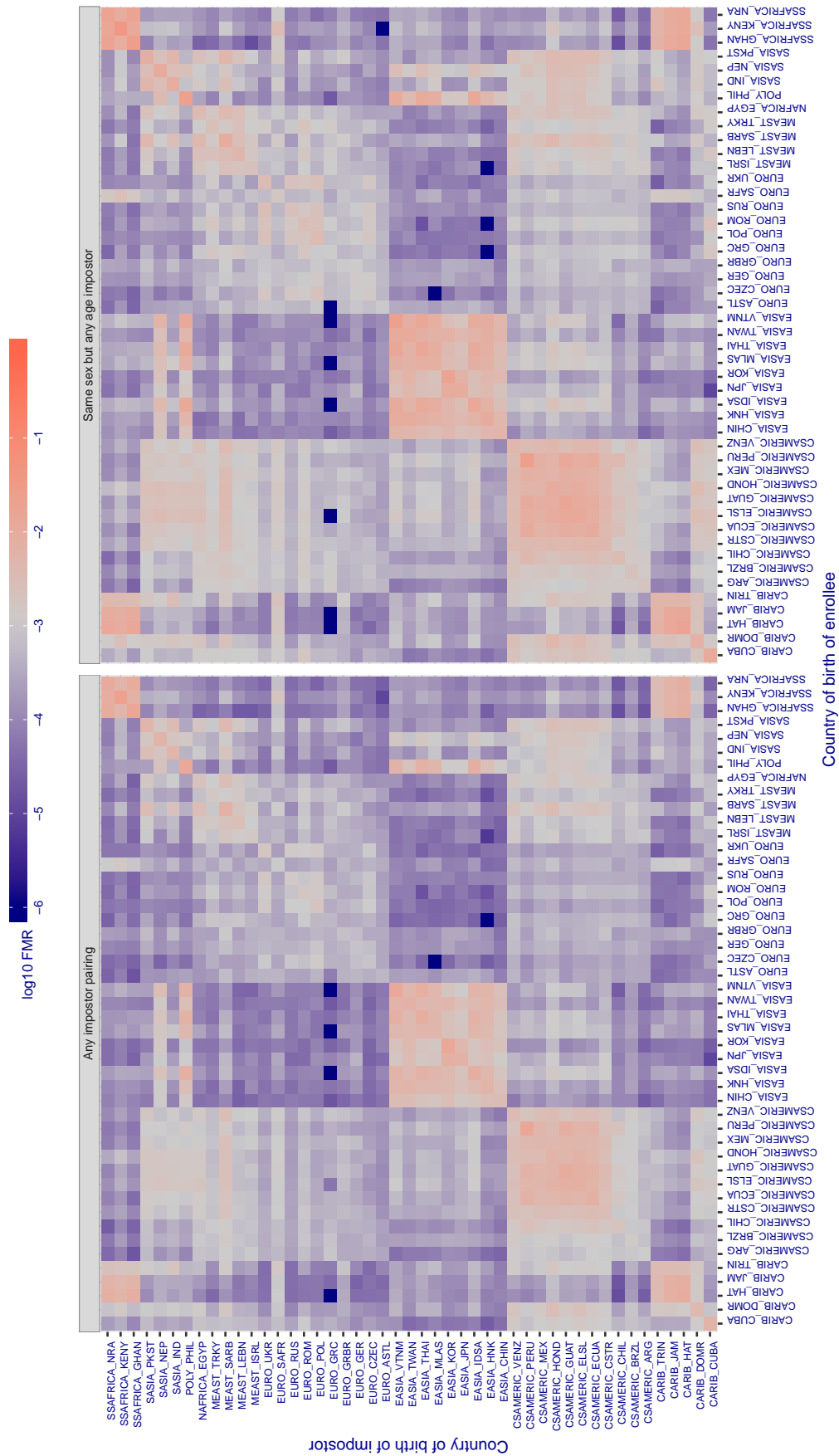


Figure 439: For algorithm saffe-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of 10<sup>10</sup> impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 50.914$  for algorithm `samtech_001`, giving  $FMR(T) = 0.001$  globally.

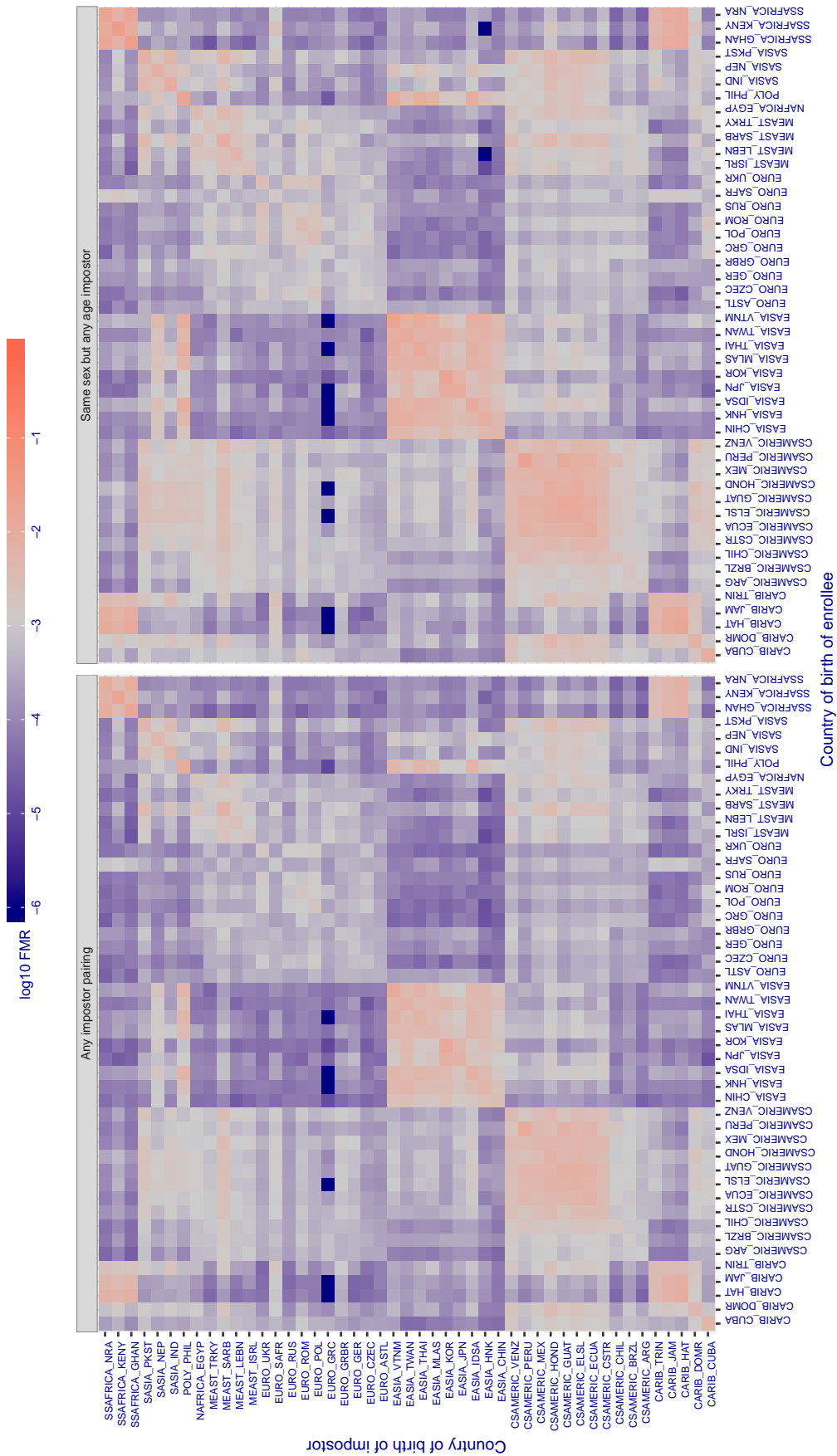


Figure 440: For algorithm `samtech-001` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 0.368$  for algorithm  $\text{sensetime}_{001}$ , giving  $\text{FMR}(T) = 0.001$  globally.

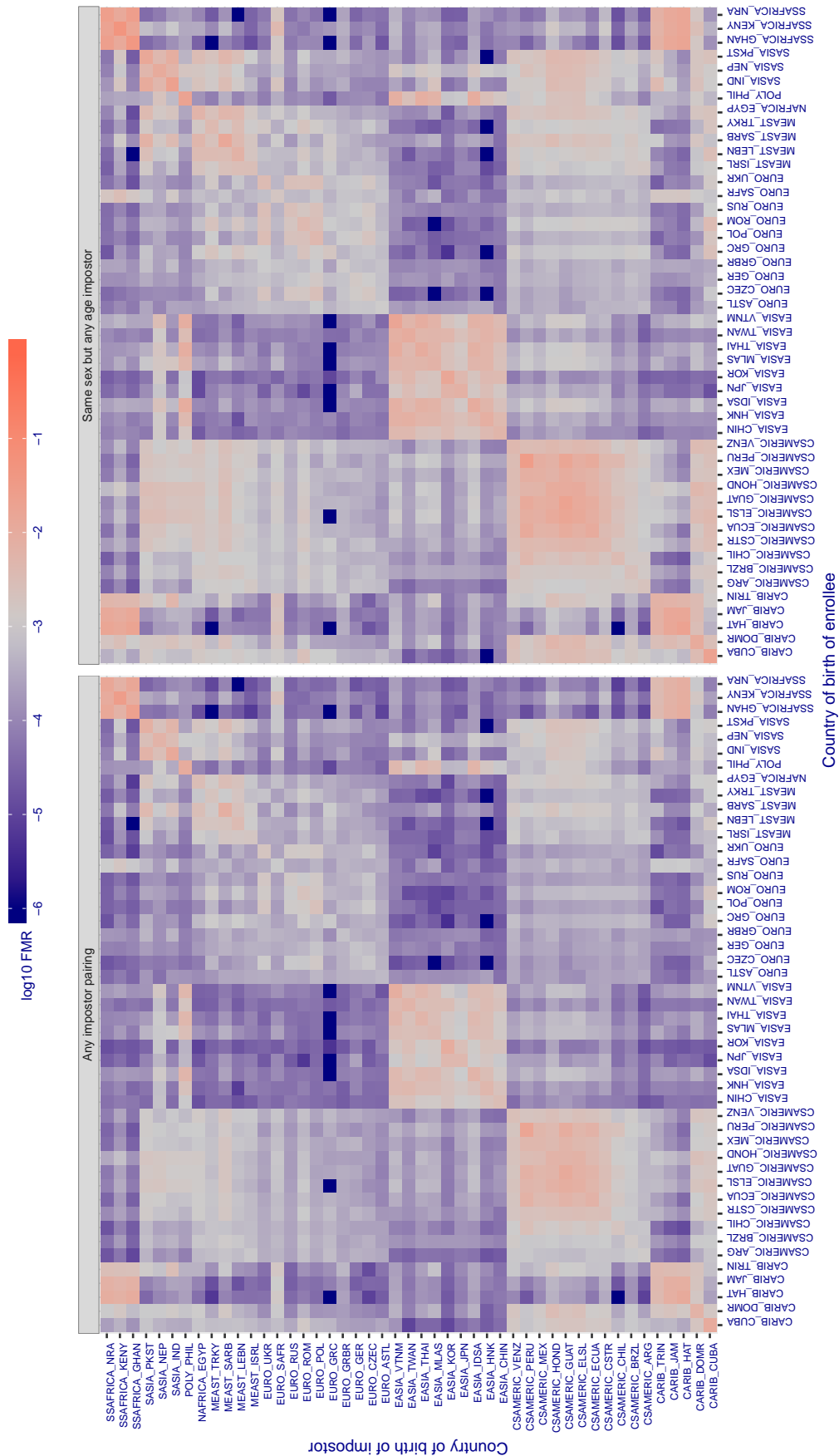


Figure 441: For algorithm  $\text{sensetime}_{001}$  operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} \text{FMR}$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.369$  for algorithm `sensetime_002`, giving  $FMR(T) = 0.001$  globally.

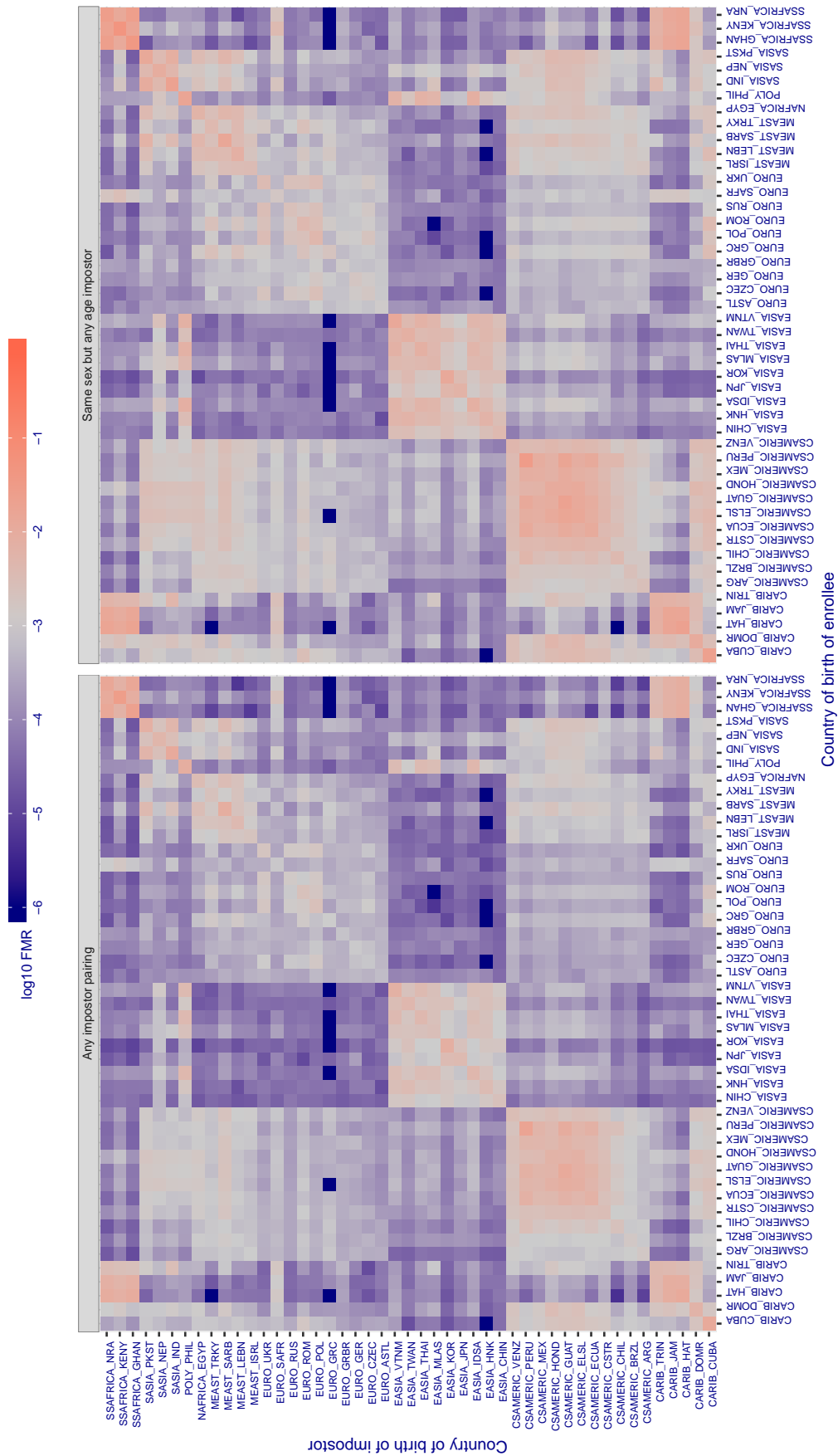


Figure 442: For algorithm `sensetime-002` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each  $+1$  increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.939$  for algorithm shaman\_000, giving  $FMR(T) = 0.001$  globally.

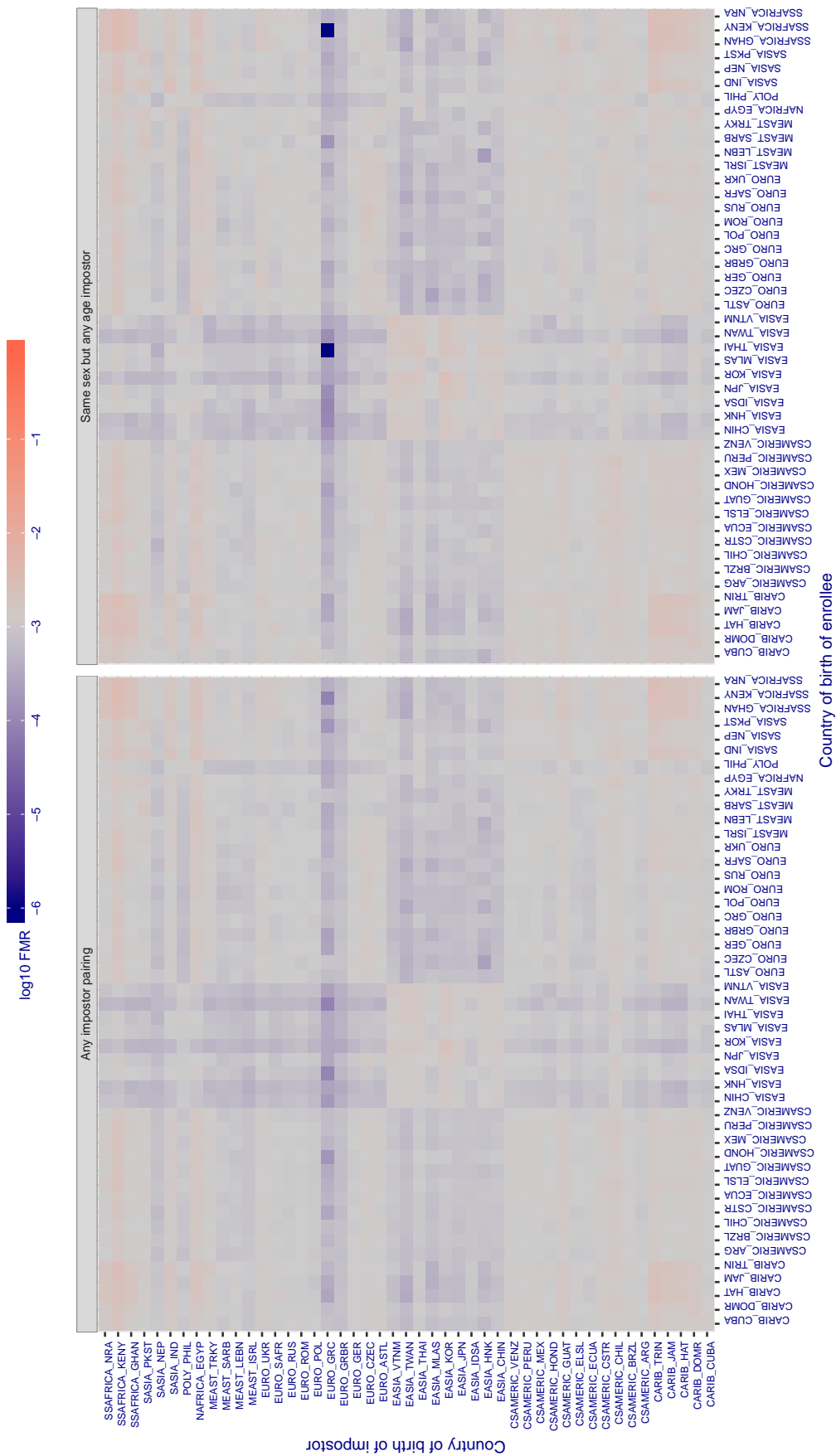


Figure 443: For algorithm shaman-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.599$  for algorithm shaman\_001, giving  $FMR(T) = 0.001$  globally.

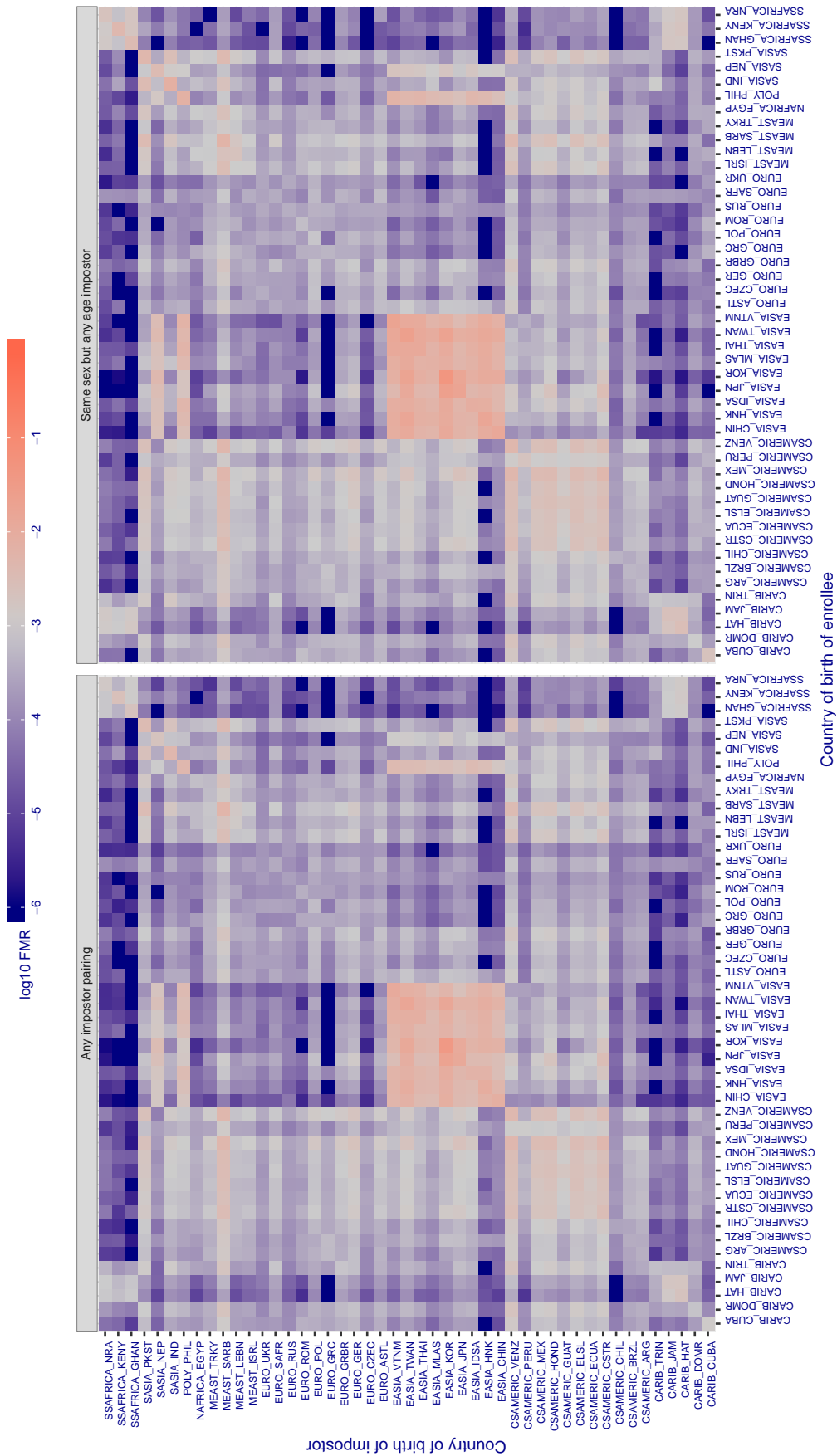


Figure 444: For algorithm shaman-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.316$  for algorithm shu\_001, giving  $FMR(T) = 0.001$  globally.

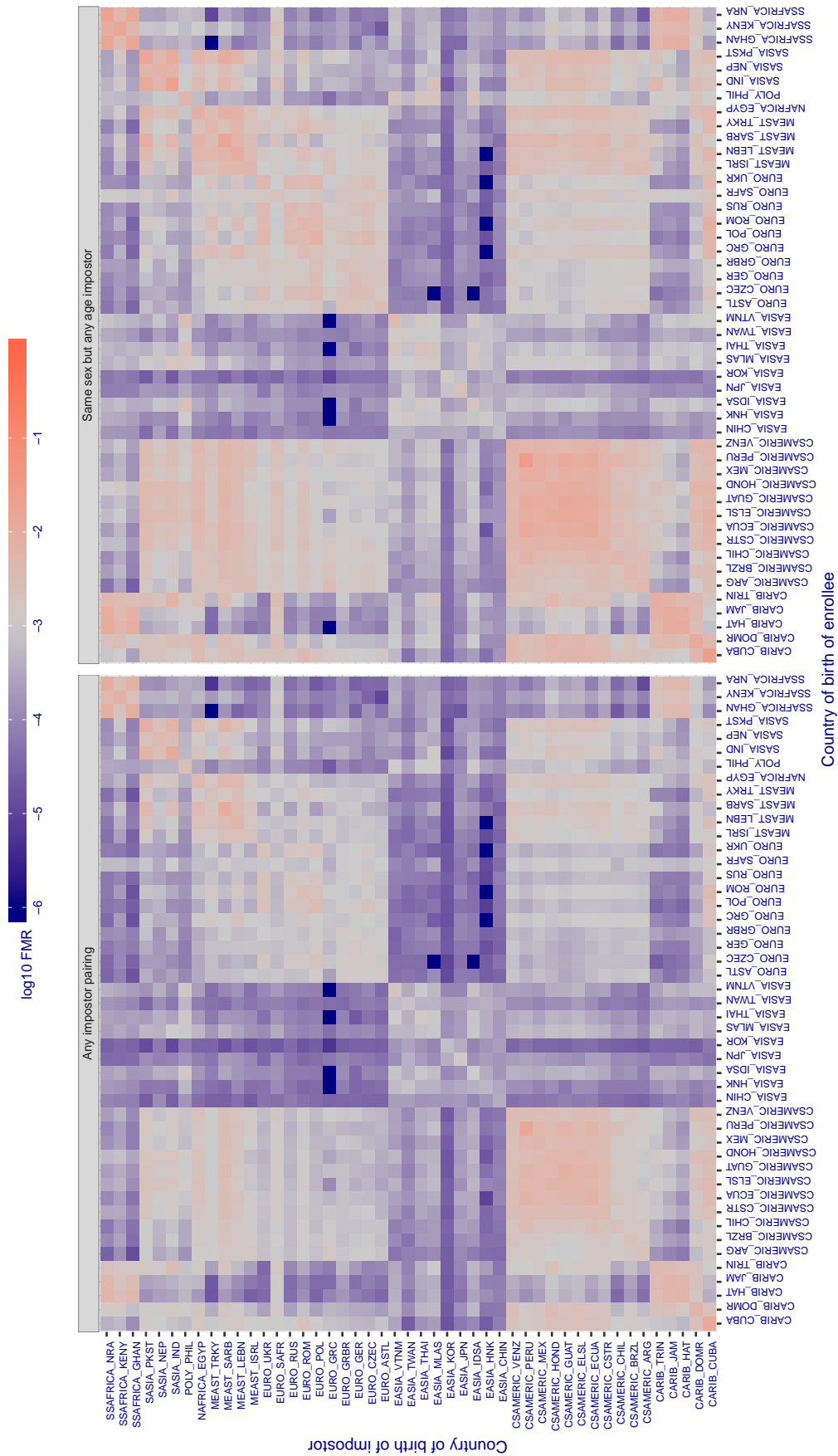


Figure 445: For algorithm shu-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.370$  for algorithm `siat_002`, giving  $FMR(T) = 0.001$  globally.

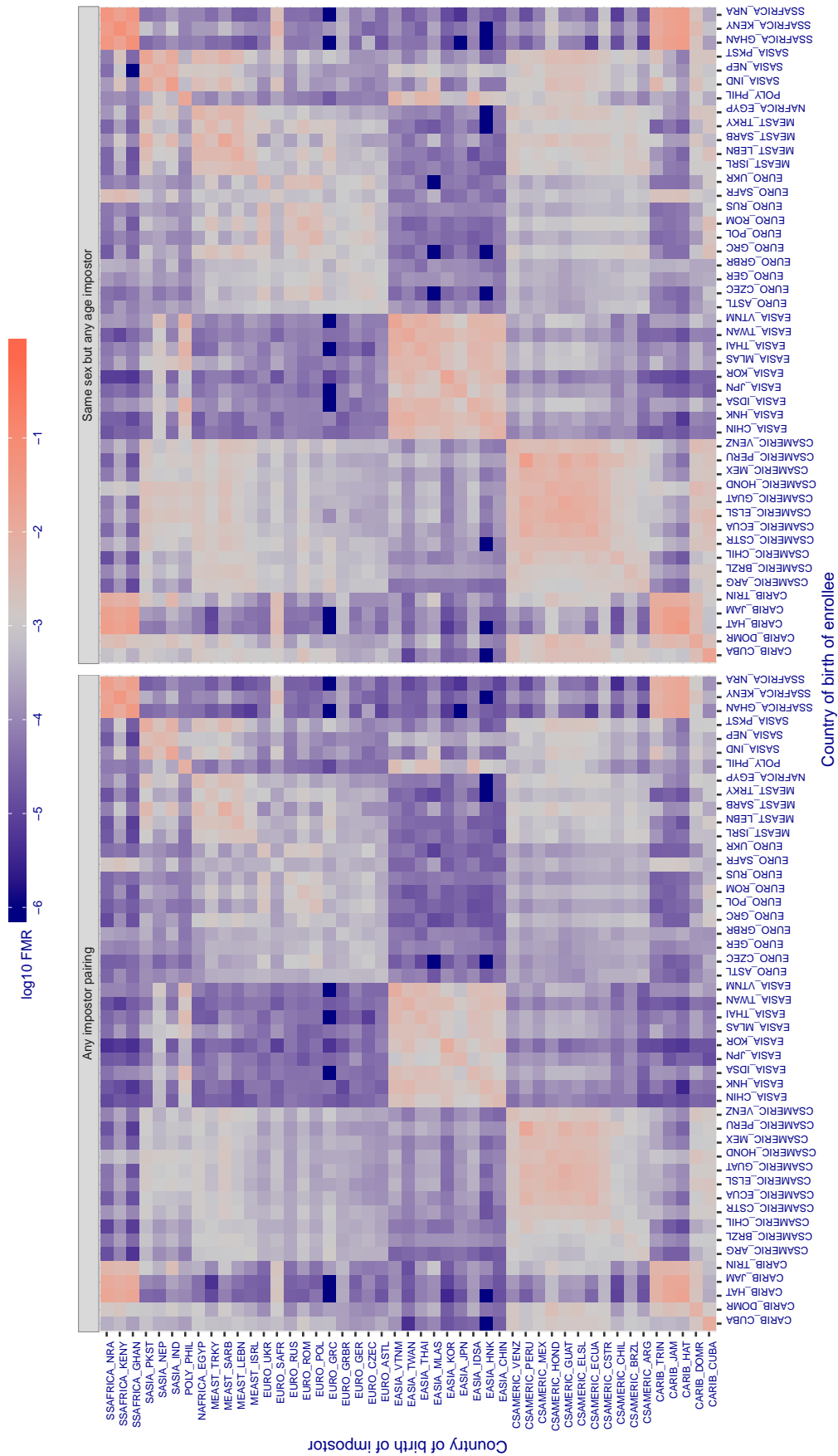


Figure 446: For algorithm `siat-002` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each  $+1$  increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.371$  for algorithm `siat_004`, giving  $FMR(T) = 0.001$  globally.

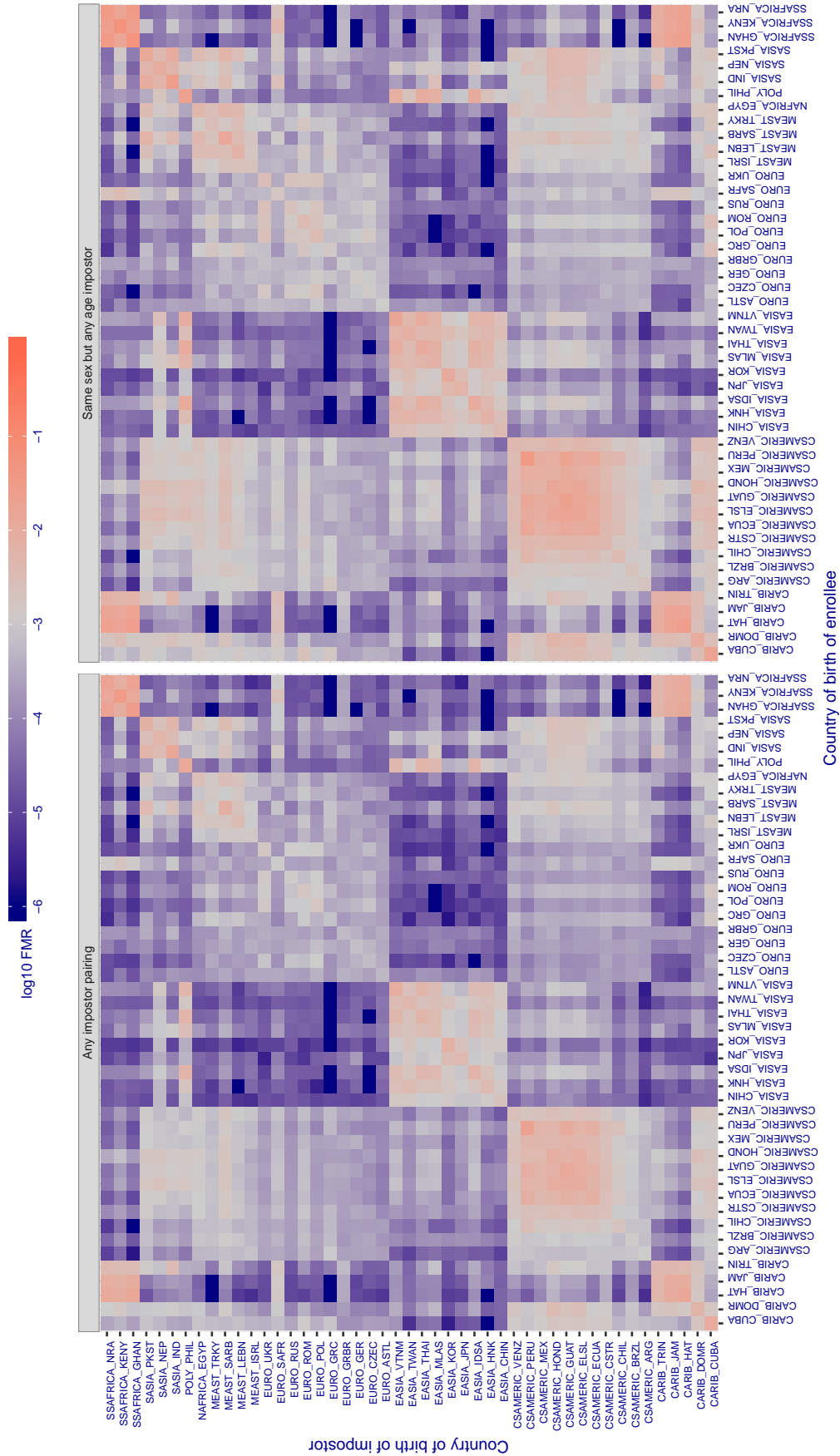


Figure 447: For algorithm `siat-004` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each  $+1$  increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 1.121$  for algorithm  $s_{jtu\_001}$ , giving  $FMR(T) = 0.001$  globally.

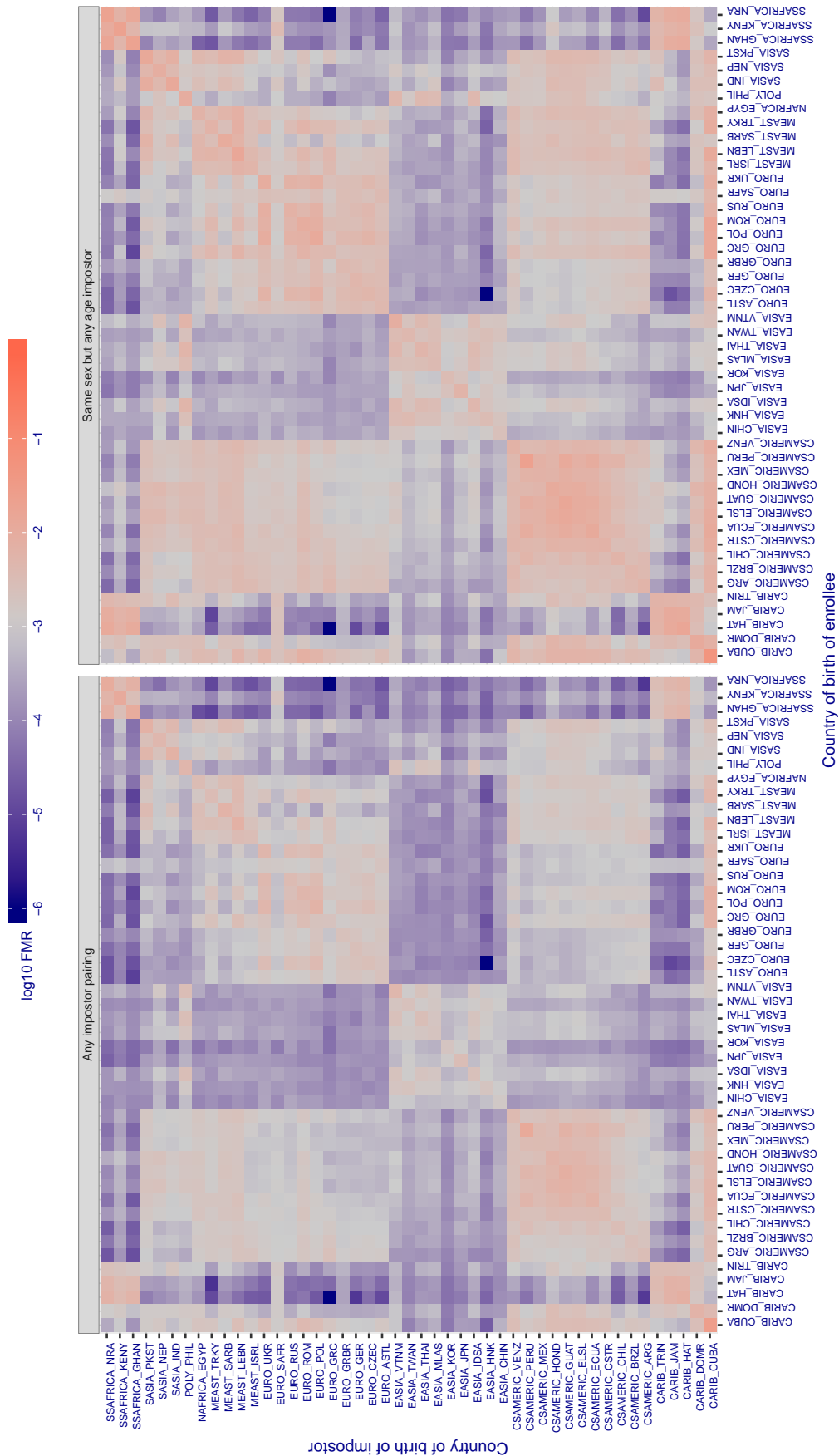


Figure 448: For algorithm  $s_{jtu\_001}$  operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 0.488$  for algorithm `smilart_002`, giving  $FMR(T) = 0.001$  globally.

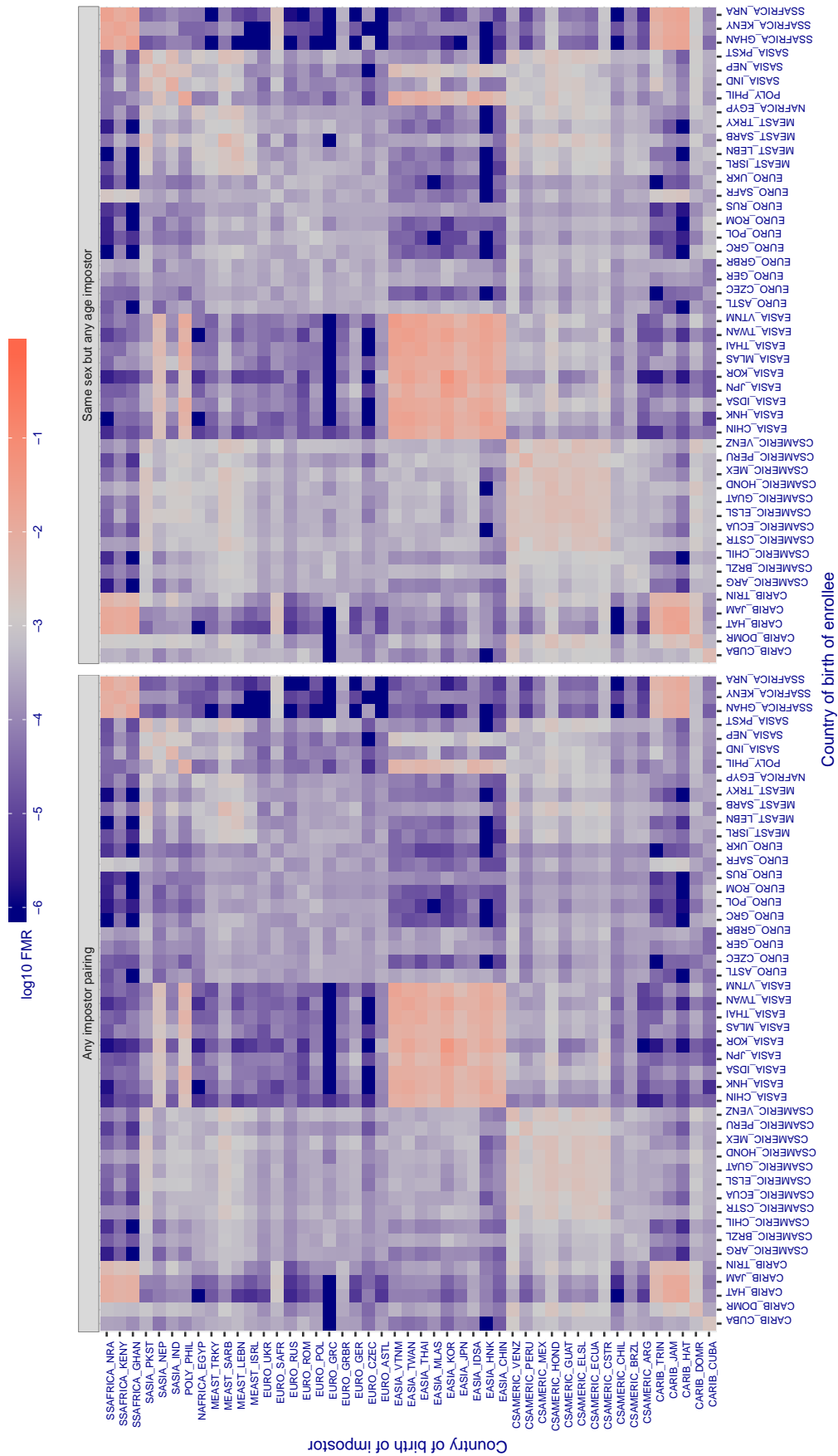


Figure 449: For algorithm `smilart-002` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each  $+1$  increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.388$  for algorithm `smilart_003`, giving  $FMR(T) = 0.001$  globally.

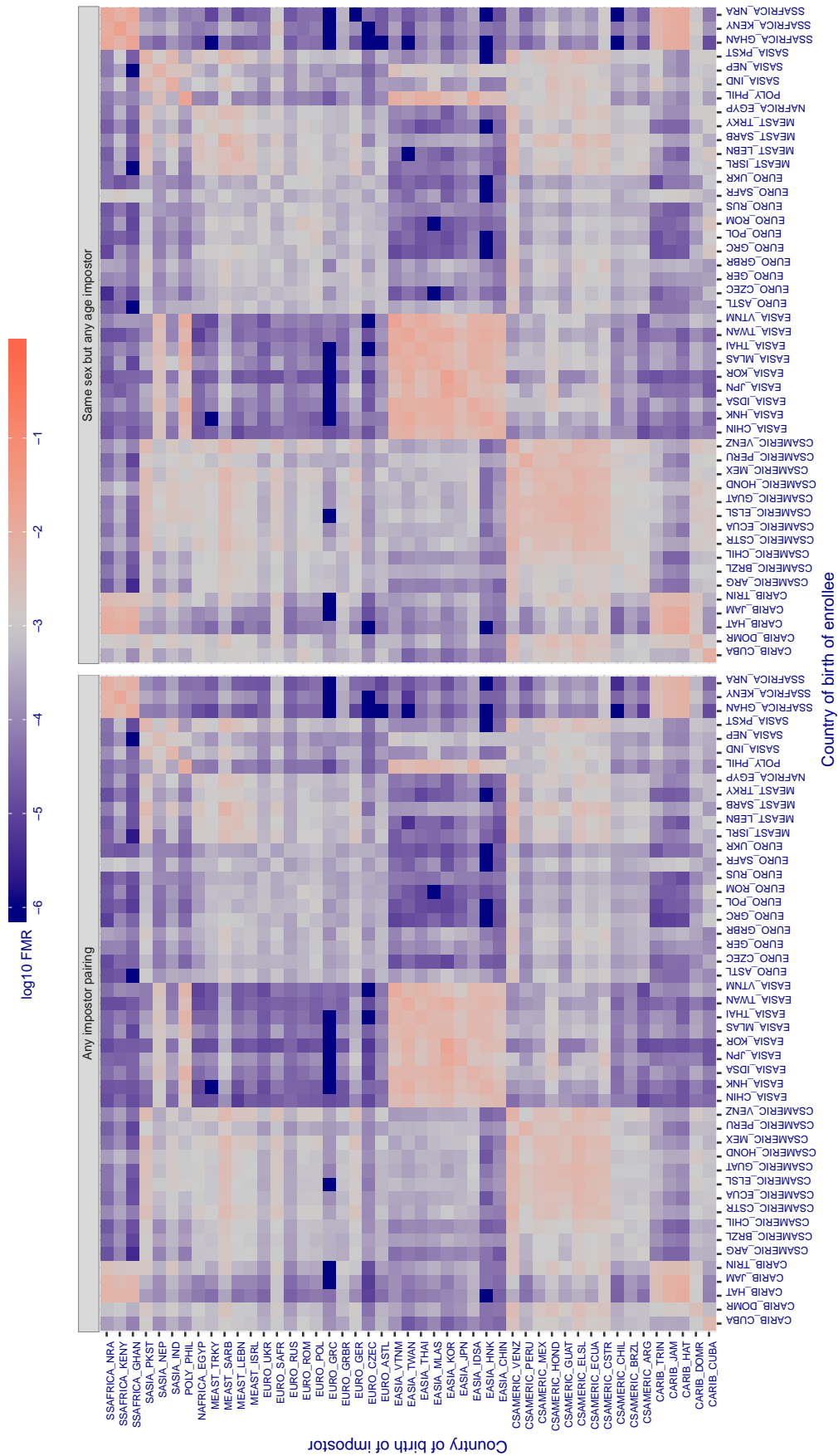


Figure 450: For algorithm `smilart-003` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each  $+1$  increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.251$  for algorithm starhybrid\_001, giving  $FMR(T) = 0.001$  globally.

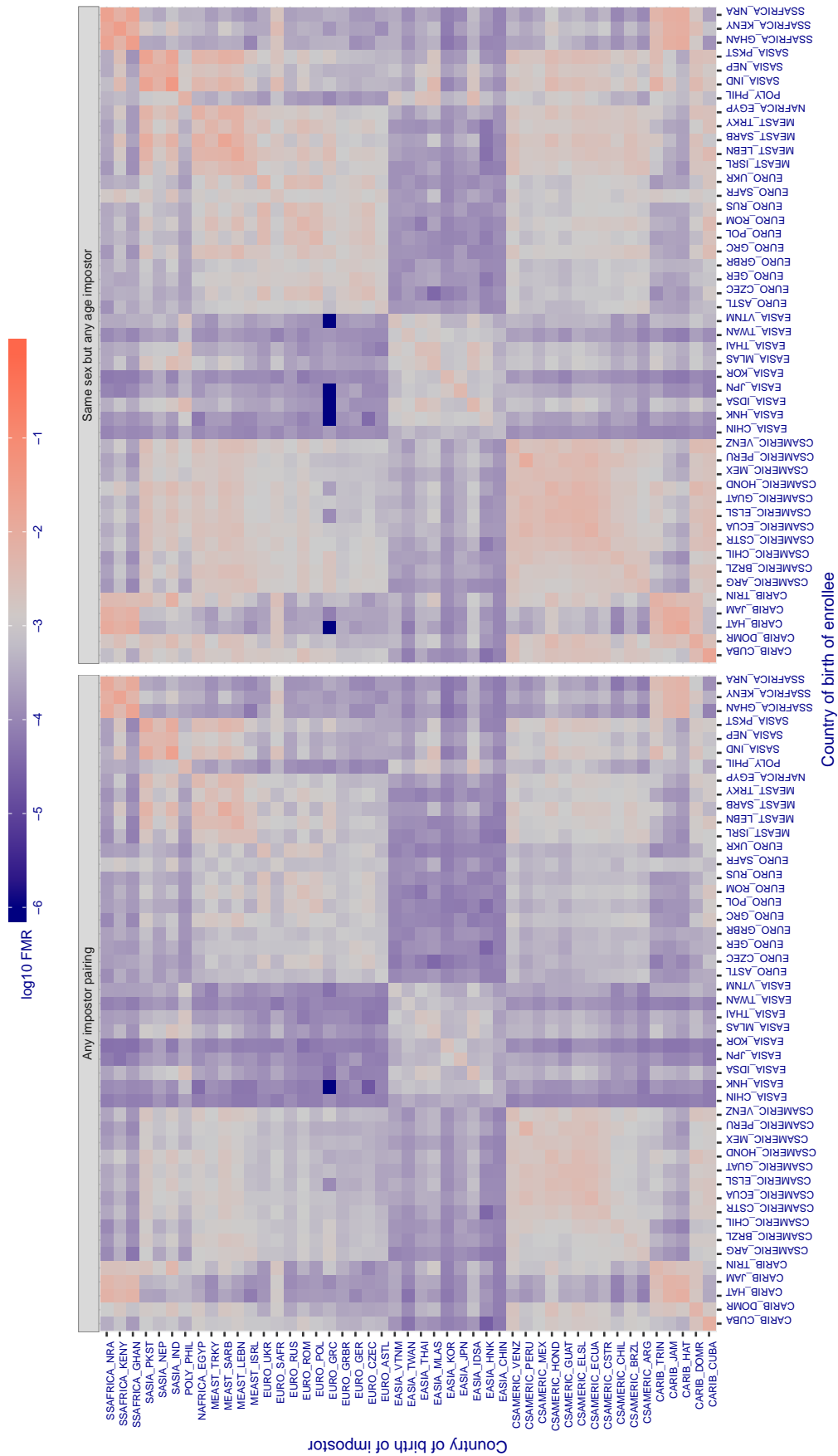


Figure 451: For algorithm starhybrid-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 0.300$  for algorithm `synesis_006`, giving  $FMR(T) = 0.001$  globally.

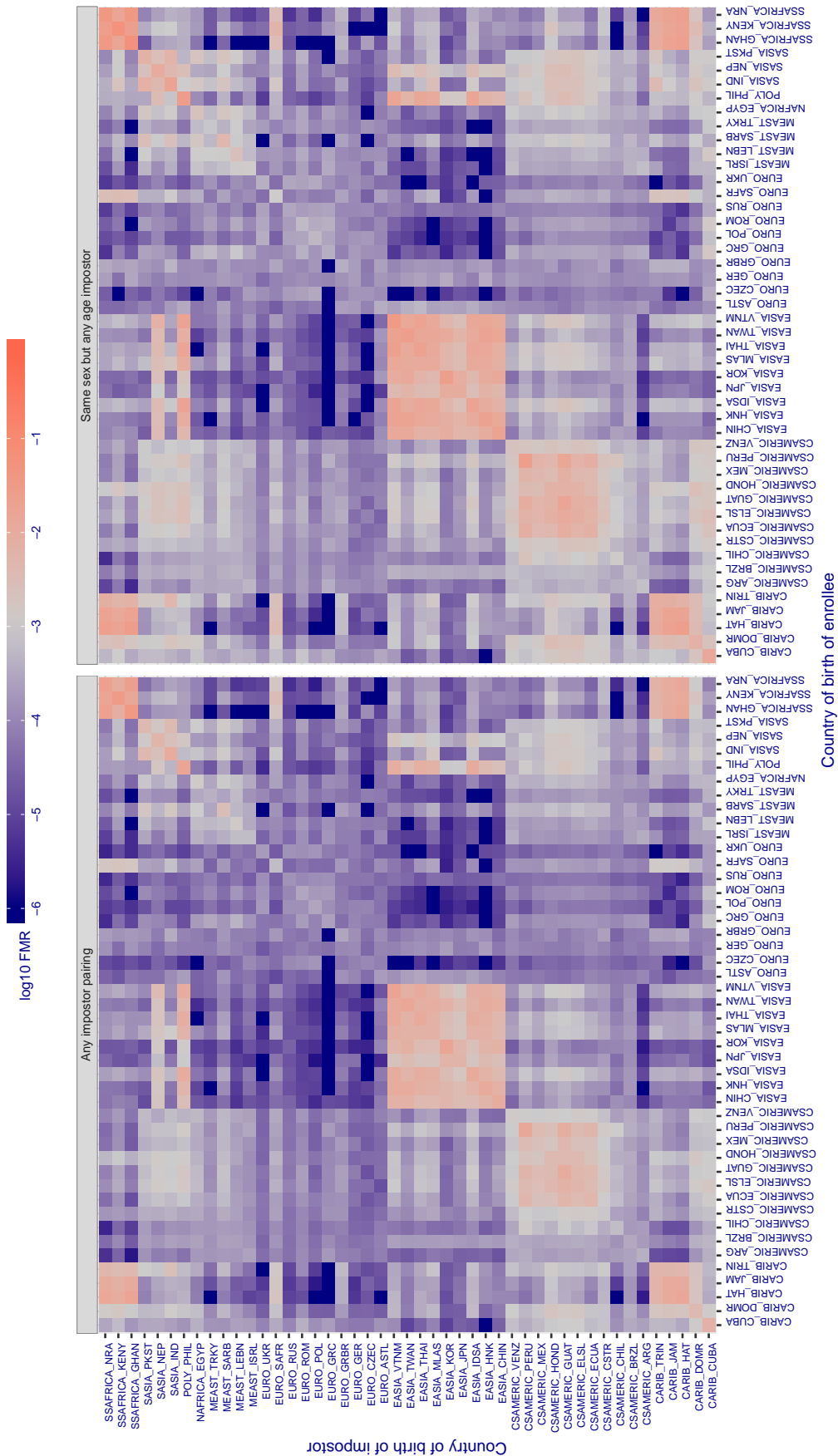


Figure 453: For algorithm `synesis-006` operating on *visa* images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each  $+1$  increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.344$  for algorithm  $\text{synology}_{000}$ , giving  $\text{FMR}(T) = 0.001$  globally.

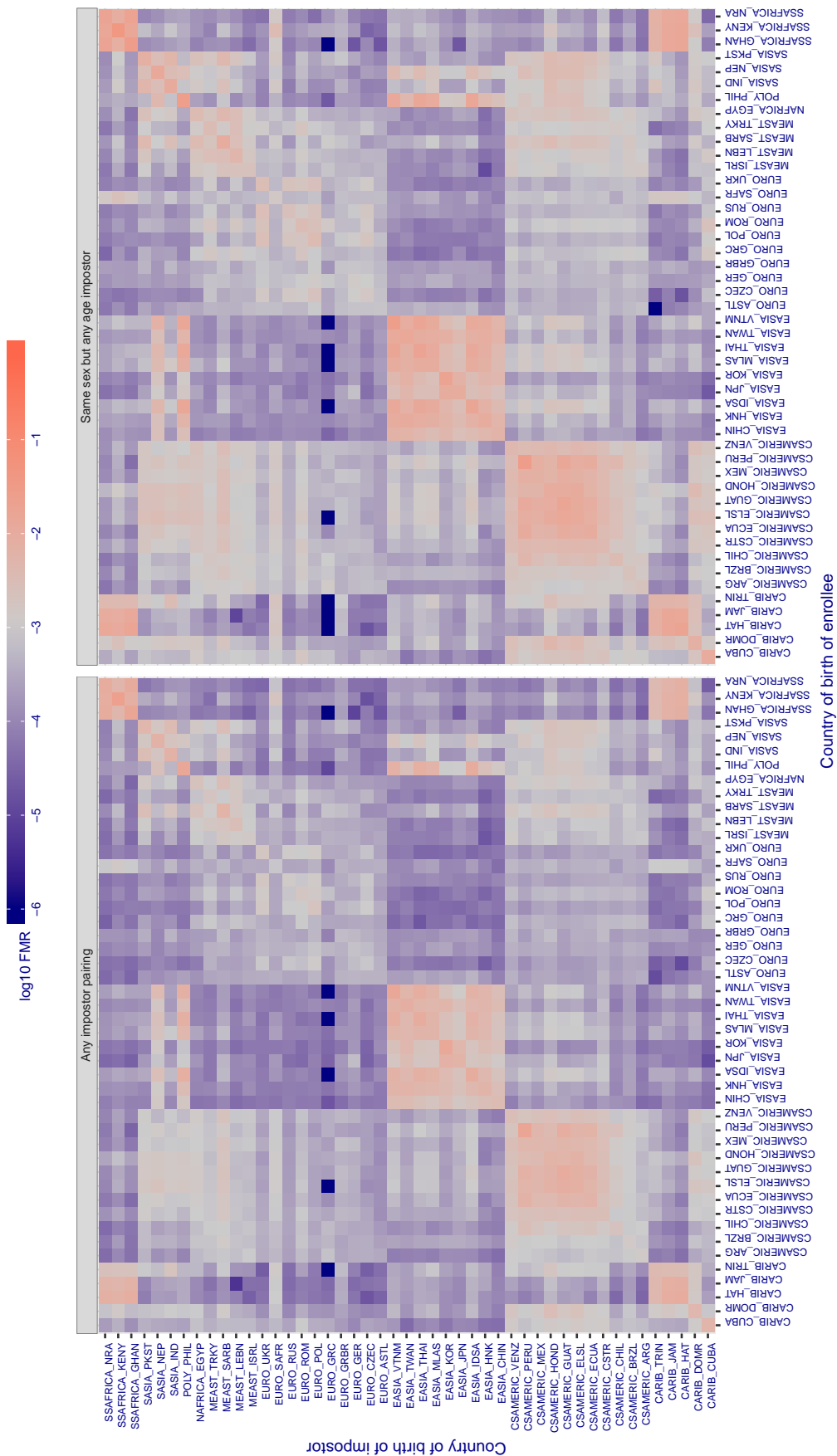


Figure 454: For algorithm  $\text{synology}_{000}$  operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each  $+1$  increase in  $\log_{10} \text{FMR}$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 147.234$  for algorithm tech5\_002, giving  $FMR(T) = 0.001$  globally.

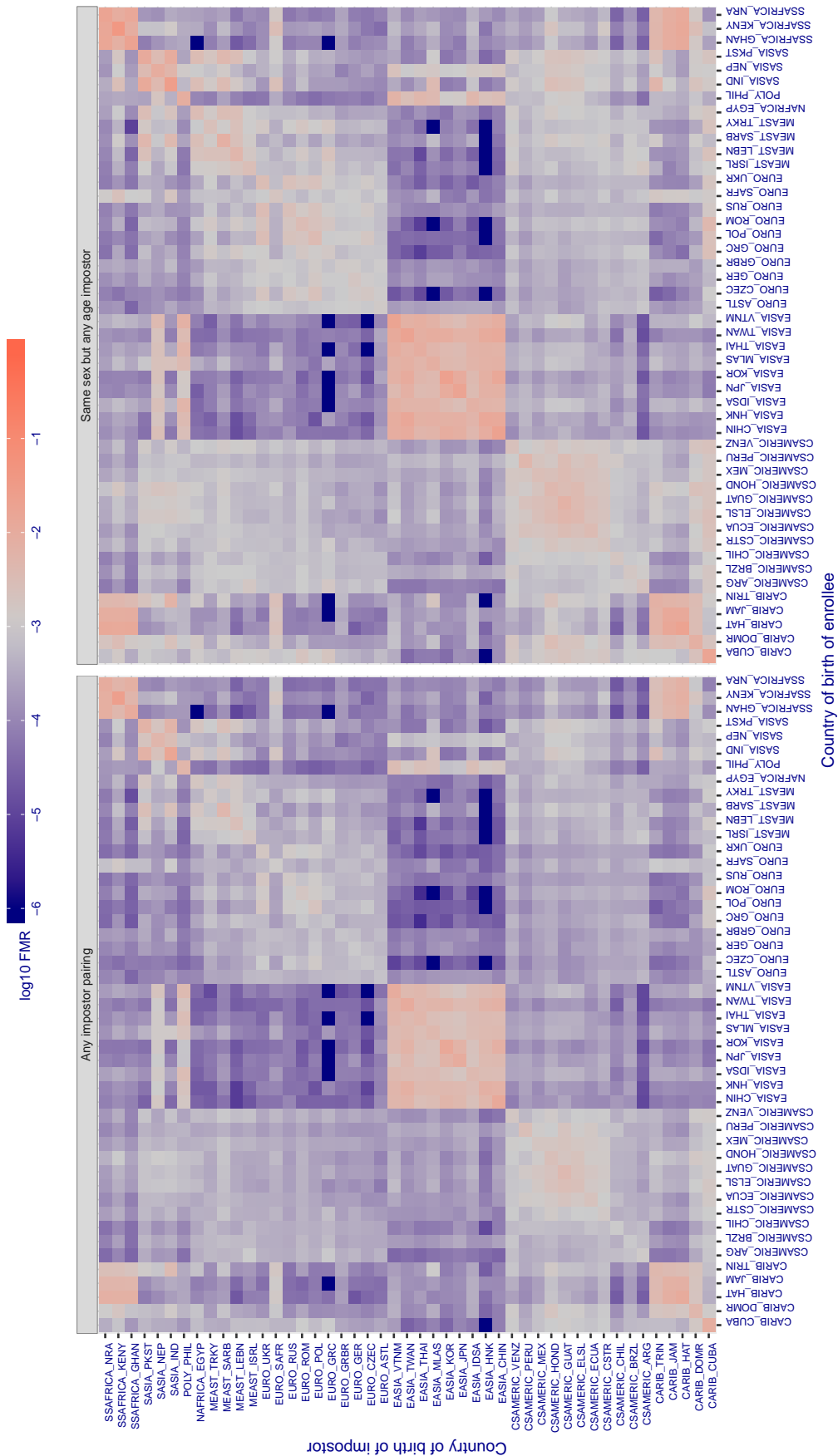


Figure 455: For algorithm tech5-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 146.607$  for algorithm tech5\_003, giving  $FMR(T) = 0.001$  globally.

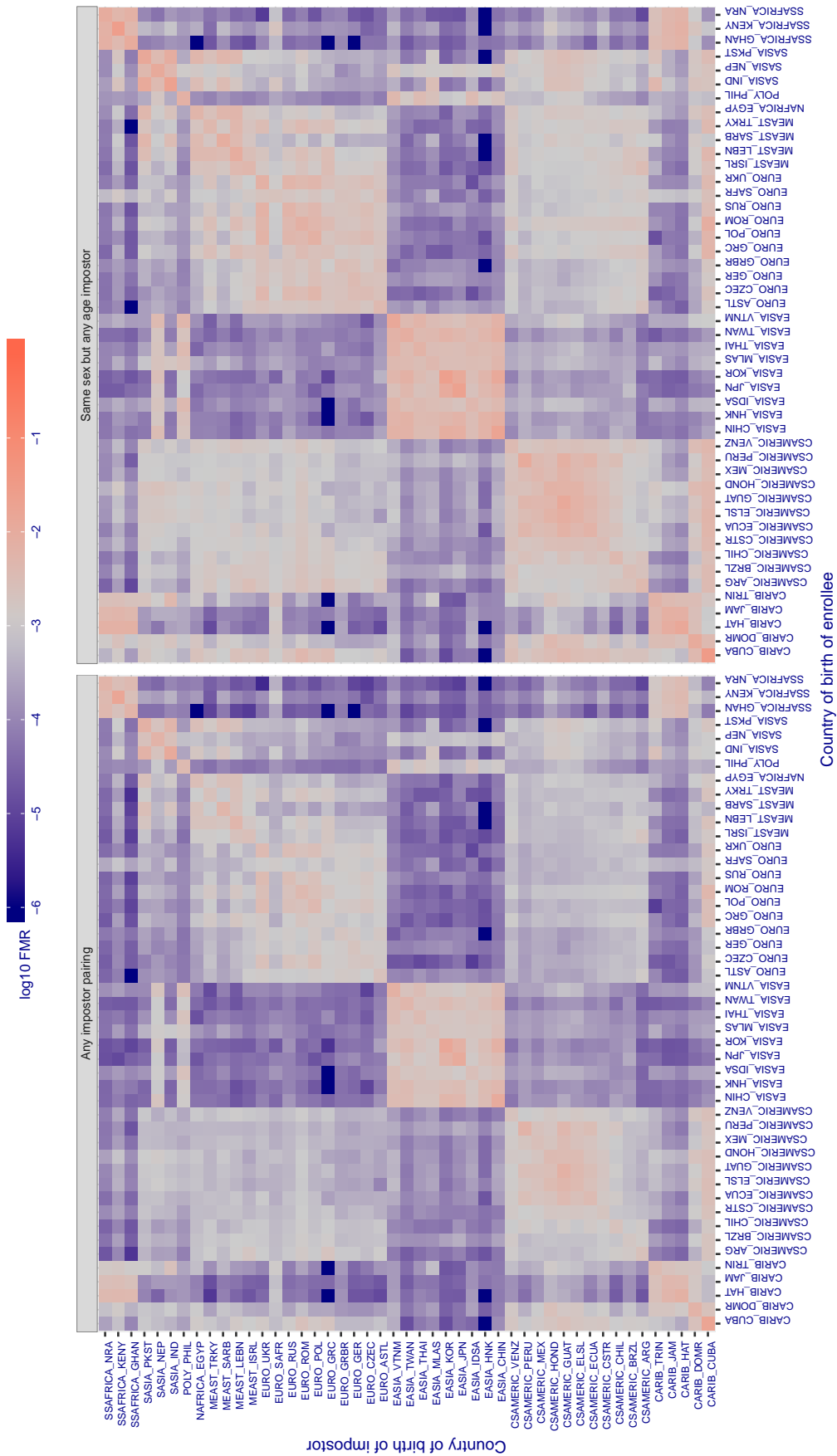


Figure 456: For algorithm tech5-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 0.769$  for algorithm `tevian_004`, giving  $FMR(T) = 0.001$  globally.

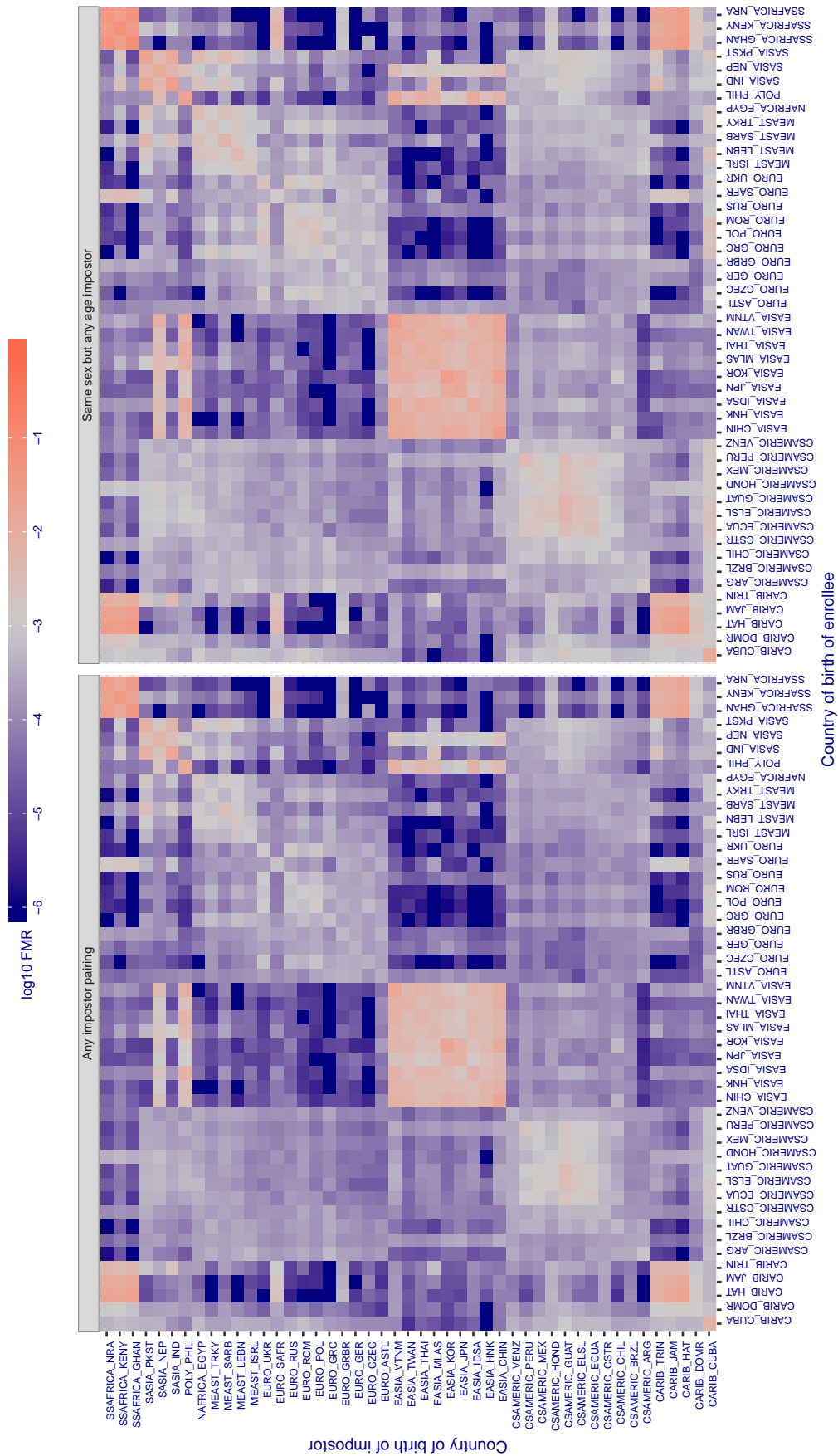


Figure 457: For algorithm `tevian-004` operating on *visa* images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 143.194$  for algorithm tiger\_002, giving  $FMR(T) = 0.001$  globally.

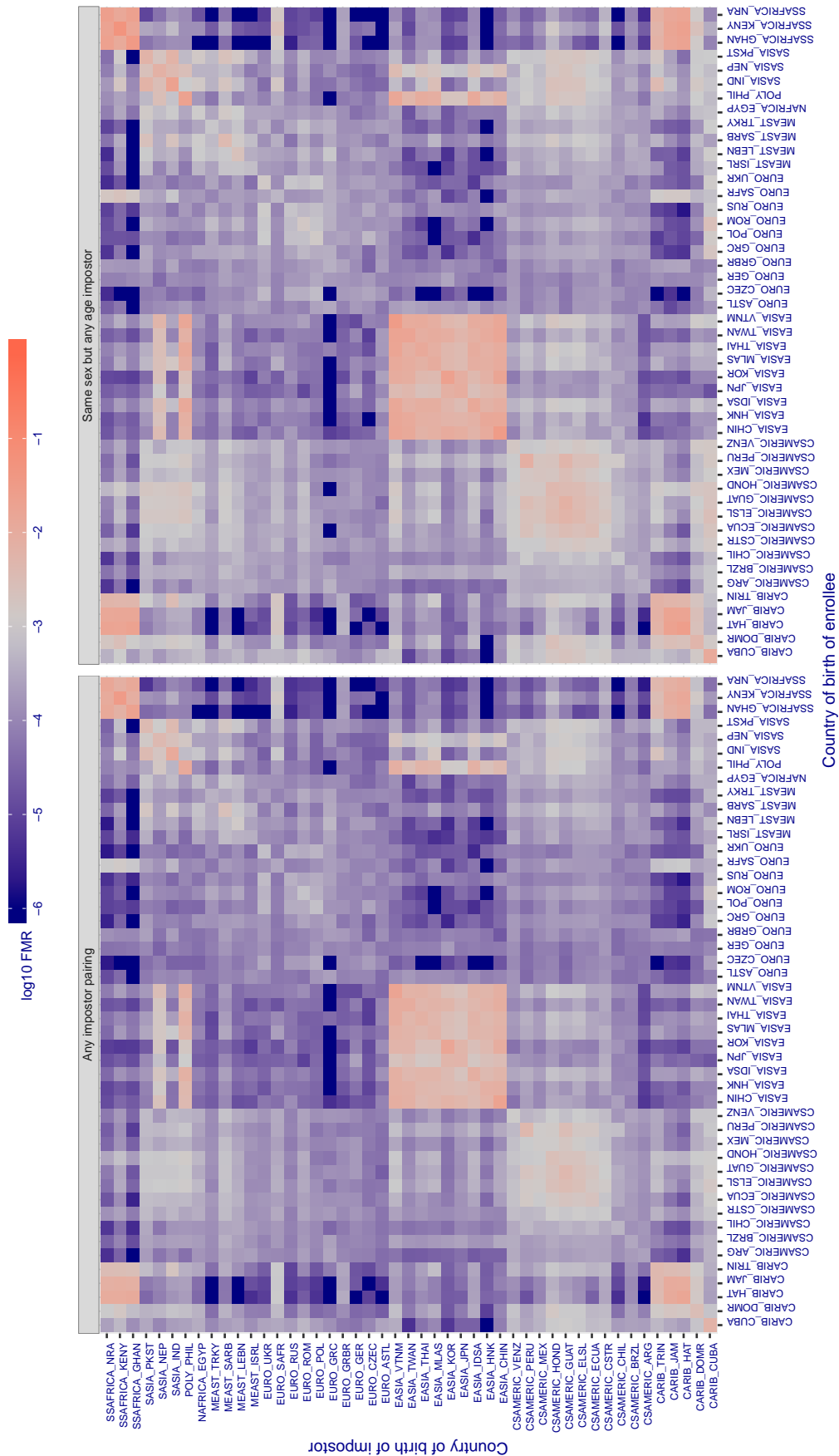


Figure 458: For algorithm tiger-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 139.101$  for algorithm tiger\_003, giving  $FMR(T) = 0.001$  globally.

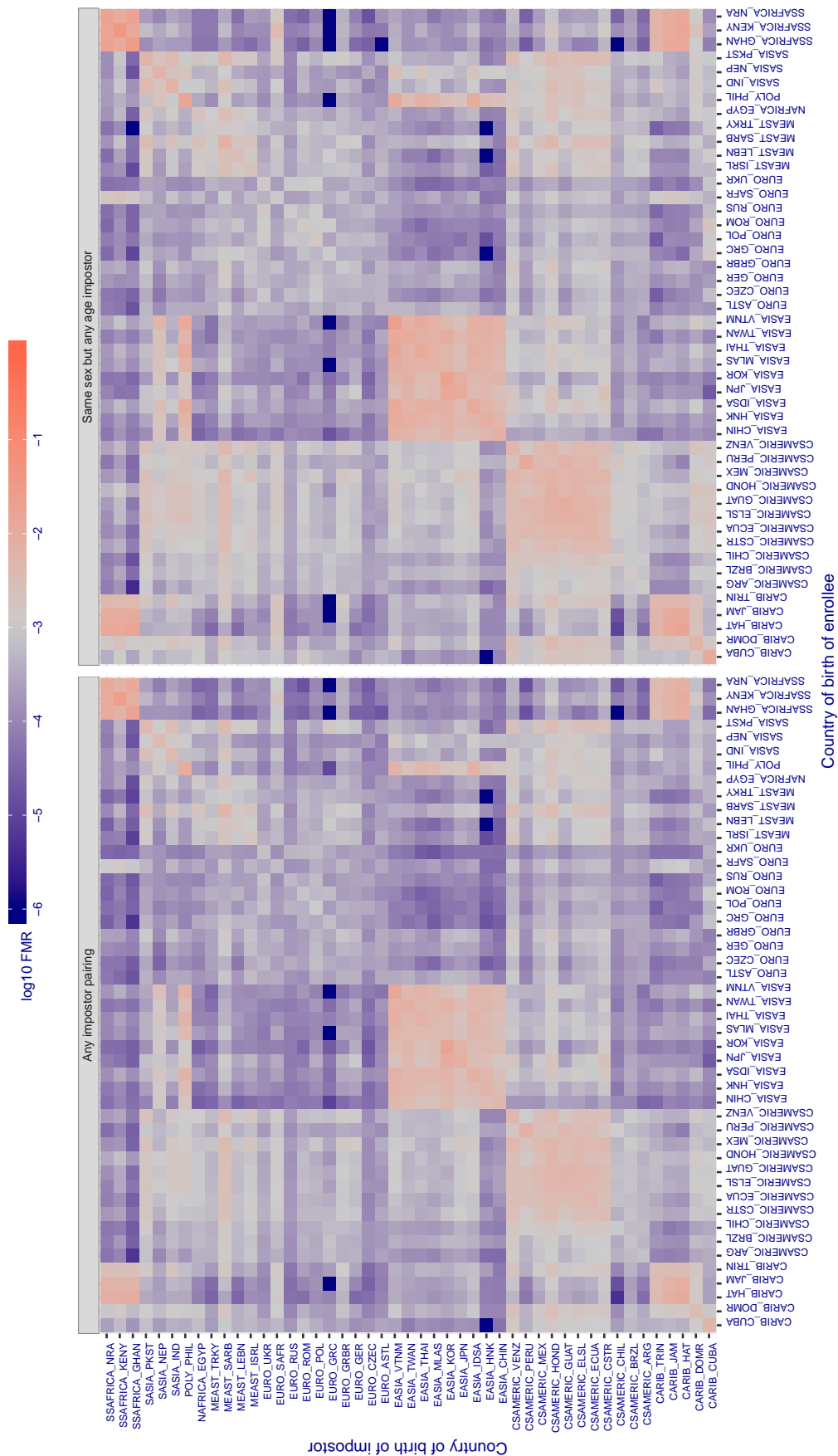


Figure 459: For algorithm tiger-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 43.483$  for algorithm tongyi\_005, giving  $FMR(T) = 0.001$  globally.

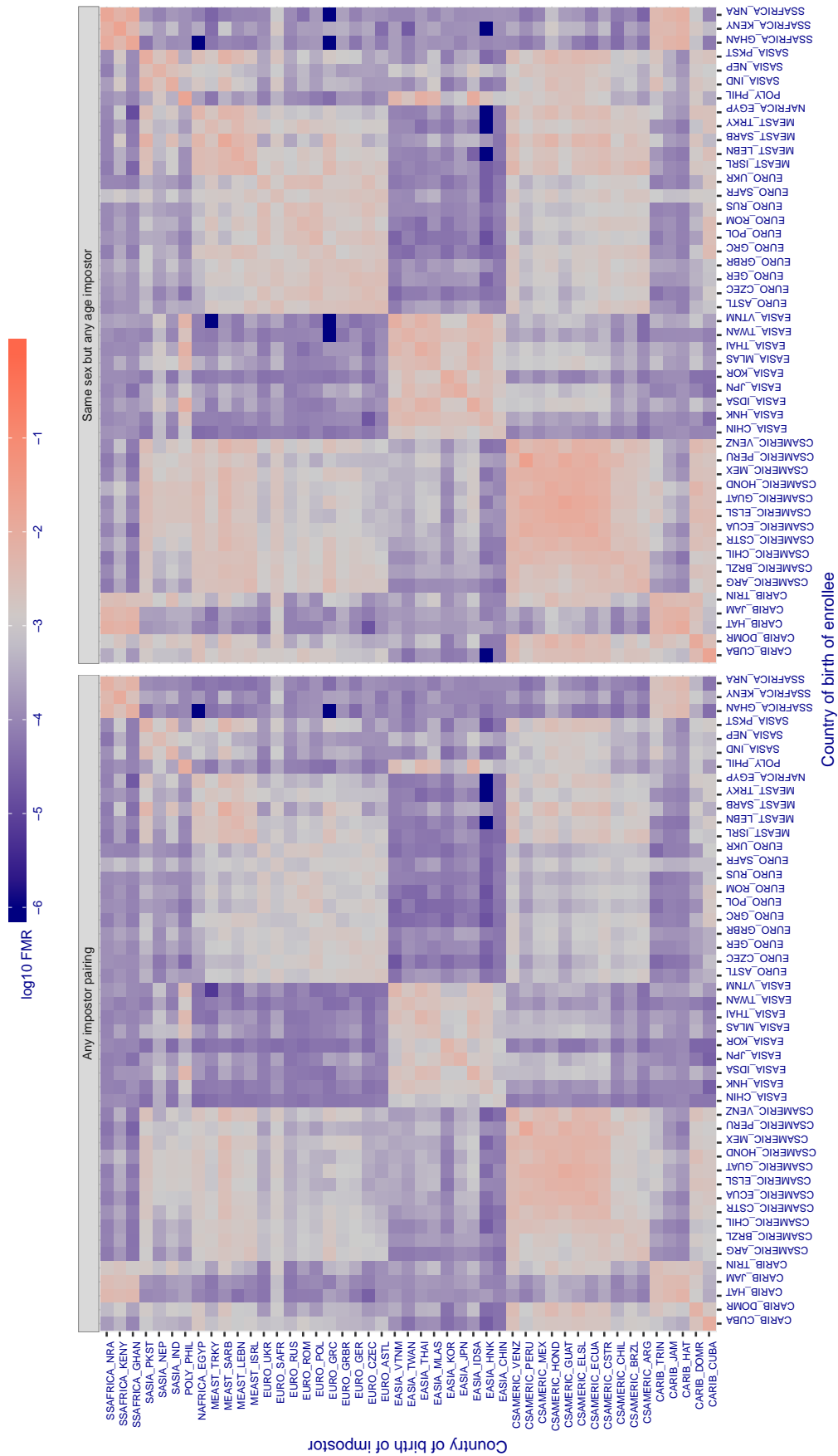


Figure 460: For algorithm tongyi-005 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.599$  for algorithm toshiba\_002, giving  $FMR(T) = 0.001$  globally.

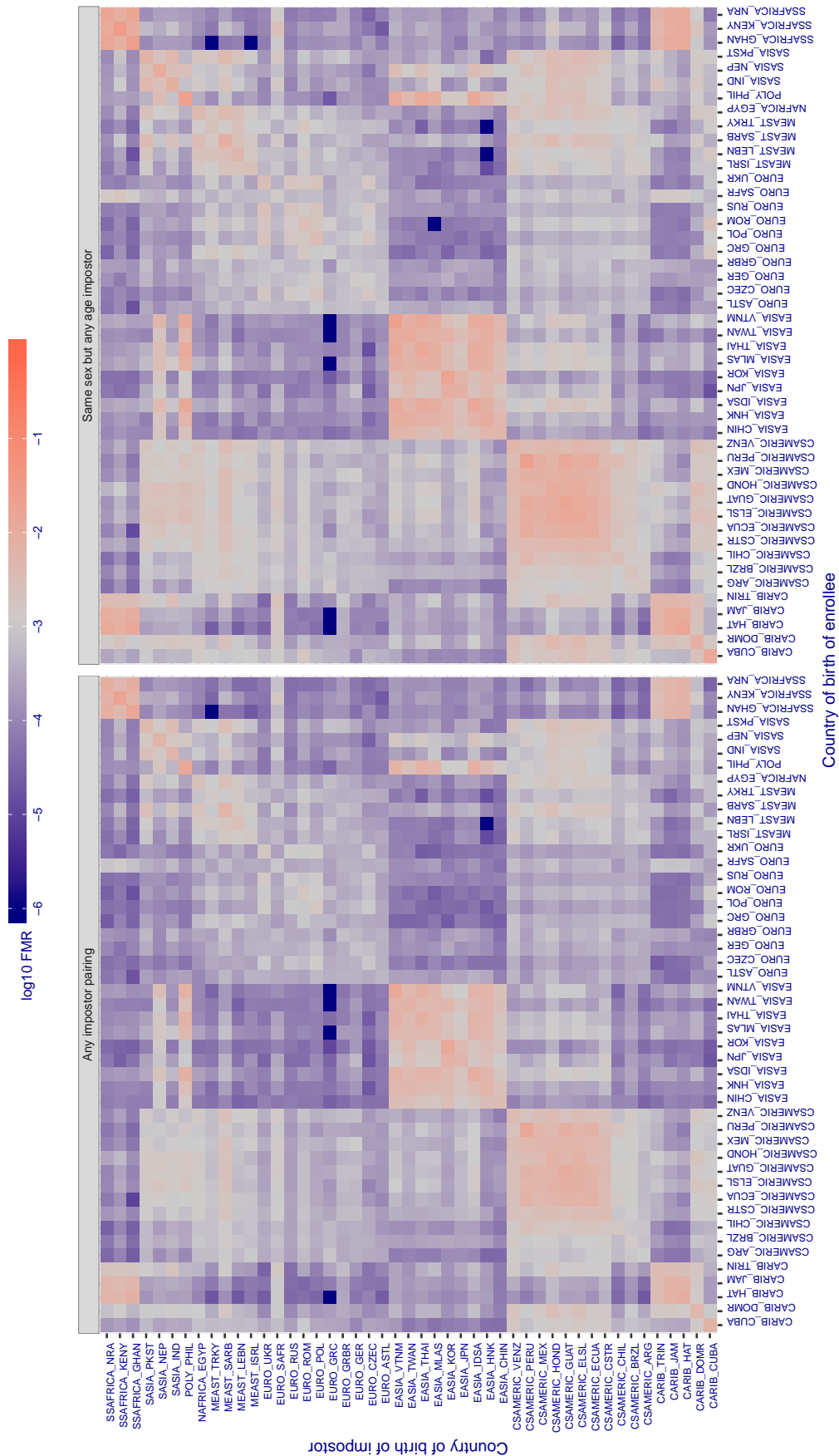


Figure 461: For algorithm toshiba-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.596$  for algorithm toshiba\_003, giving  $FMR(T) = 0.001$  globally.

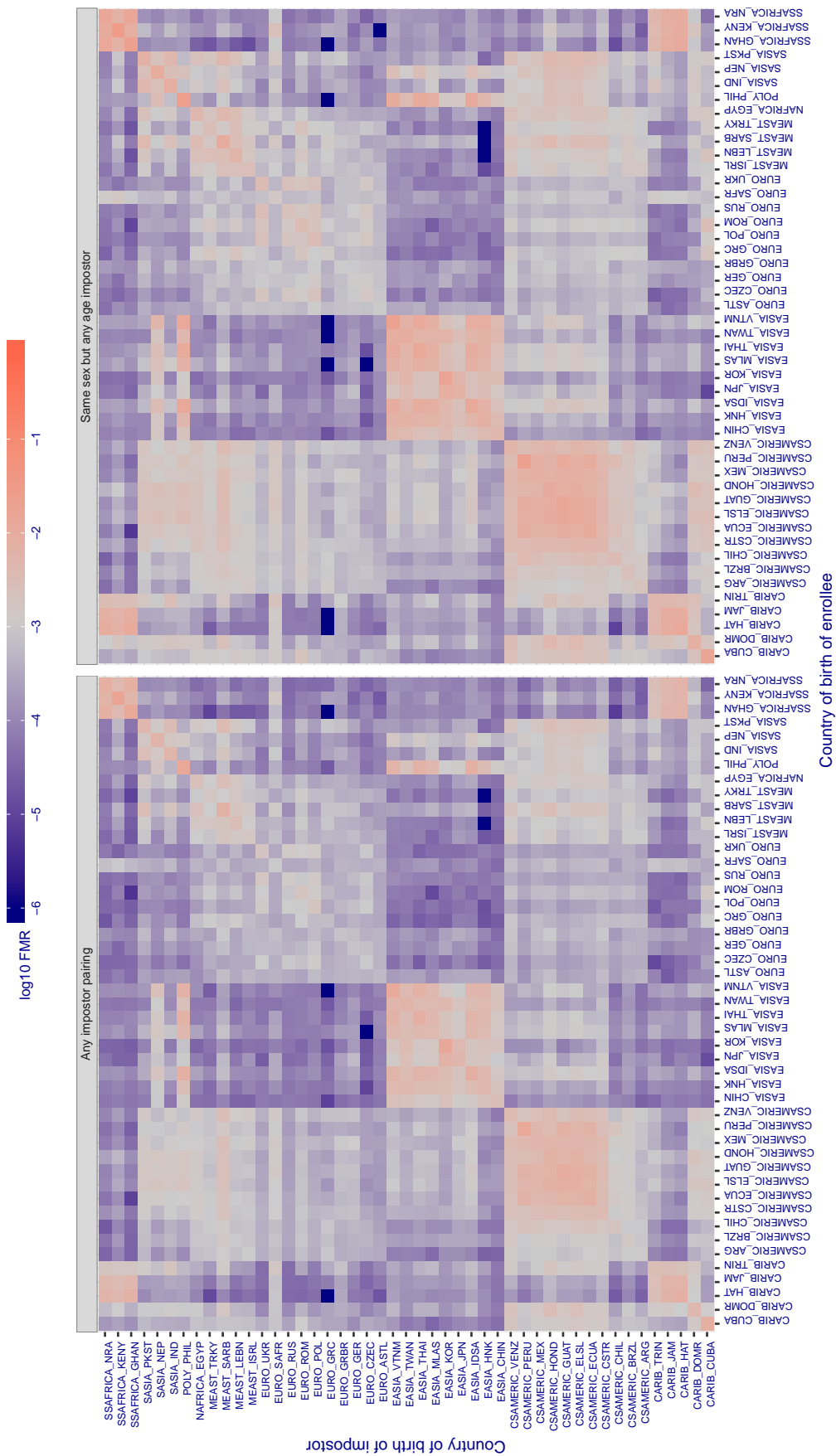


Figure 462: For algorithm toshiba-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.278$  for algorithm trueface\_000, giving  $FMR(T) = 0.001$  globally.

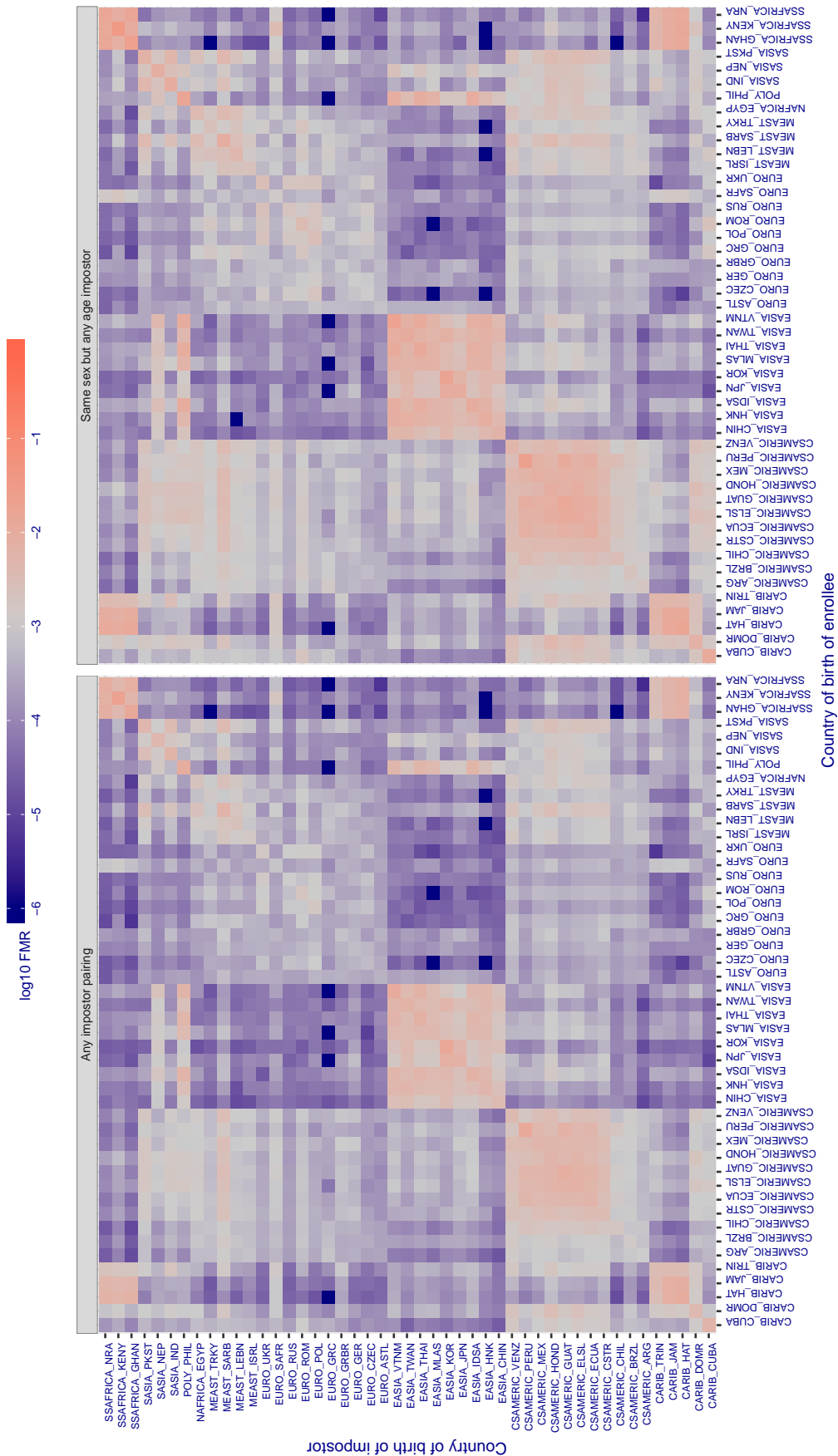


Figure 463: For algorithm trueface-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 0.048$  for algorithm `ulsee_001`, giving  $FMR(T) = 0.001$  globally.

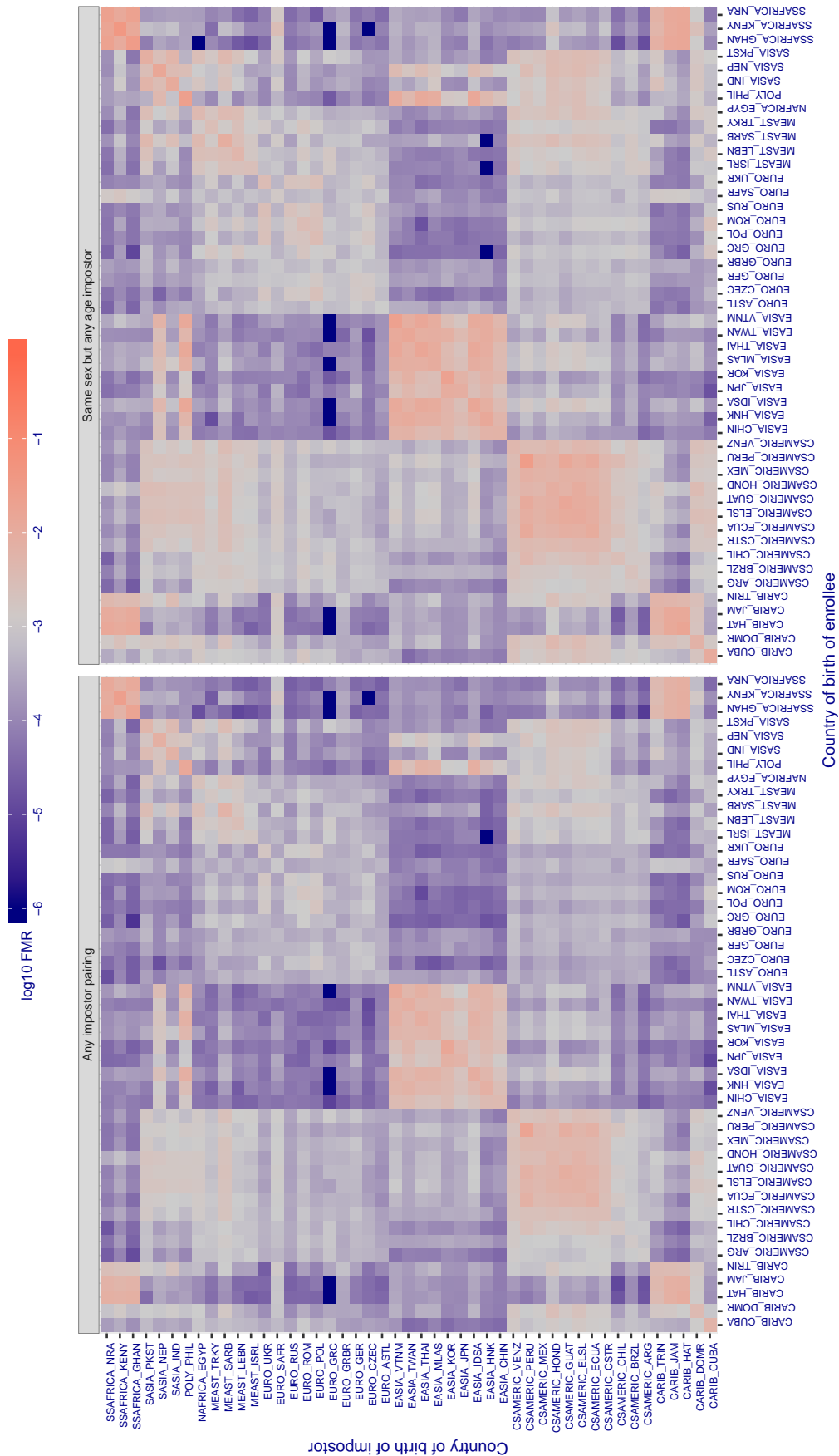


Figure 464: For algorithm `ulsee-001` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 0.681$  for algorithm uluface\_002, giving  $FMR(T) = 0.001$  globally.

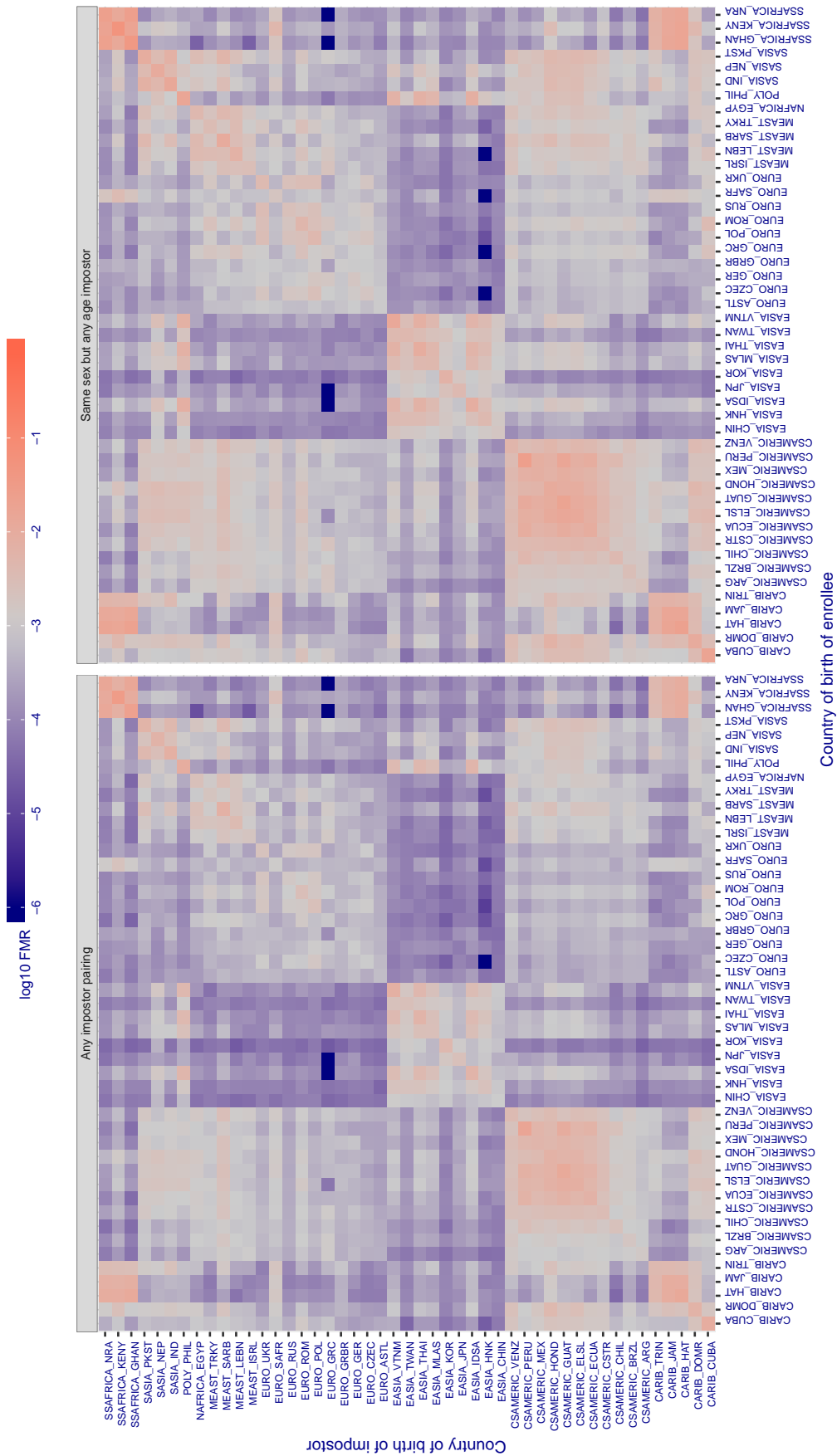


Figure 465: For algorithm uluface-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.384$  for algorithm upc\_001, giving  $FMR(T) = 0.001$  globally.

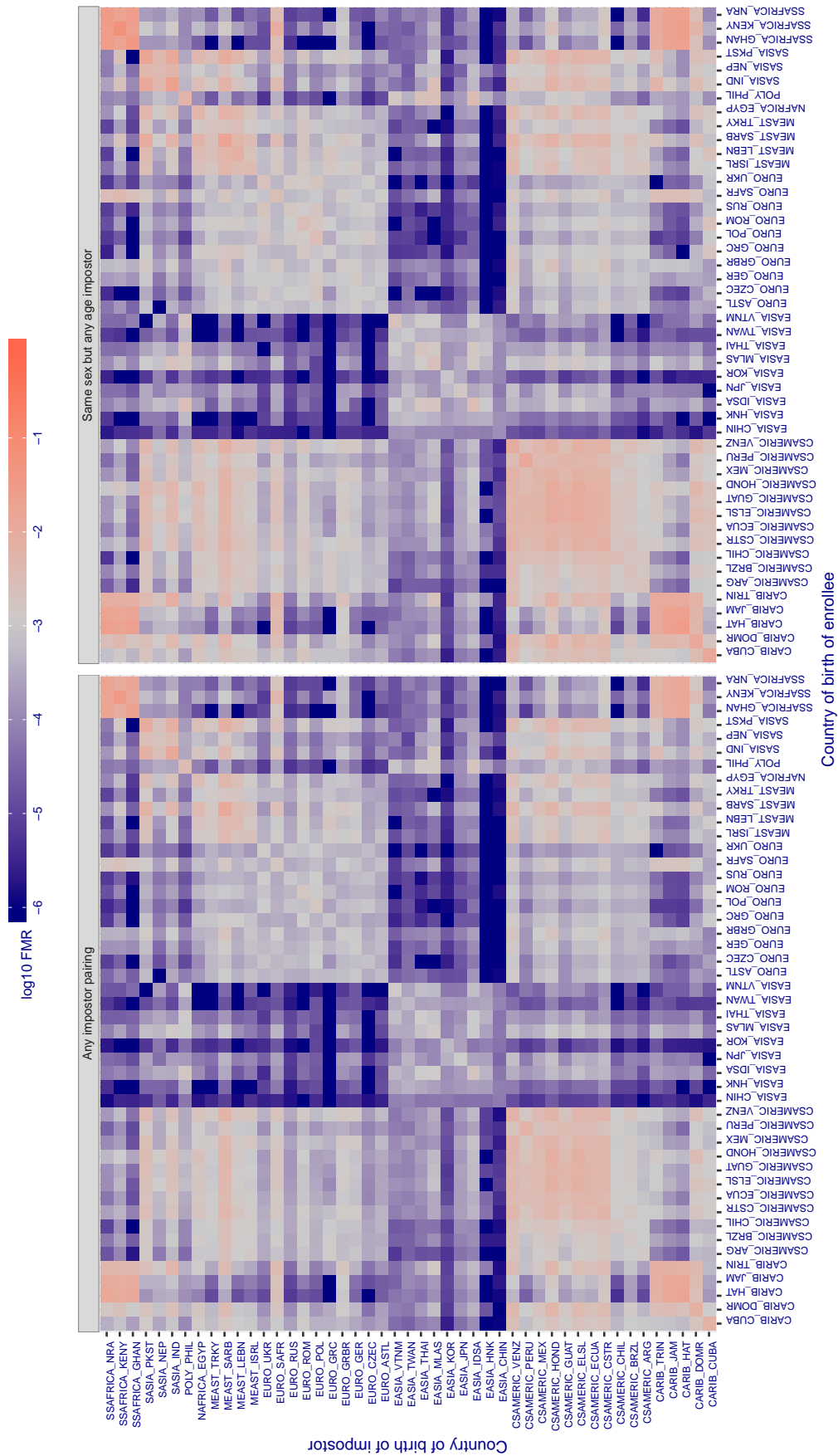


Figure 466: For algorithm upc-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.310$  for algorithm vcog\_002, giving  $FMR(T) = 0.001$  globally.

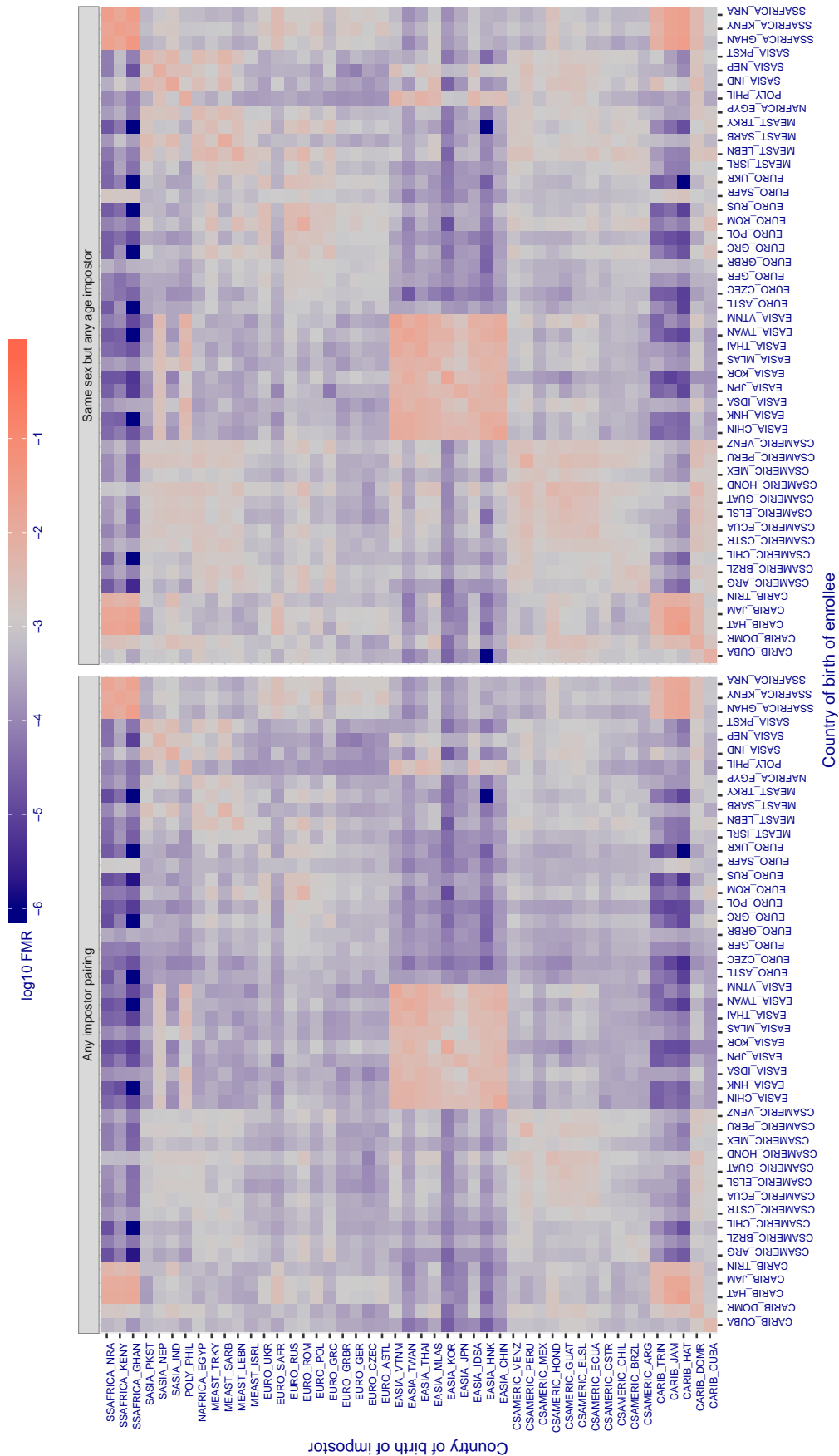


Figure 467: For algorithm vcog-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 66.962$  for algorithm `vd_001`, giving  $FMR(T) = 0.001$  globally.

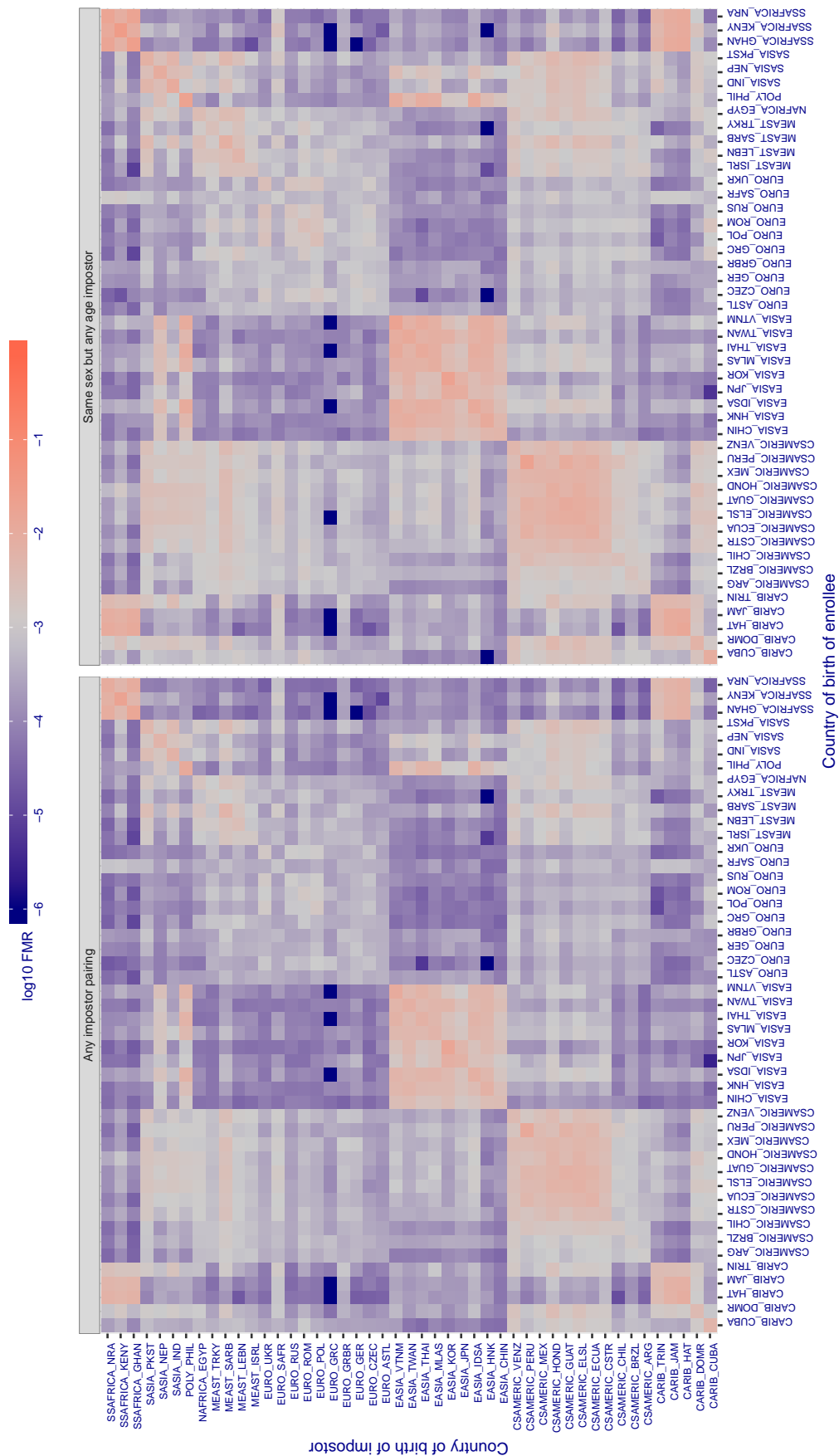


Figure 468: For algorithm `vd-001` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 2.897$  for algorithm veridas\_001, giving  $FMR(T) = 0.001$  globally.

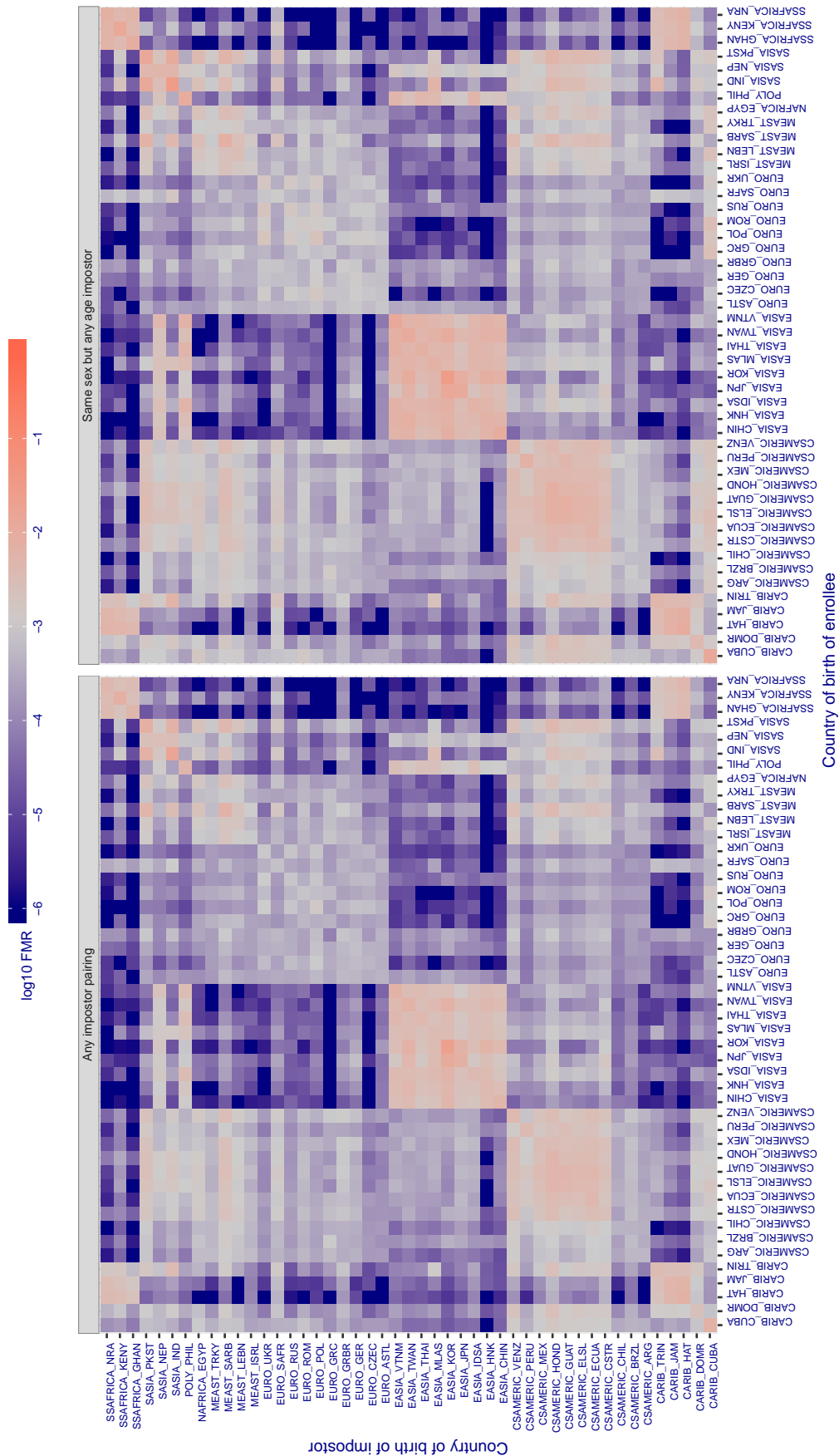


Figure 469: For algorithm veridas-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 3.010$  for algorithm veridas\_002, giving  $FMR(T) = 0.001$  globally.

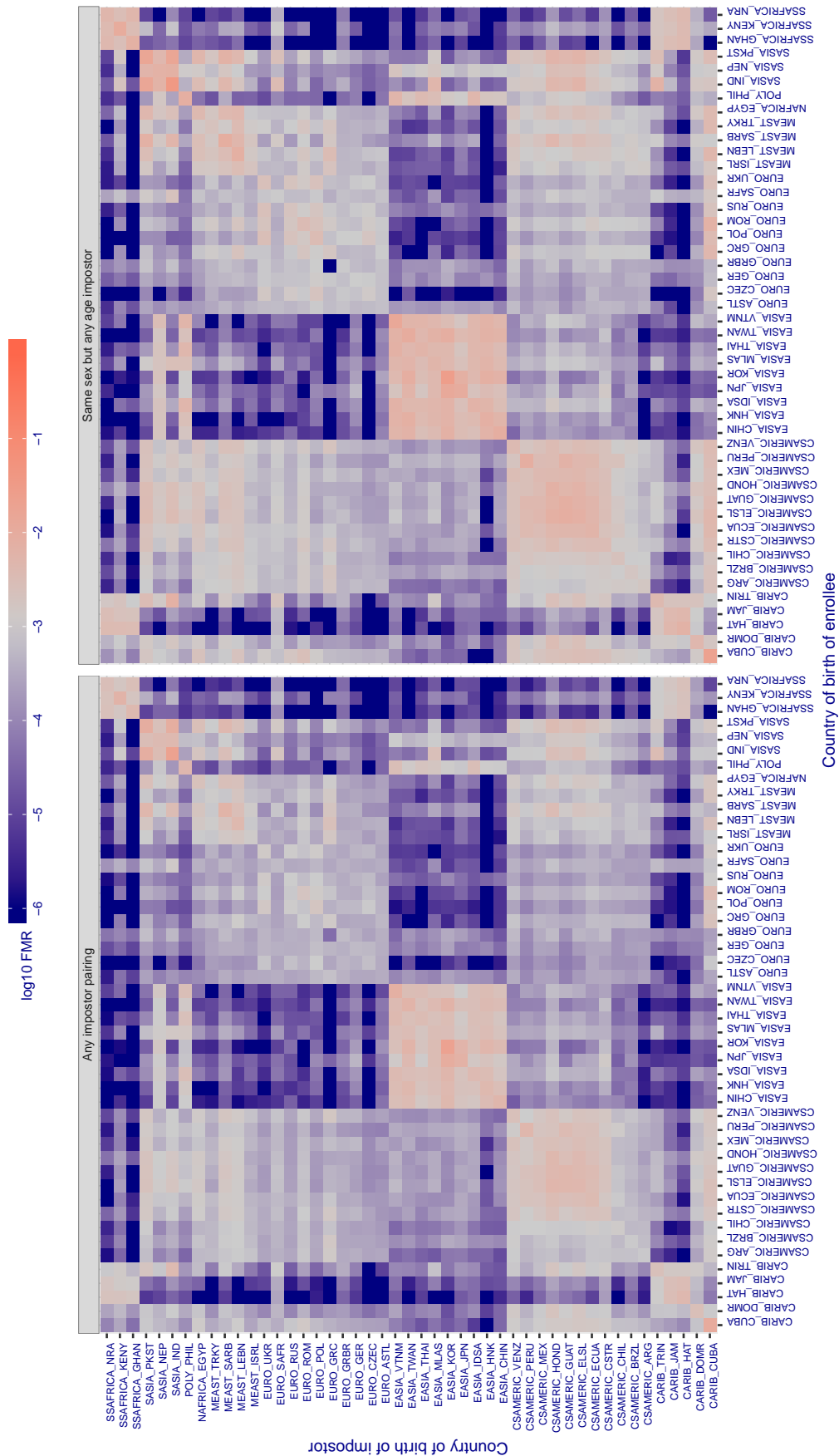


Figure 470: For algorithm veridas-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 2.677$  for algorithm via\_000, giving  $FMR(T) = 0.001$  globally.

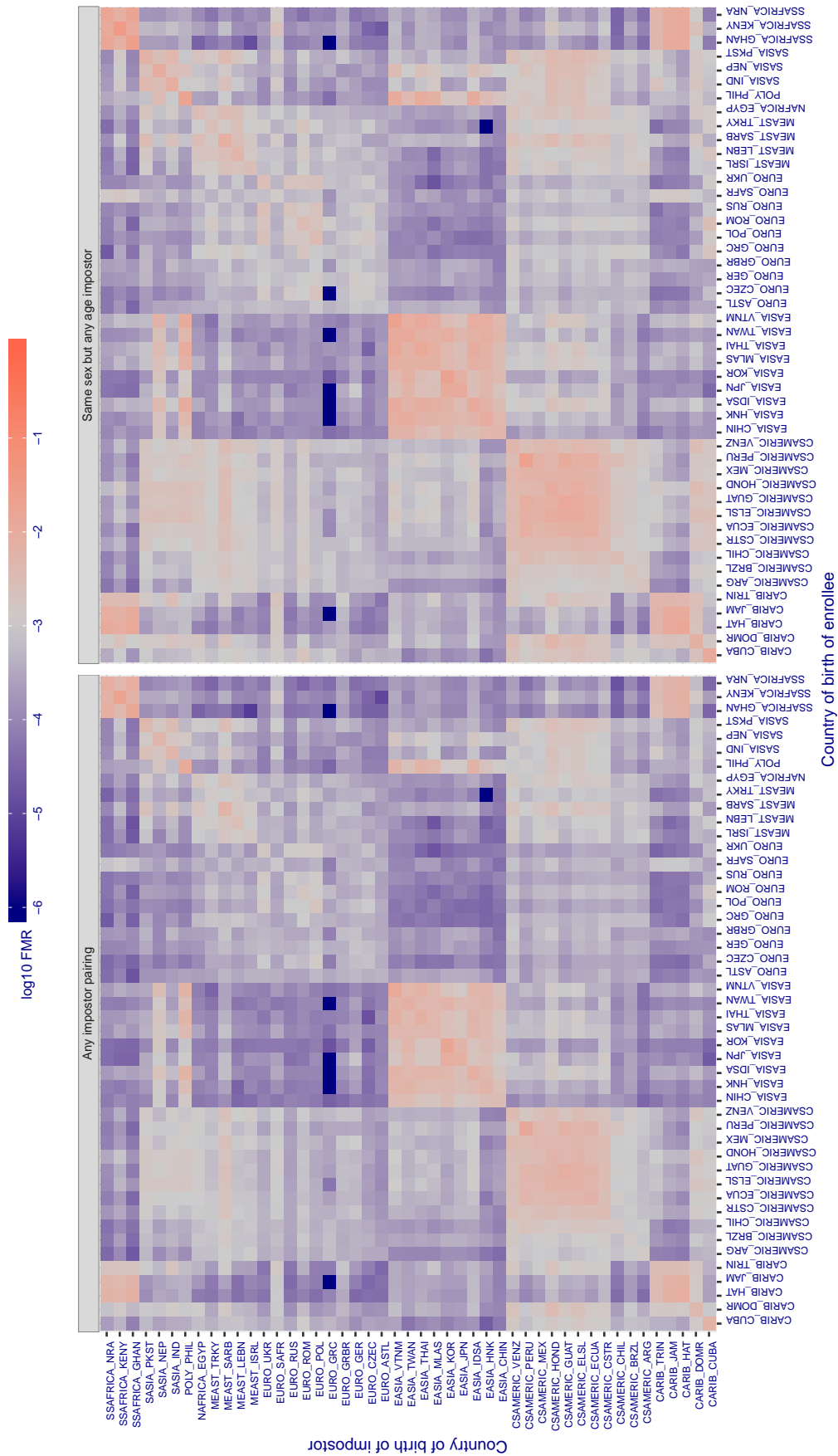


Figure 471: For algorithm via-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 0.755$  for algorithm videonetics\_001, giving  $FMR(T) = 0.001$  globally.

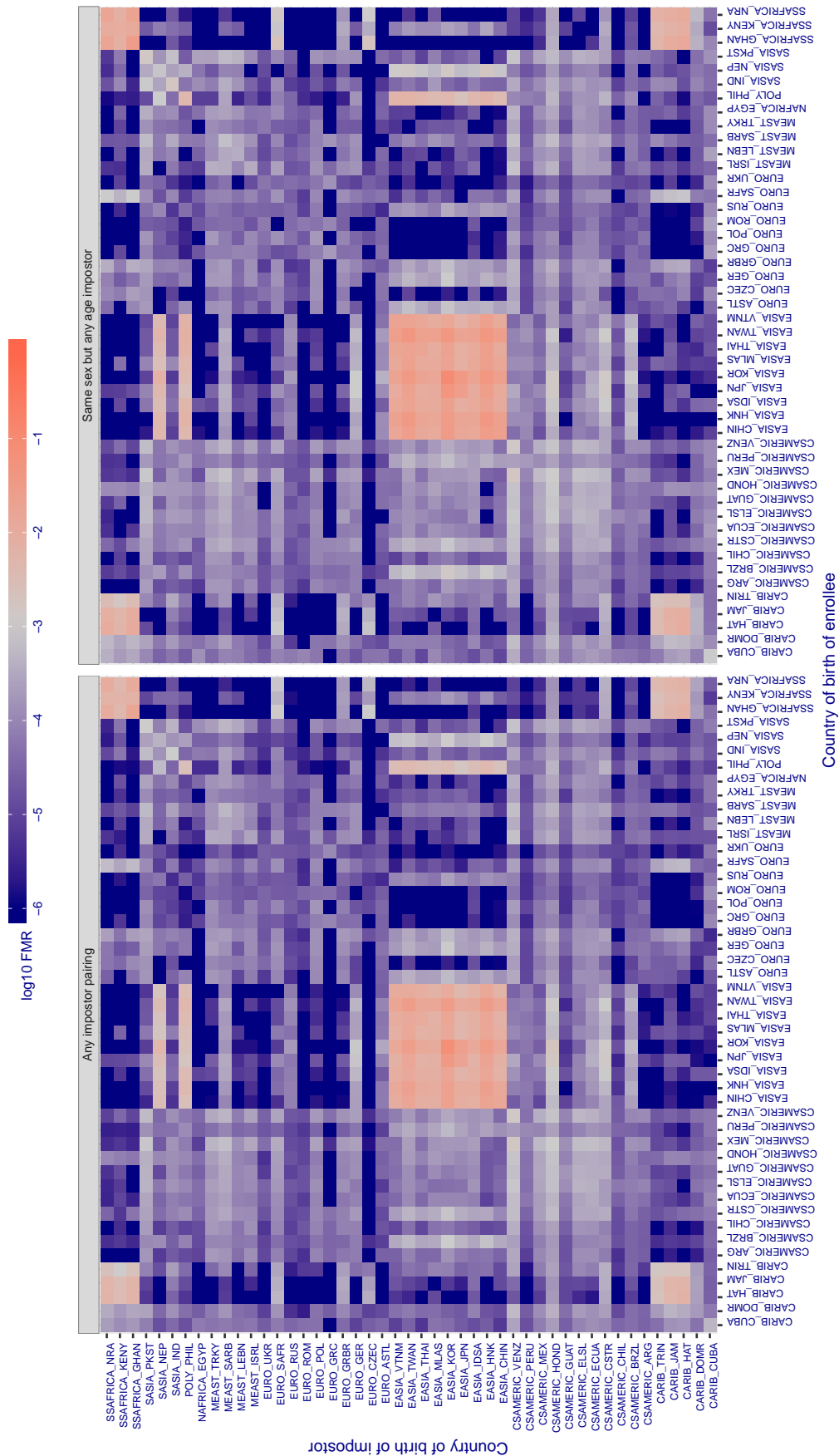


Figure 472: For algorithm videonetics-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 2.809$  for algorithm `vigilantsolutions_006`, giving  $FMR(T) = 0.001$  globally.

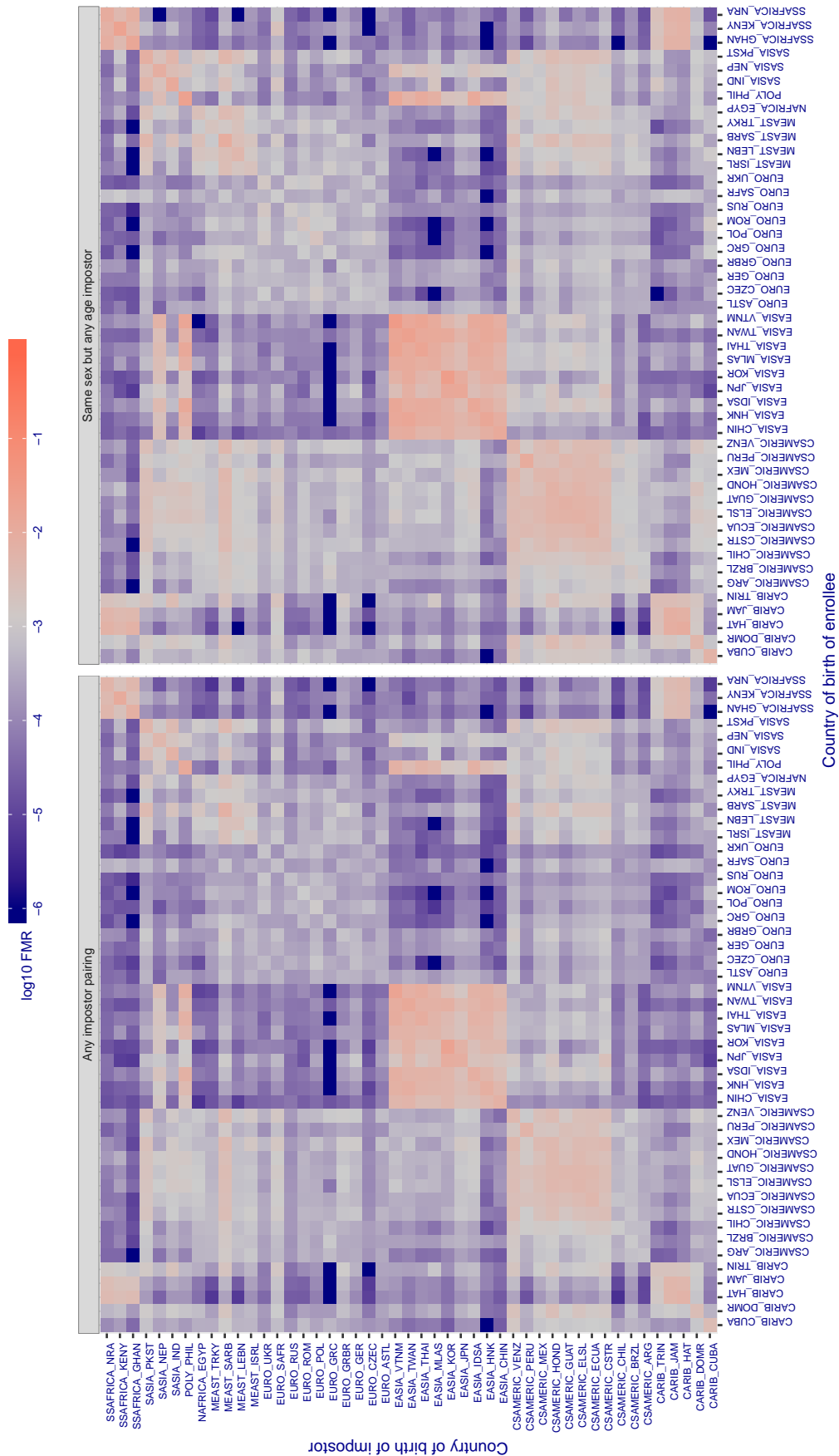


Figure 473: For algorithm `vigilantsolutions-006` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 2.755$  for algorithm `vigilantsolutions_007`, giving  $FMR(T) = 0.001$  globally.

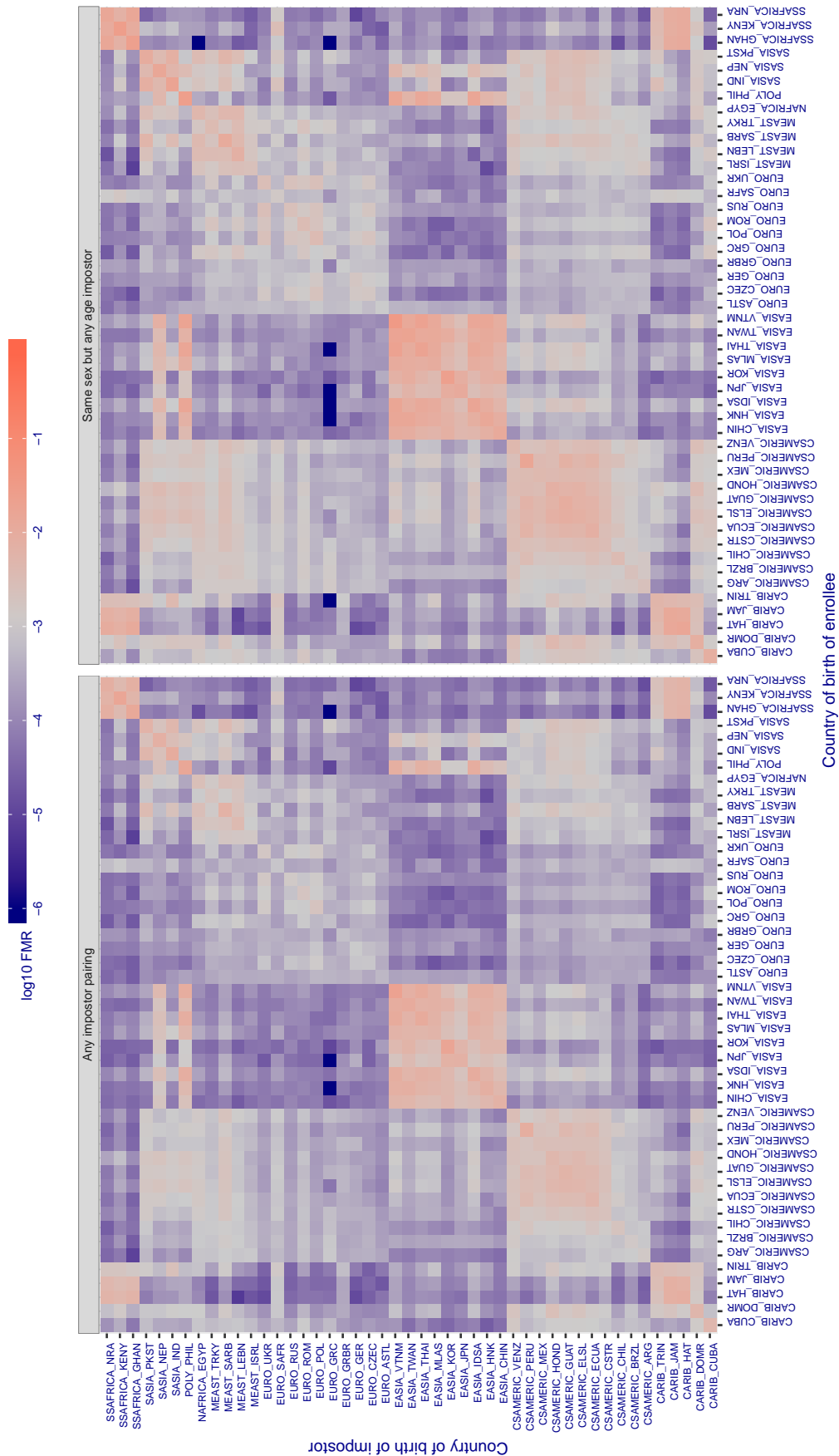


Figure 474: For algorithm `vigilantsolutions-007` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.336$  for algorithm vion\_000, giving  $FMR(T) = 0.001$  globally.

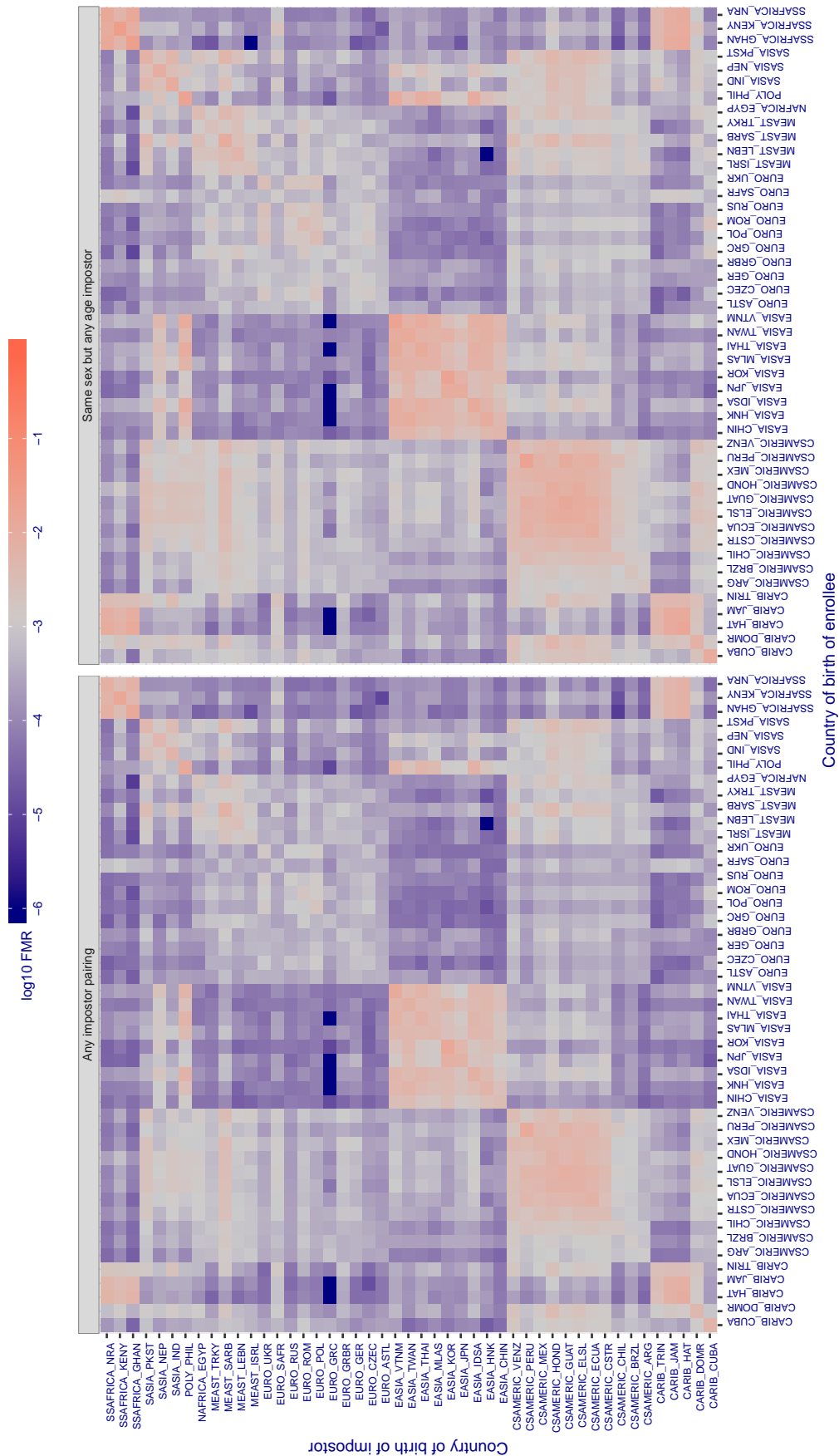


Figure 475: For algorithm vion-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.340$  for algorithm visionbox\_000, giving  $FMR(T) = 0.001$  globally.

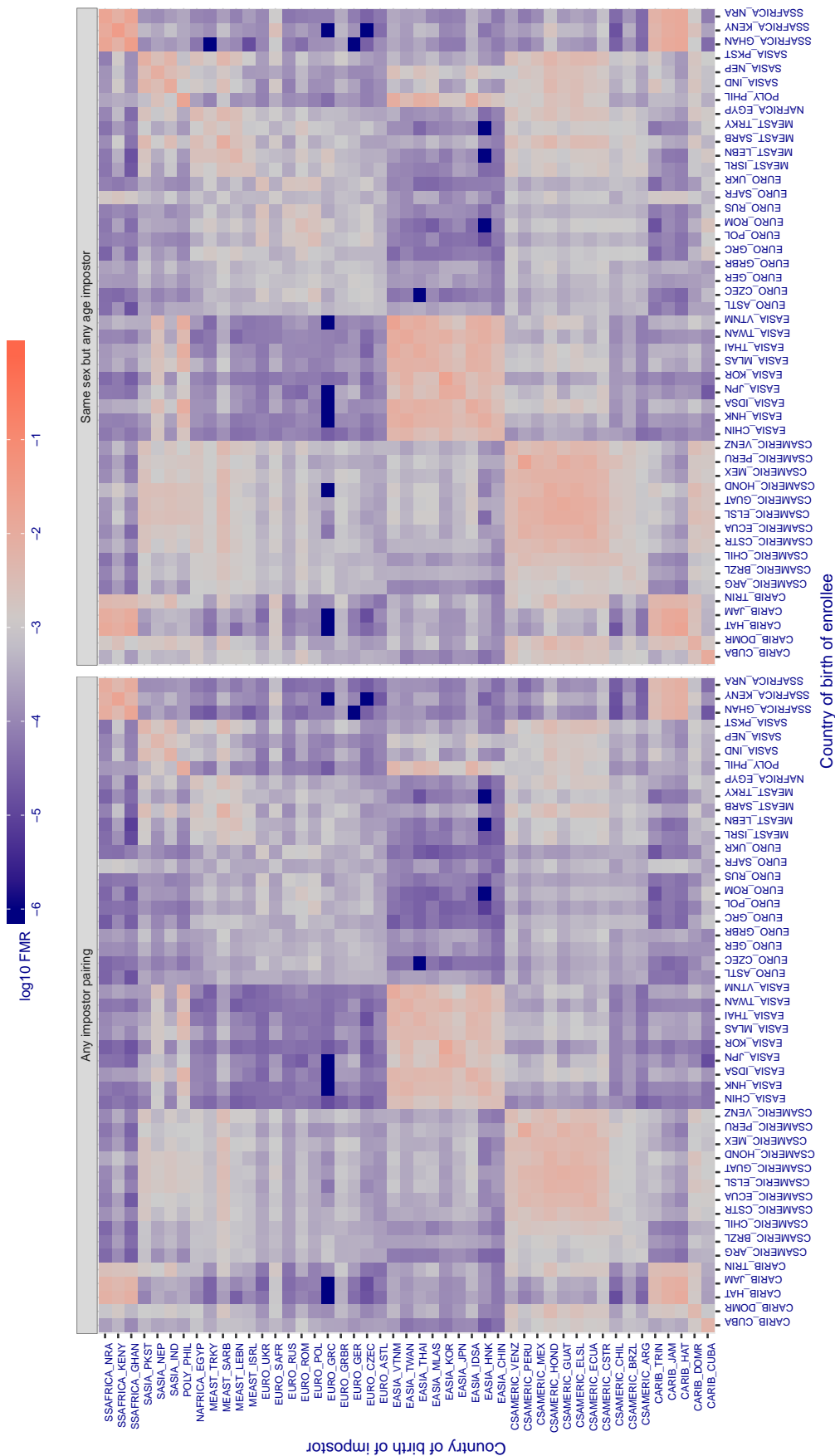


Figure 476: For algorithm visionbox-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.296$  for algorithm visionbox\_001, giving  $FMR(T) = 0.001$  globally.

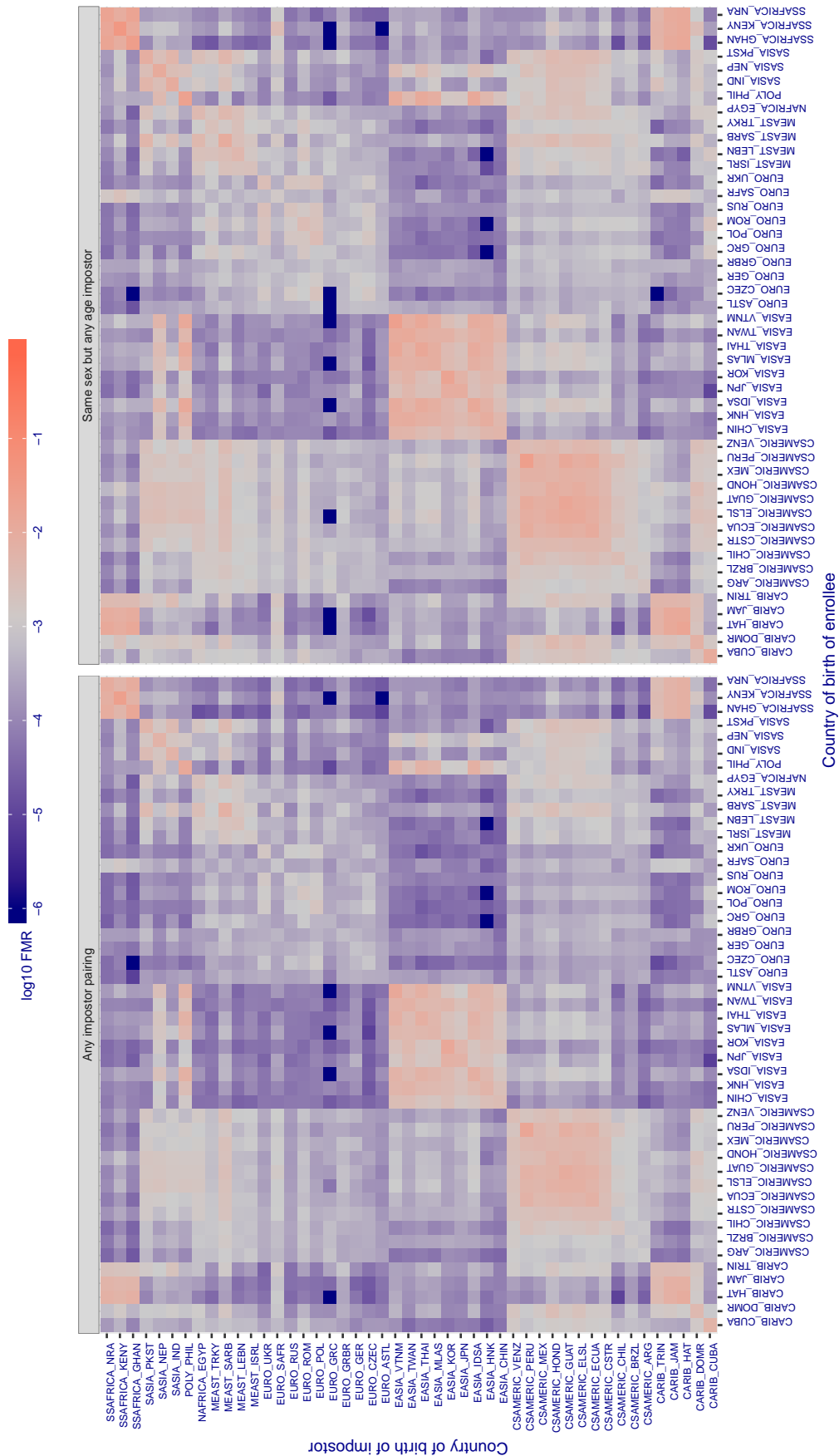


Figure 477: For algorithm visionbox-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

**Cross country FMR at threshold  $T = 0.444$  for algorithm visionlabs\_006, giving  $FMR(T) = 0.001$  globally.**

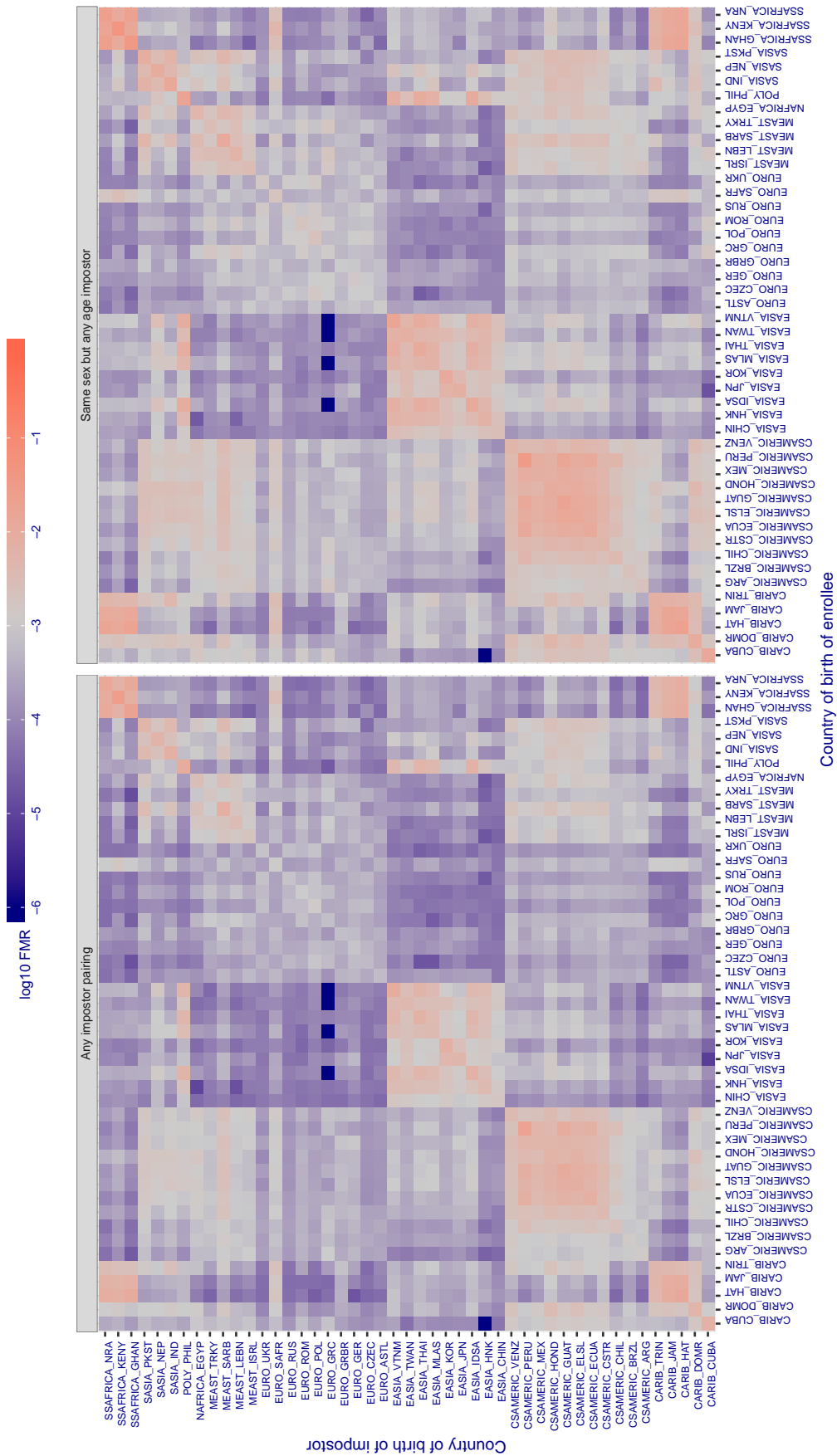


Figure 478: For algorithm visionlabs-006 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.459$  for algorithm visionlabs\_007, giving  $FMR(T) = 0.001$  globally.

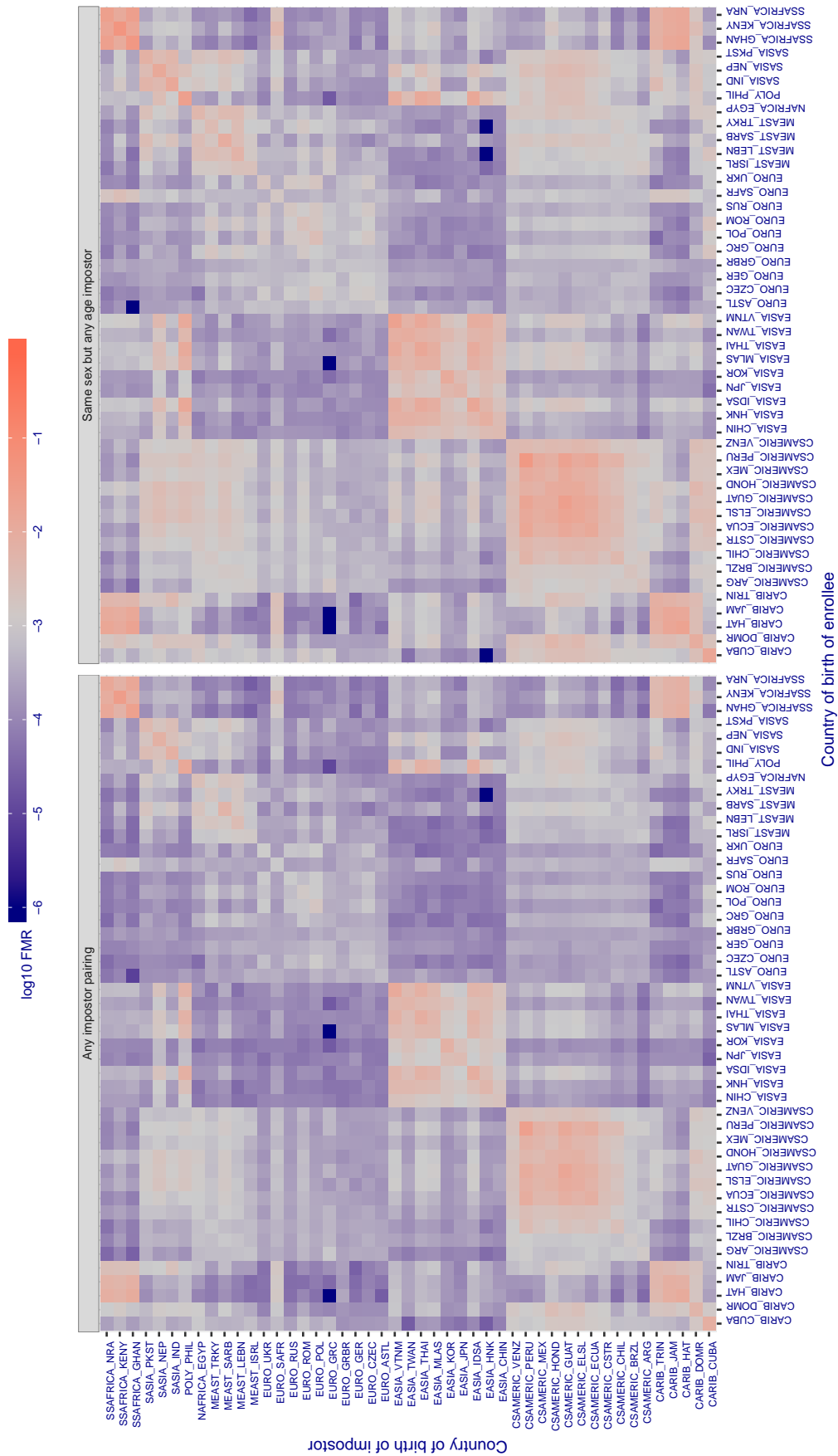


Figure 479: For algorithm visionlabs-007 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold  $T = 995.311$  for algorithm vocord\_006, giving  $FMR(T) = 0.001$  globally.

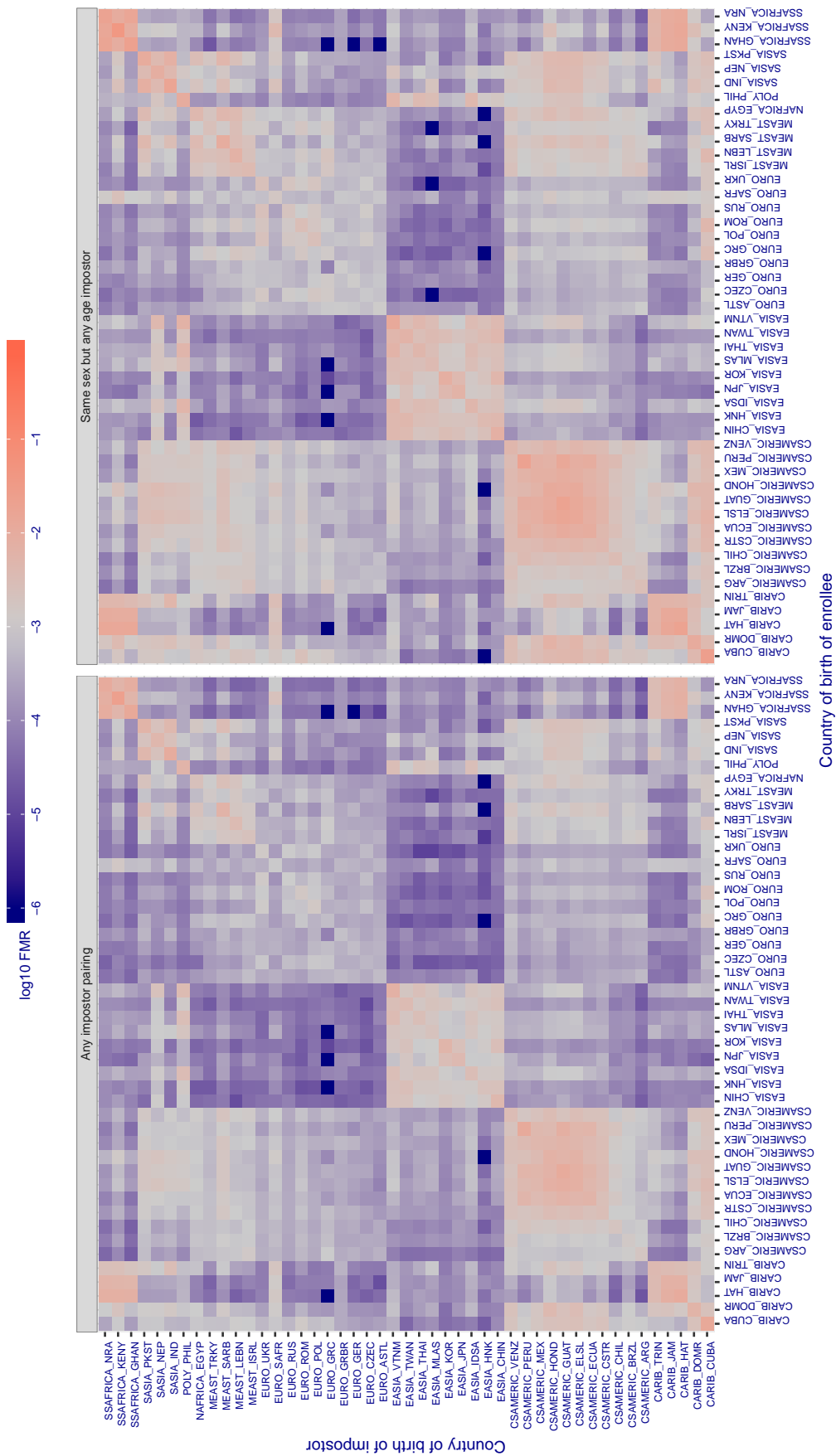


Figure 480: For algorithm vocord-006 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 994.723$  for algorithm vocord\_007, giving  $FMR(T) = 0.001$  globally.

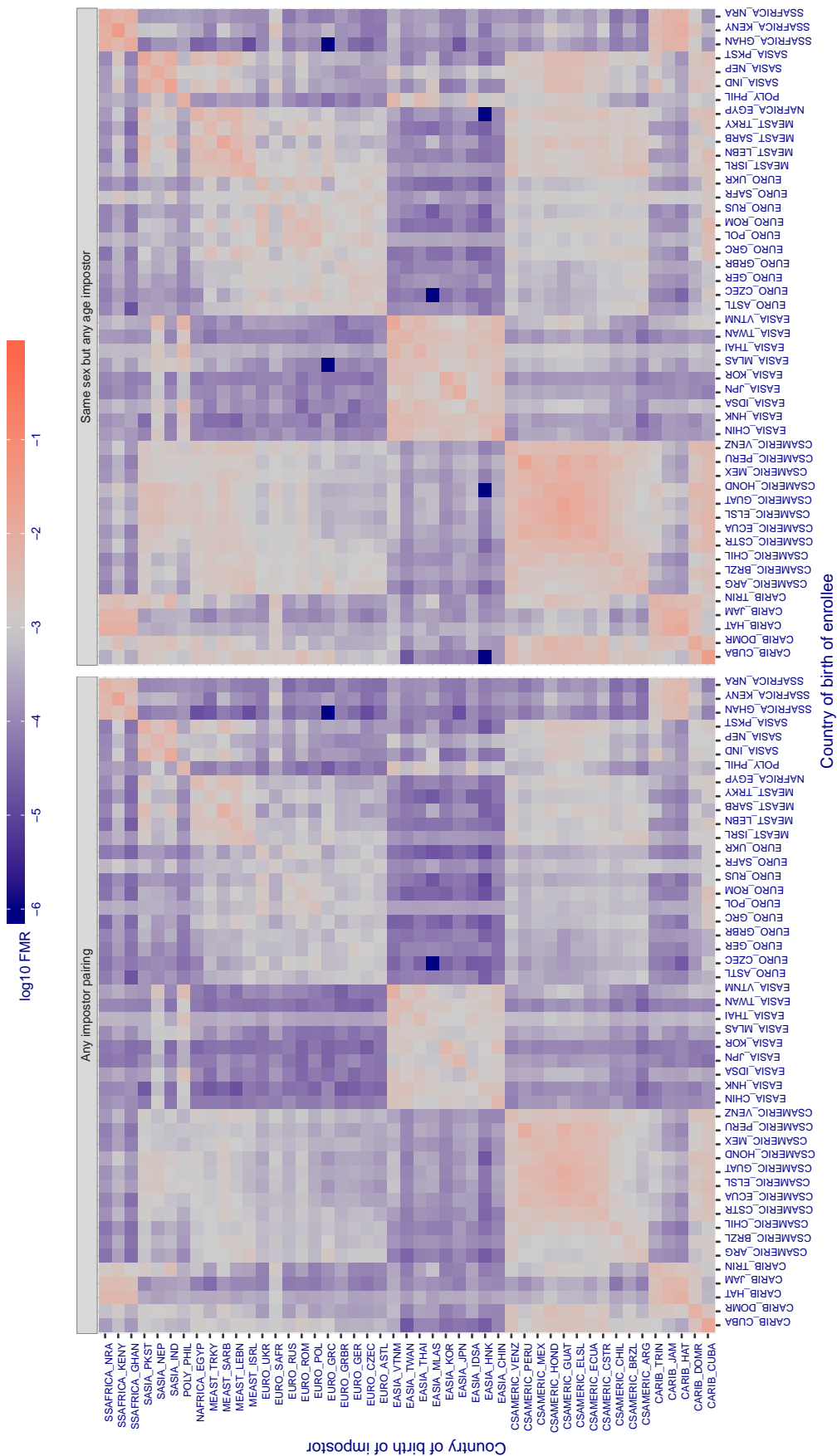


Figure 481: For algorithm vocord-007 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.314$  for algorithm  $winsense_{000}$ , giving  $FMR(T) = 0.001$  globally.

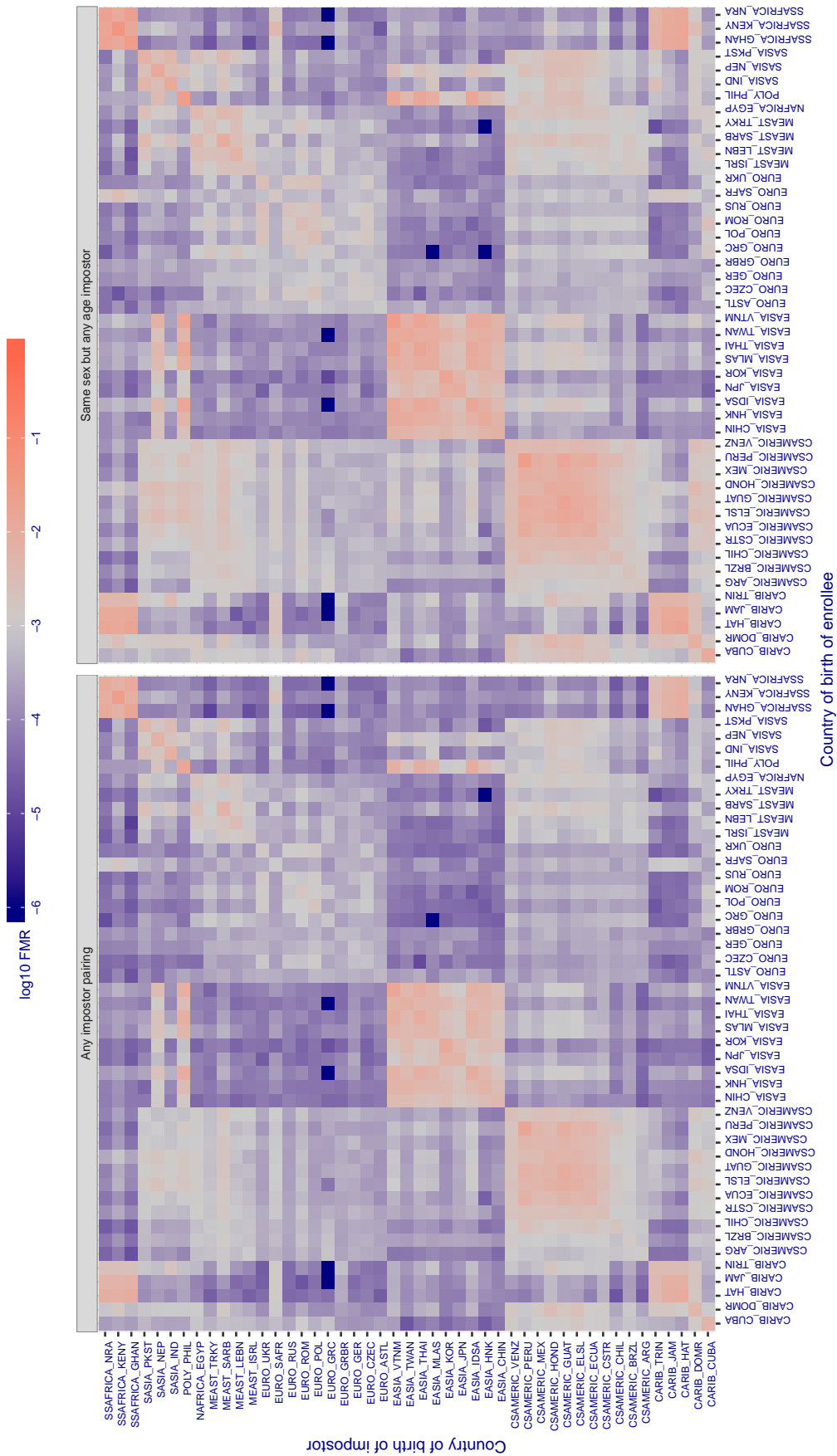


Figure 482: For algorithm  $winsense_{000}$  operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 0.326$  for algorithm  $x$ -laboratory\_000, giving  $FMR(T) = 0.001$  globally.

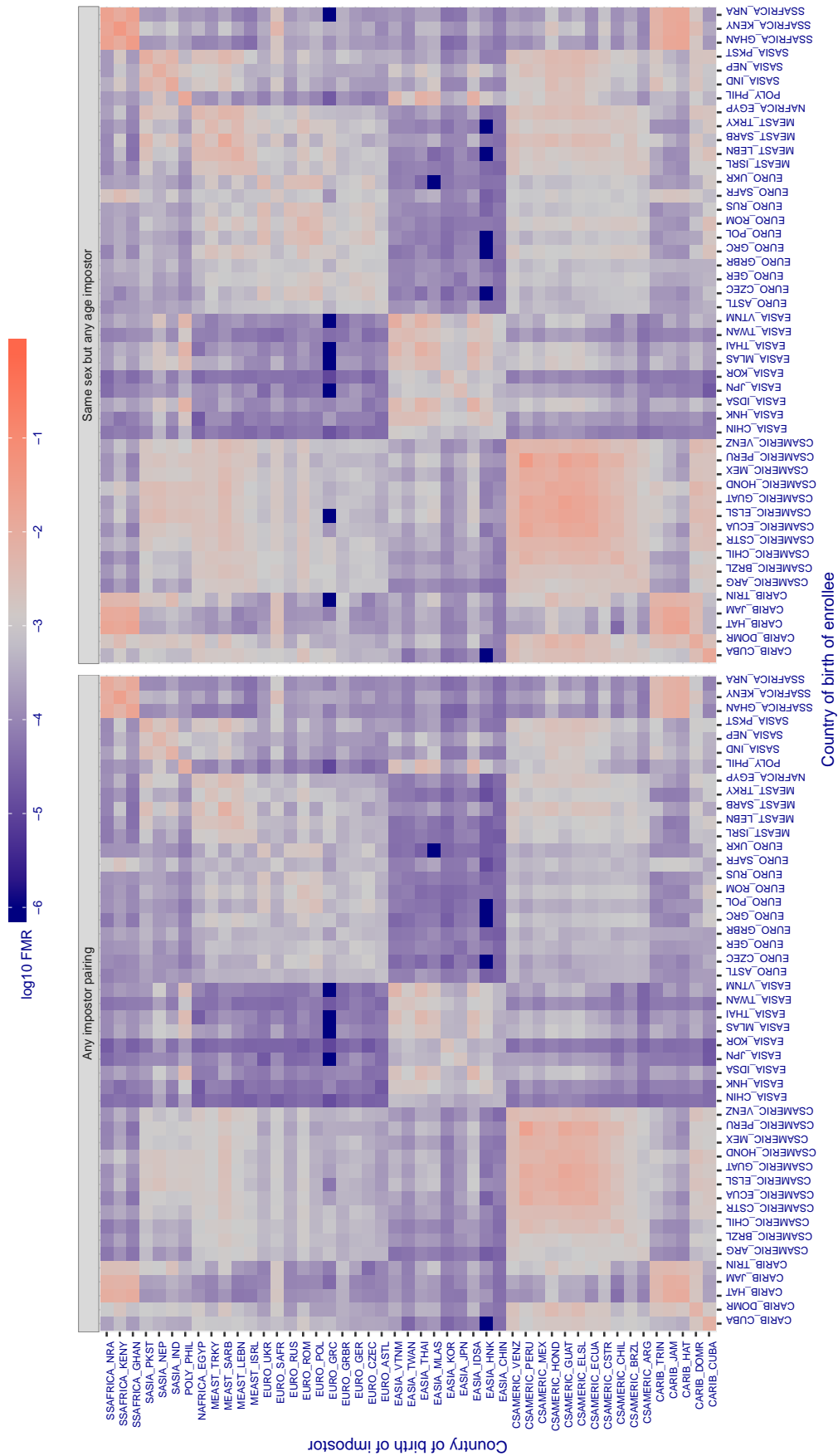


Figure 483: For algorithm  $x$ -laboratory-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each  $+1$  increase in  $\log_{10}$  FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 5.333$  for algorithm yisheng\_004, giving  $FMR(T) = 0.001$  globally.

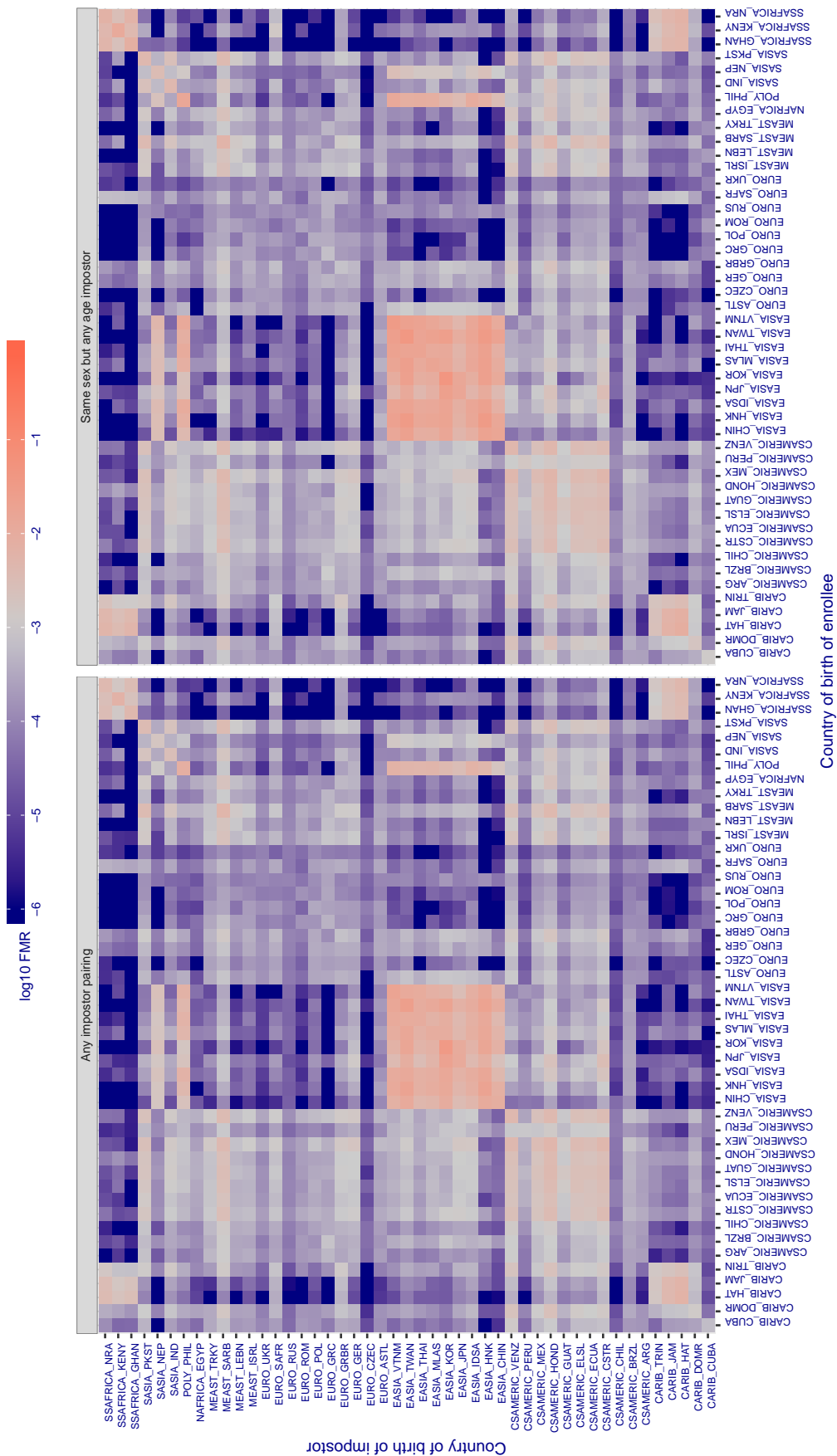


Figure 484: For algorithm yisheng-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold  $T = 37.550$  for algorithm yitu\_003, giving  $FMR(T) = 0.001$  globally.

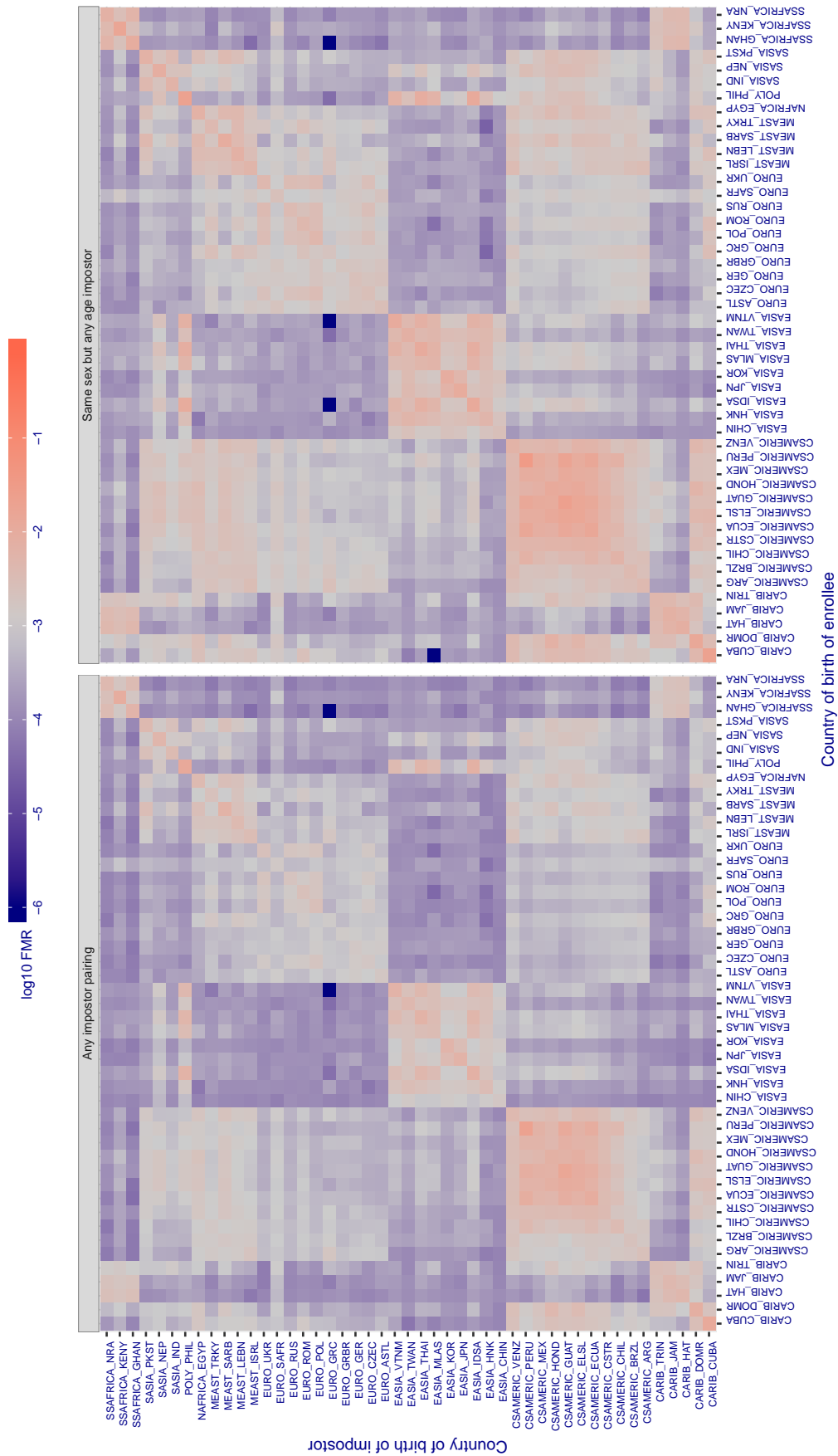


Figure 485: For algorithm yitu-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all on the order of  $10^{10}$  impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in  $\log_{10} FMR$  corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

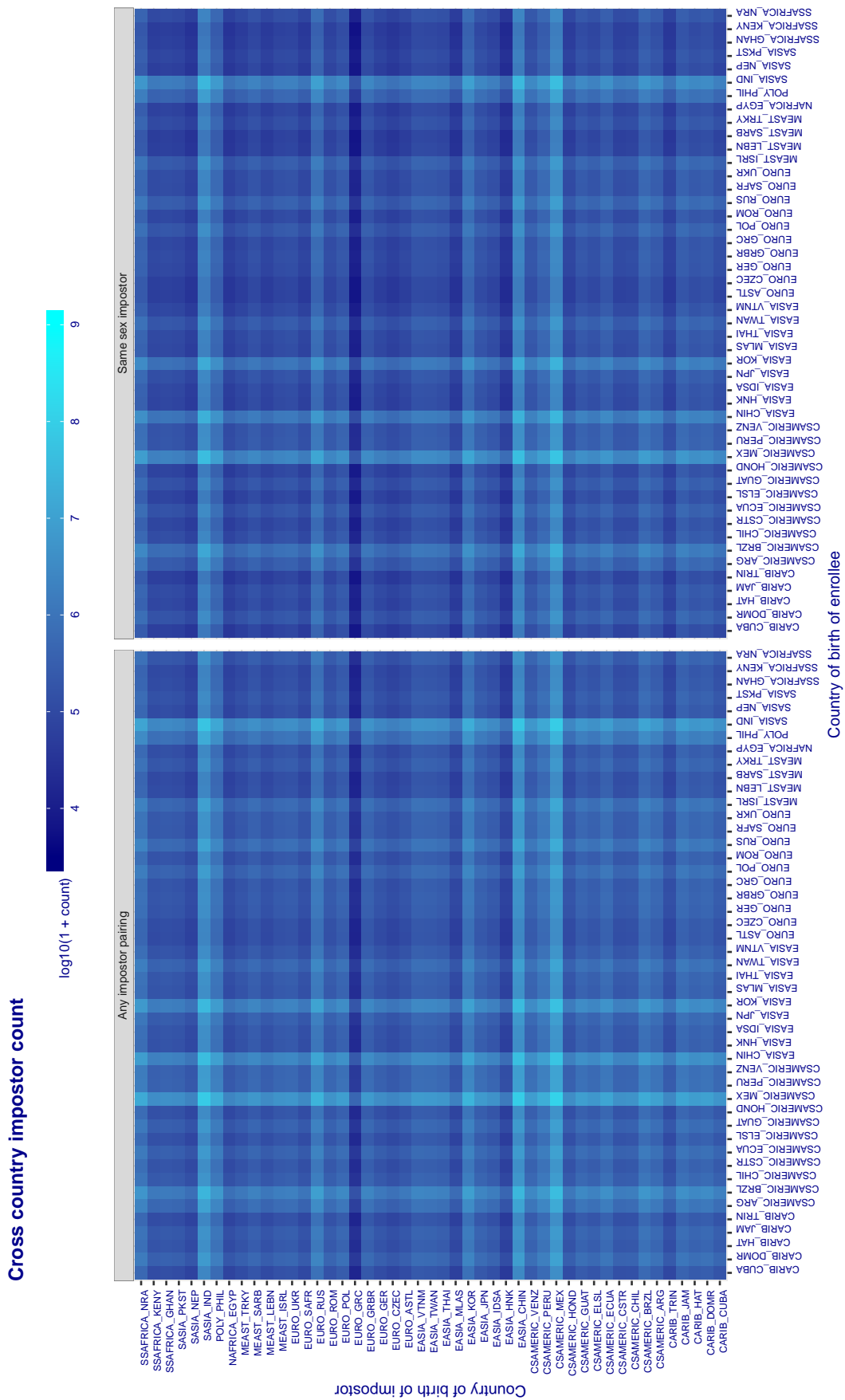


Figure 486: For visa images, the heatmap shows the count of impostor comparisons of faces from different individuals who were born in the given country pair.



### 3.6.2 Effect of age on impostors

**Background:** This section shows the effect of age on the impostor distribution. The ideal behaviour is that the age of the enrollee and the impostor would not affect impostor scores. This would support FMR stability over sub-populations.

**Goals:**

- ▷ To show the effect of relative ages of the impostor and enrollee on false match rates.
- ▷ To determine whether some algorithms have better impostor distribution stability.

**Methods:**

- ▷ Define 14 age group bins, spanning 0 to over 100 years old.
- ▷ Compute FMR over all impostor comparisons for which the subjects in the enrollee and impostor images have ages in two bins.
- ▷ Compute FMR over all impostor comparisons for which the subjects are additionally of the same sex, and born in the same geographic region.

**Results:**

The notable aspects are:

- ▷ Diagonal dominance: Impostors are more likely to be matched against their same age group.
- ▷ Same sex and same region impostors are more successful. On the diagonal, an impostor is more likely to succeed by posing as someone of the same sex. If  $\Delta \log_{10} \text{FMR} = 0.2$ , then same-sex same-region FMR exceeds the all-pairs FMR by factor of  $10^{0.2} = 1.6$ .
- ▷ Young children impostors give elevated FMR against young children. Older adult impostor give elevated FMR against older adults. These effects are quite large, for example if  $\Delta \log_{10} \text{FMR} = 1.0$  larger than a 32 year old, then these groups have higher FMR by a factor of  $10^1 = 10$ . This would imply an FMR above 0.01 for a nominal (global) FMR = 0.001.
- ▷ Algorithms vary.
- ▷ We computed the same quantities for a global FMR = 0.0001. The effects are similar.

Note the calculations in this section include impostors paired across all countries of birth.

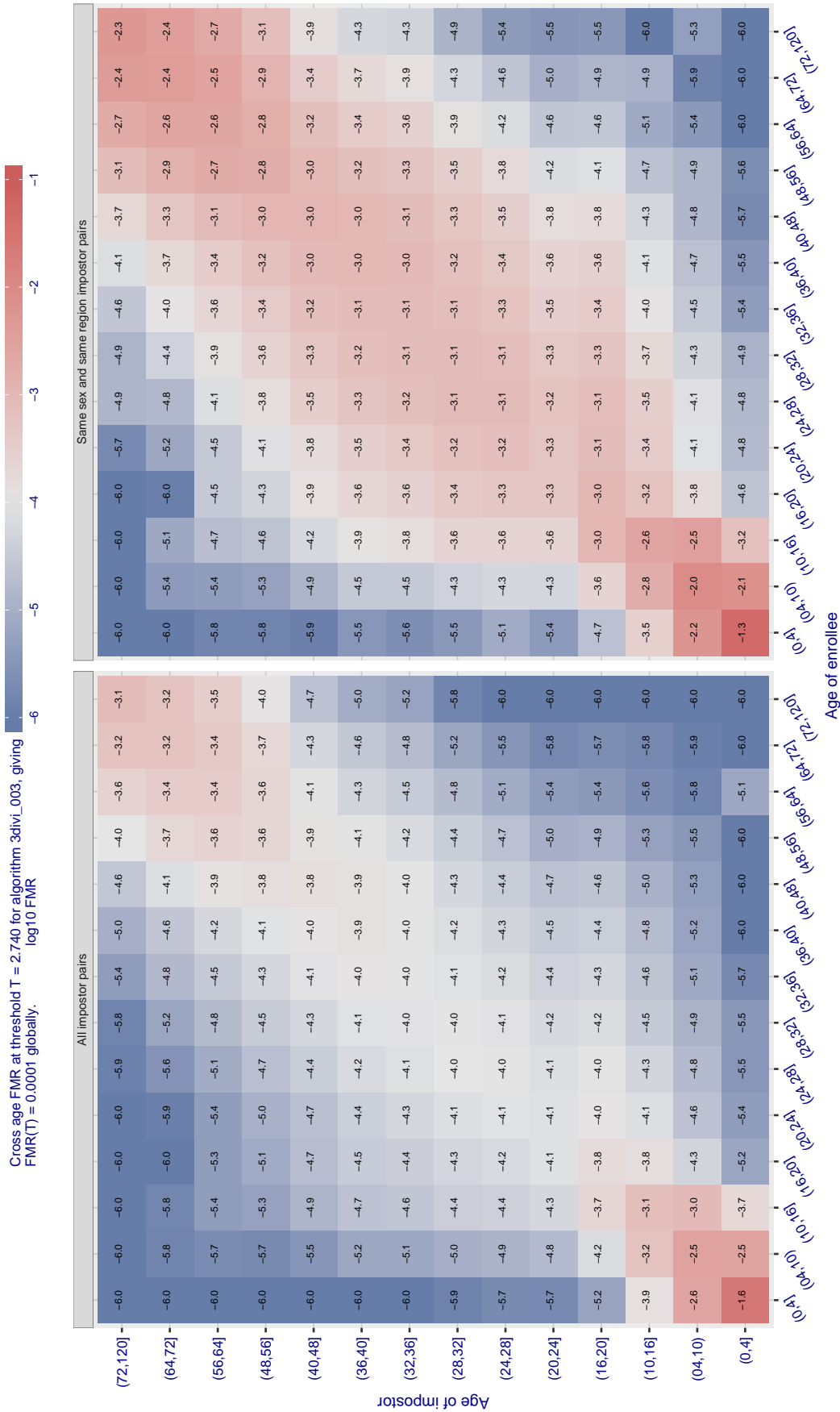


Figure 487: For algorithm 3divi-003 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

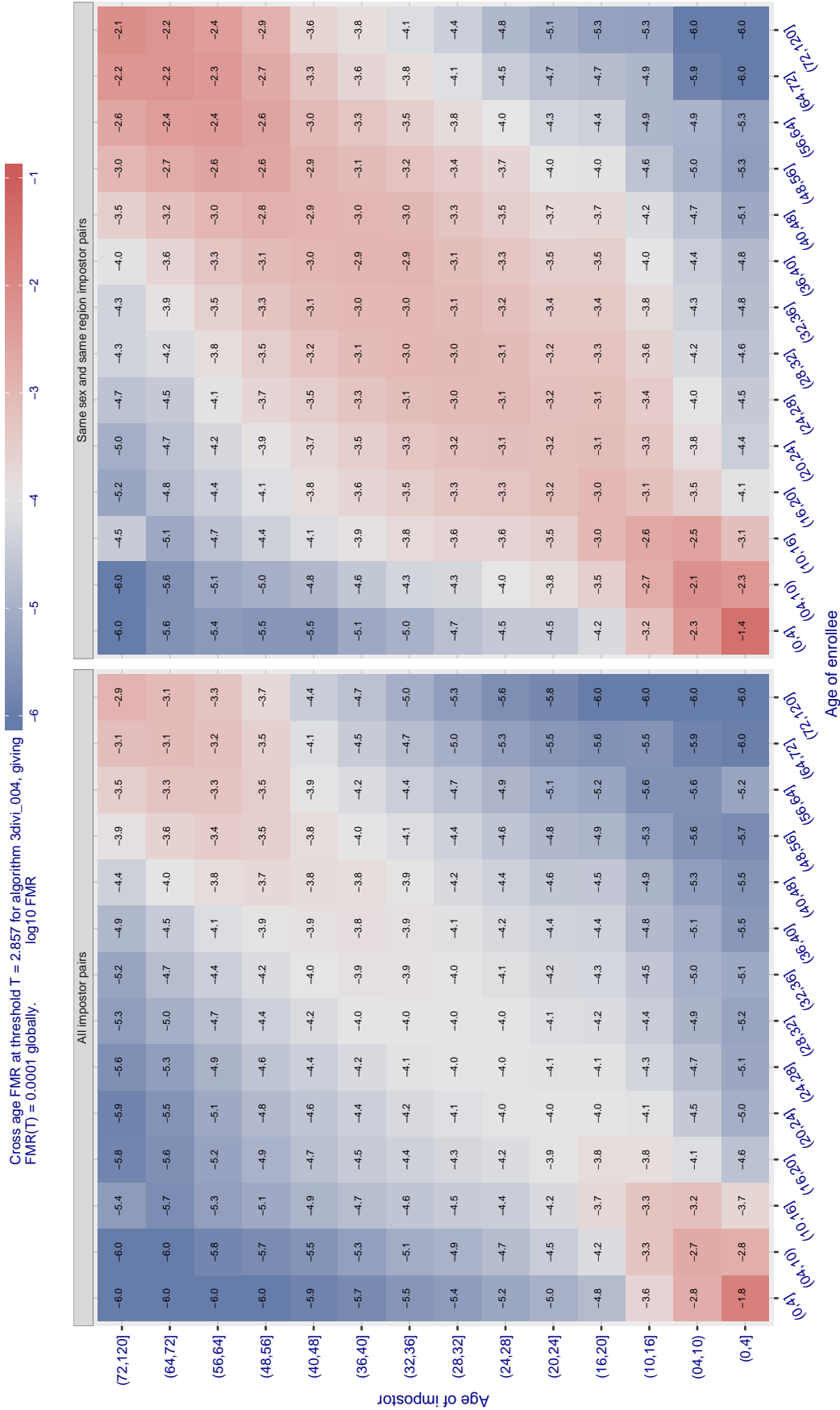


Figure 488: For algorithm 3divi-004 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.713$  for algorithm *adera\_001*, giving  $\log_{10} \text{FMR}(T) = 0.0001$  globally.

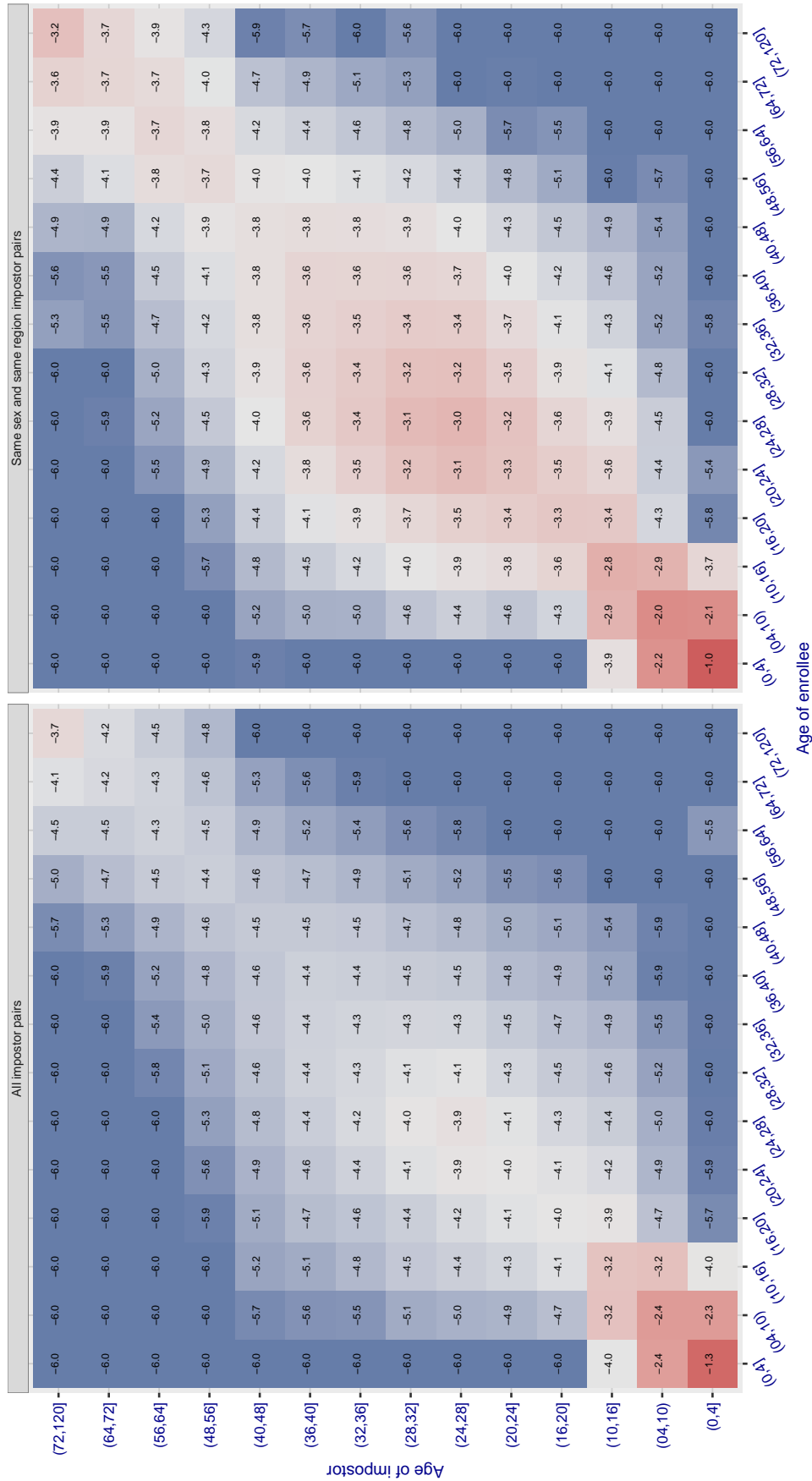


Figure 489: For algorithm *adera-001* operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

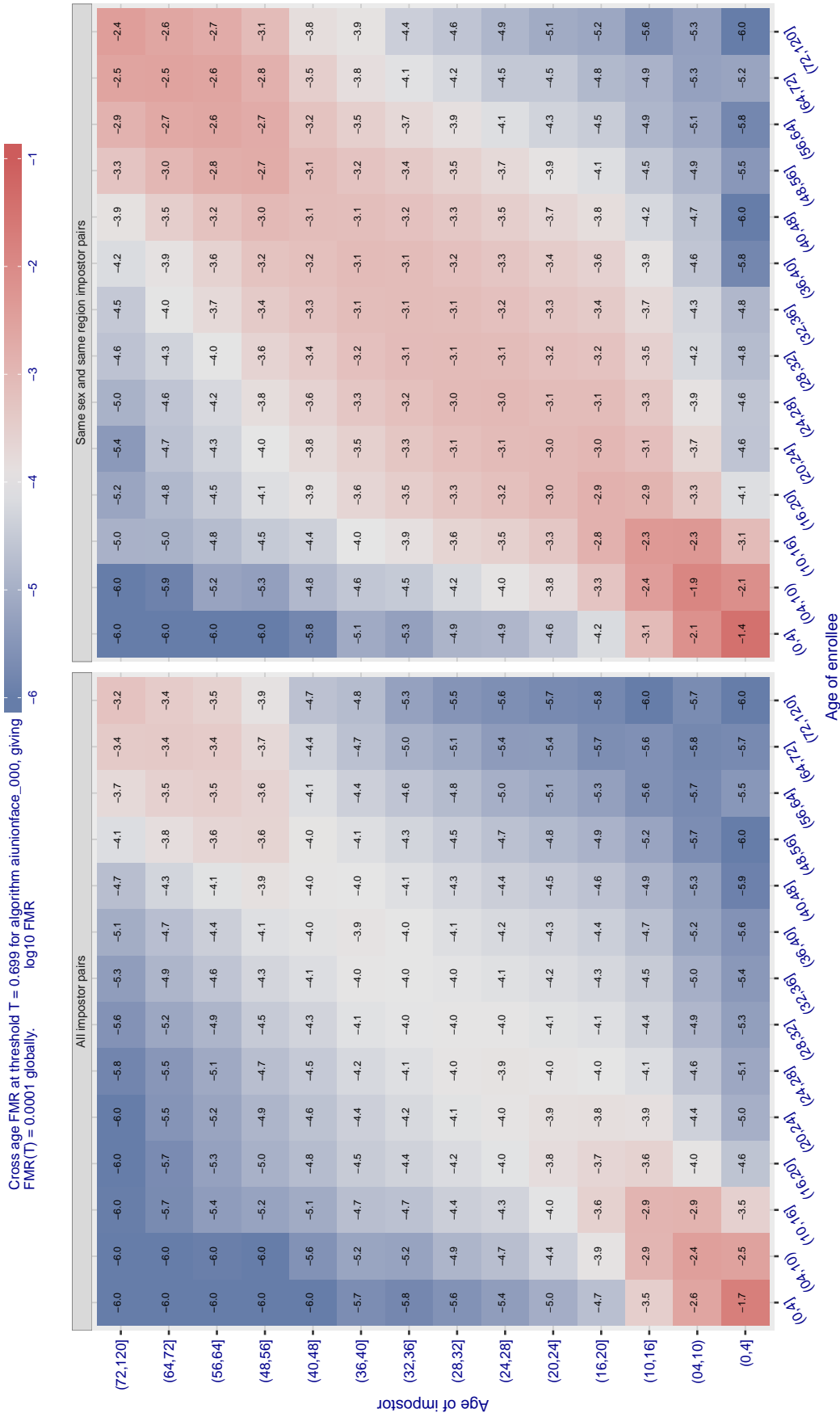


Figure 490: For algorithm aiunionface-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.702$  for algorithm alchera\_000, giving  $FMR(T) = 0.0001$  globally.

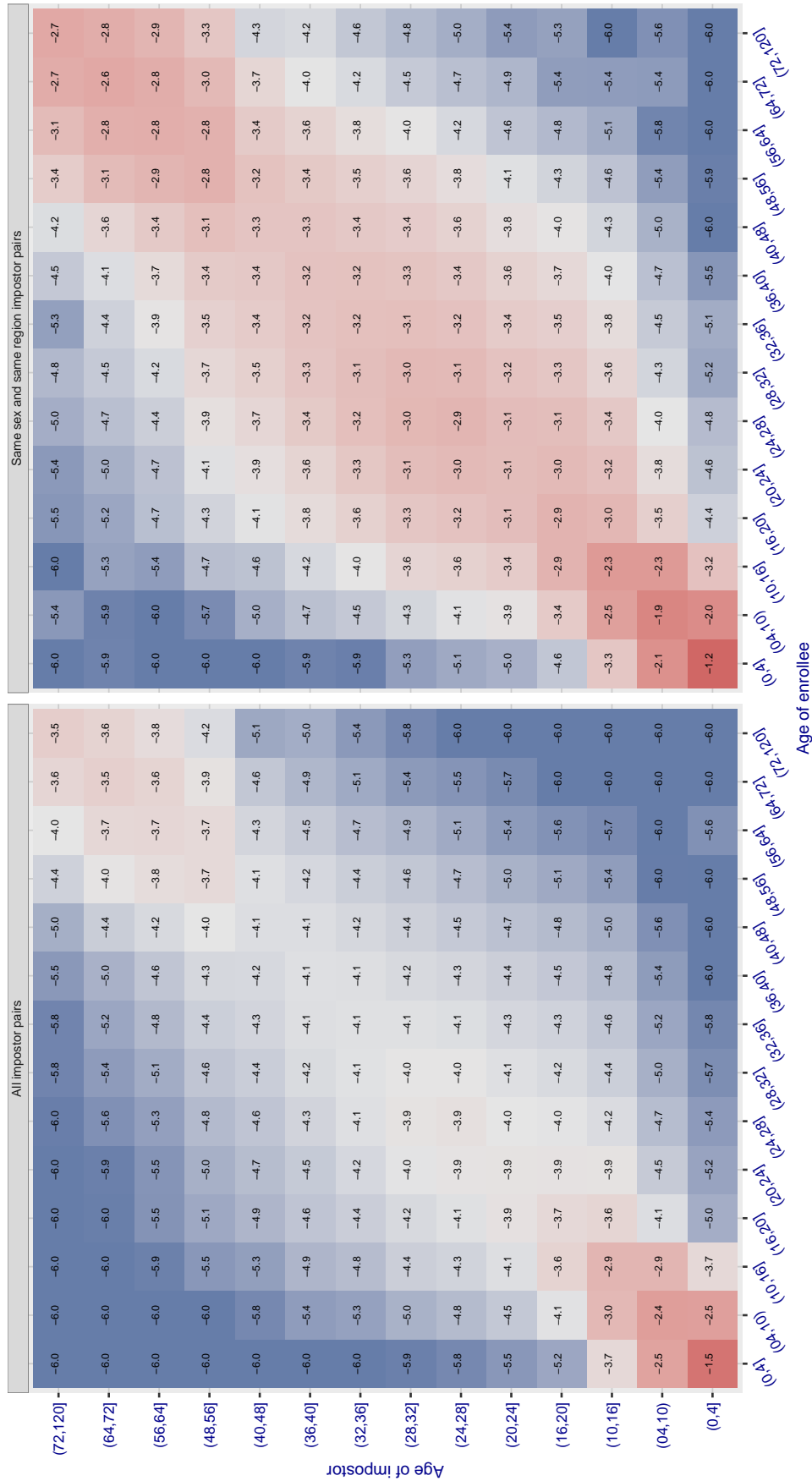


Figure 491: For algorithm alchera-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

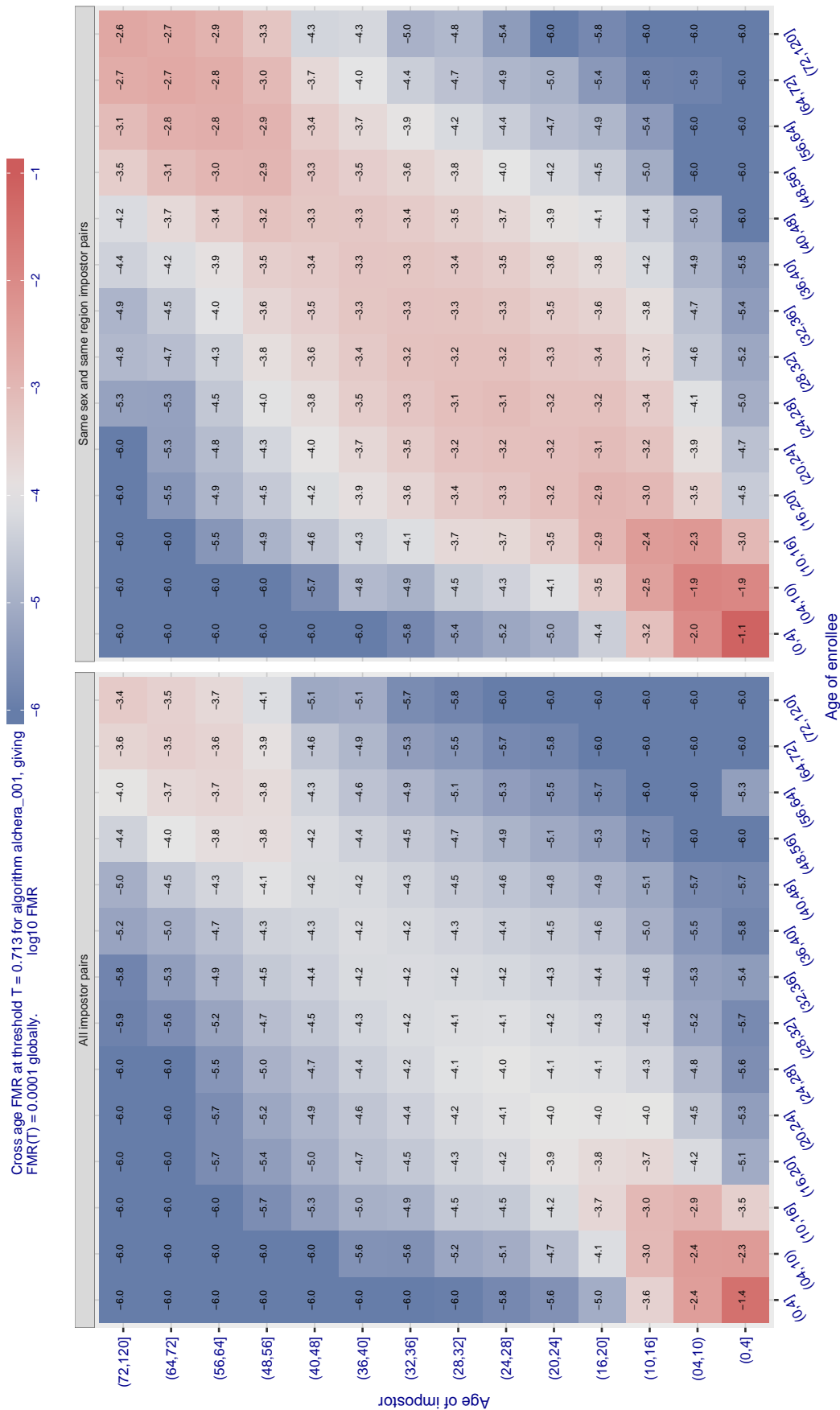


Figure 492: For algorithm alchera-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.



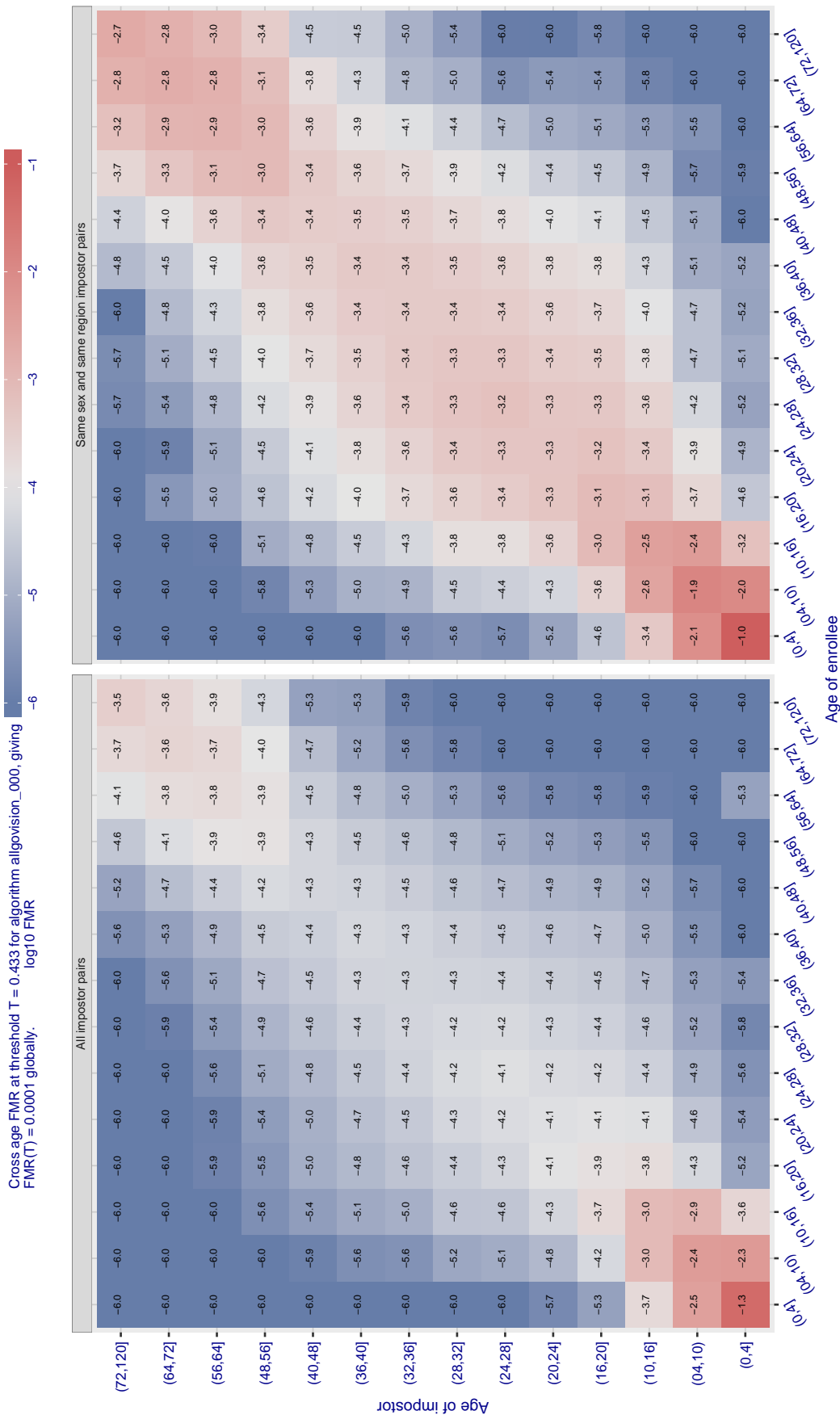


Figure 493: For algorithm `allgovision-000` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.396$  for algorithm `alphaface_001`, giving  $FMR(T) = 0.0001$  globally.

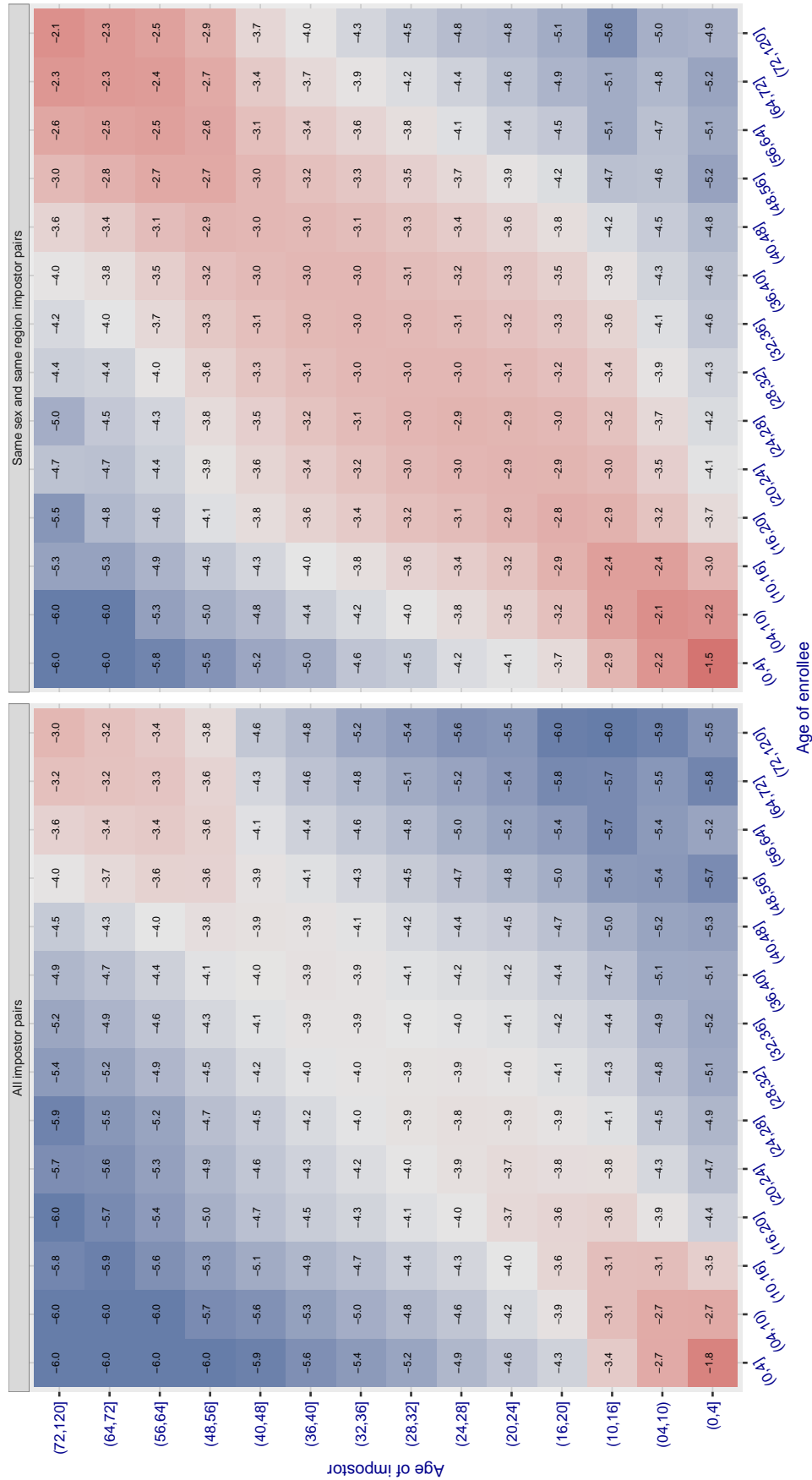


Figure 494: For algorithm `alphaface-001` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

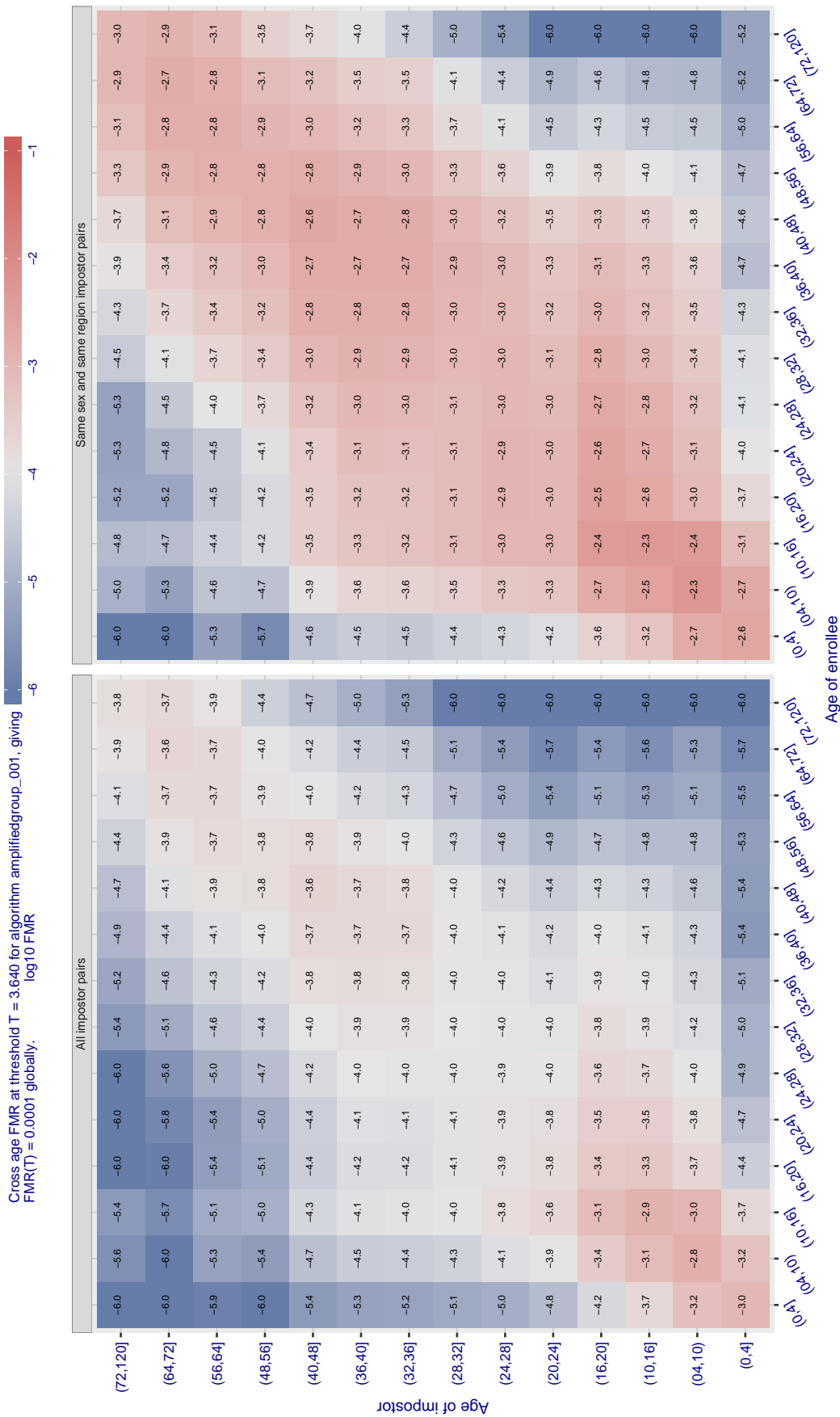


Figure 495: For algorithm amplifiedgroup-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

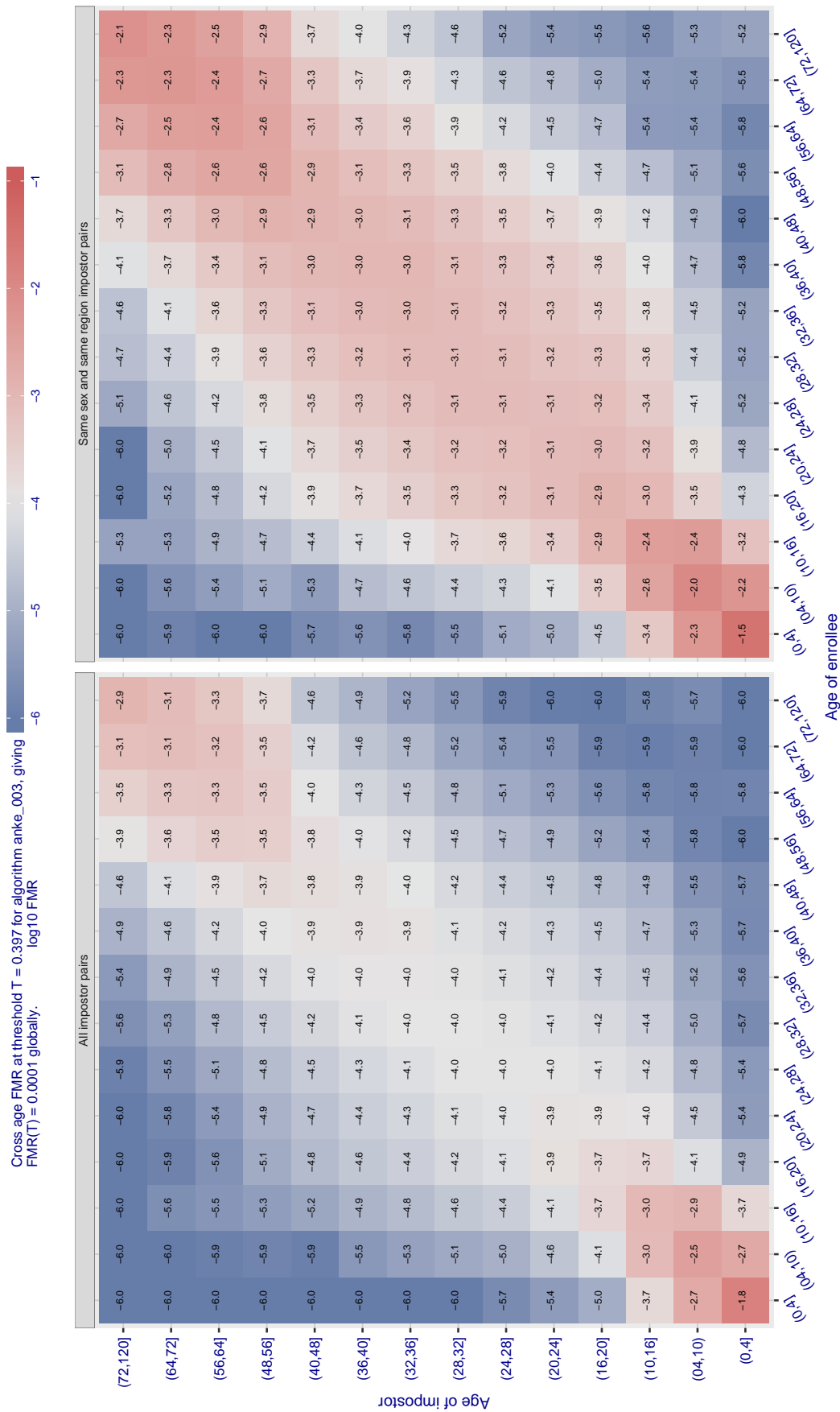


Figure 496: For algorithm anke-003 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

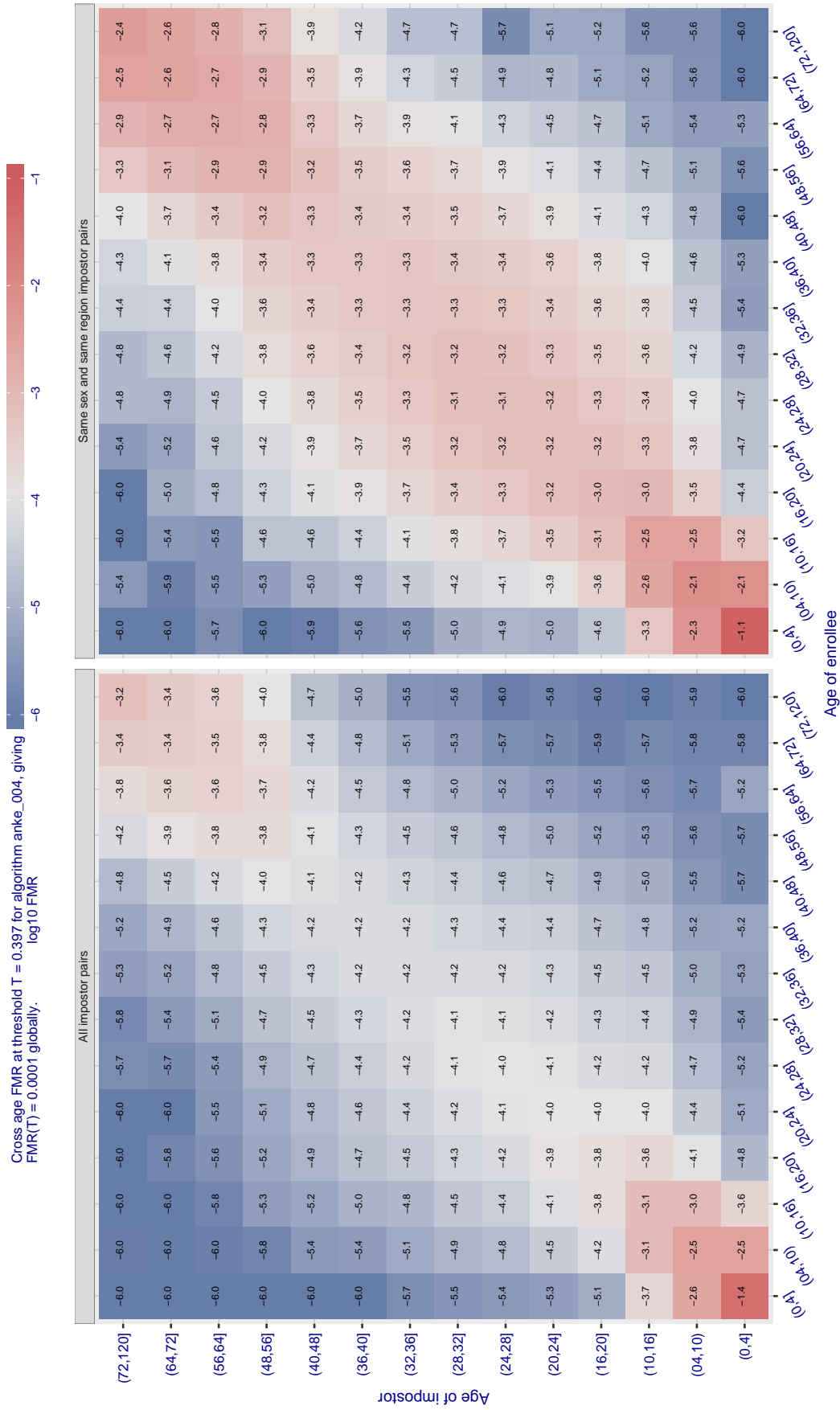


Figure 497: For algorithm anke-004 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

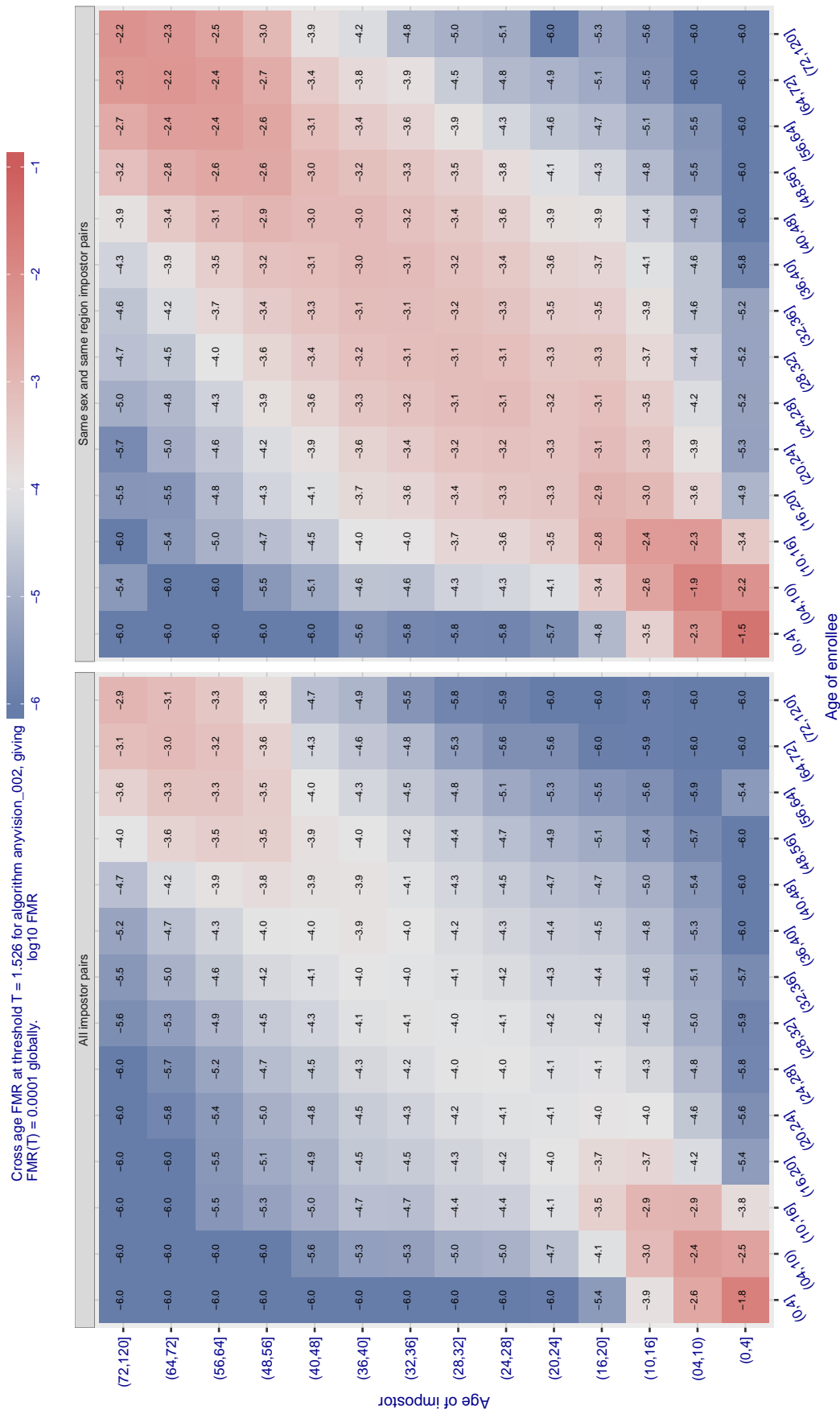


Figure 498: For algorithm anyvision-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

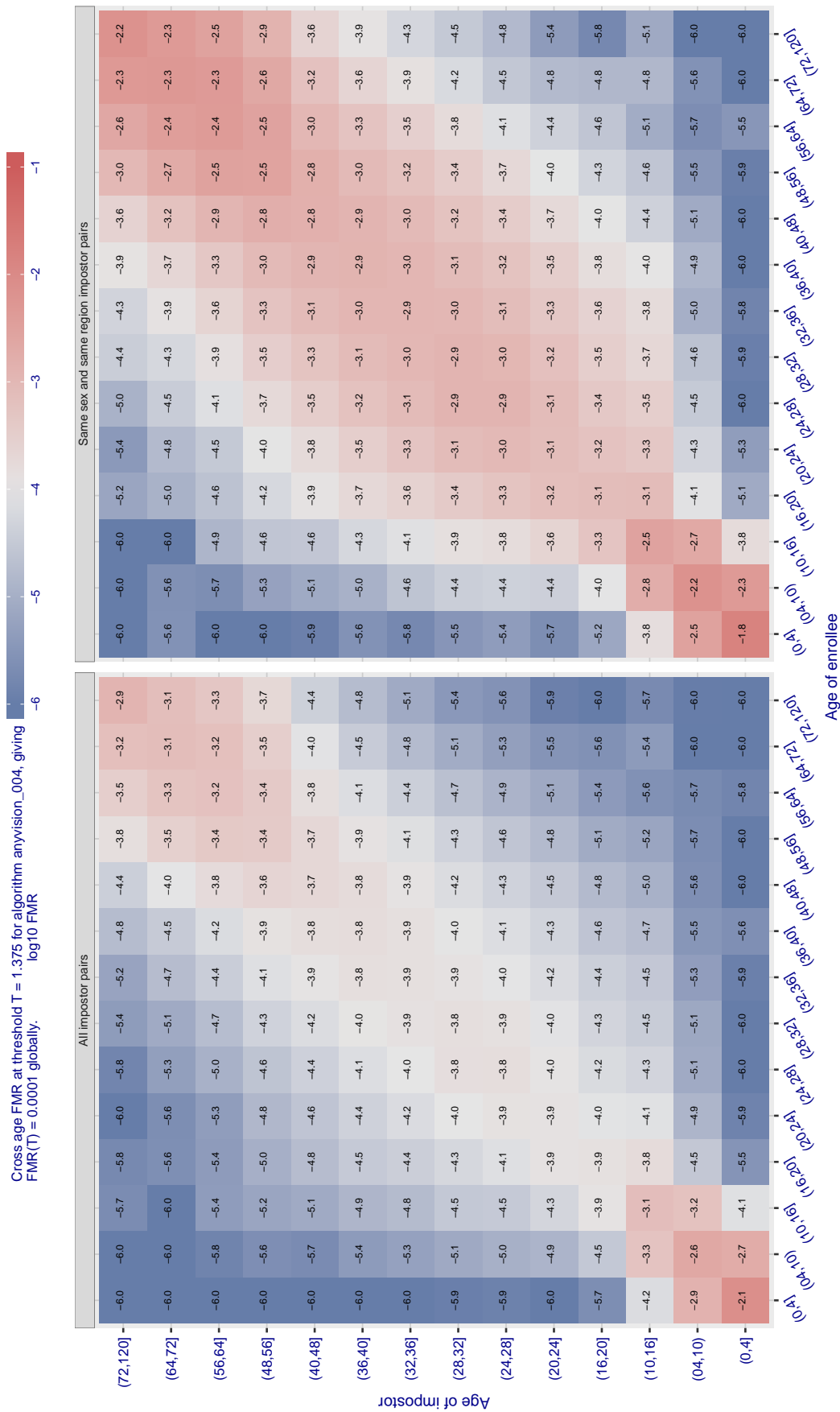


Figure 499: For algorithm anyvision-004 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.



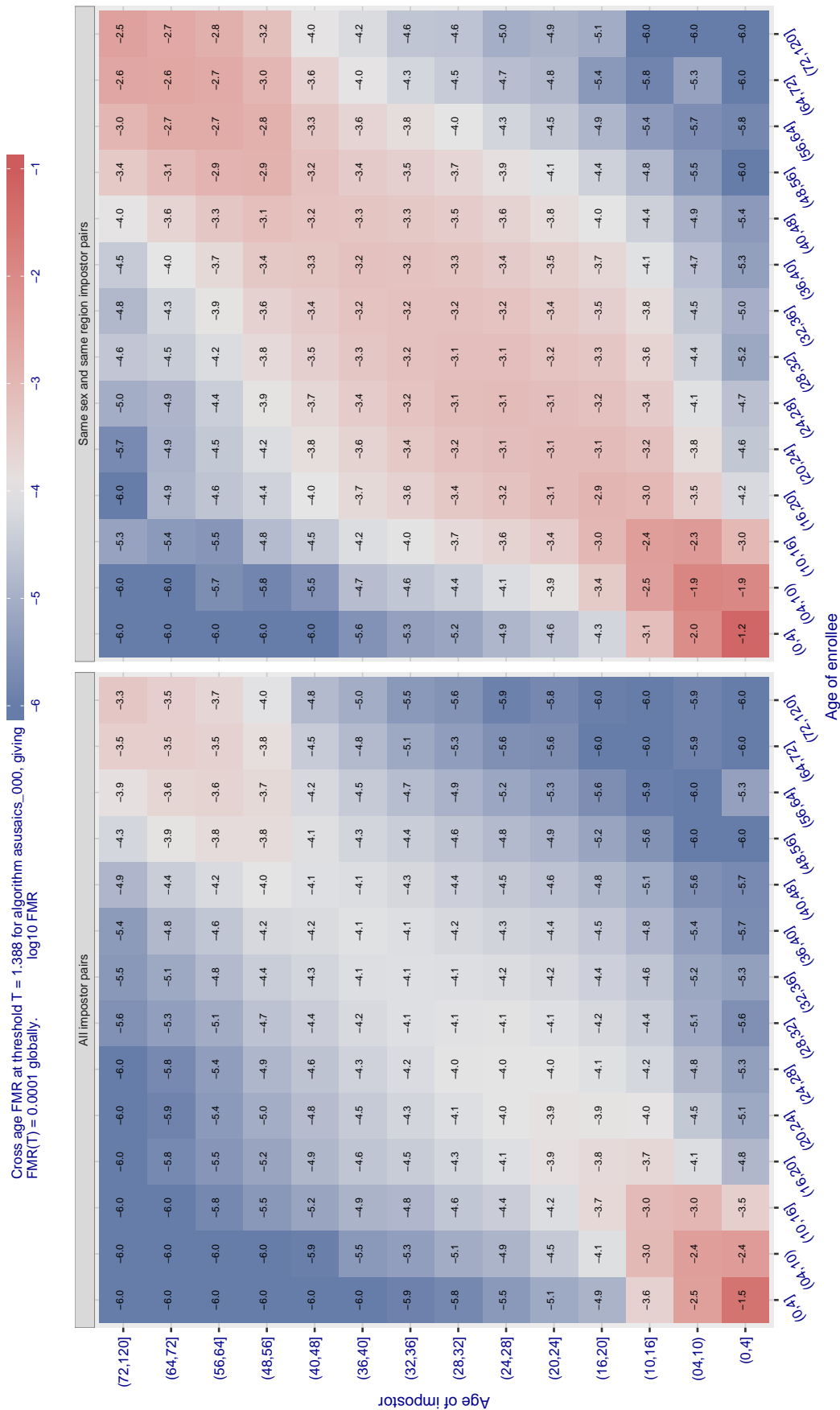


Figure 500: For a algorithm asusaics-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

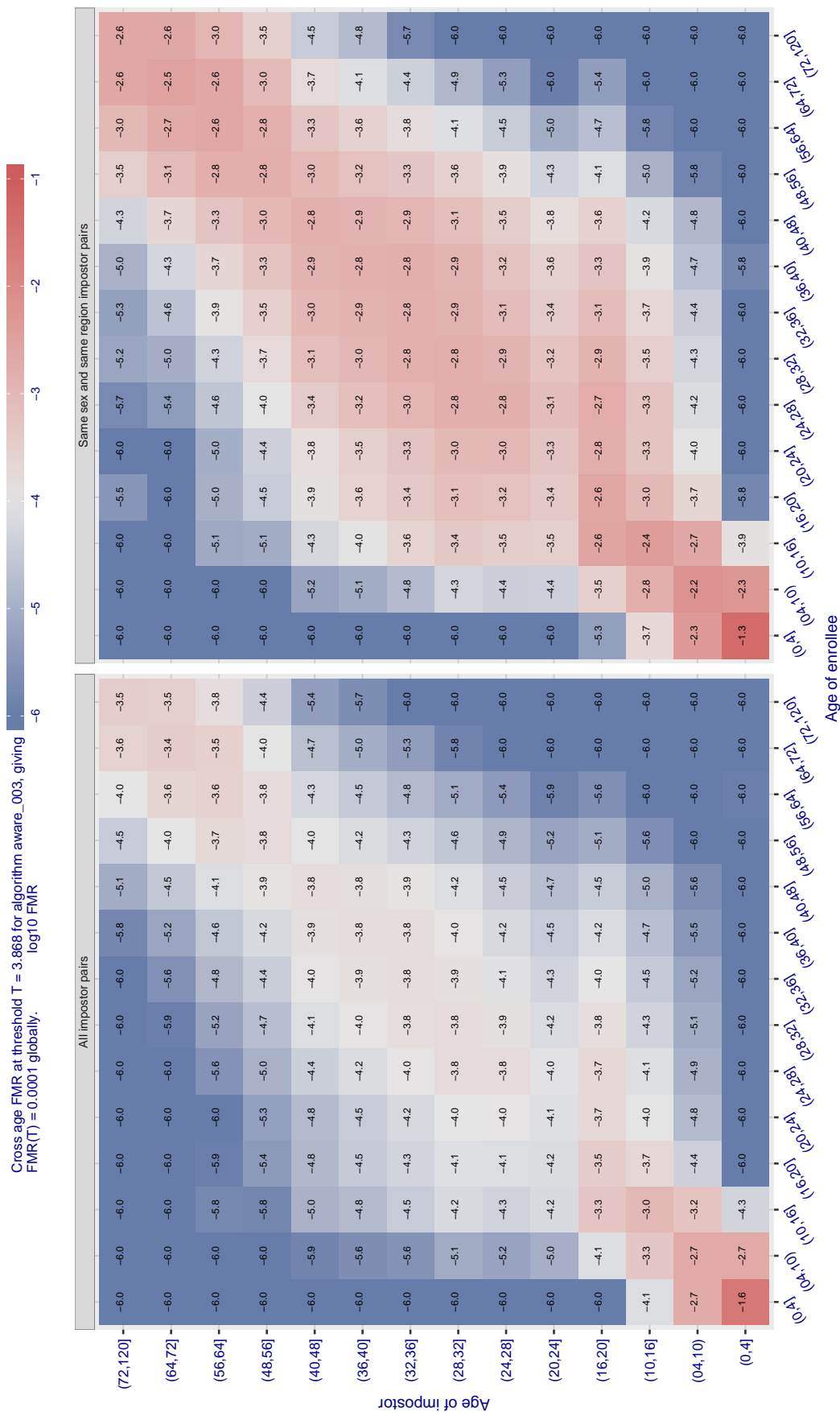


Figure 501: For algorithm aware-003 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

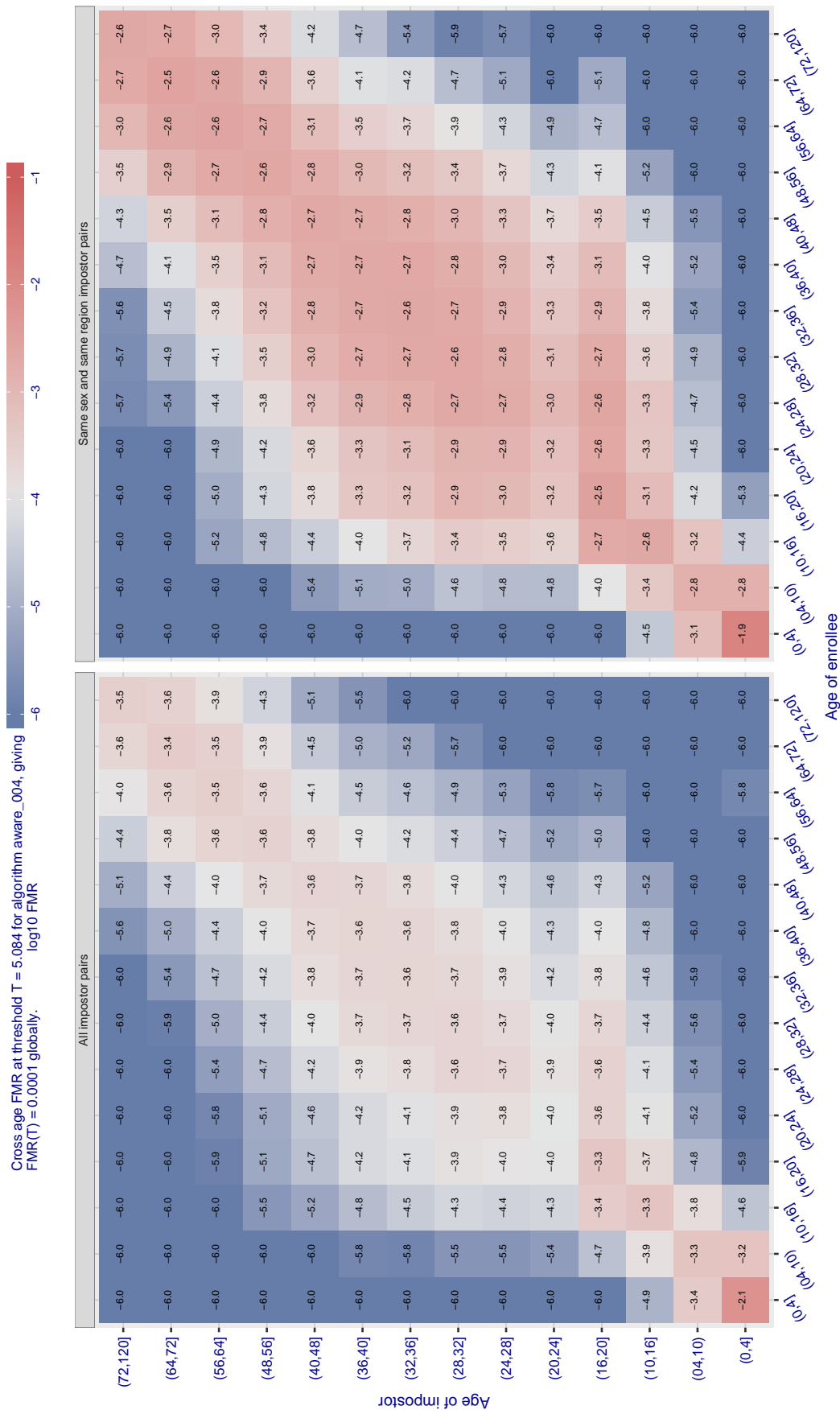


Figure 502: For algorithm aware-004 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.799$  for algorithm awiros\_001, giving  $FMR(T) = 0.0001$  globally.

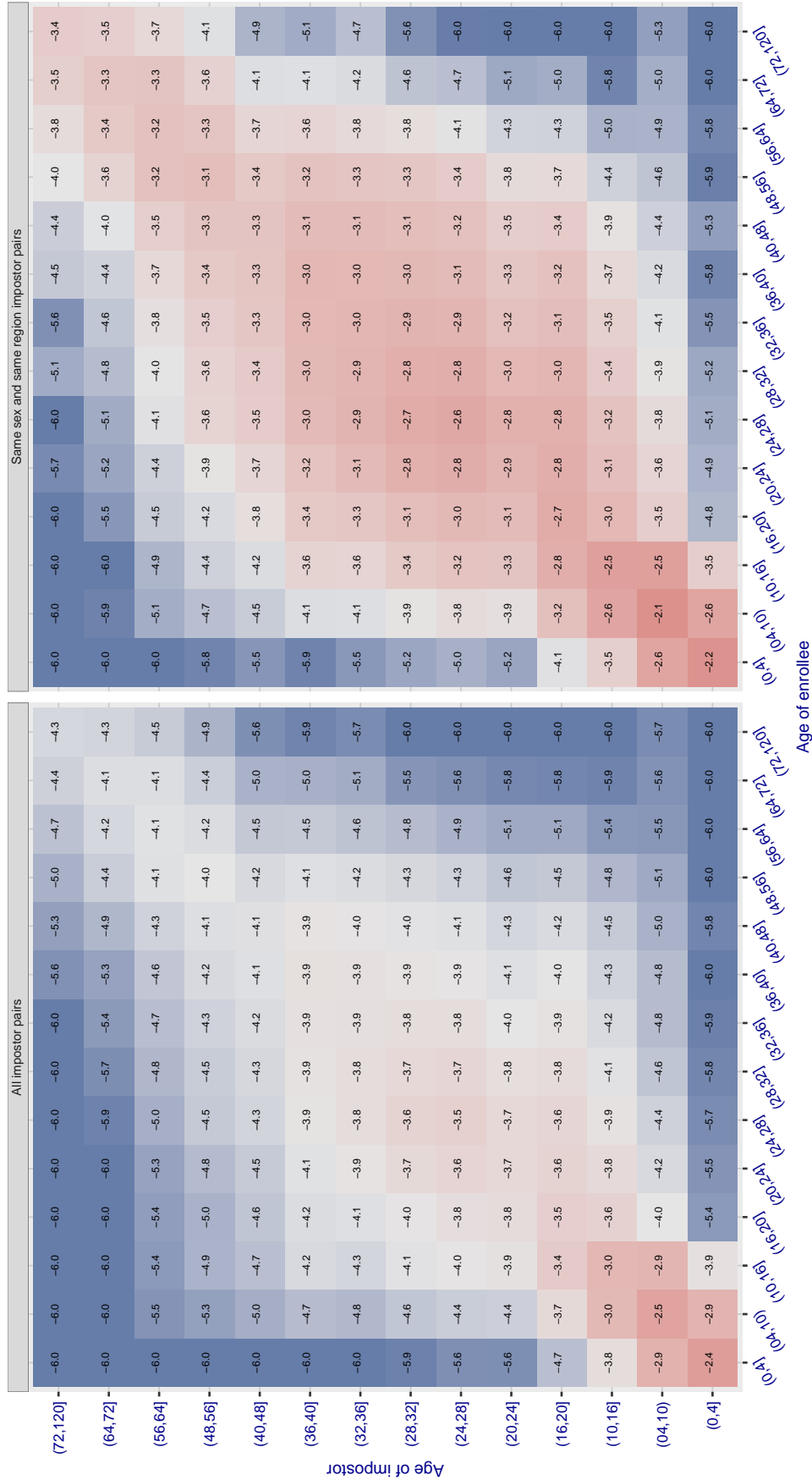


Figure 503: For algorithm awiros-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.919$  for algorithm ayonix\_000, giving  $FMR(T) \approx 0.0001$  globally.

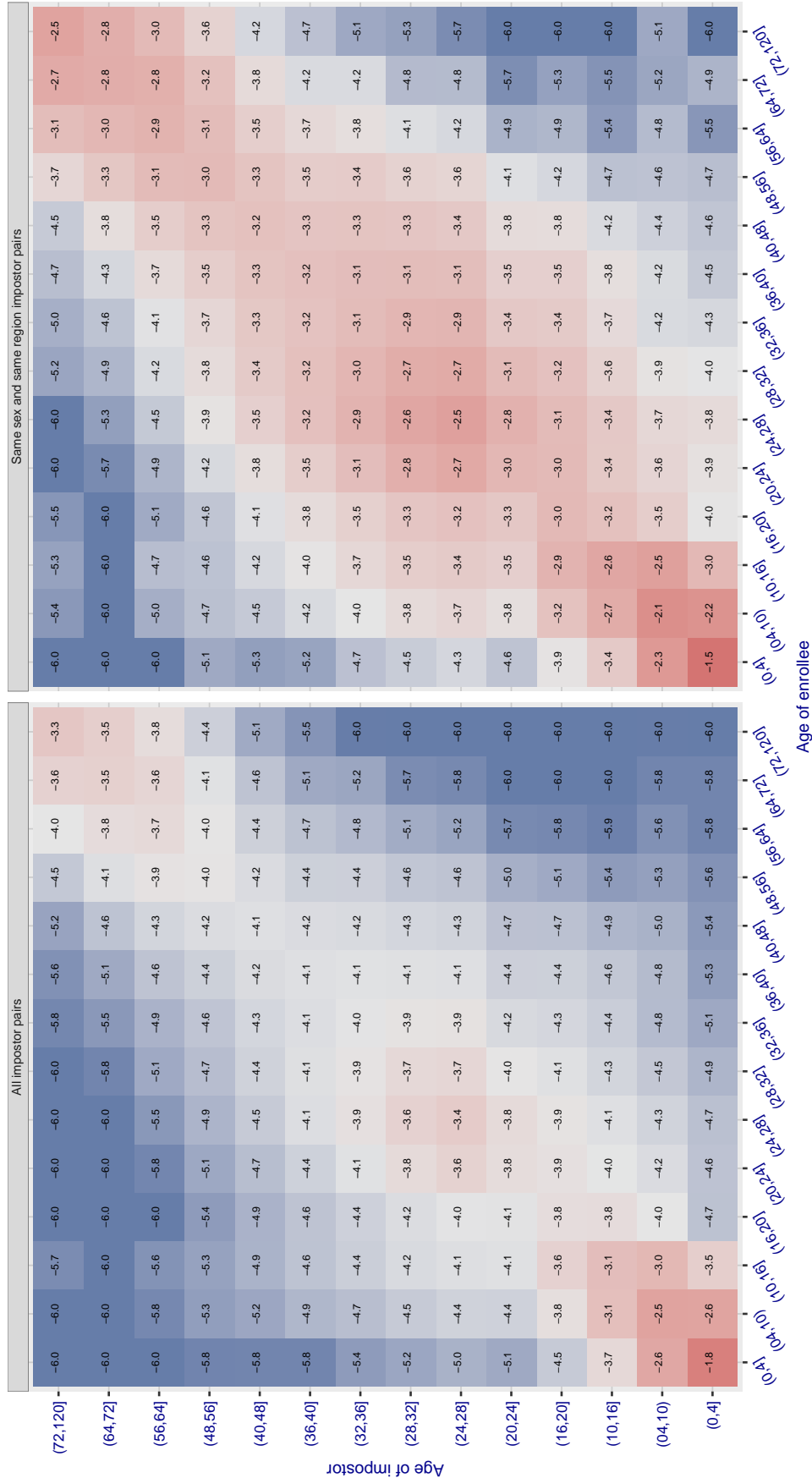


Figure 504: For algorithm ayonix-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

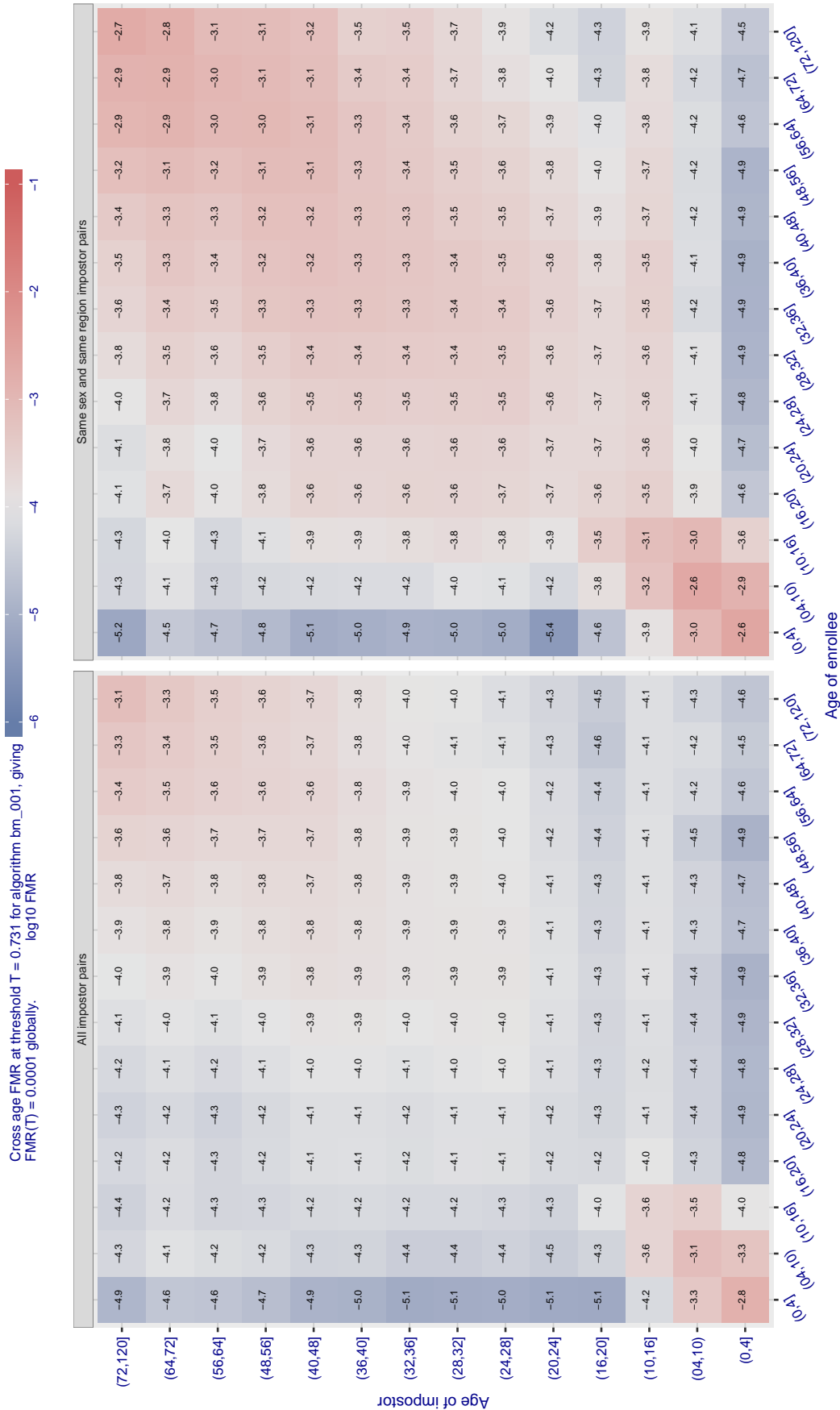


Figure 505: For algorithm bm-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.388$  for algorithm camvi\_002, giving  $FMR(T) = 0.0001$  globally.

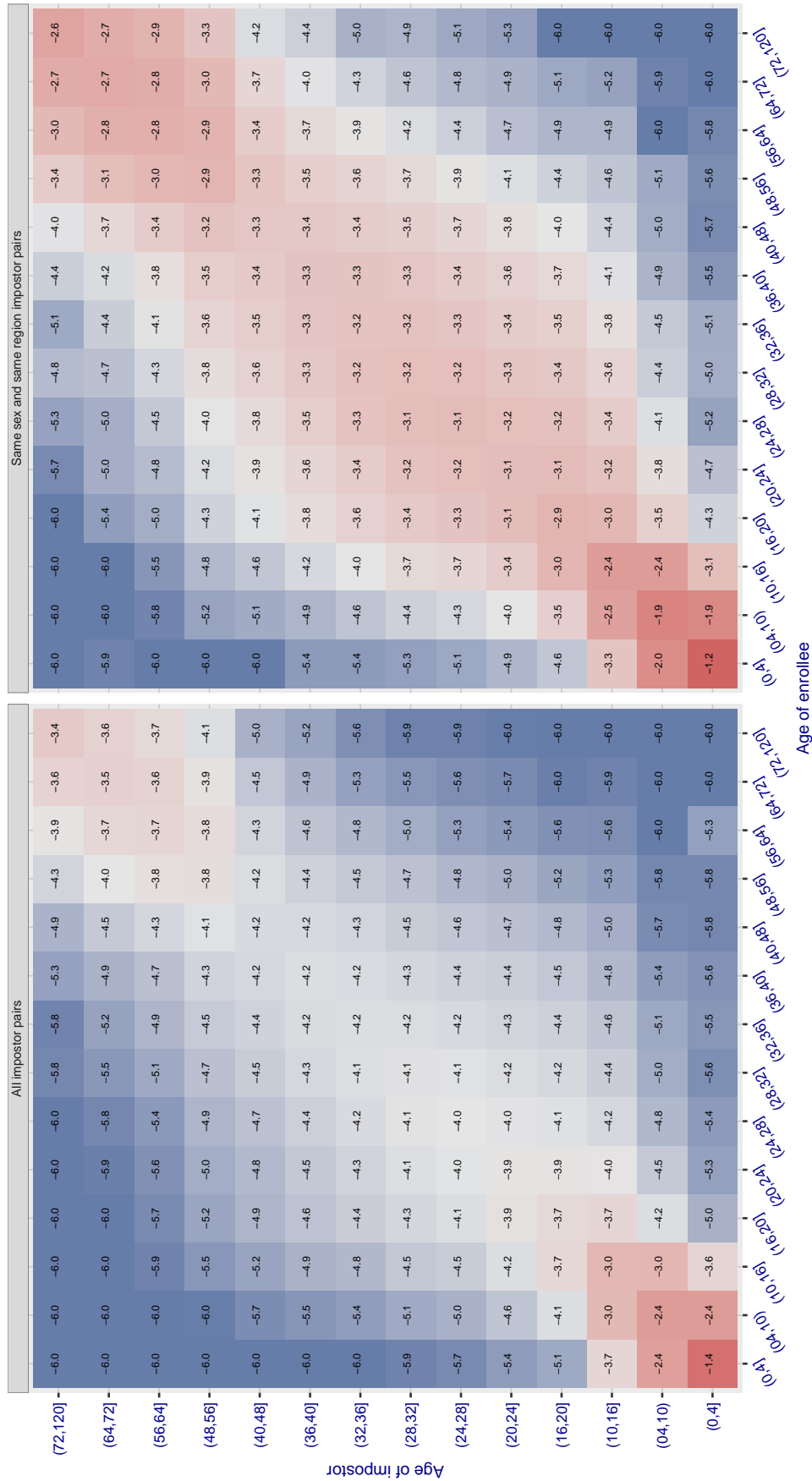


Figure 506: For algorithm camvi-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.



Cross age FMR at threshold  $T = 0.377$  for algorithm camvi\_004, giving  $FMR(T) = 0.0001$  globally.

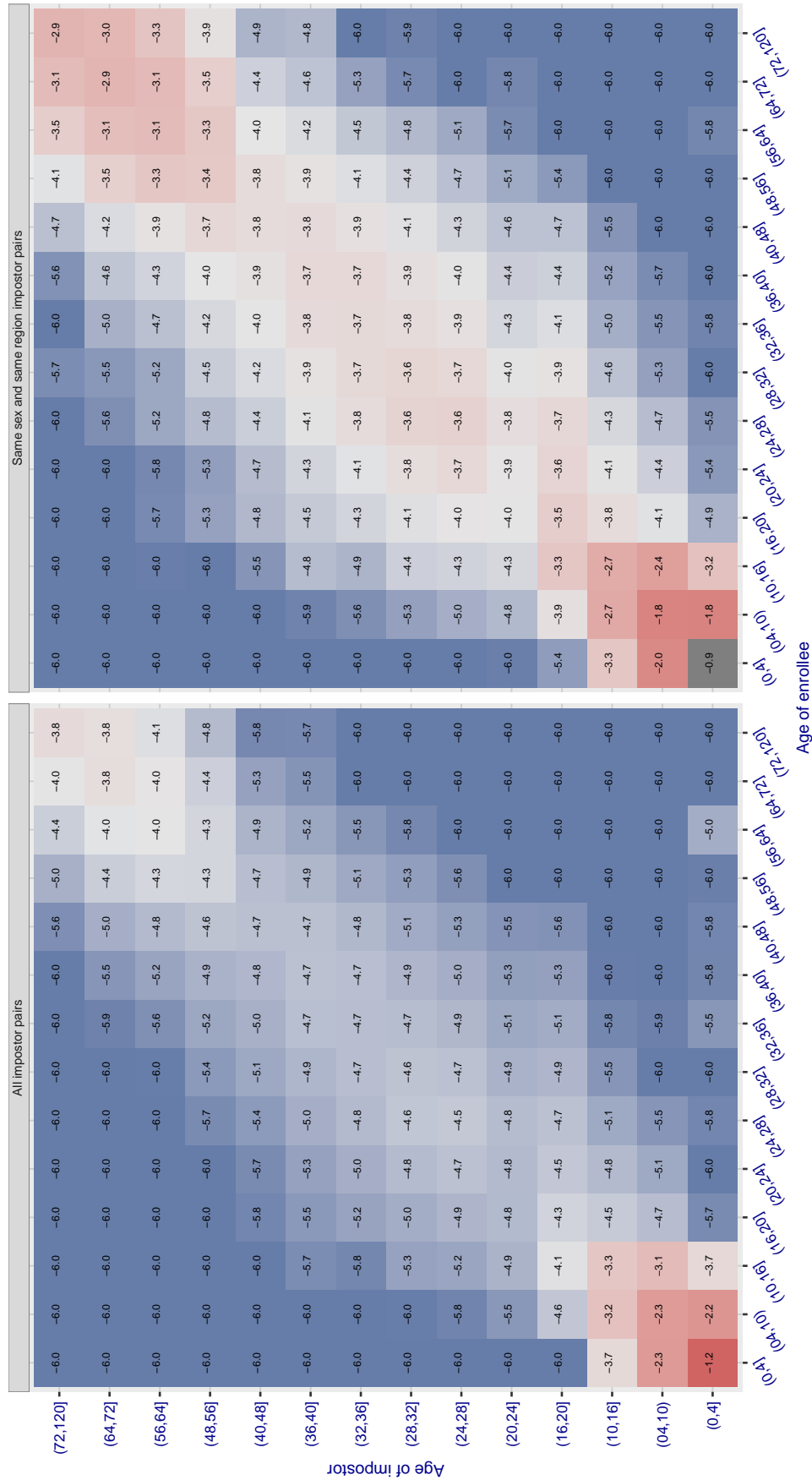


Figure 507: For algorithm camvi-004 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

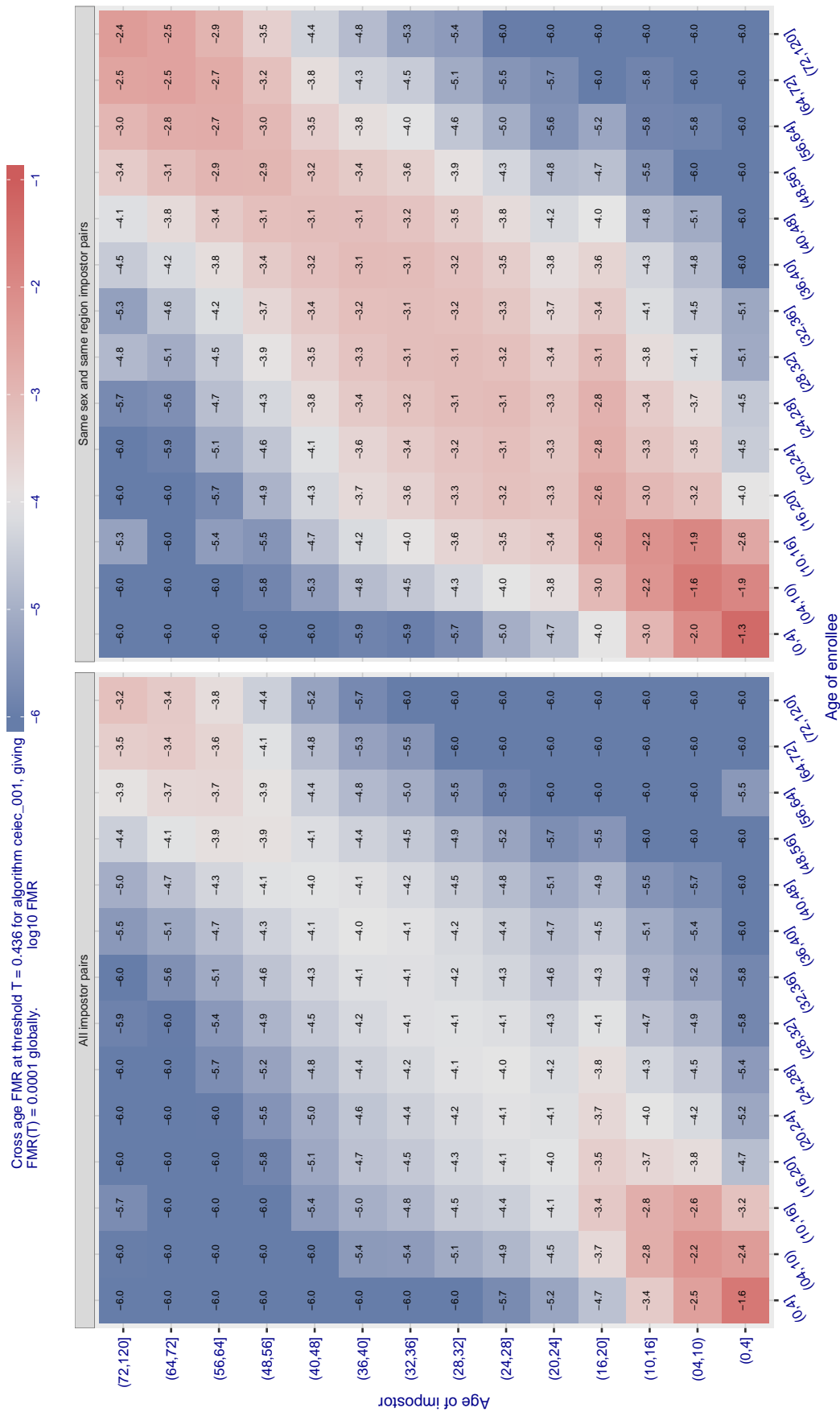


Figure 508: For algorithm ceiec-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.325$  for algorithm ceiec\_002, giving  $\log_{10}$  FMR

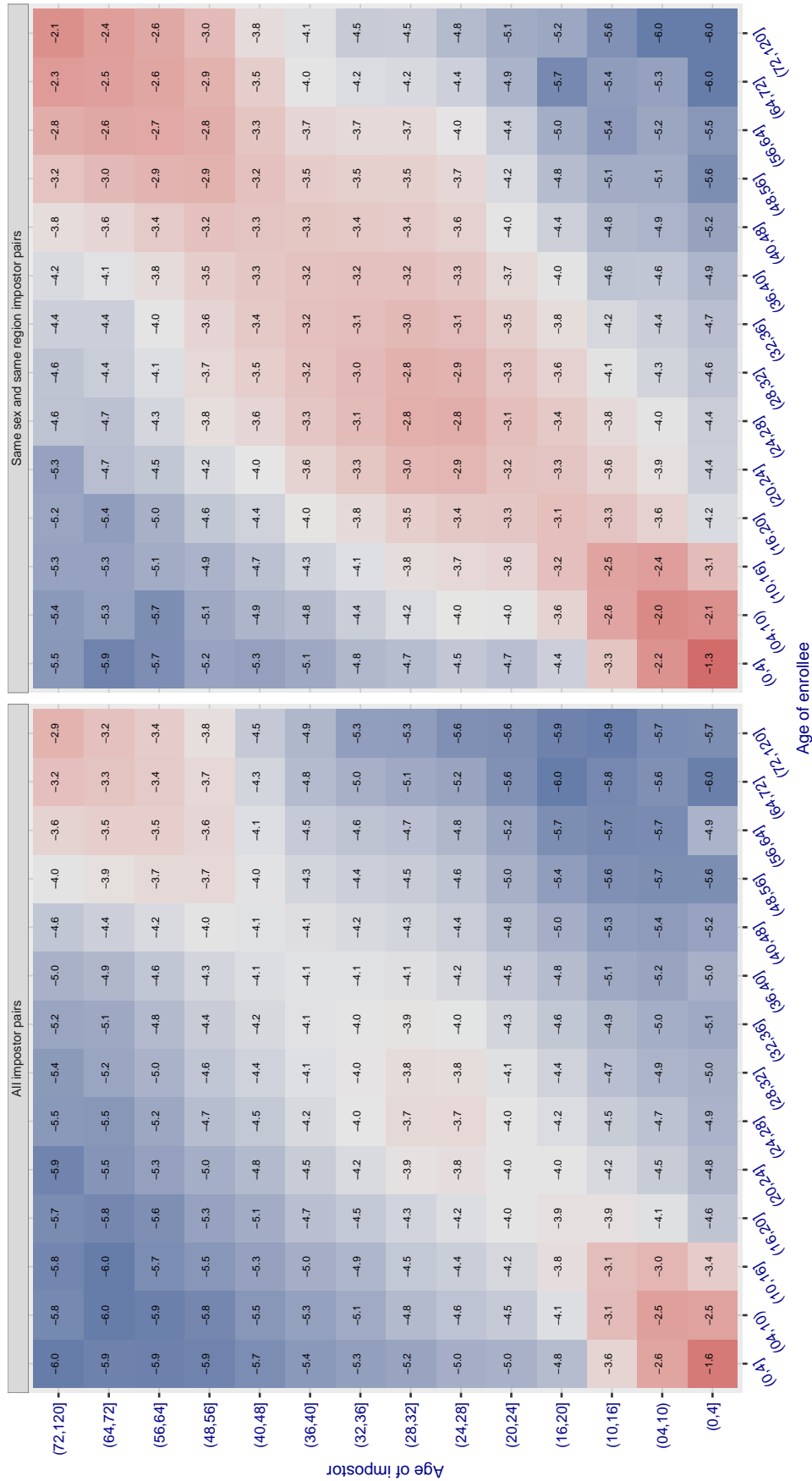


Figure 509: For algorithm ceiec-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 106.748$  for algorithm `chtface_001`, giving  $FMR(T) = 0.0001$  globally.

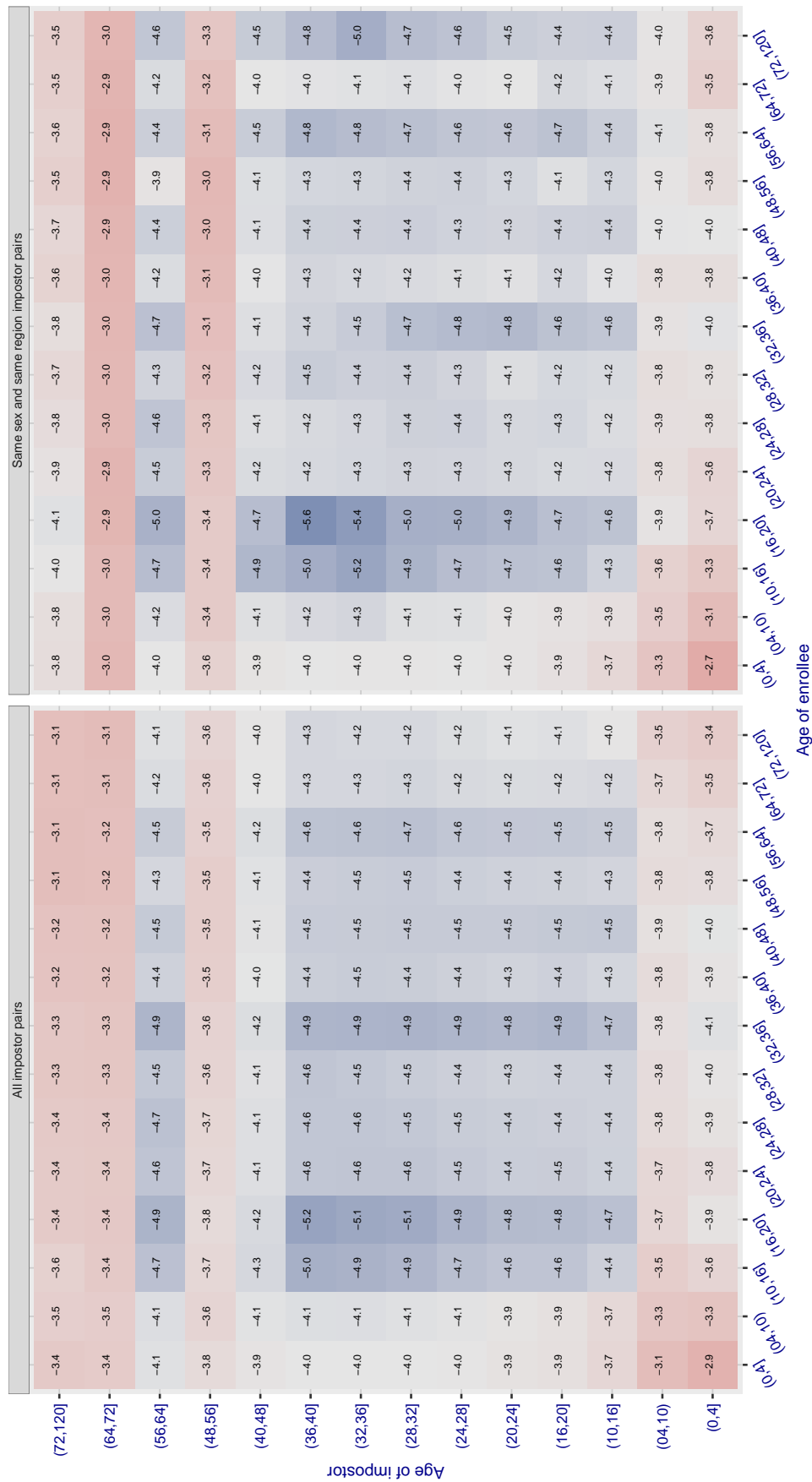


Figure 510: For algorithm `chtface-001` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

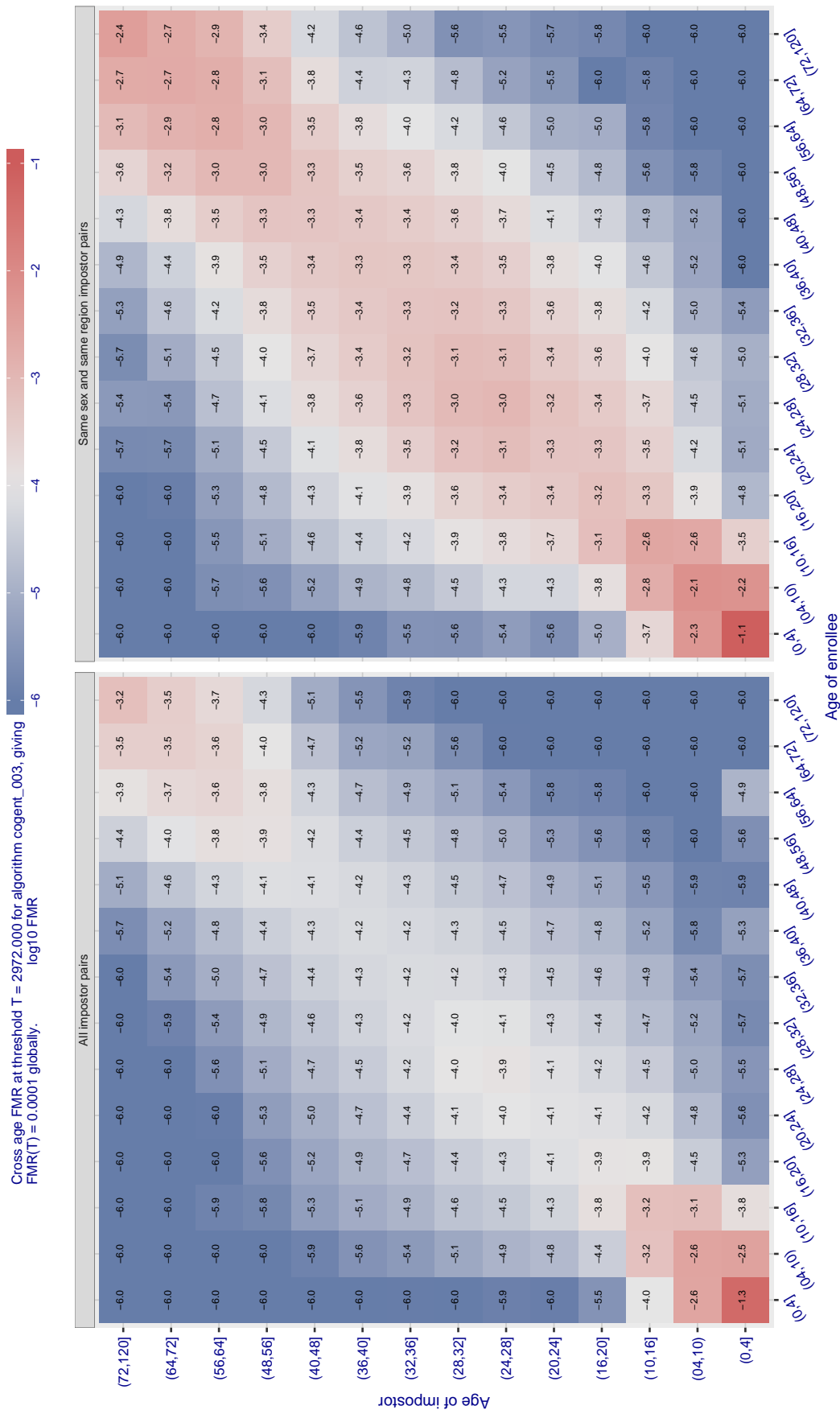


Figure 511: For algorithm cogent-003 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

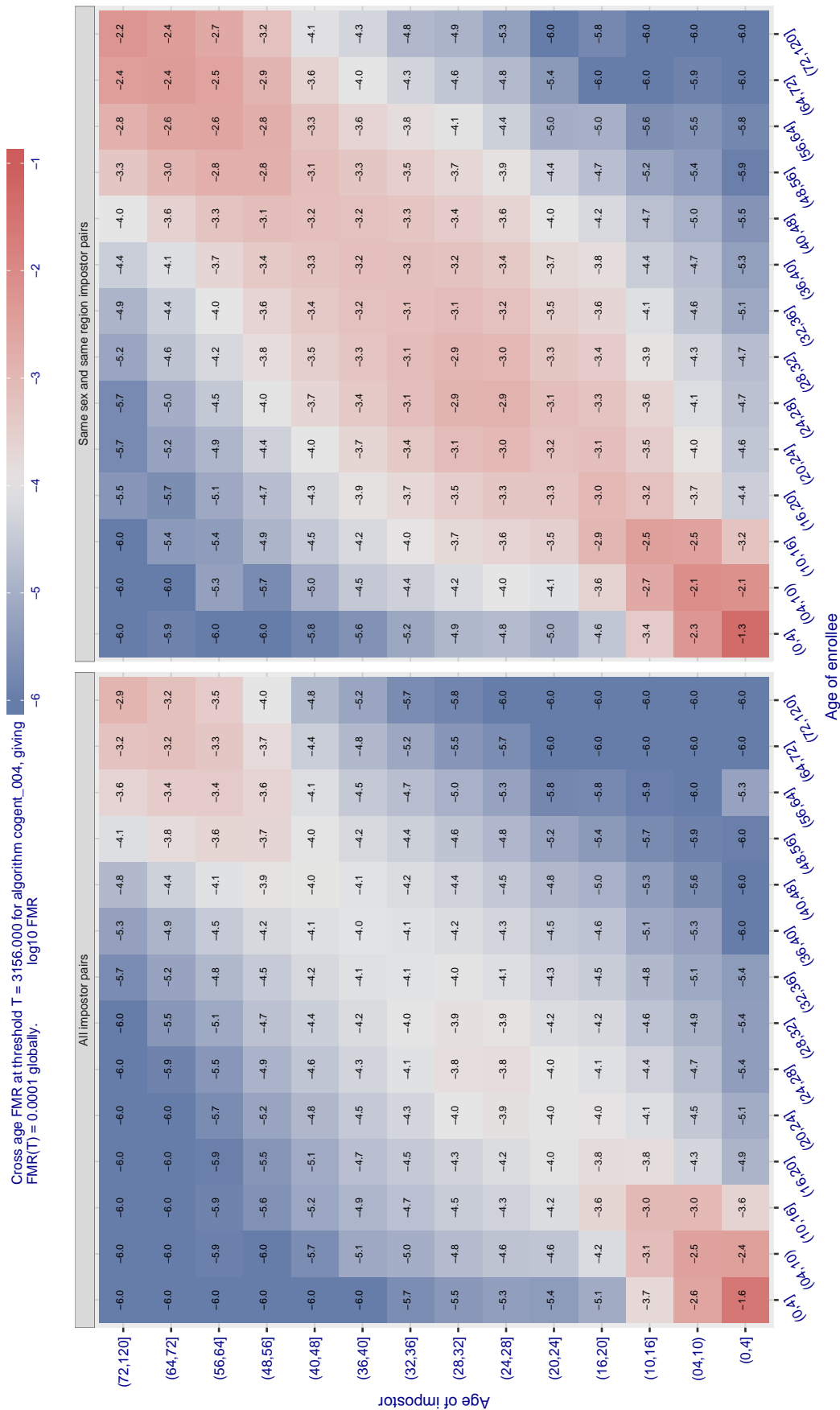


Figure 512: For algorithm cogent-004 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.565$  for algorithm `cognitec_000`, giving  $FMR(T) = 0.0001$  globally.

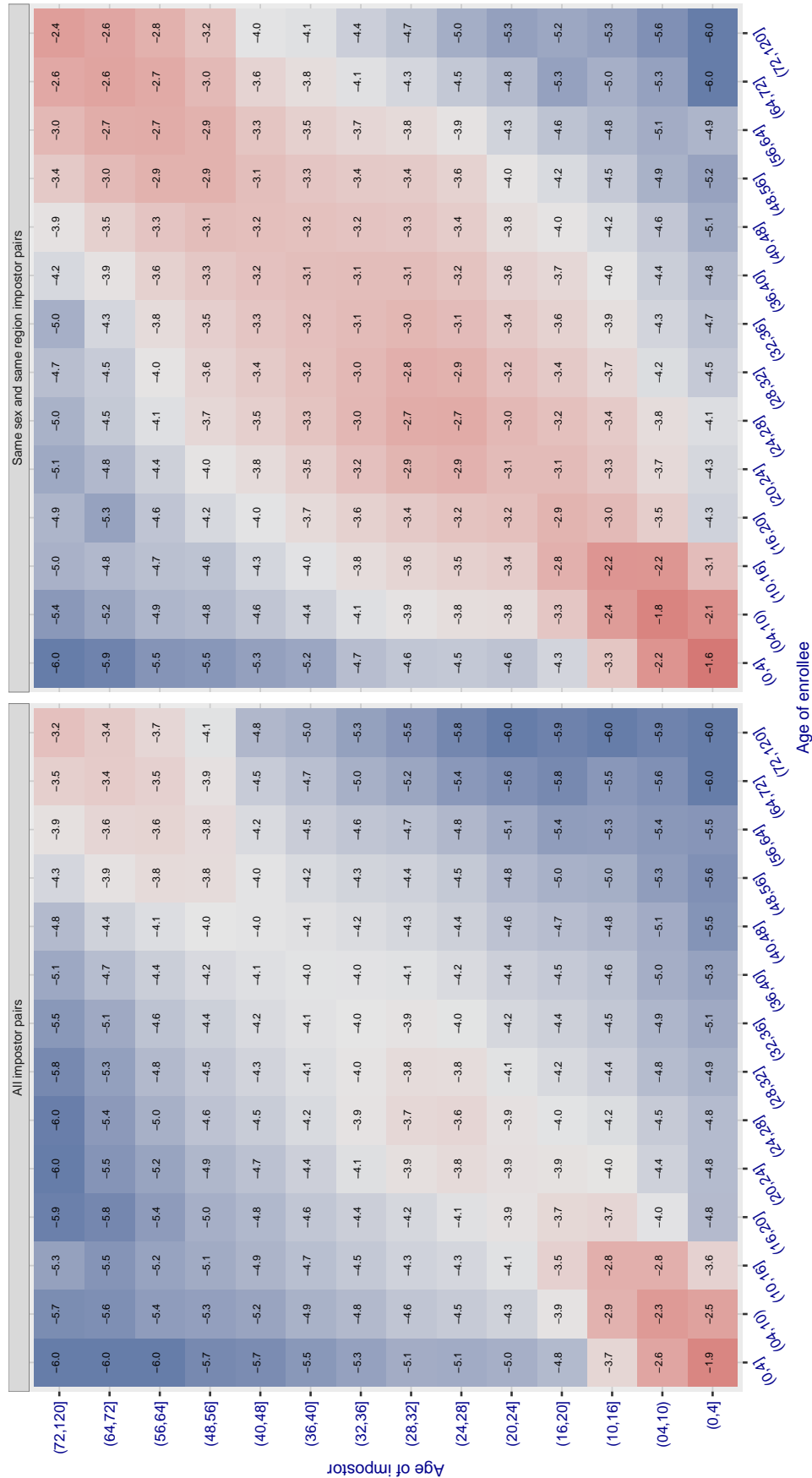


Figure 513: For algorithm `cognitec-000` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.



Cross age FMR at threshold  $T = 0.565$  for algorithm `cognitec_001`, giving  $FMR(T) = 0.0001$  globally.

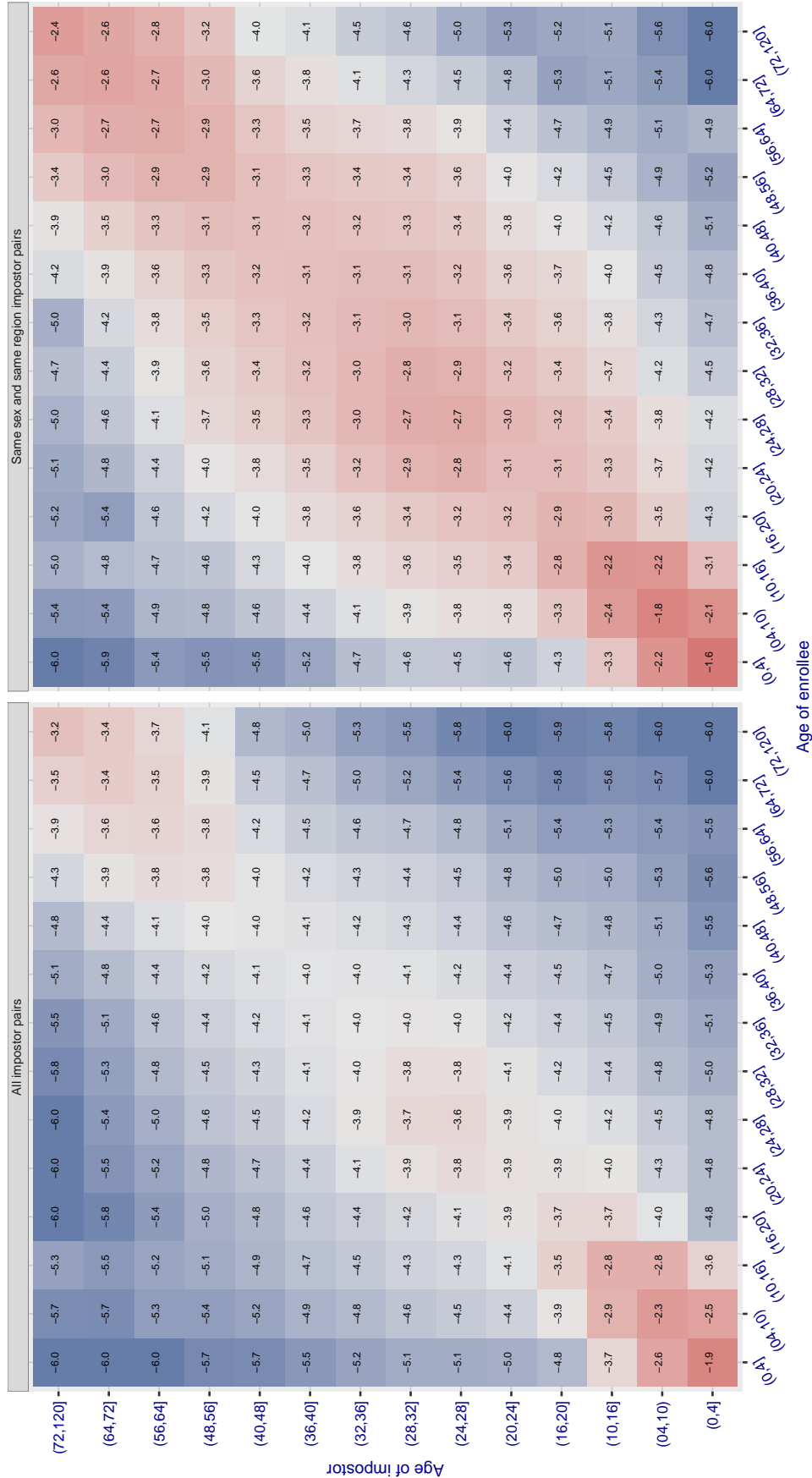


Figure 514: For algorithm `cognitec-001` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

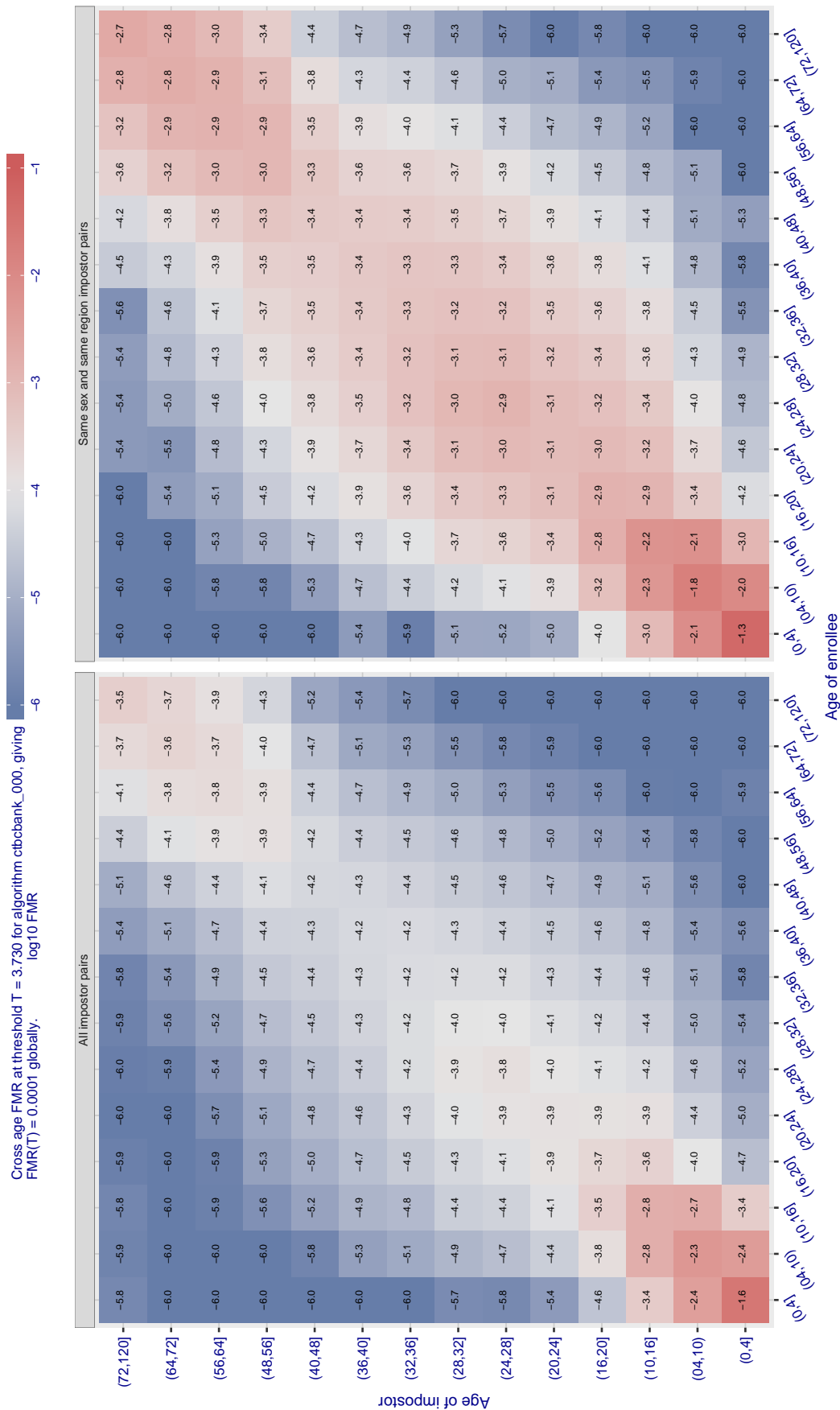


Figure 515: For algorithm ctbcbank-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.



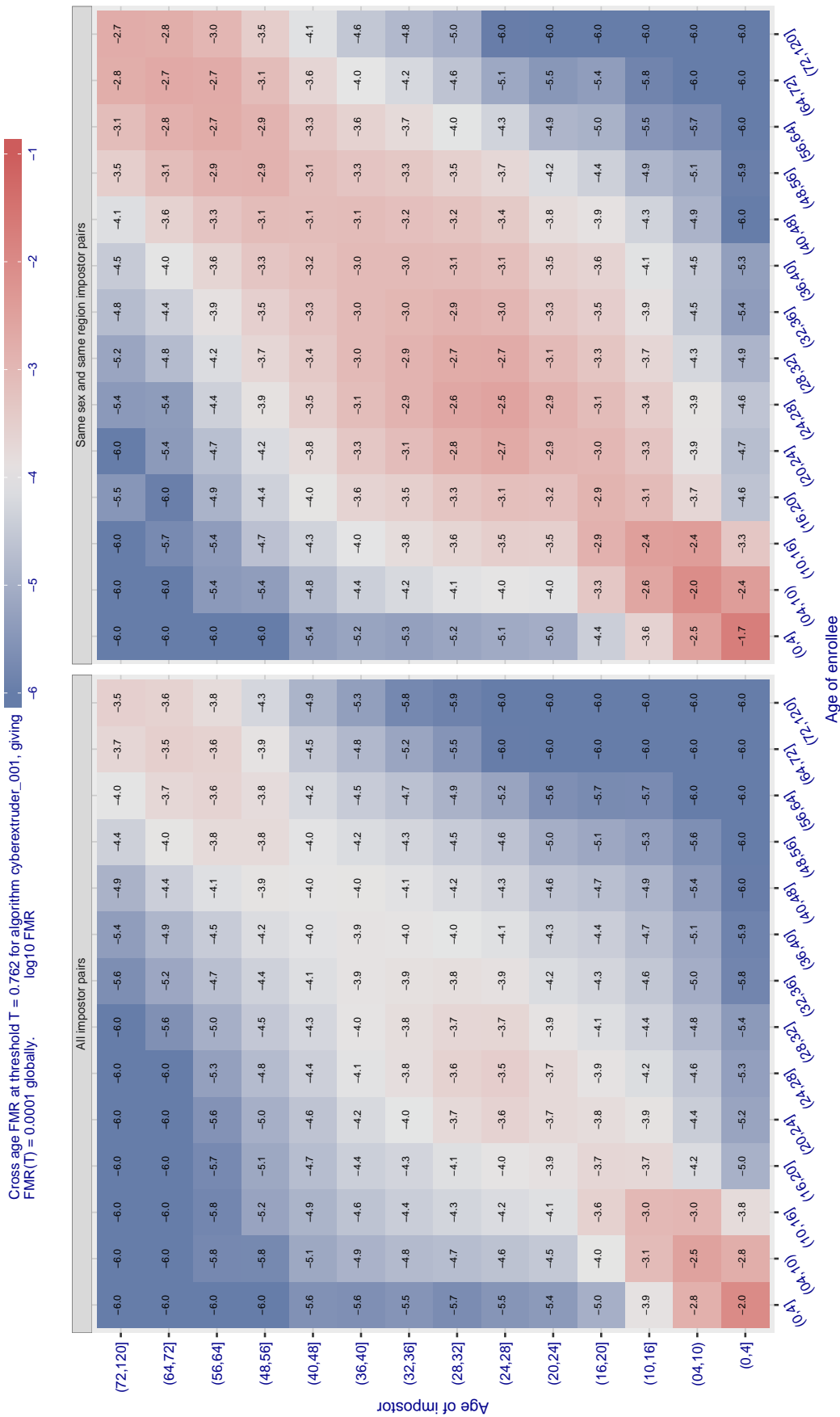


Figure 517: For algorithm cybertruder-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

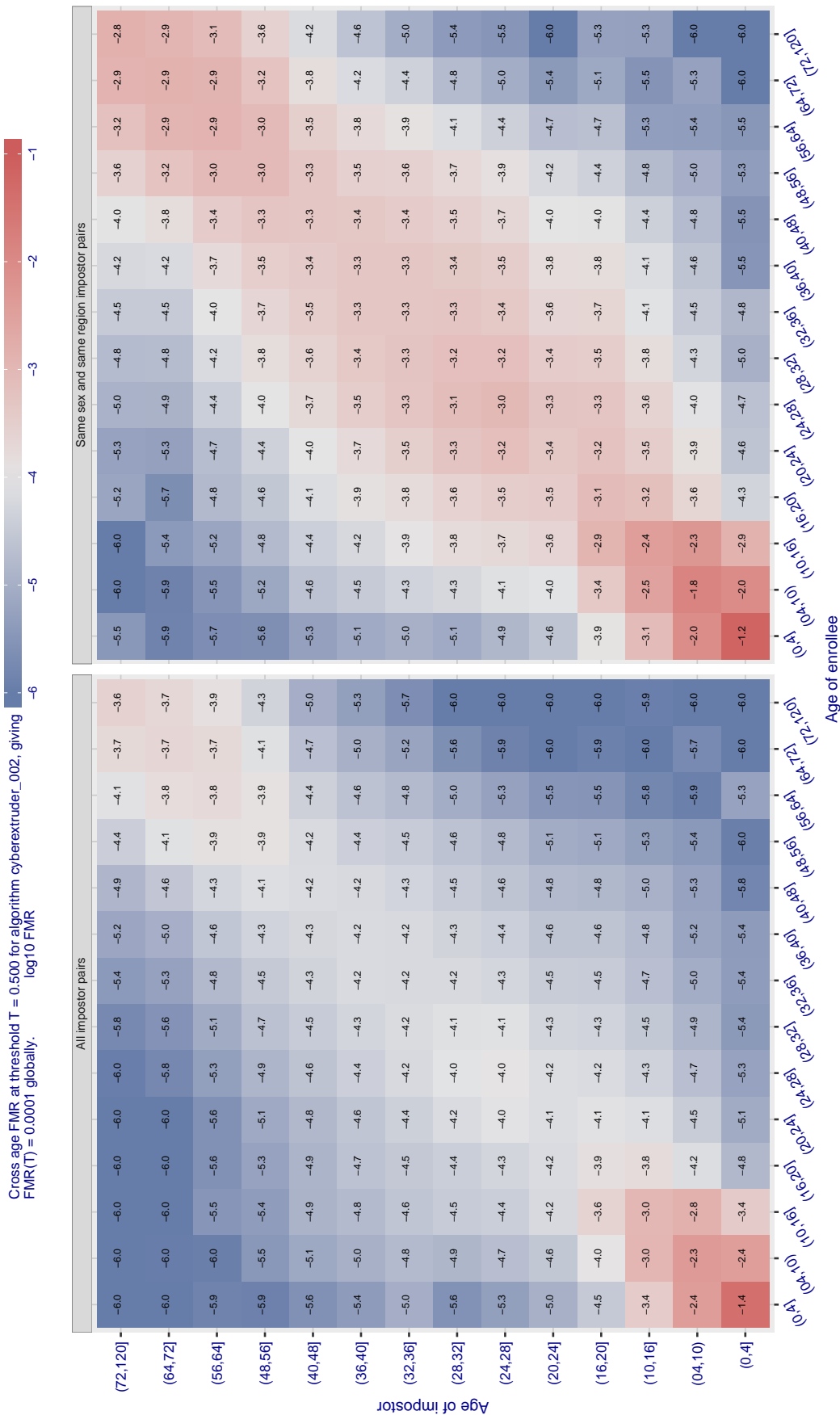


Figure 518: For algorithm cyberextruder-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

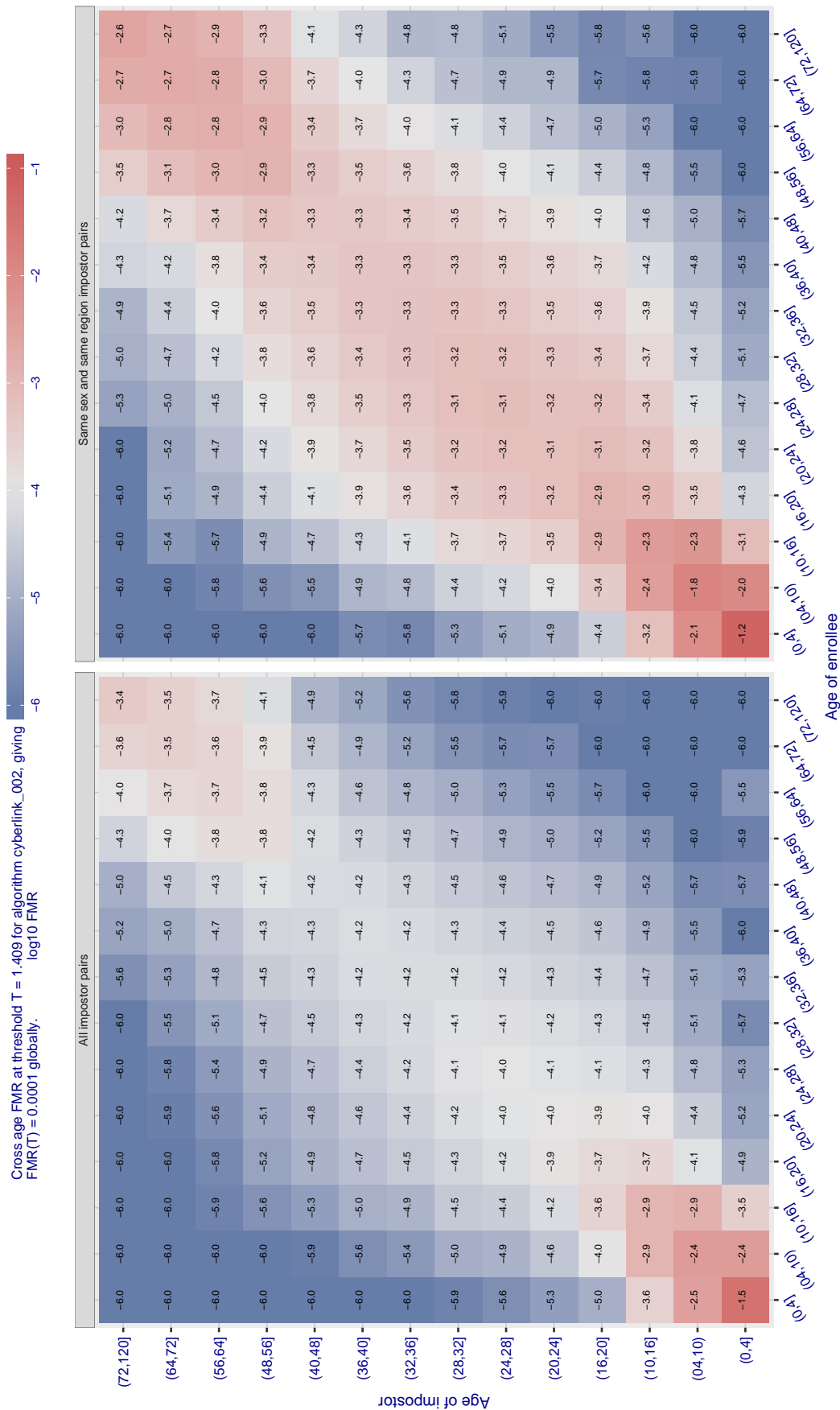


Figure 519: For algorithm cyberlink-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

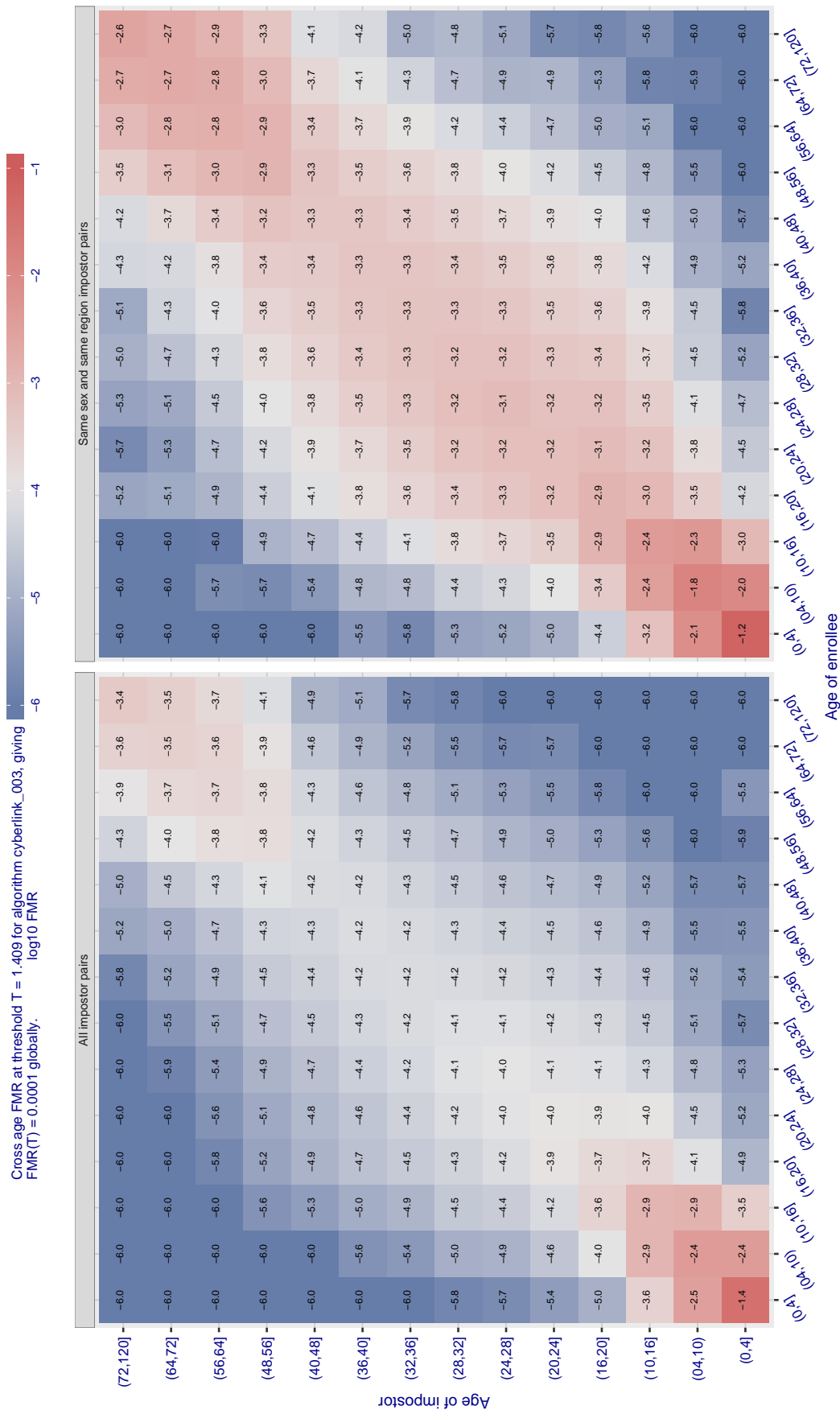


Figure 520: For algorithm cyberlink-003 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.



Cross age FMR at threshold  $T = 6696.000$  for algorithm dahua\_002, giving  $FMR(T) = 0.0001$  globally.

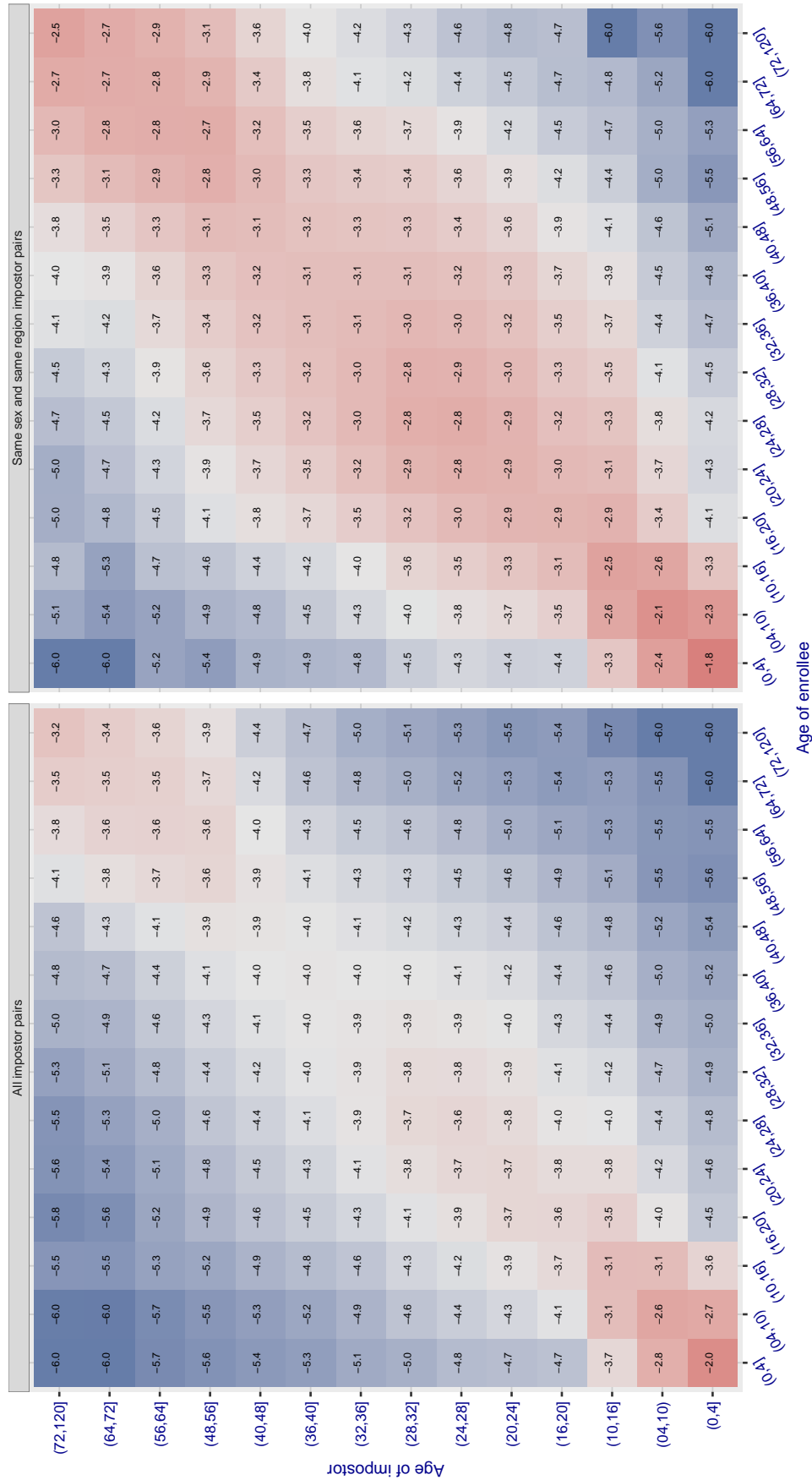


Figure 521: For algorithm dahua-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 6034.000$  for algorithm dahua\_003, giving  $FMR(T) = 0.0001$  globally.

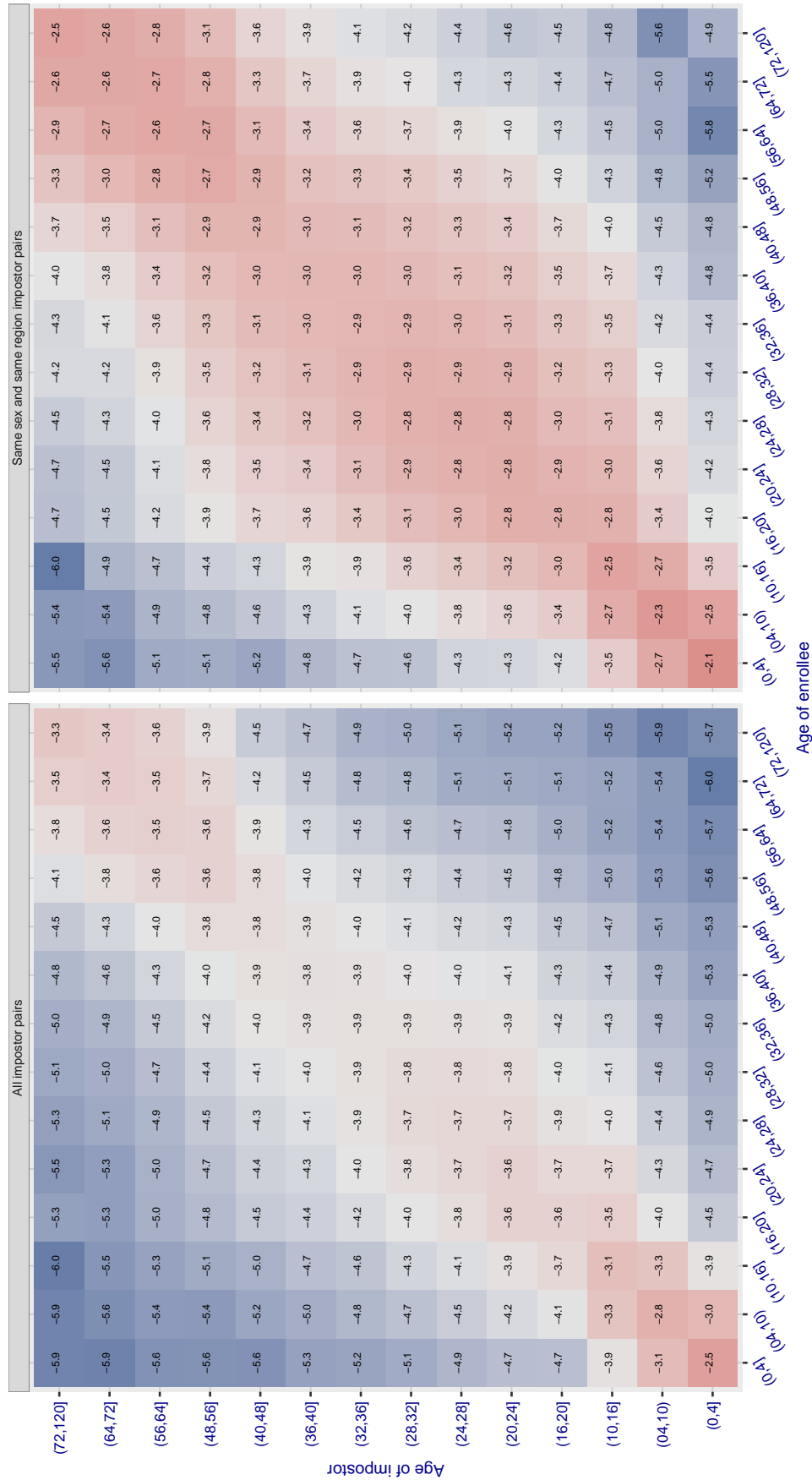


Figure 522: For algorithm dahua-003 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

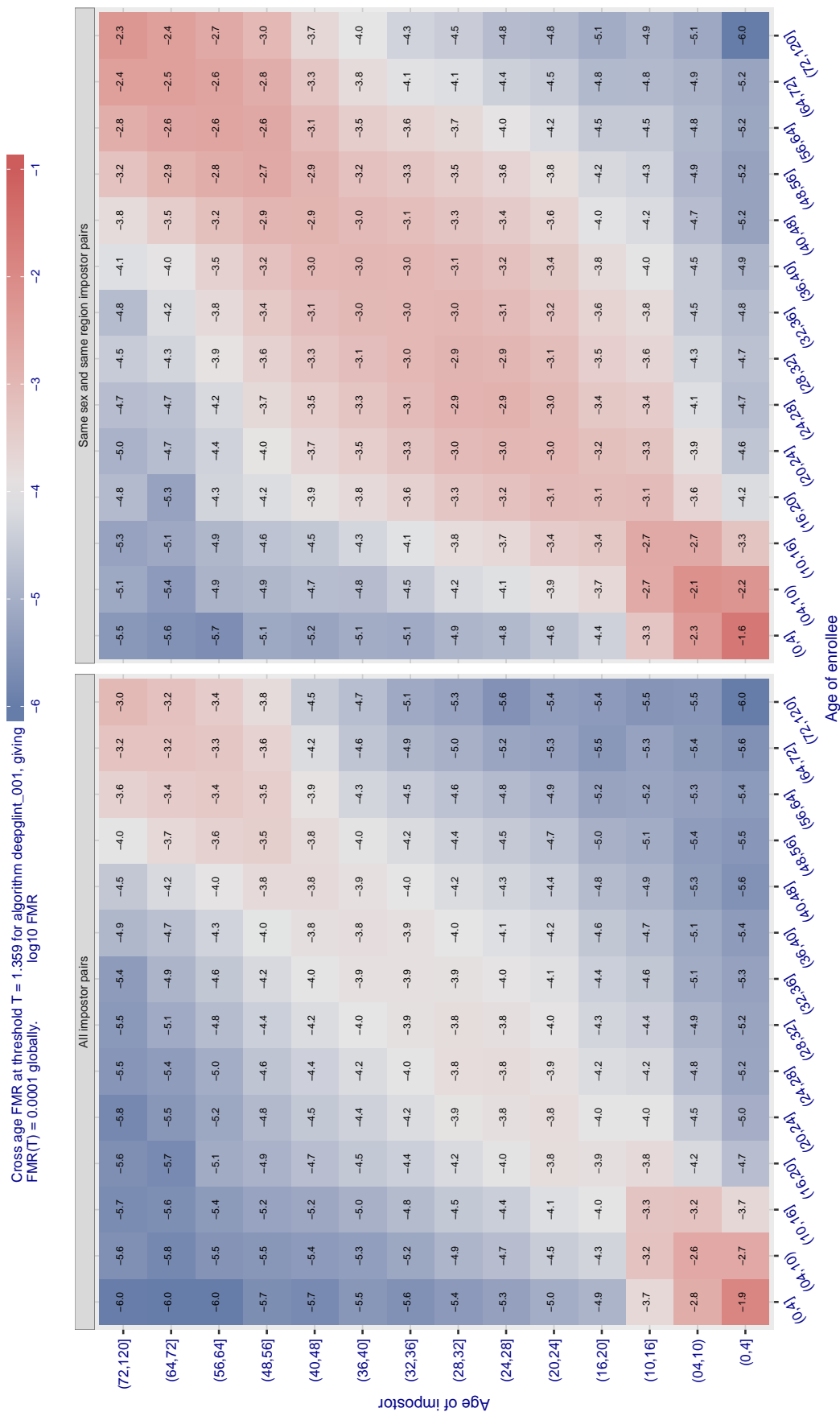


Figure 523: For algorithm deepglint-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

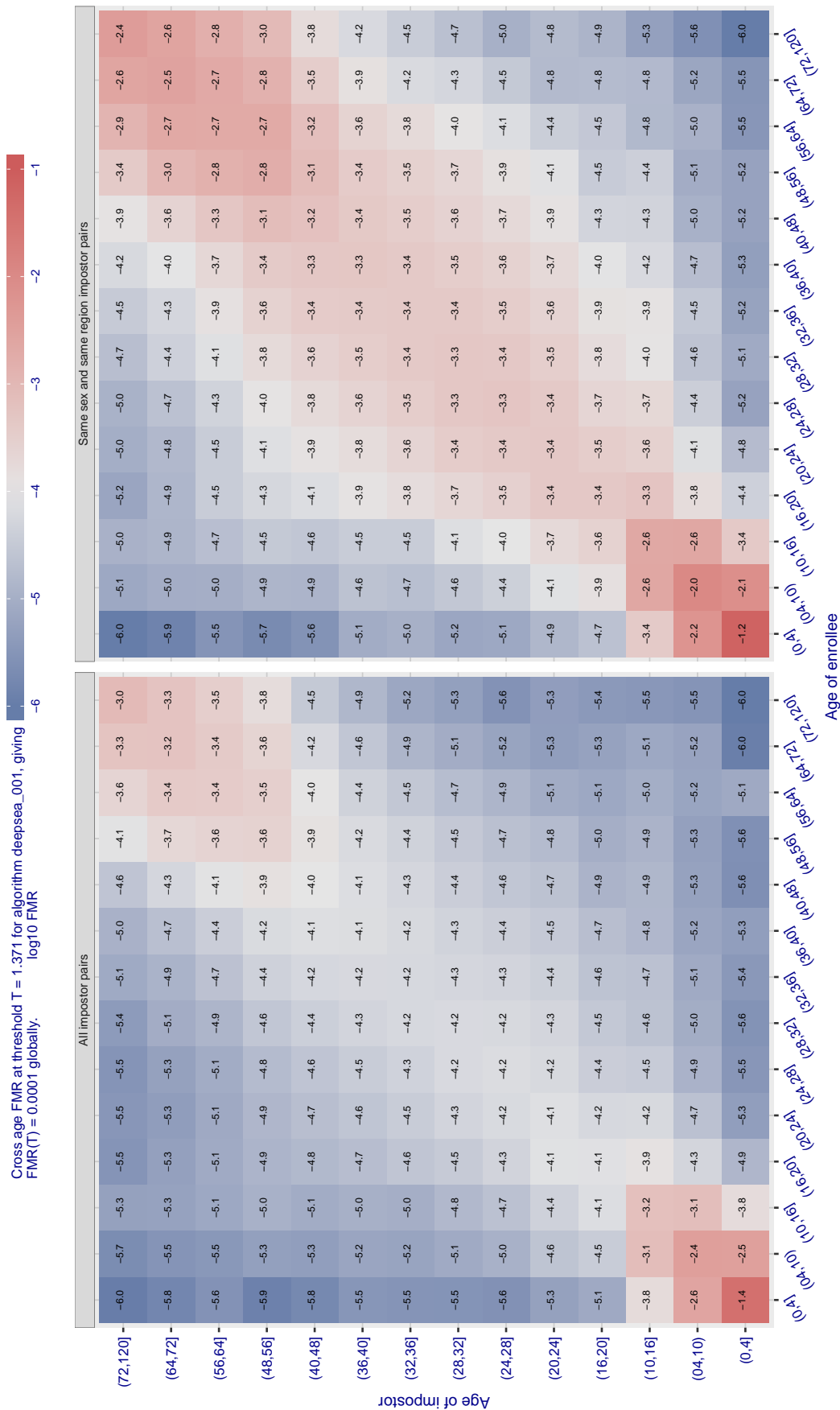


Figure 524: For algorithm deepsea-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

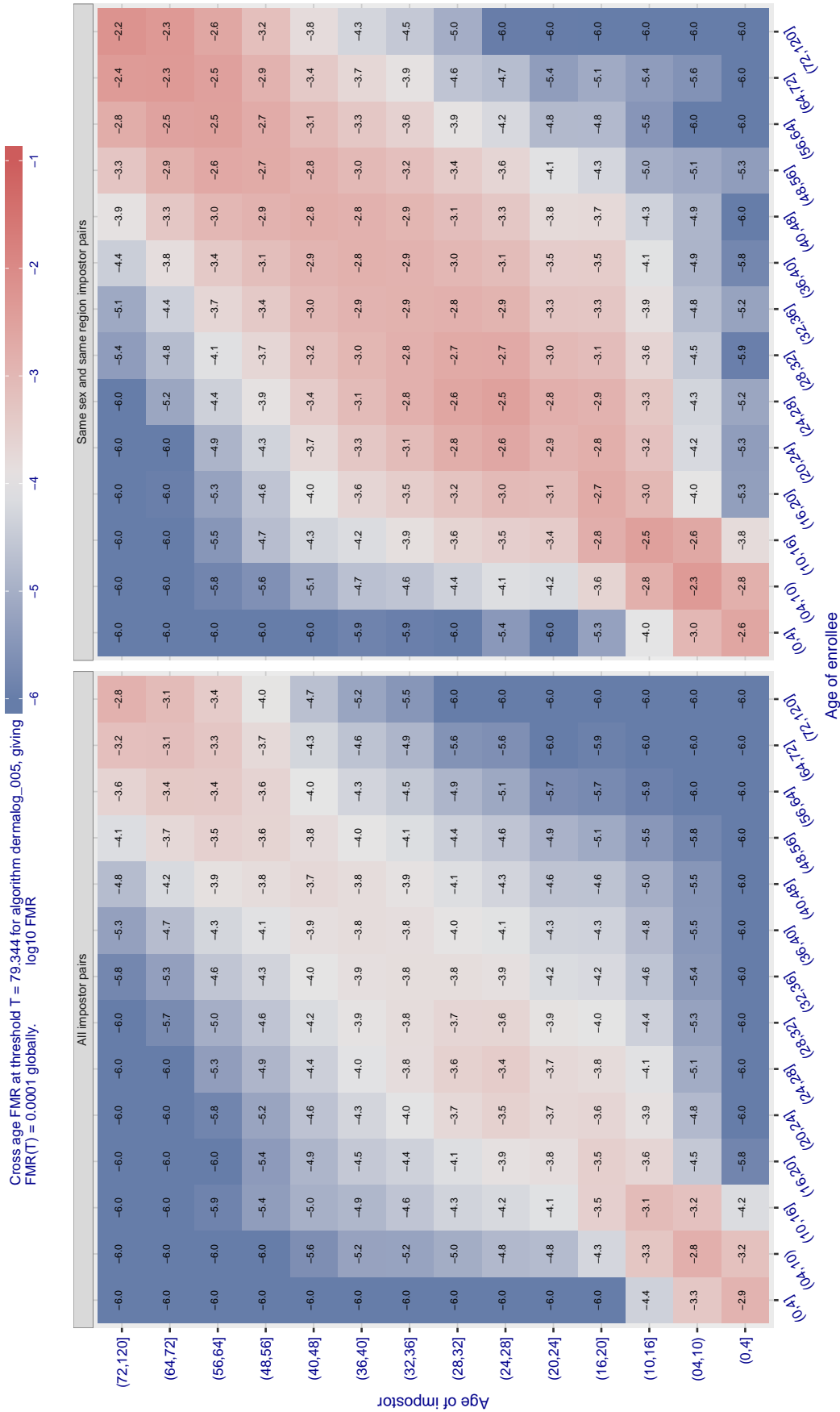


Figure 525: For algorithm dermalog-005 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

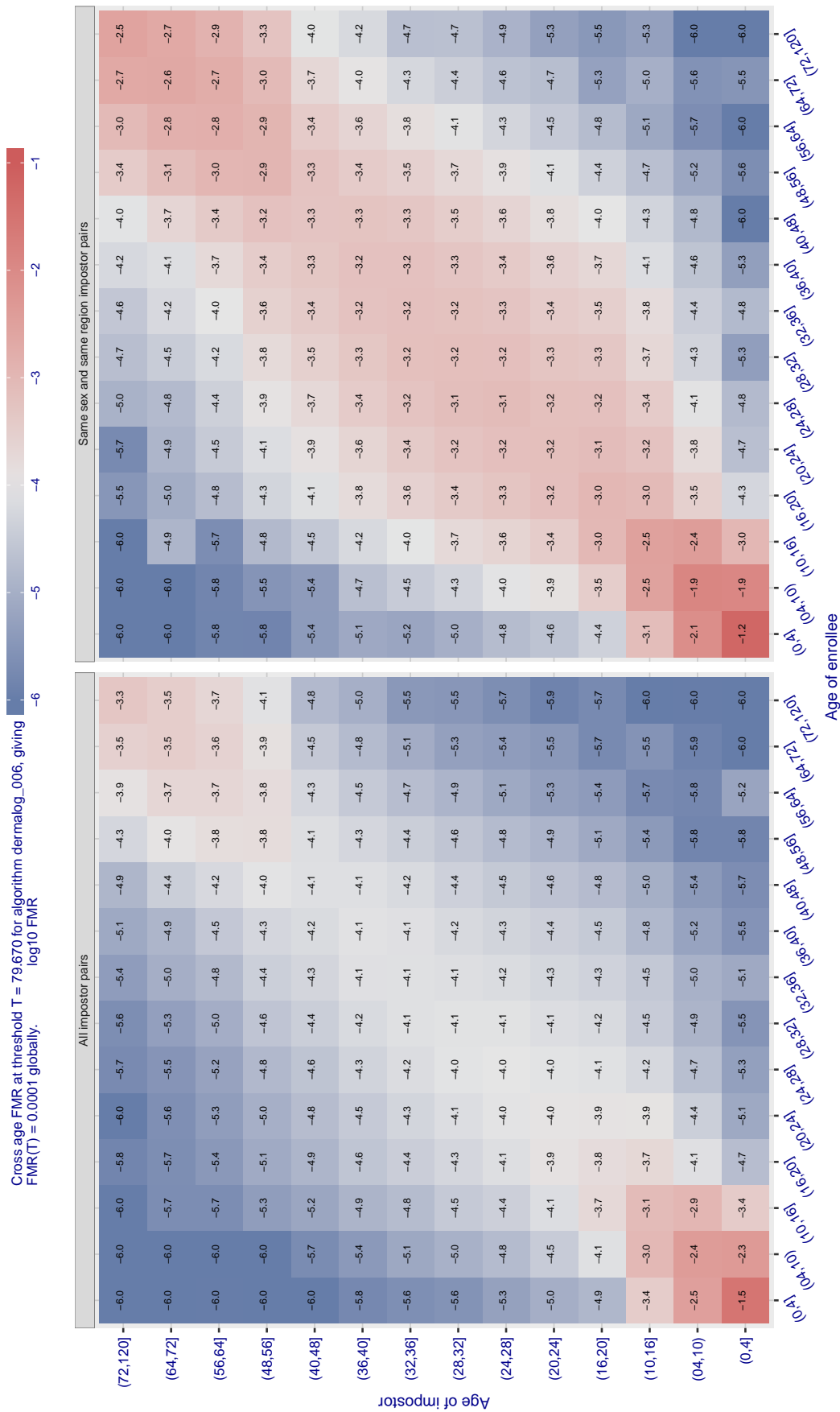


Figure 526: For algorithm dermalog-006 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

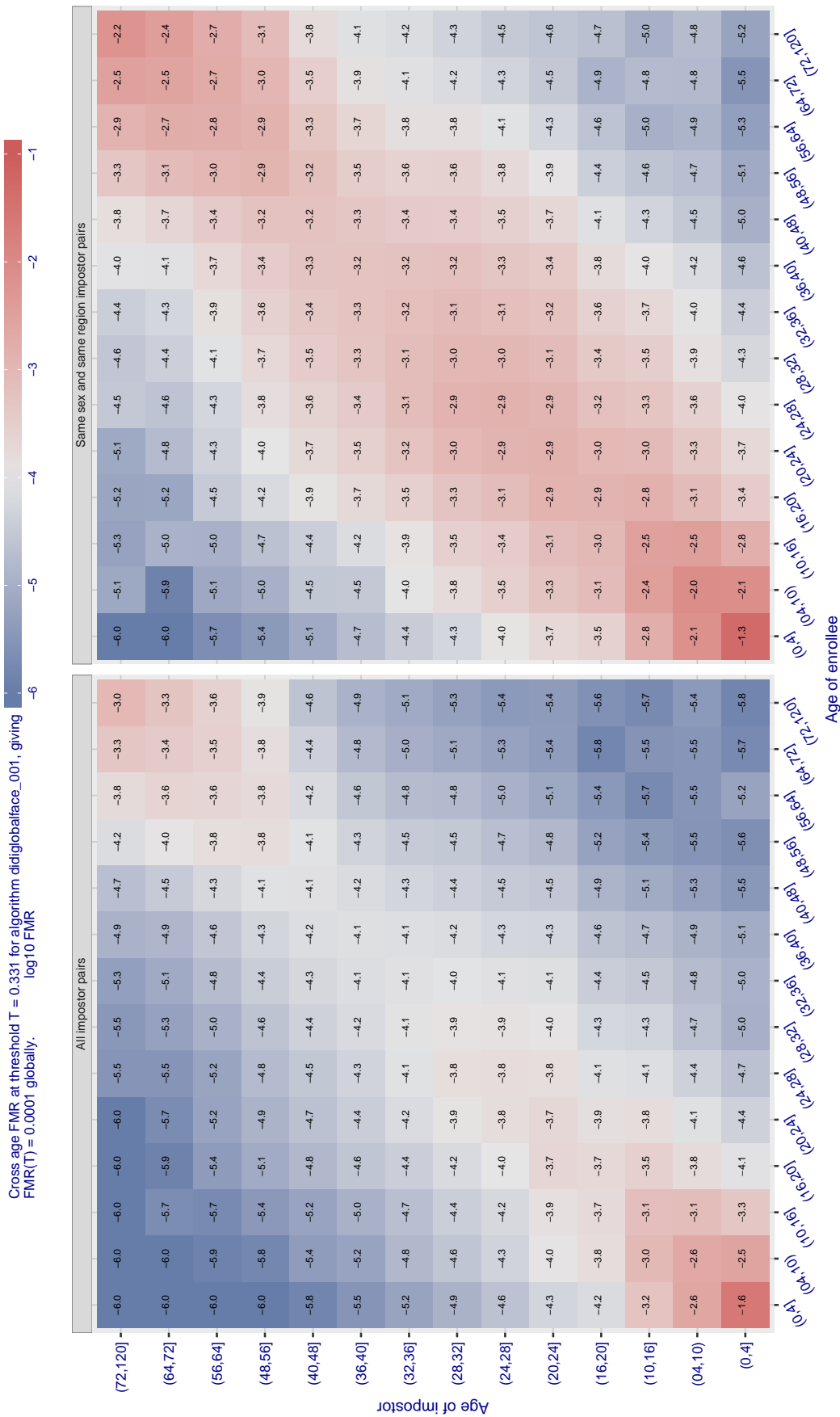


Figure 527: For algorithm didiglobface-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.



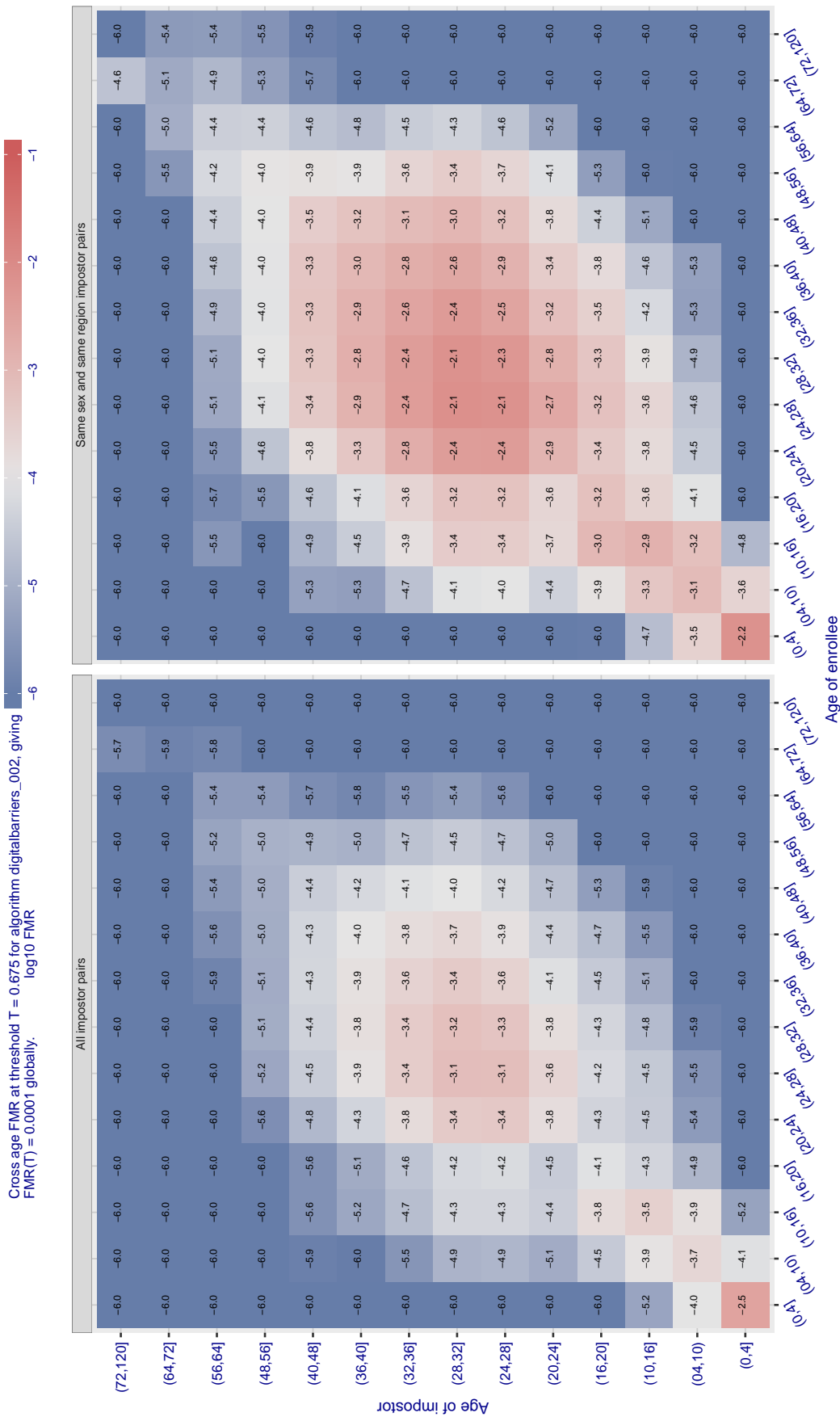


Figure 528: For algorithm digitalbarriers-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

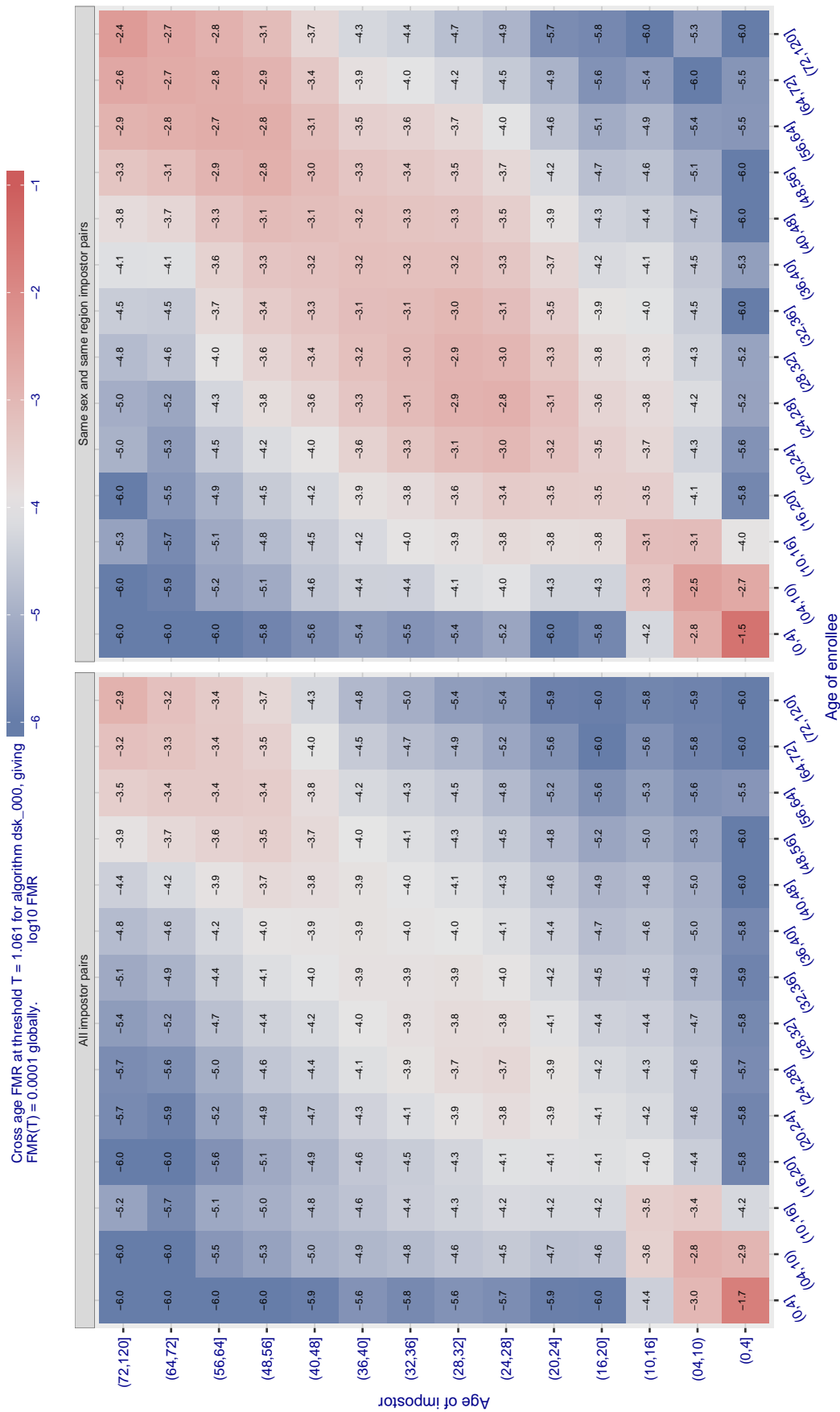


Figure 529: For algorithm `dsk-000` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

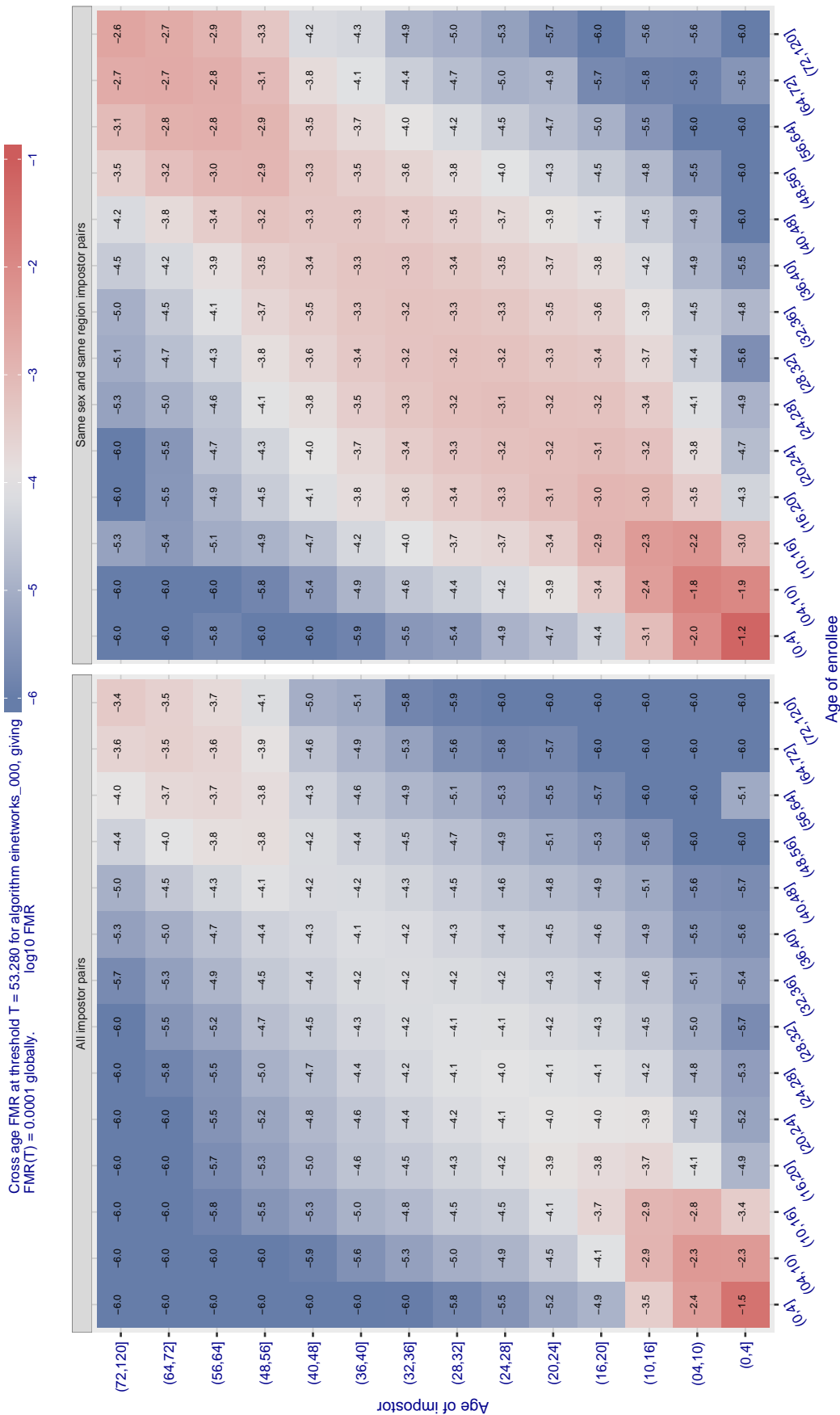


Figure 530: For algorithm einetworks-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

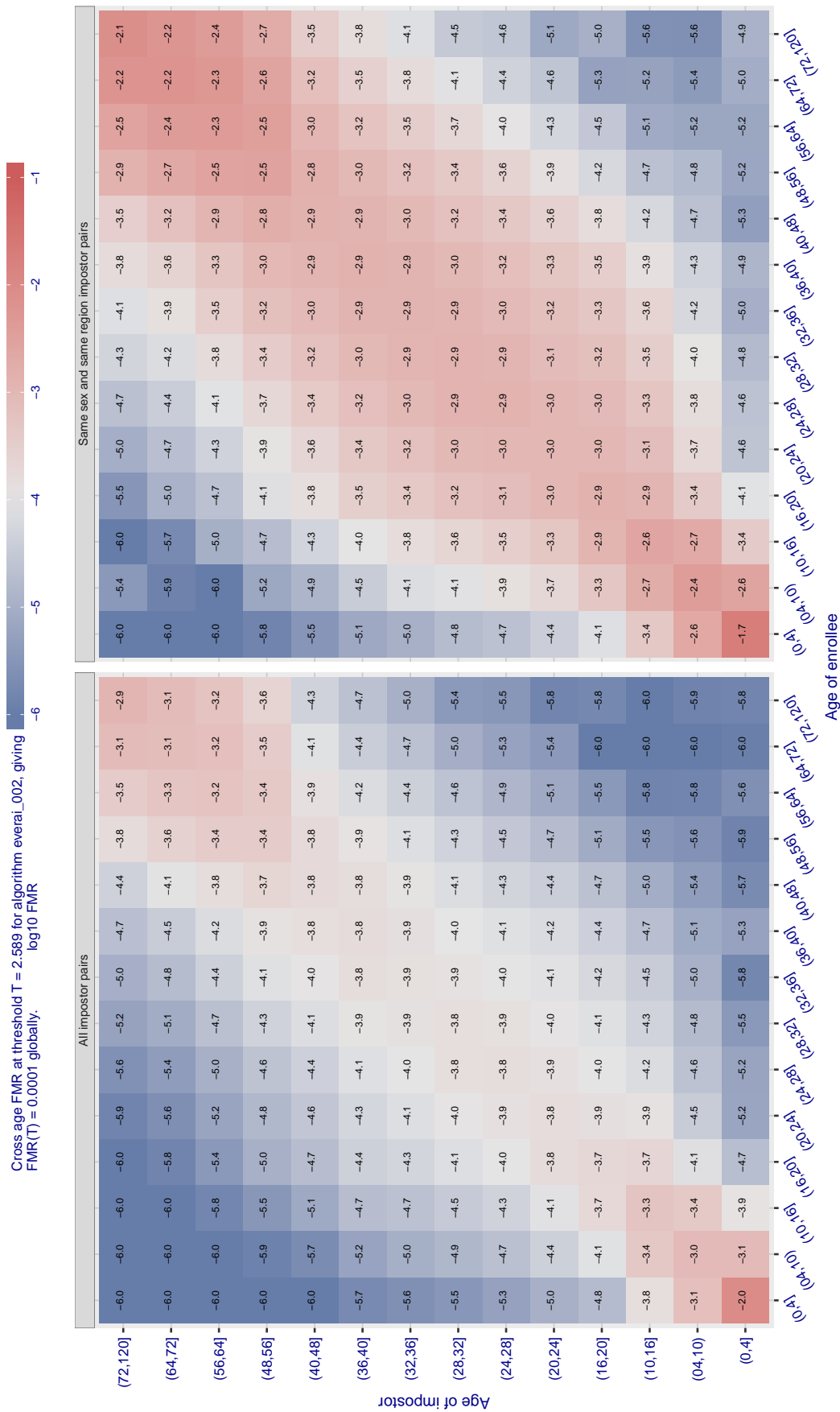


Figure 531: For algorithm everai-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.



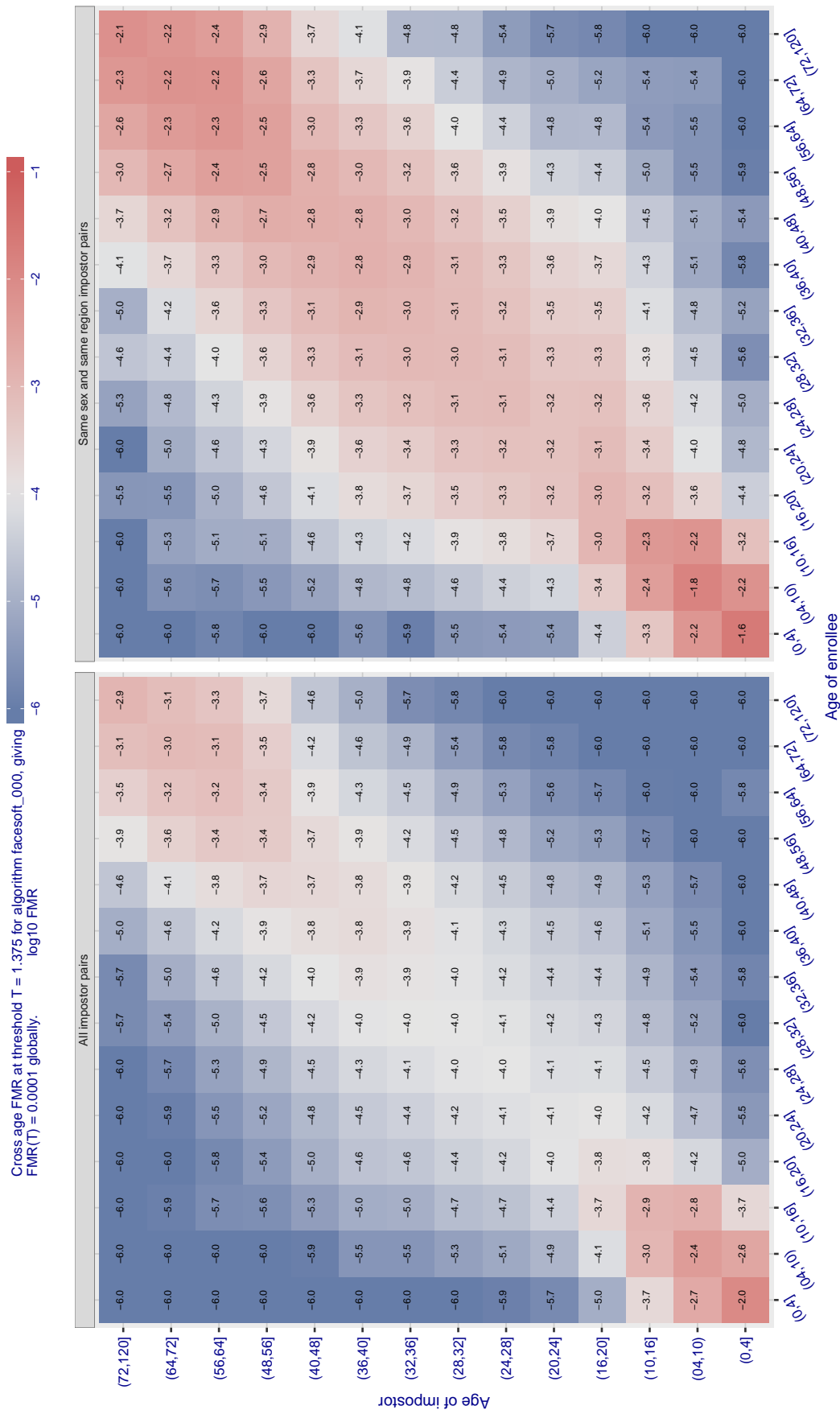


Figure 533: For algorithm facesoft-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

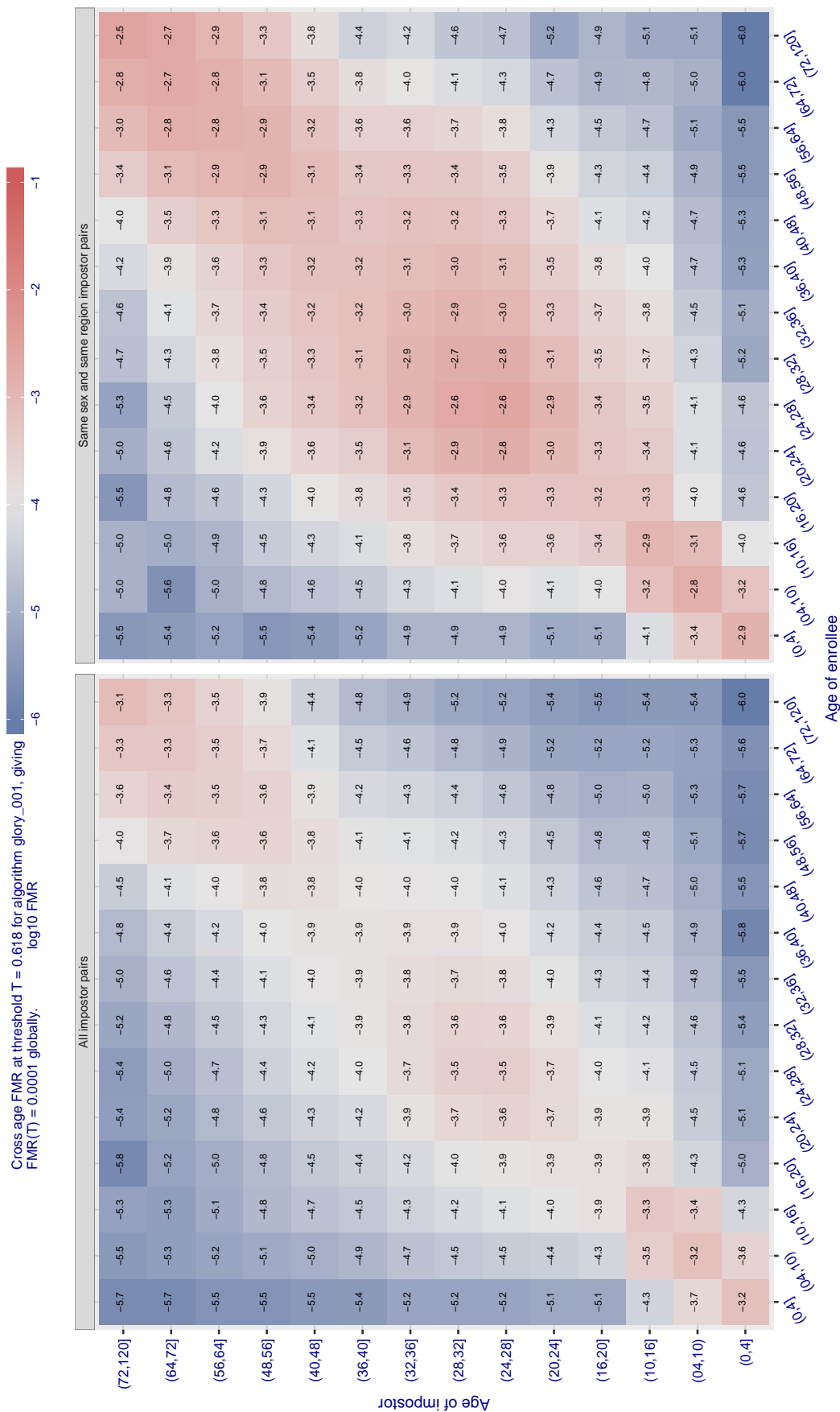


Figure 534: For algorithm glory-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.



Cross age FMR at threshold  $T = 0.454$  for algorithm gorilla\_003, giving  $FMR(T) = 0.0001$  globally.

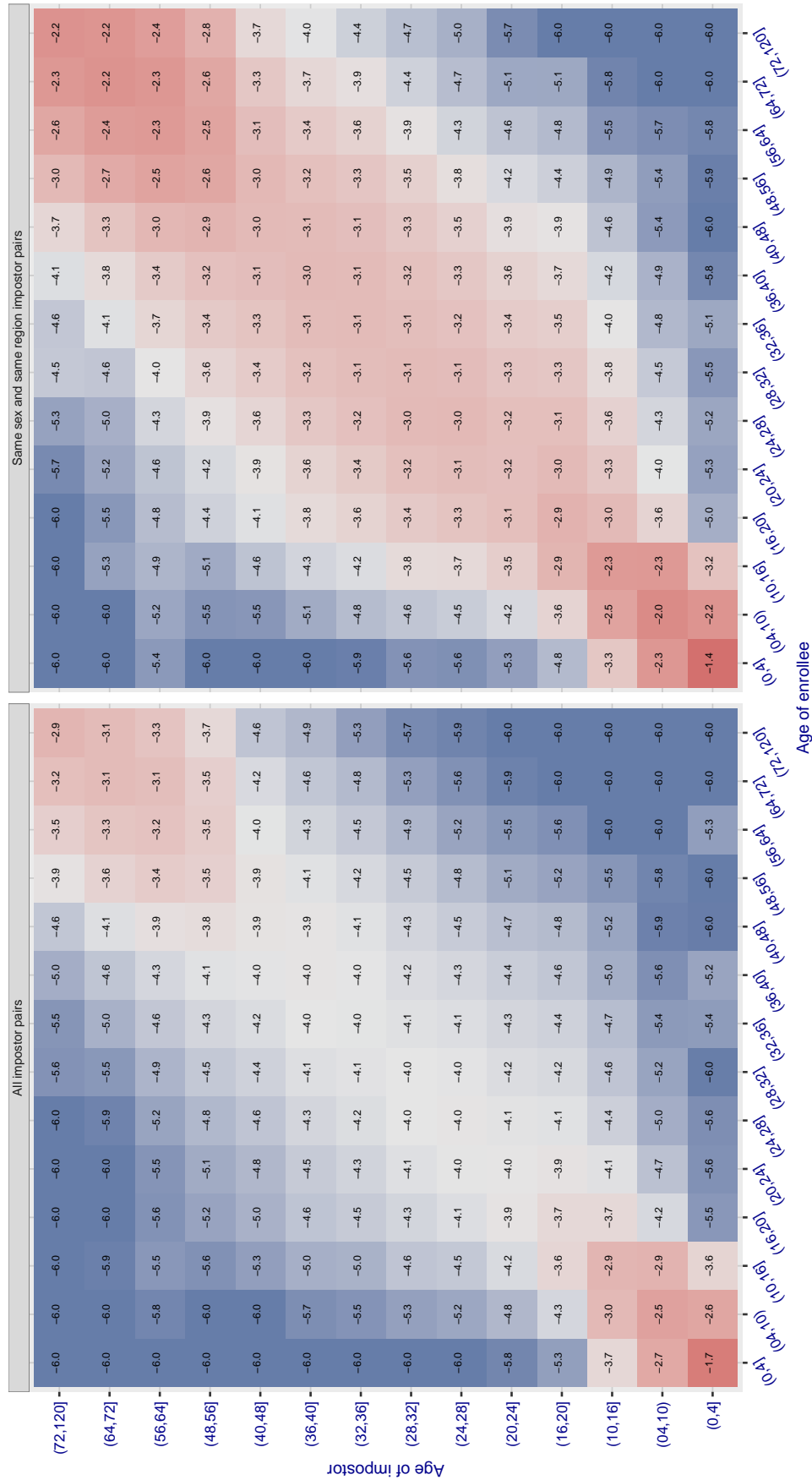


Figure 535: For algorithm gorilla-003 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

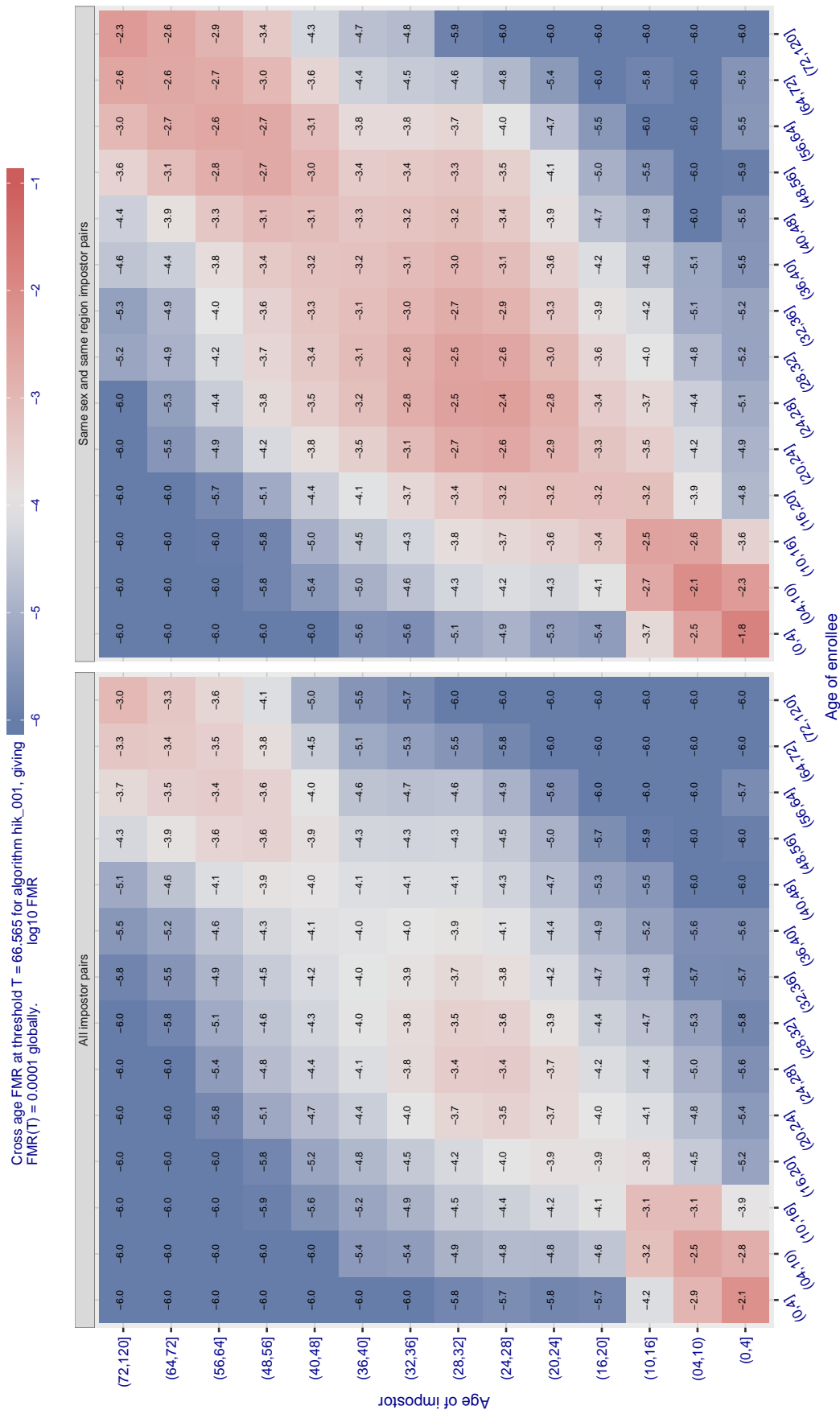


Figure 536: For algorithm hik-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

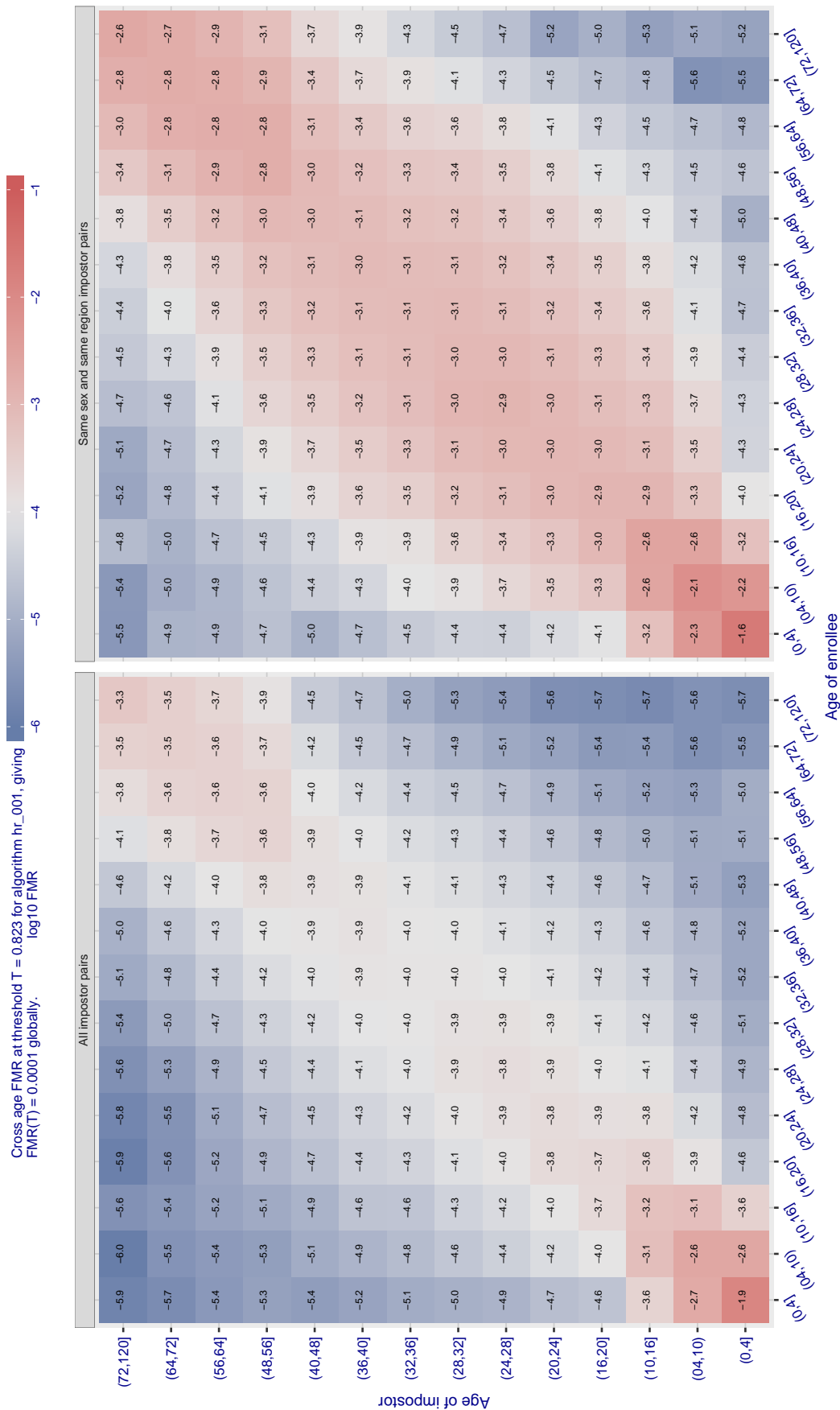


Figure 537: For algorithm hr-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

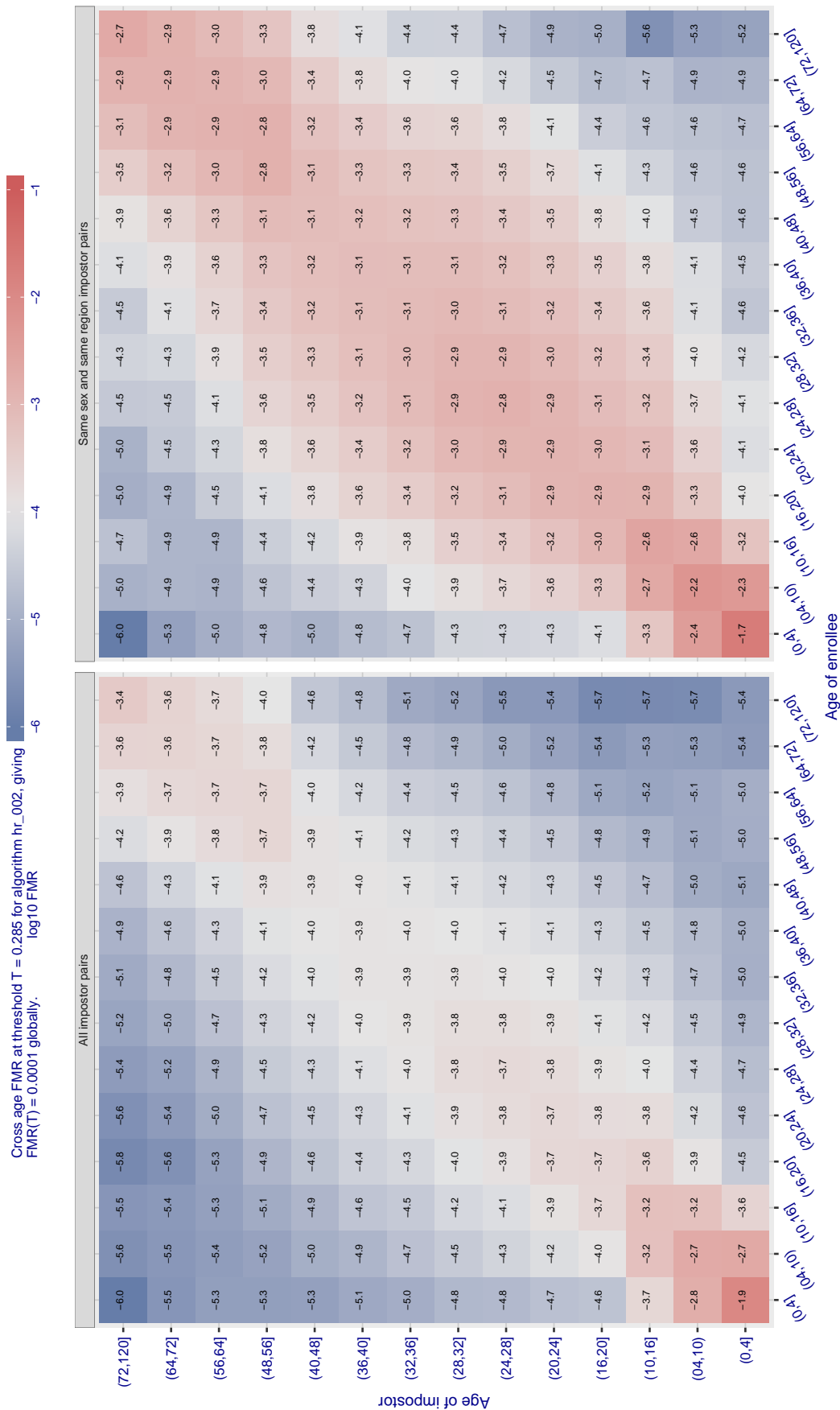


Figure 538: For algorithm hr-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

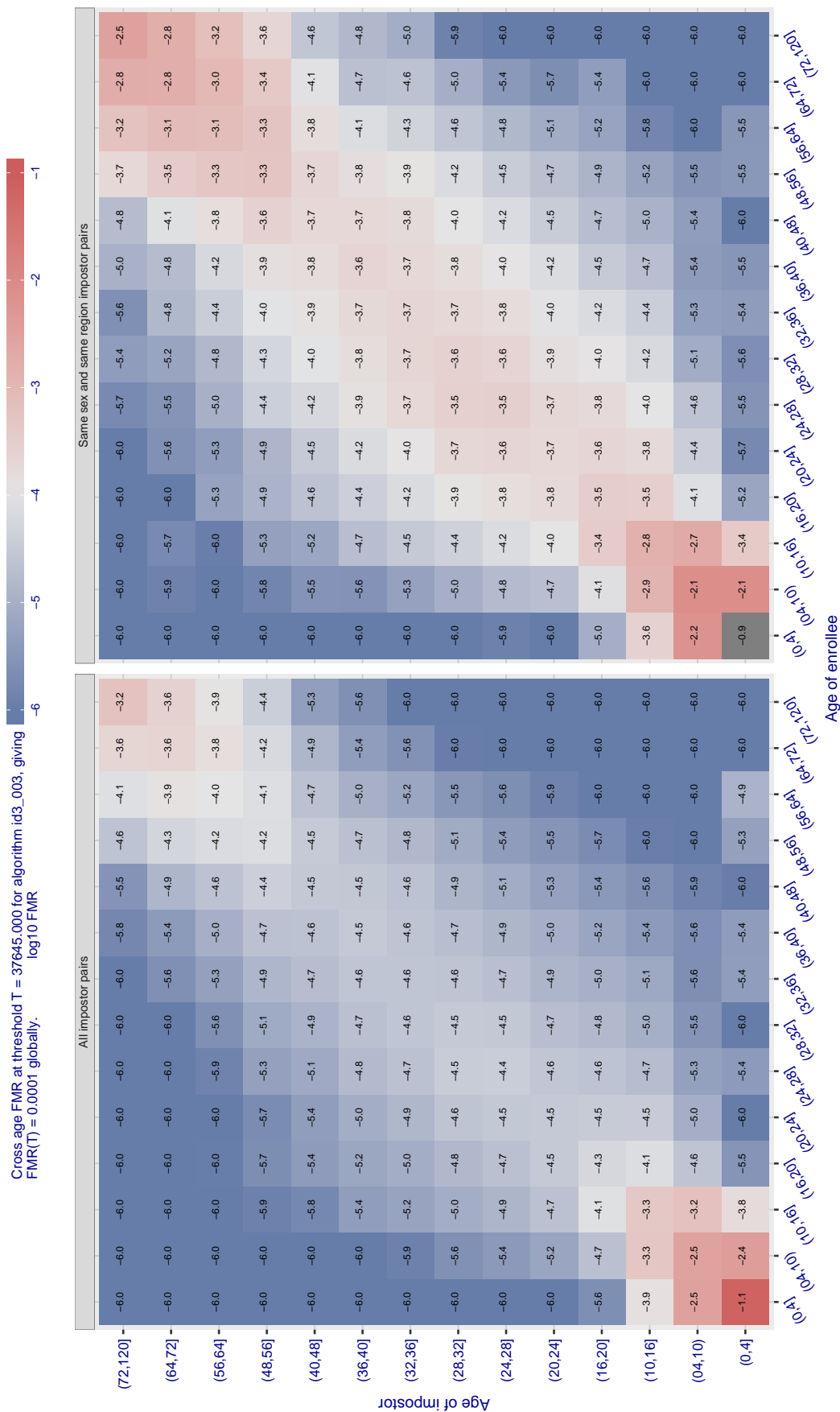


Figure 539: For algorithm id3-003 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

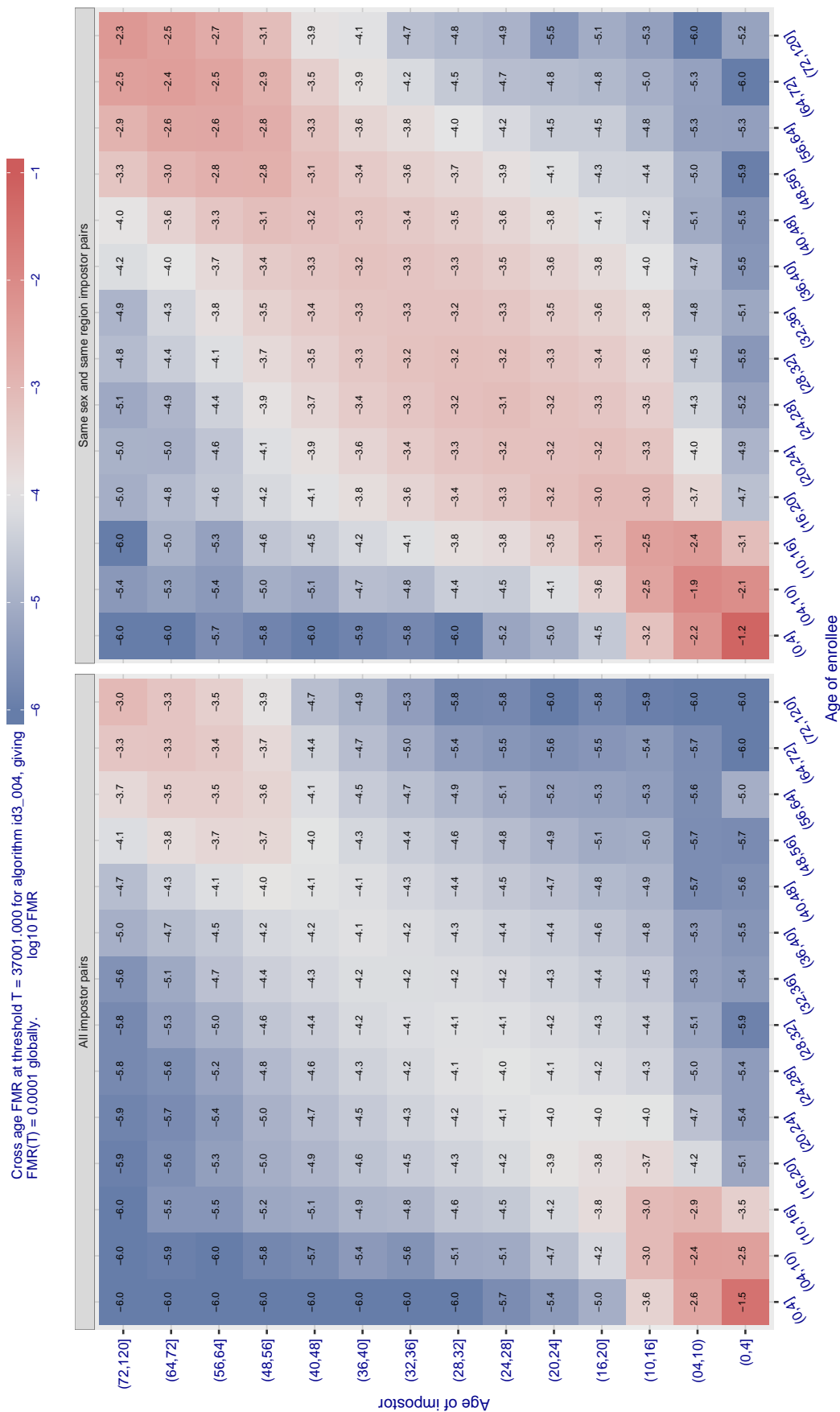


Figure 540: For algorithm `id3-004` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

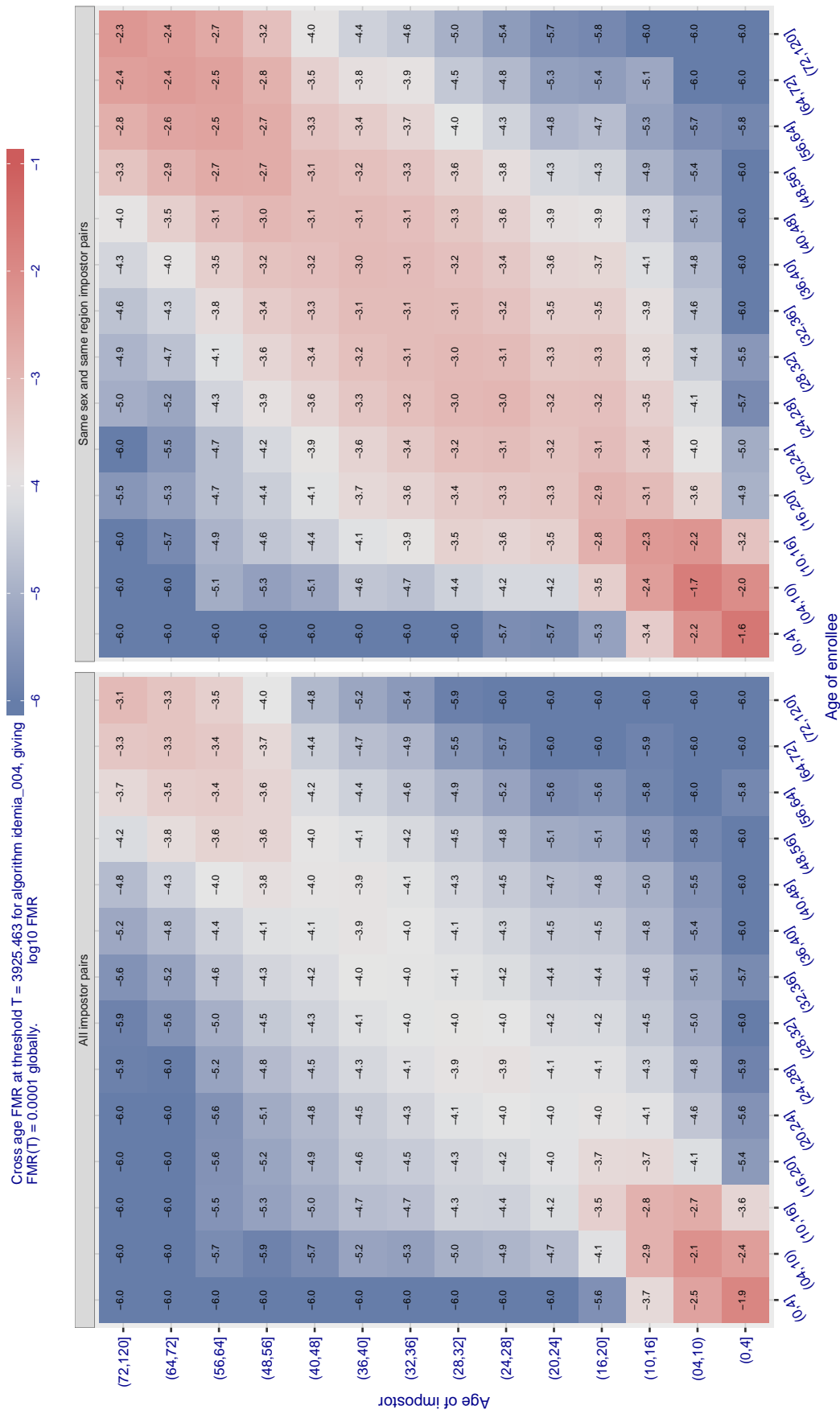


Figure 541: For algorithm idemia-004 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

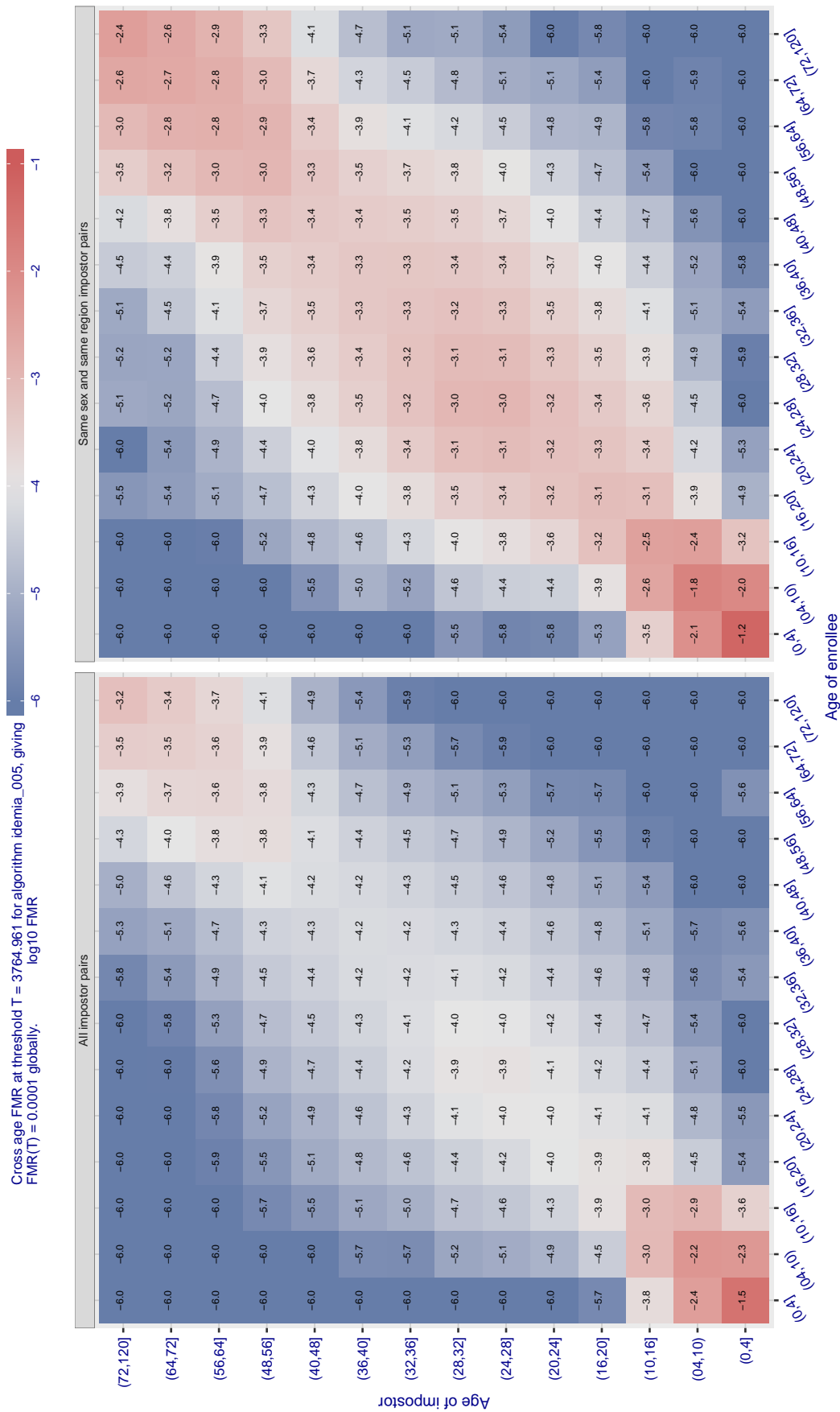


Figure 542: For algorithm idemia-005 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.



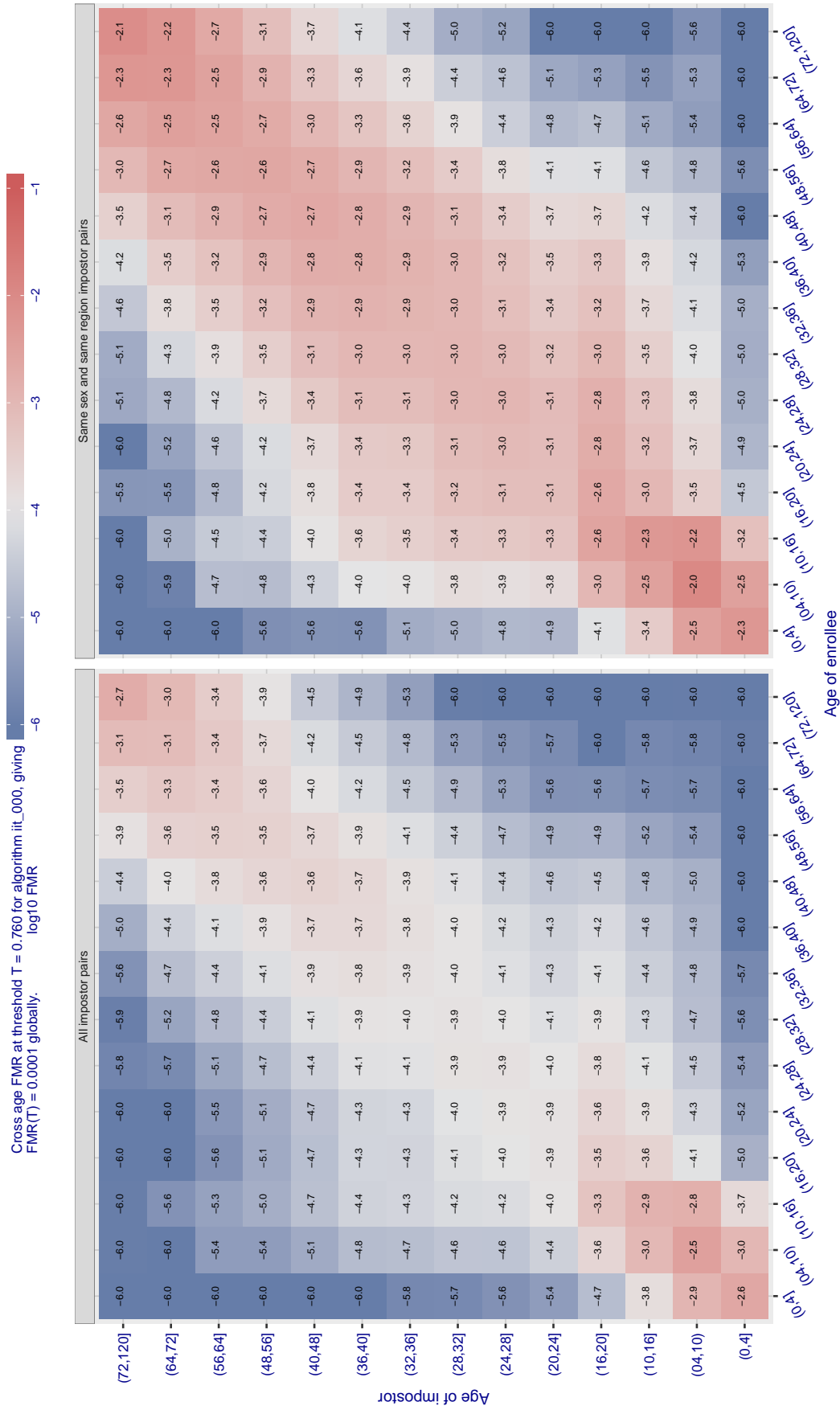


Figure 543: For algorithm  $it_{000}$  operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

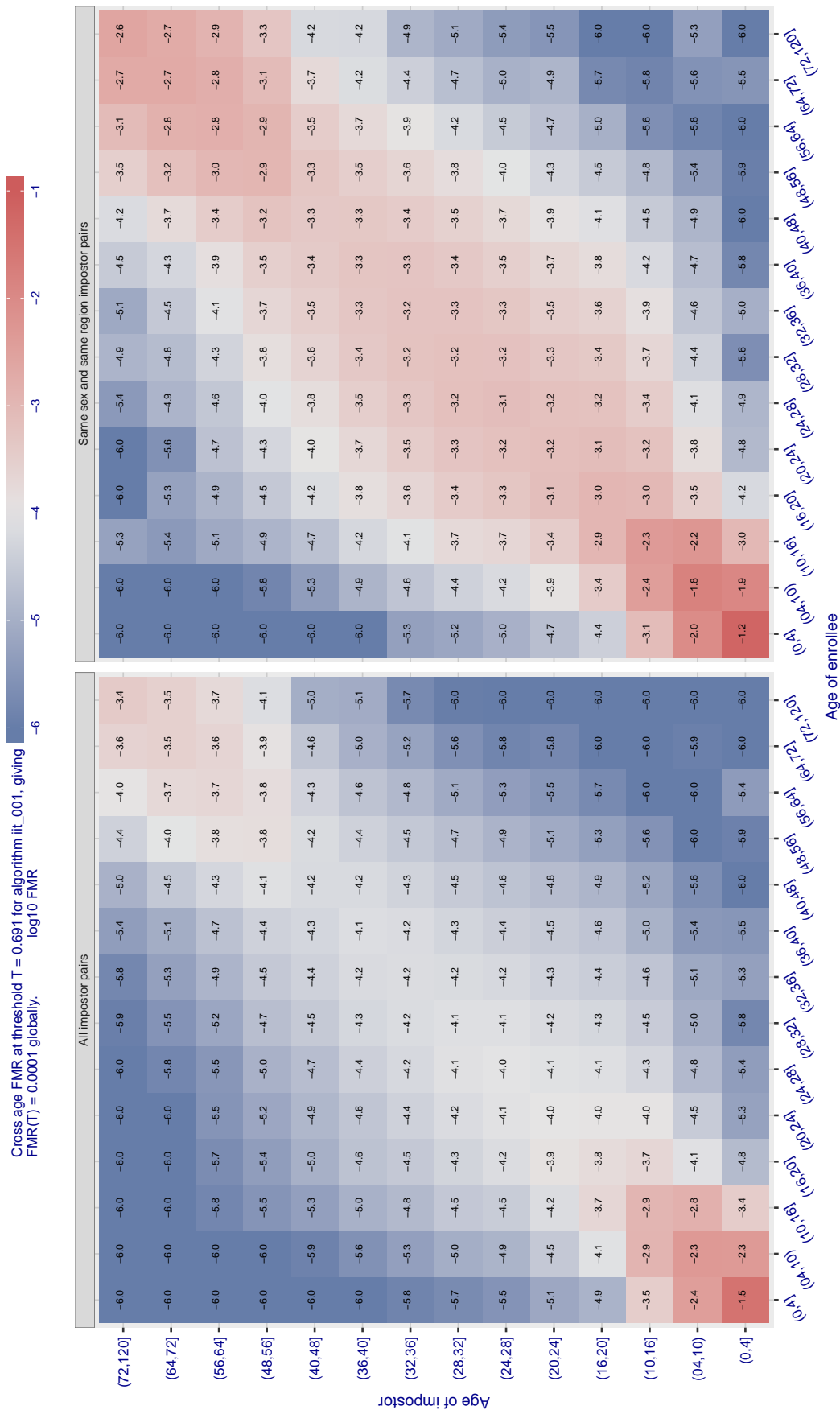


Figure 544: For algorithm `it_001` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

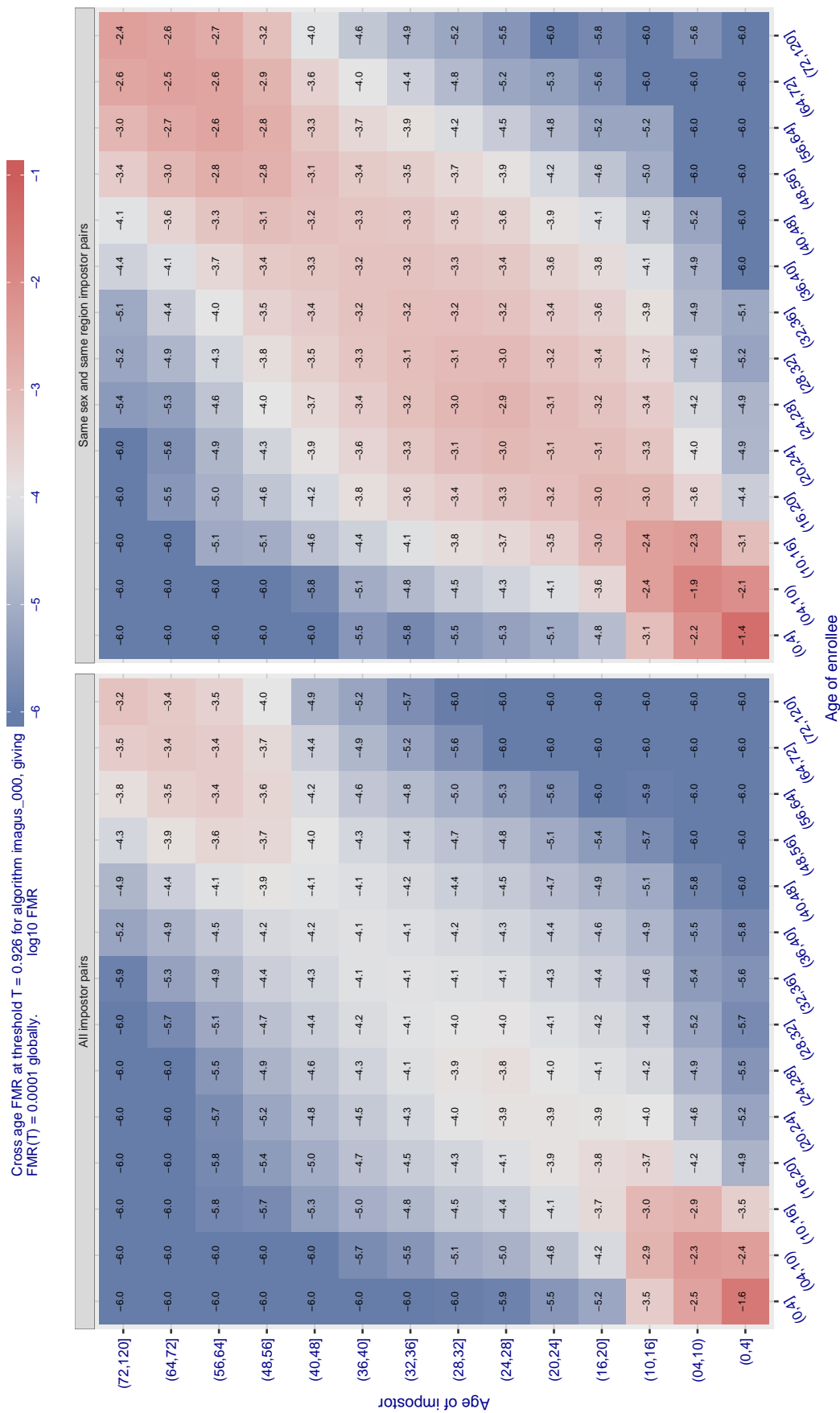


Figure 545: For algorithm `imagus-000` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

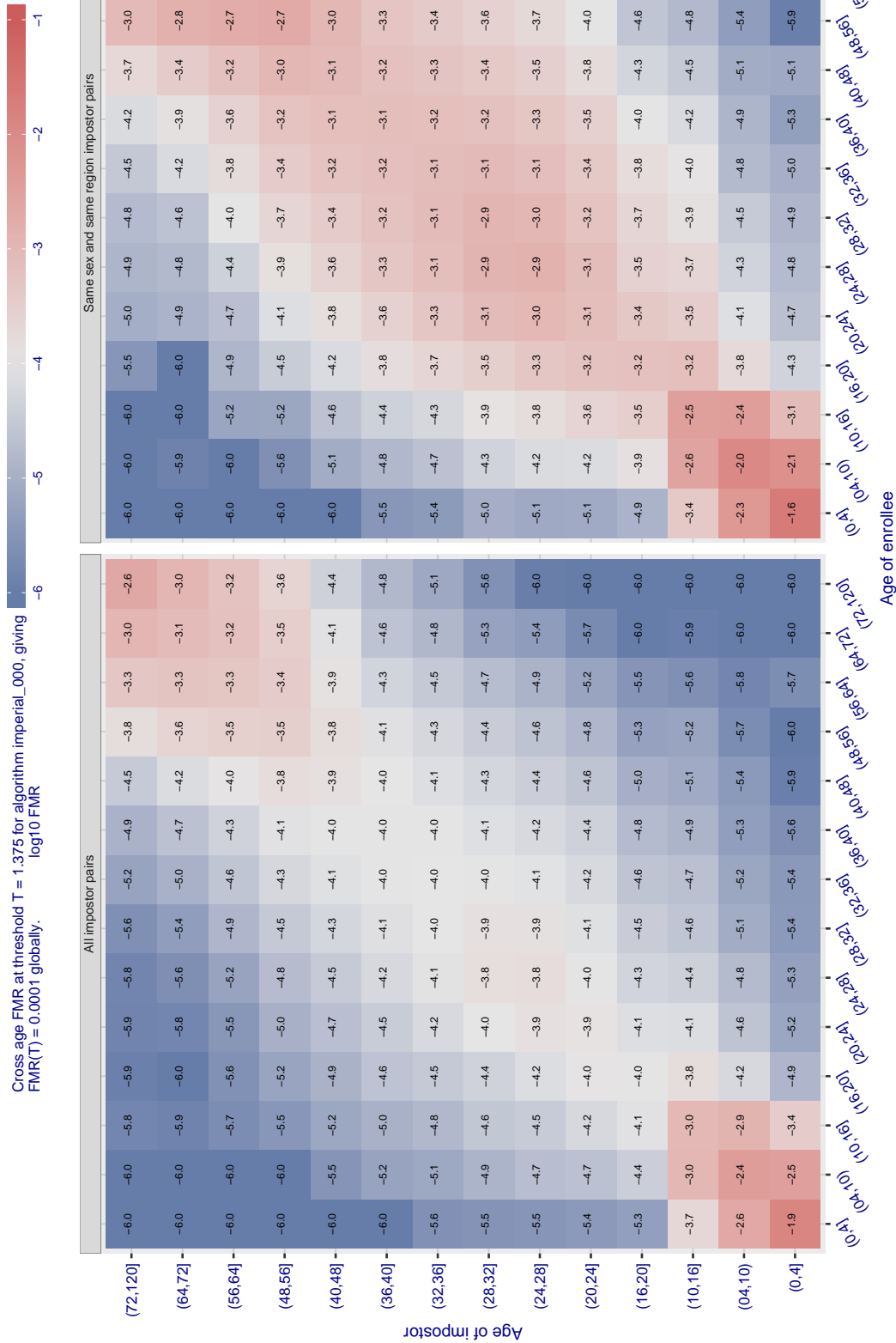


Figure 546: For algorithm imperial-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

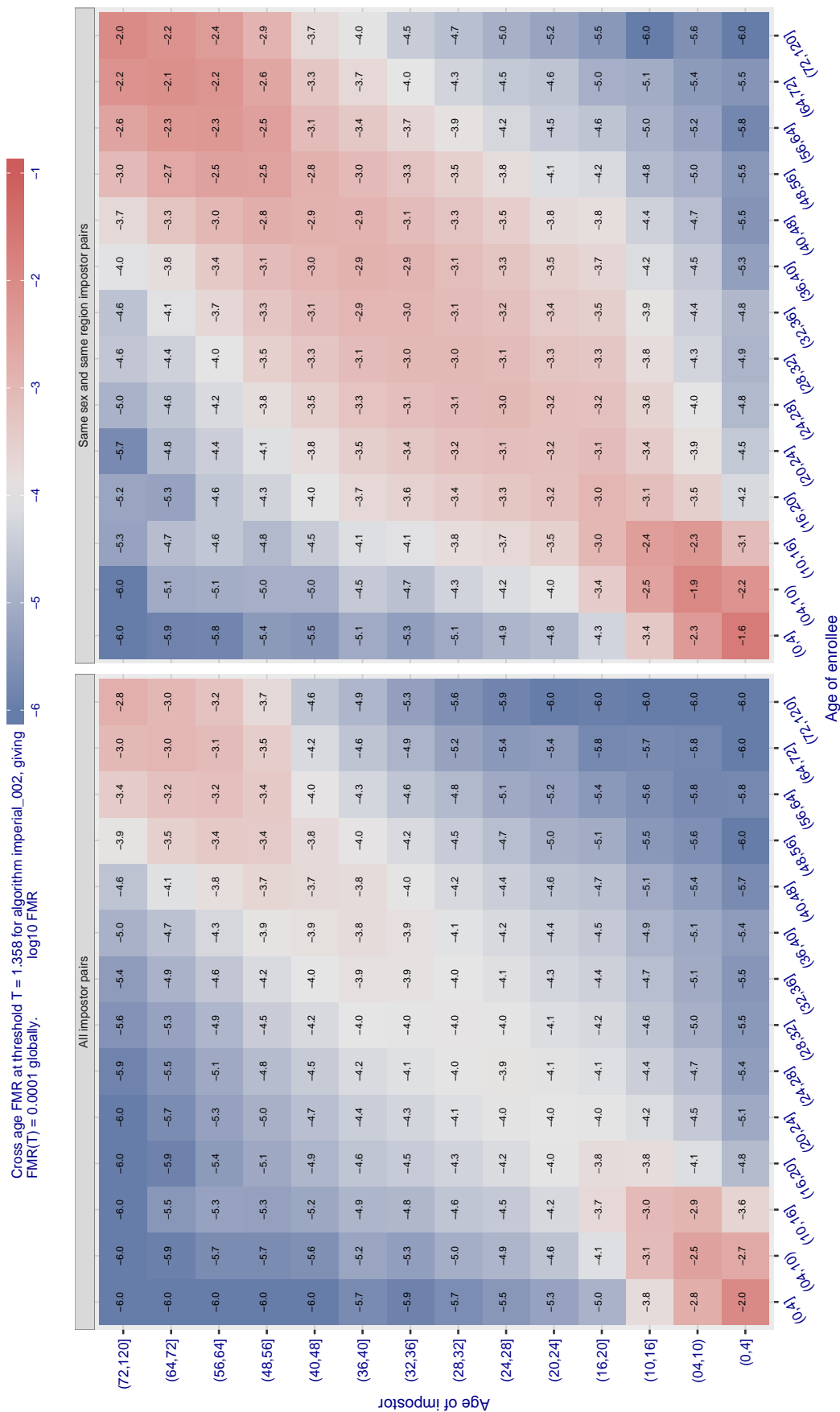


Figure 547: For algorithm imperial-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 1.398$  for algorithm incode\_004, giving  $\log_{10} \text{FMR}(T) = 0.0001$  globally.

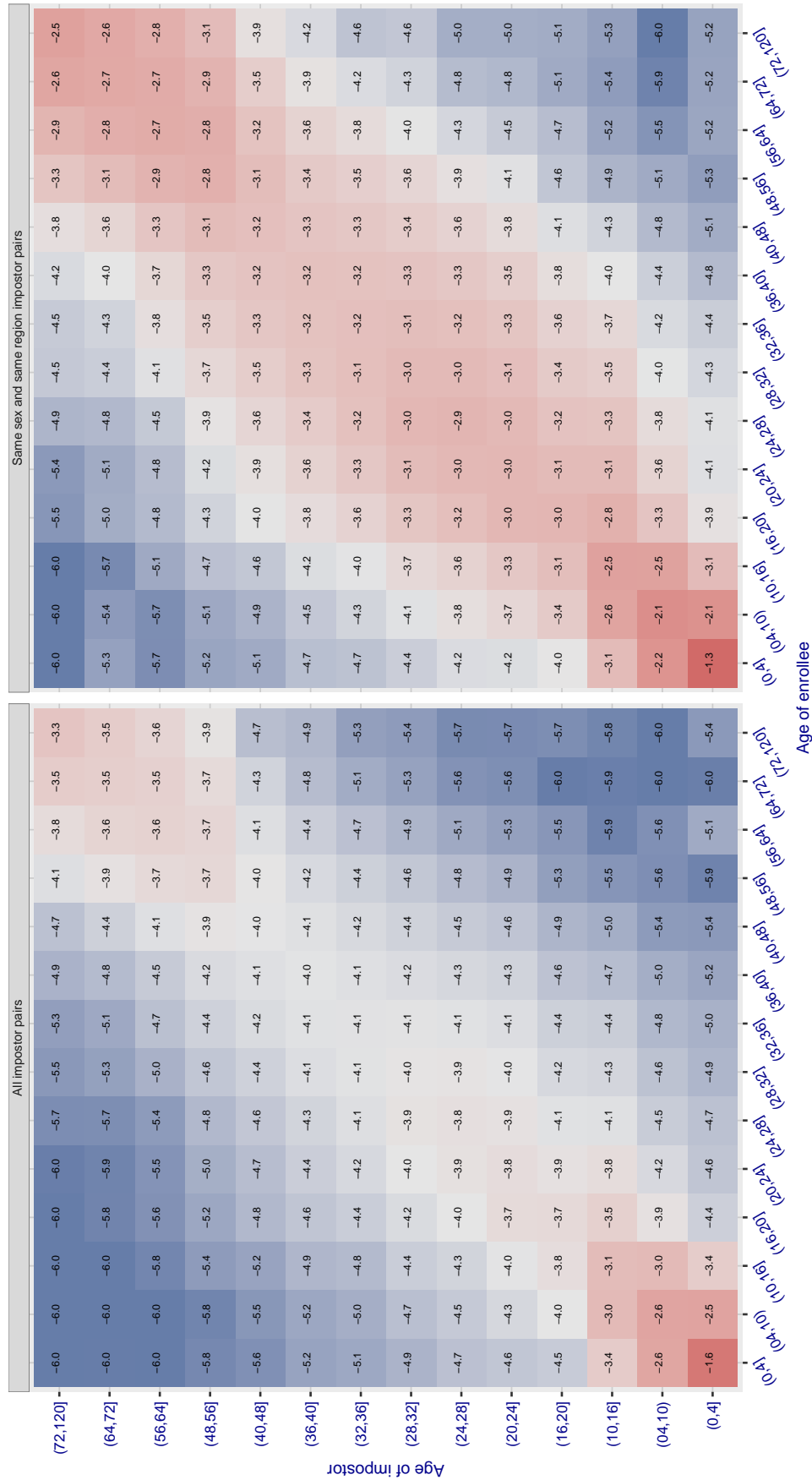


Figure 548: For algorithm incode-004 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 1.391$  for algorithm `incode_005`, giving  $FMR(T) = 0.0001$  globally.

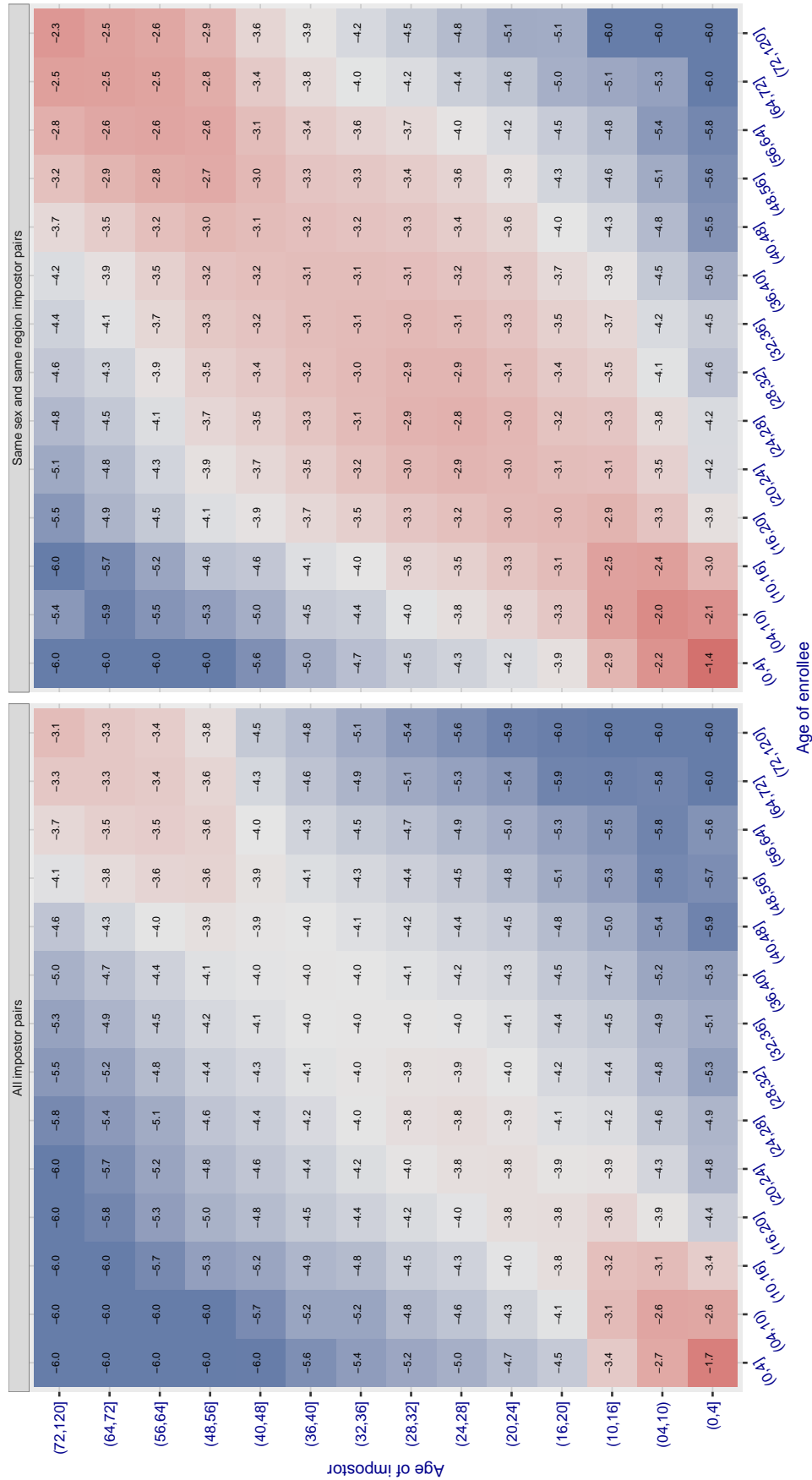


Figure 549: For algorithm `incode-005` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

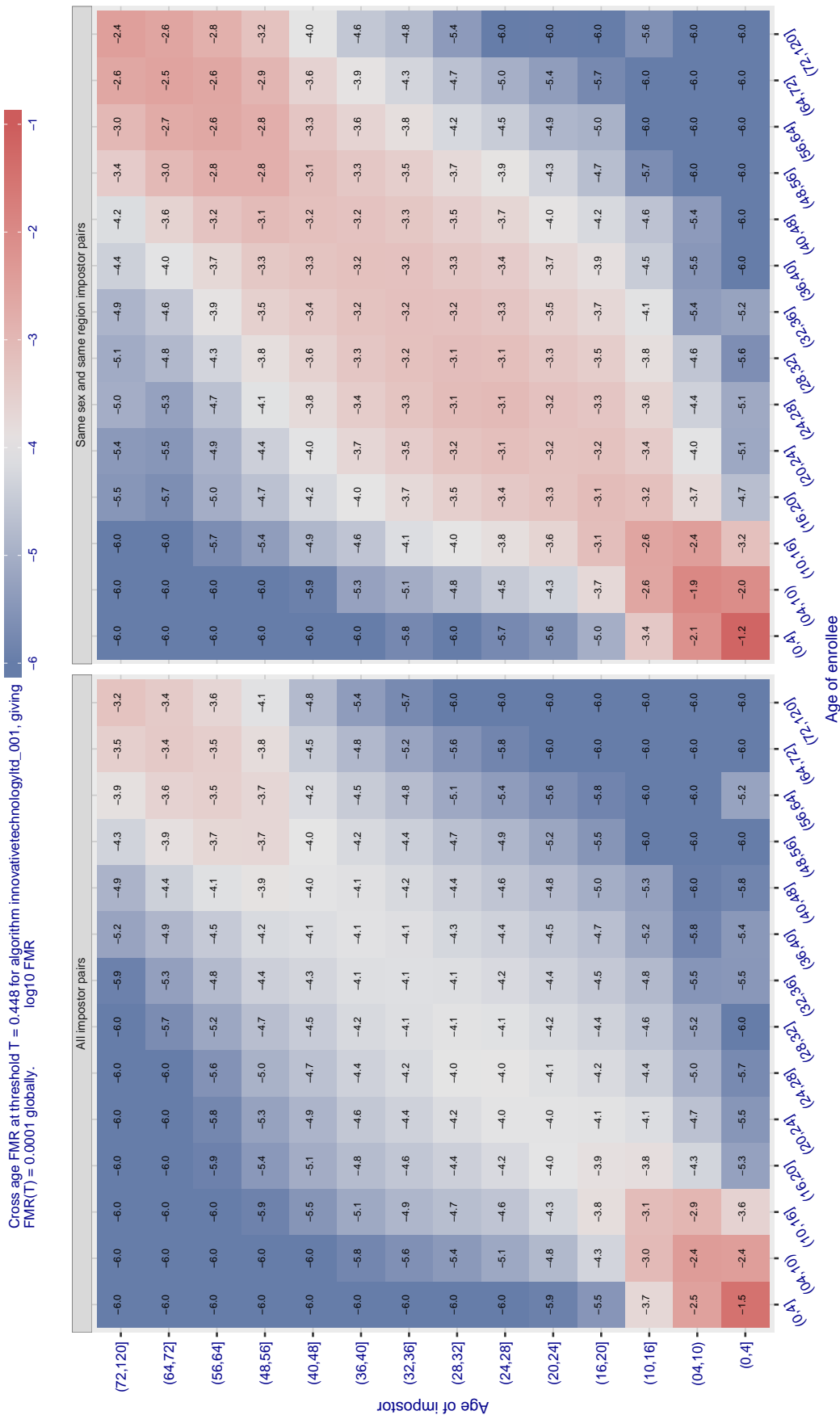


Figure 550: For algorithm innovatetechnology/td-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.



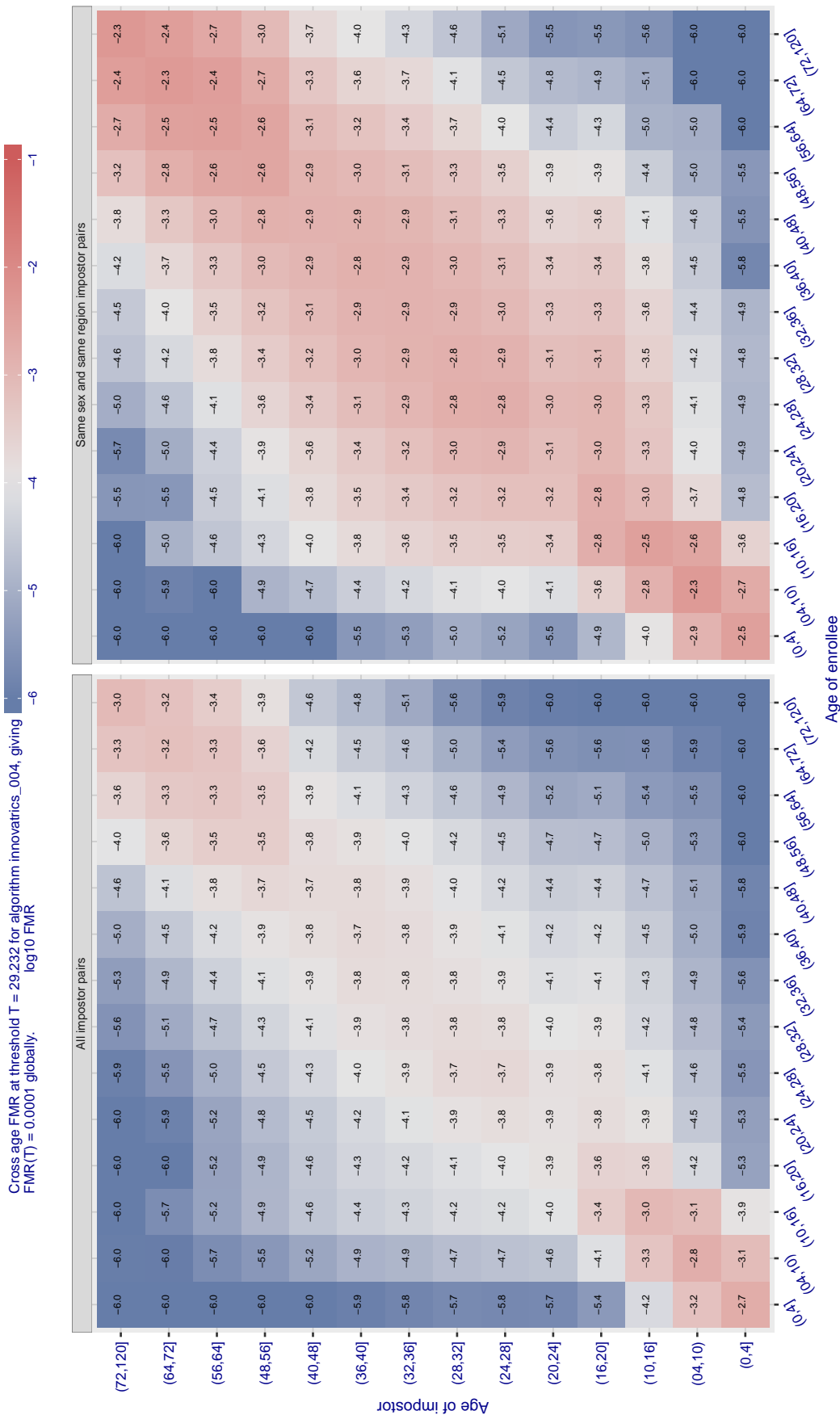


Figure 551: For algorithm innovatrics-004 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

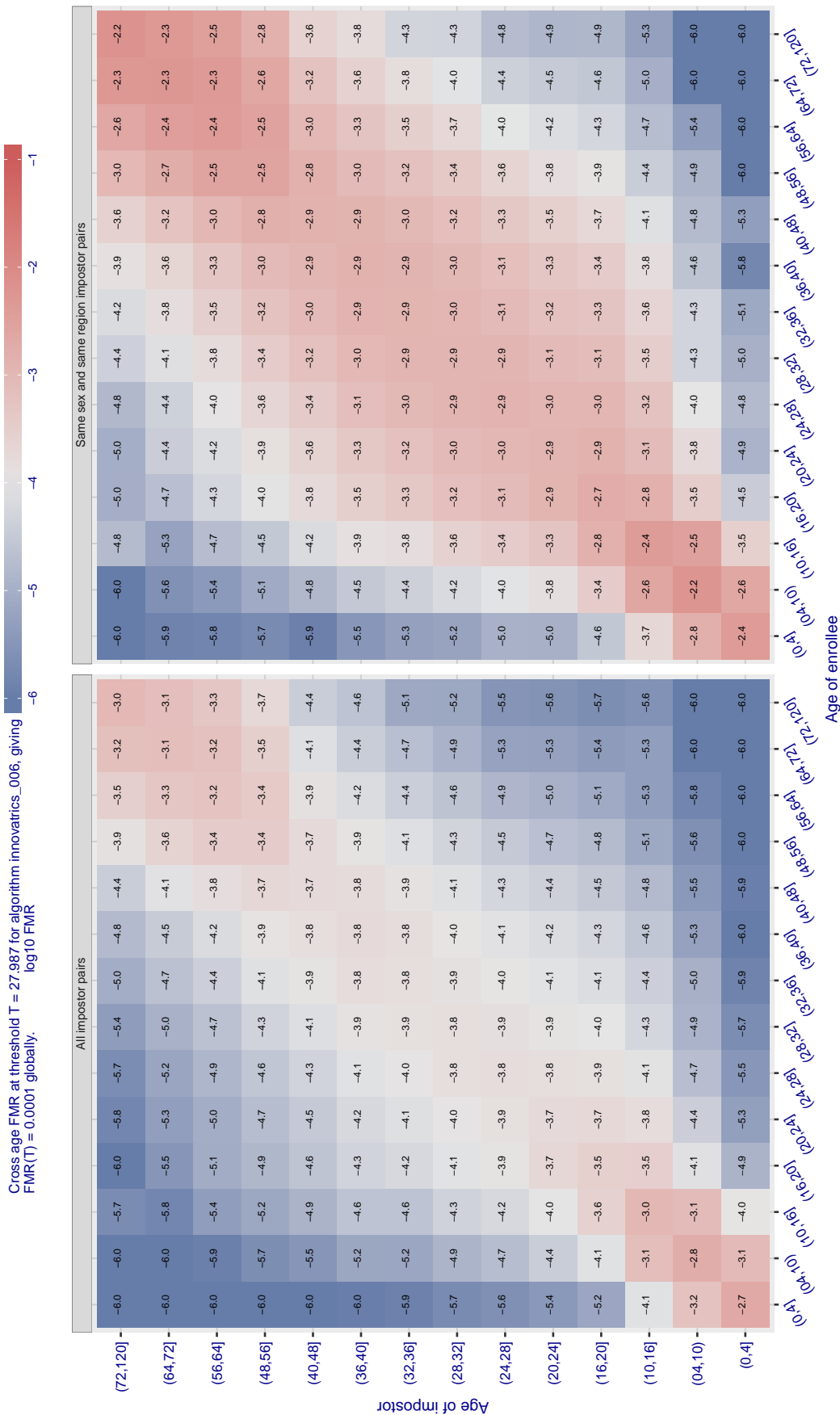


Figure 552: For algorithm innovatrics-006 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

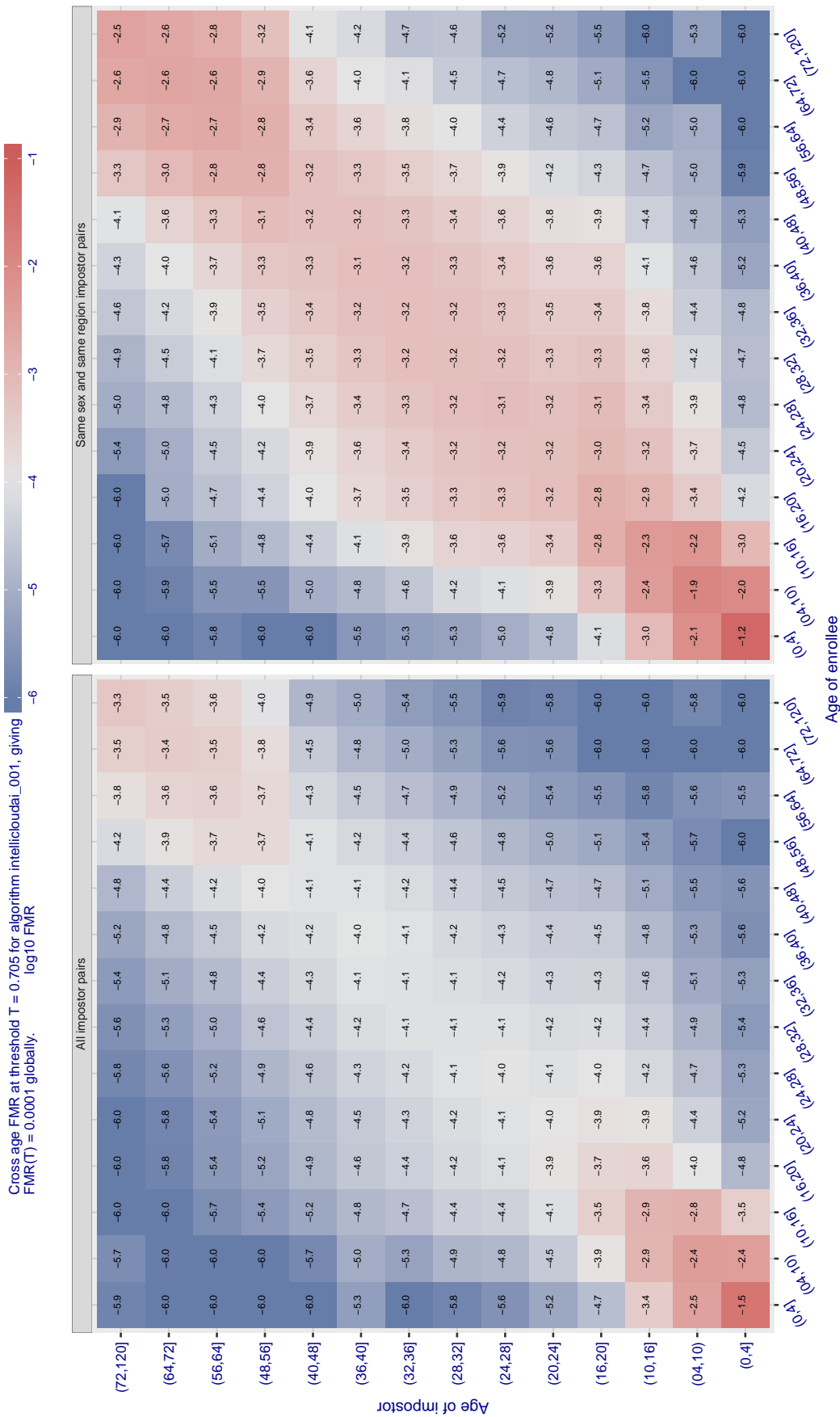


Figure 553: For algorithm `intellcloudai-001` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

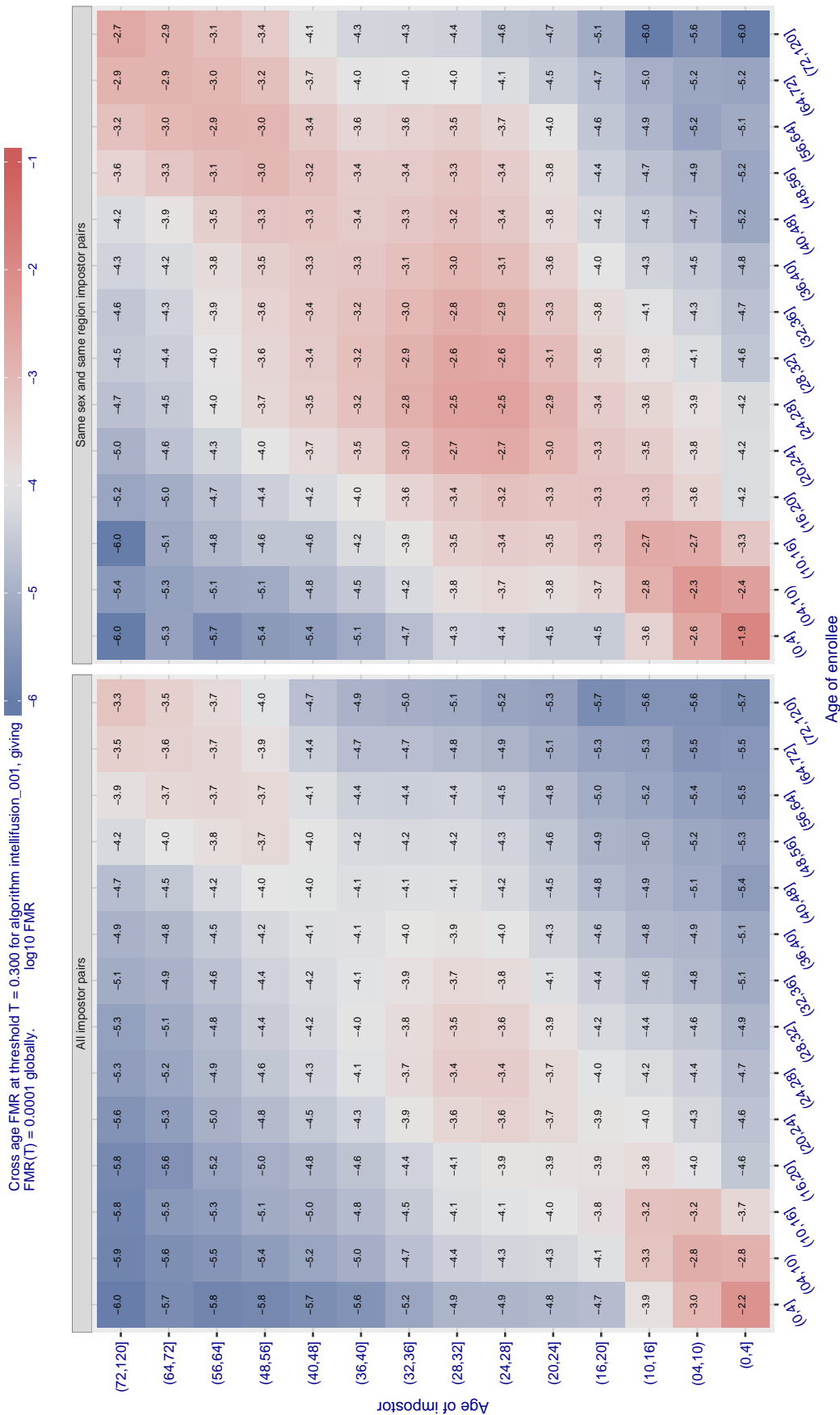


Figure 554: For algorithm `intellifusion-001` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

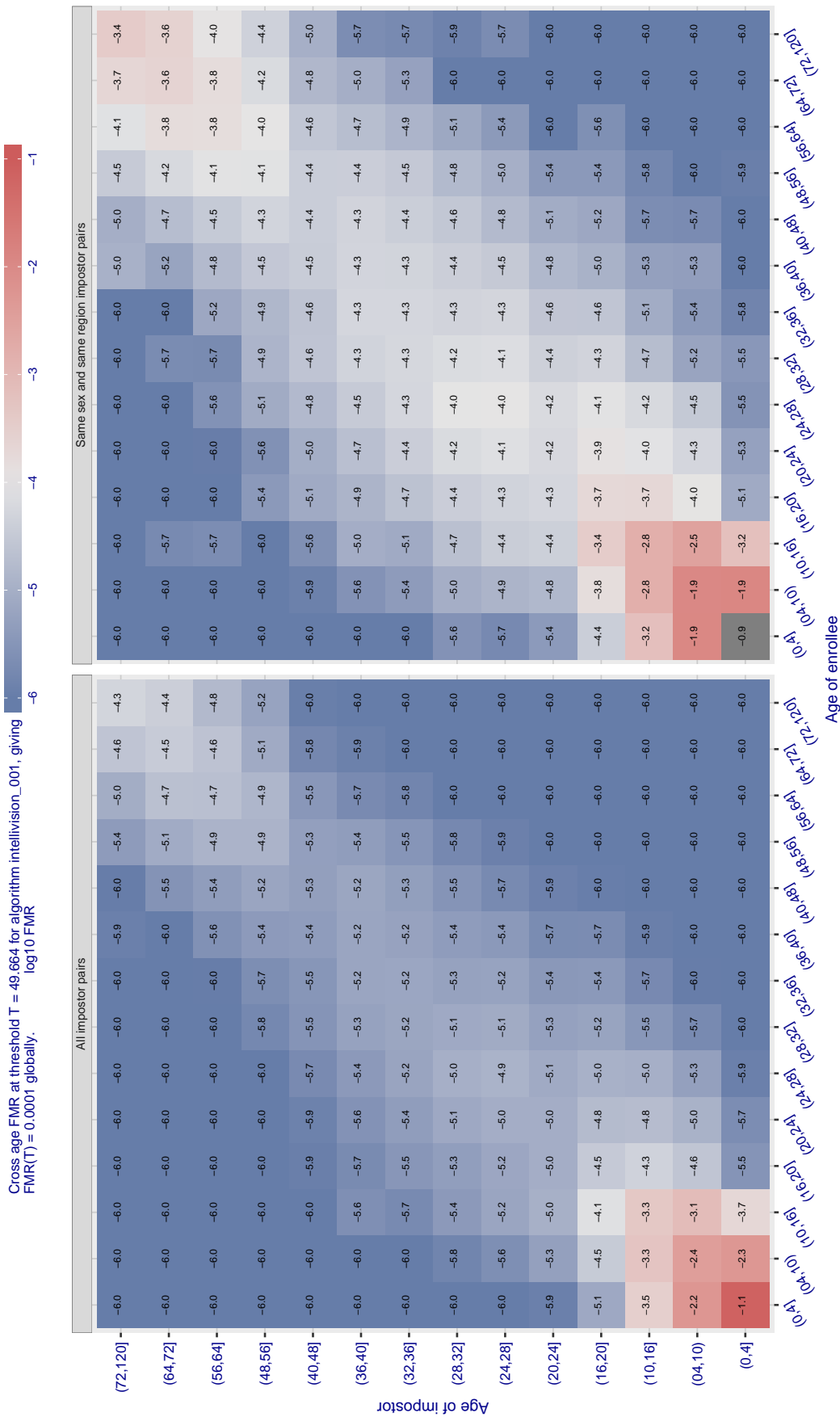


Figure 555: For algorithm `intellivision-001` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

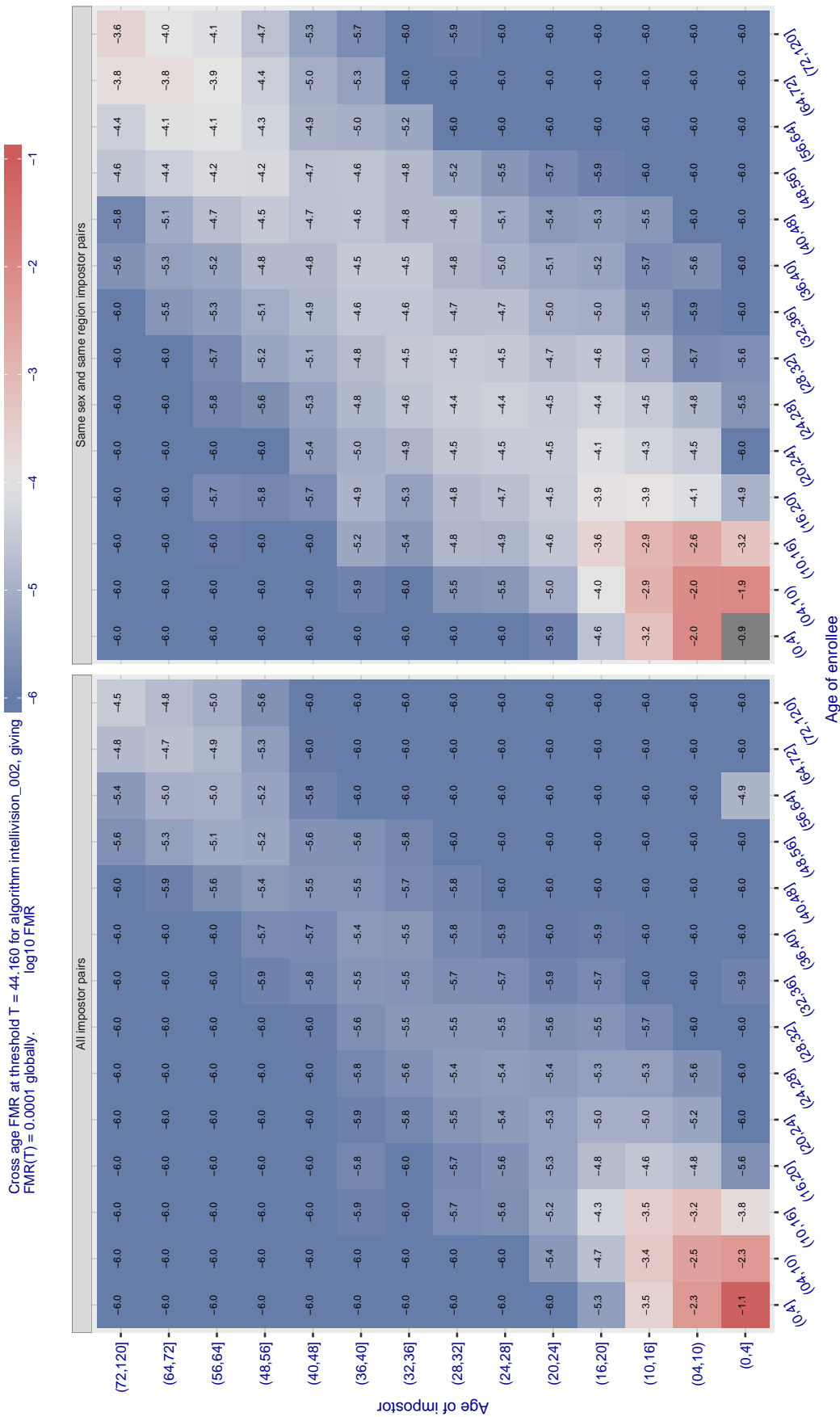


Figure 556: For algorithm intellivision-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

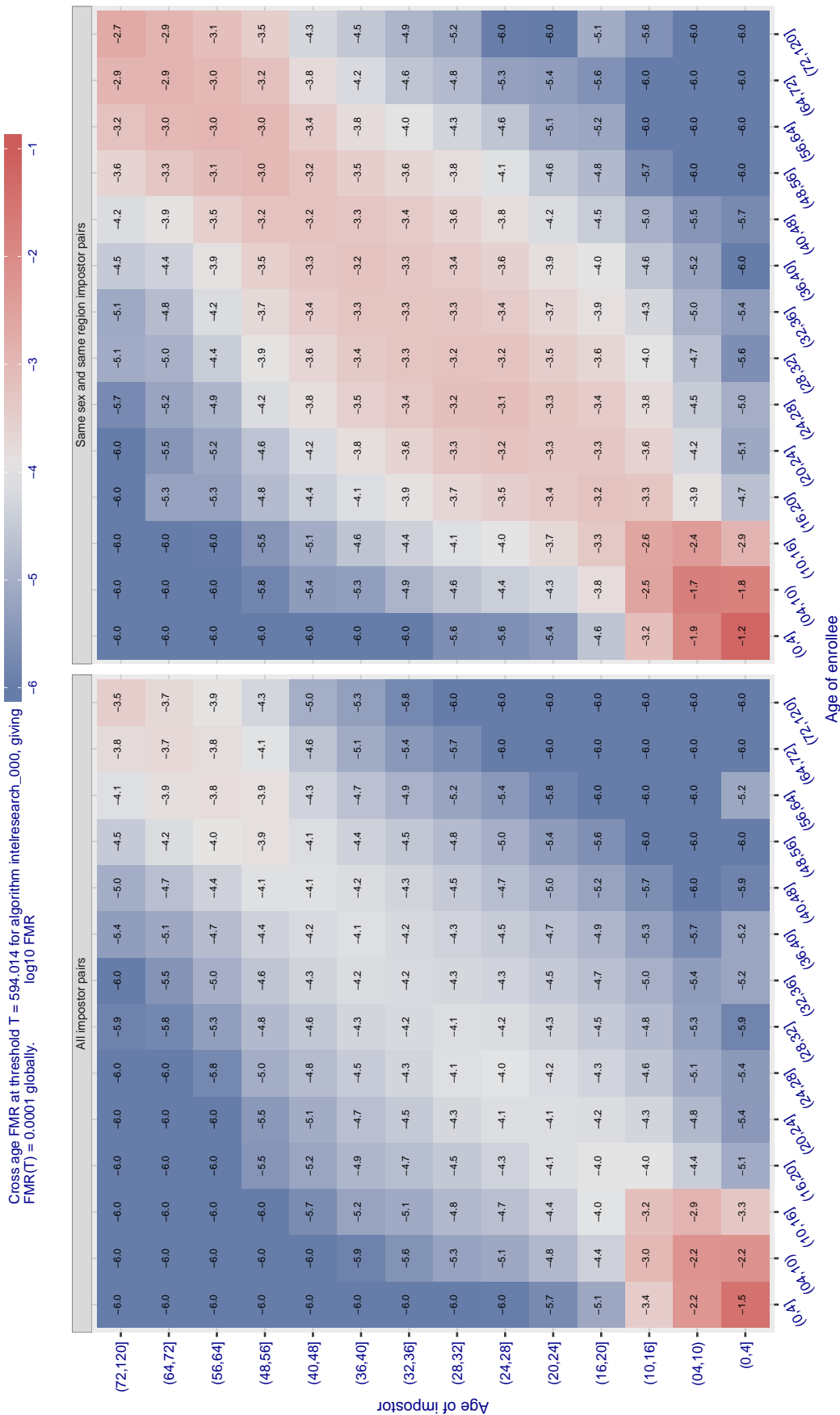


Figure 557: For algorithm intelresearch-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

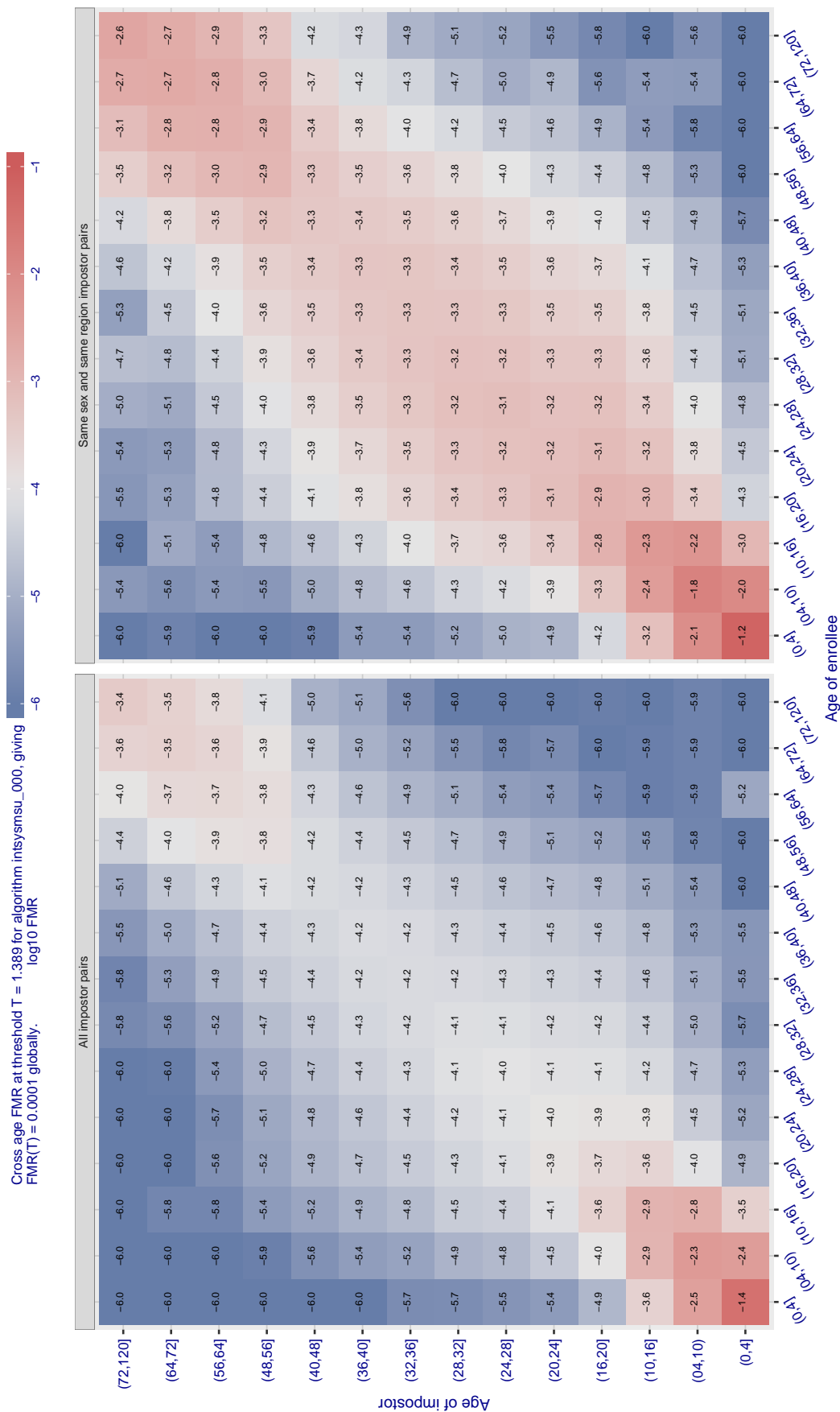


Figure 558: For algorithm `intsysmsu-000` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.



Cross age FMR at threshold  $T = 1.971$  for algorithm `intsysmsu_001`, giving  $FMR(T) = 0.0001$  globally.

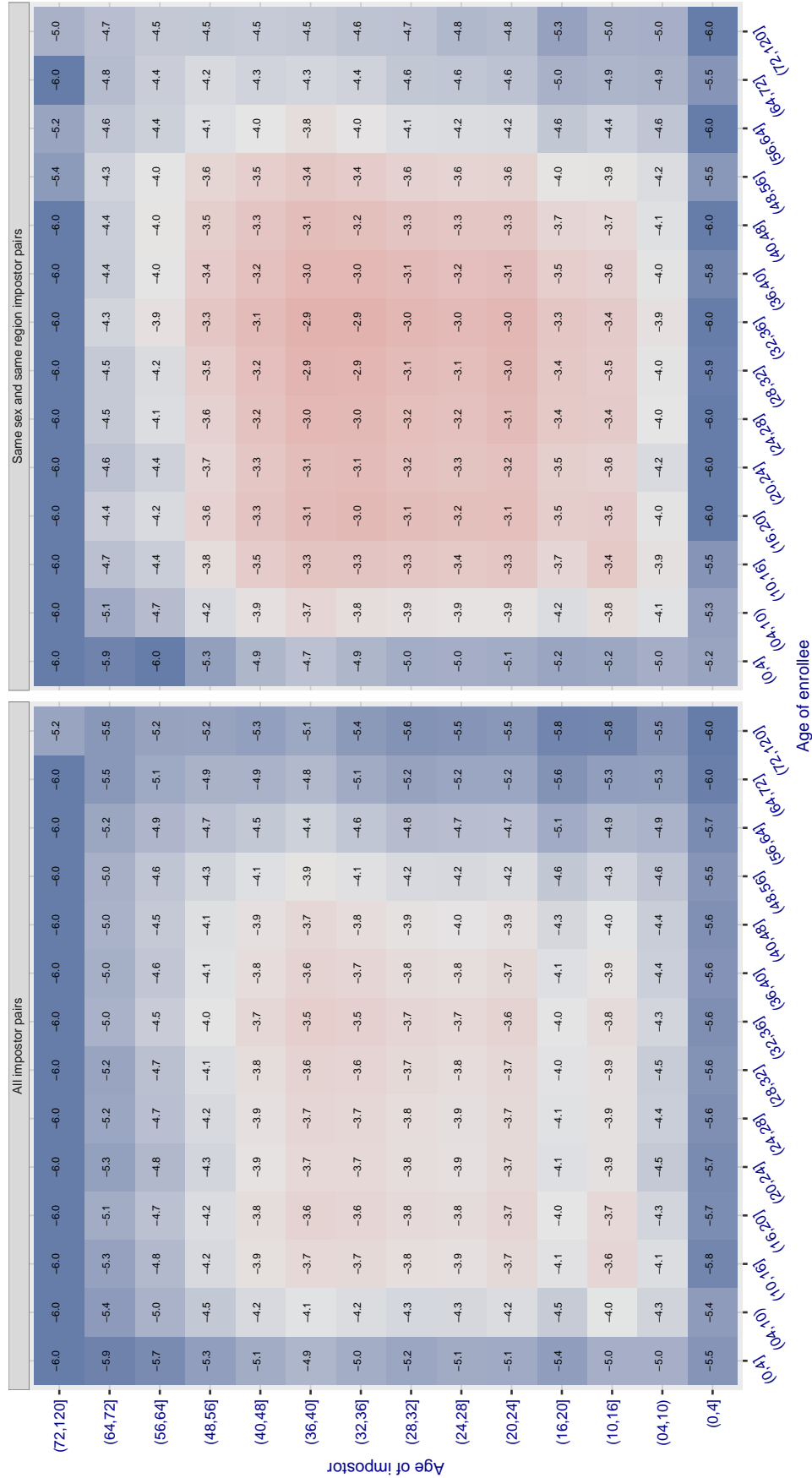


Figure 559: For algorithm `intsysmsu-001` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 1.361$  for algorithm `iqface_000`, giving  $FMR(T) = 0.0001$  globally.

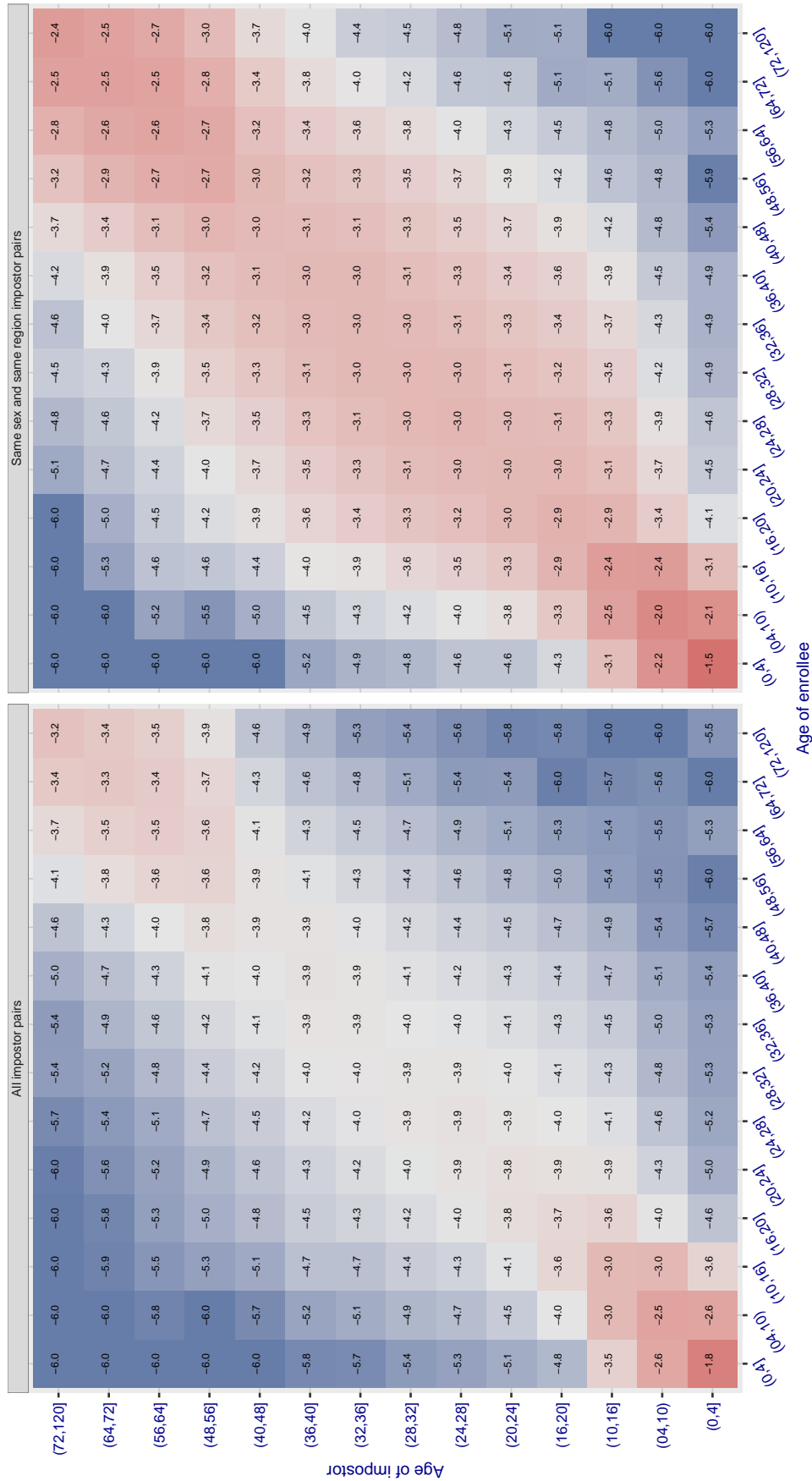


Figure 560: For algorithm `iqface-000` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

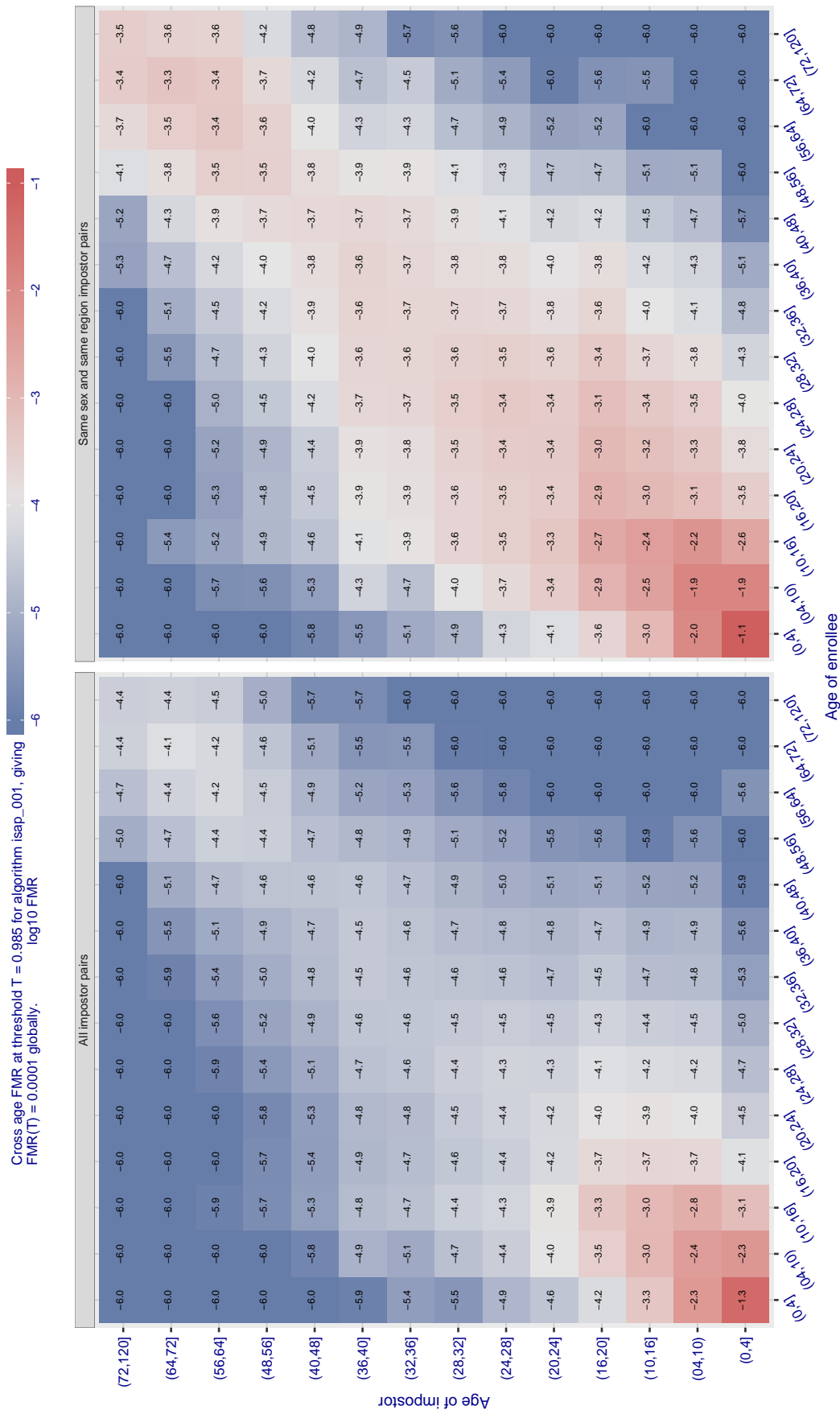


Figure 561: For algorithm isap-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

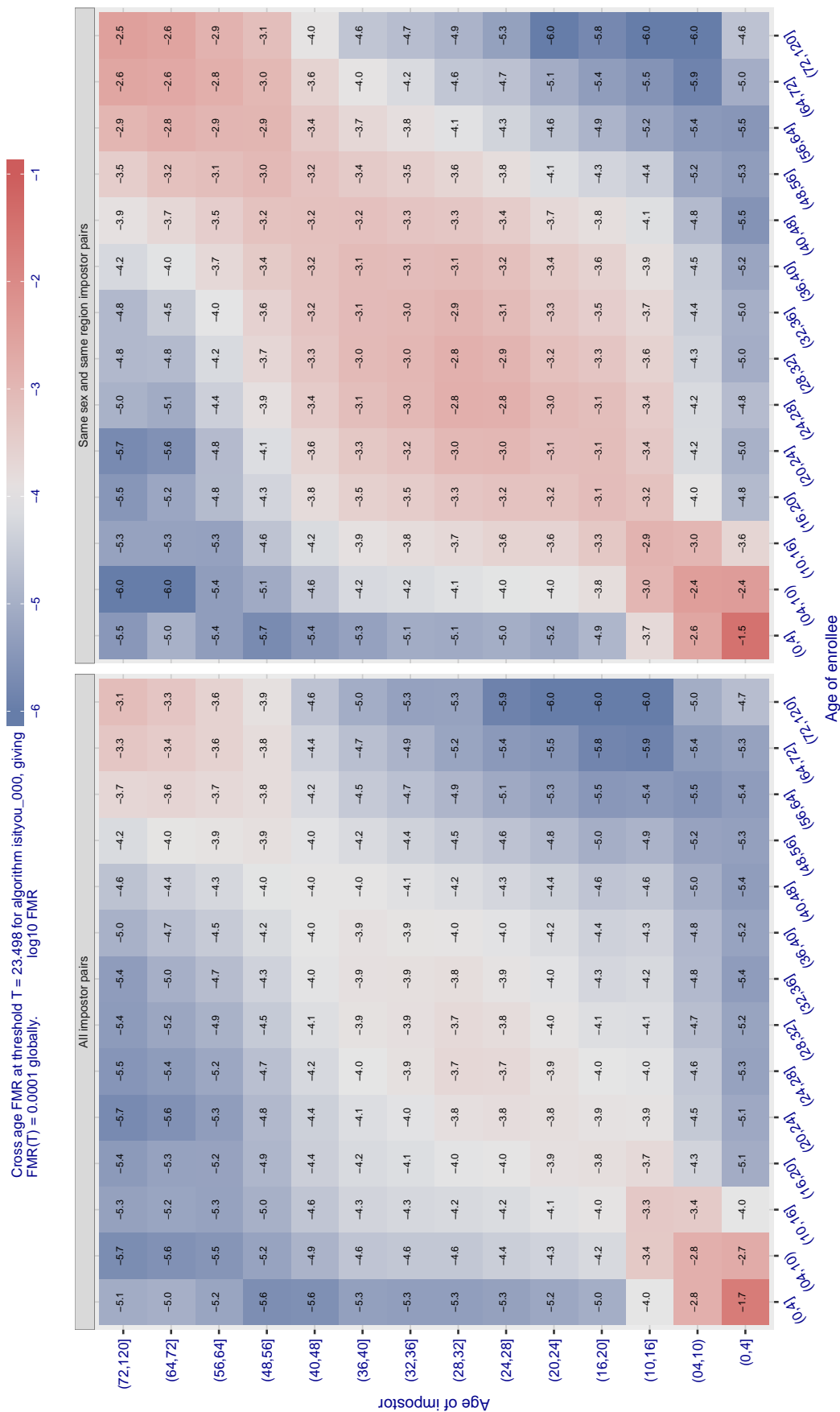


Figure 562: For algorithm `isityou-000` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

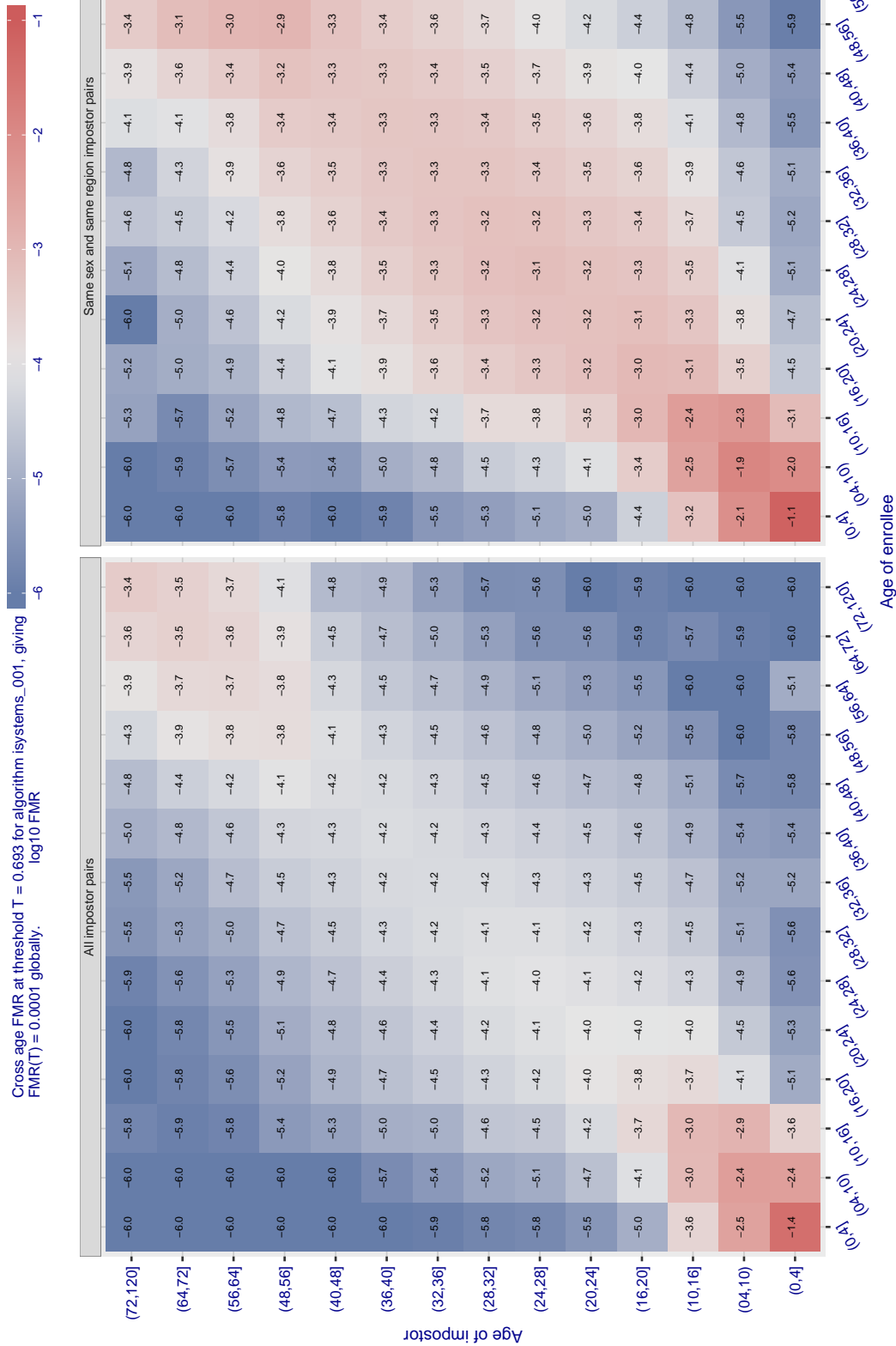


Figure 563: For algorithm isystems-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.690$  for algorithm isystems\_002, giving  $\log_{10} \text{FMR}(T) = 0.0001$  globally.

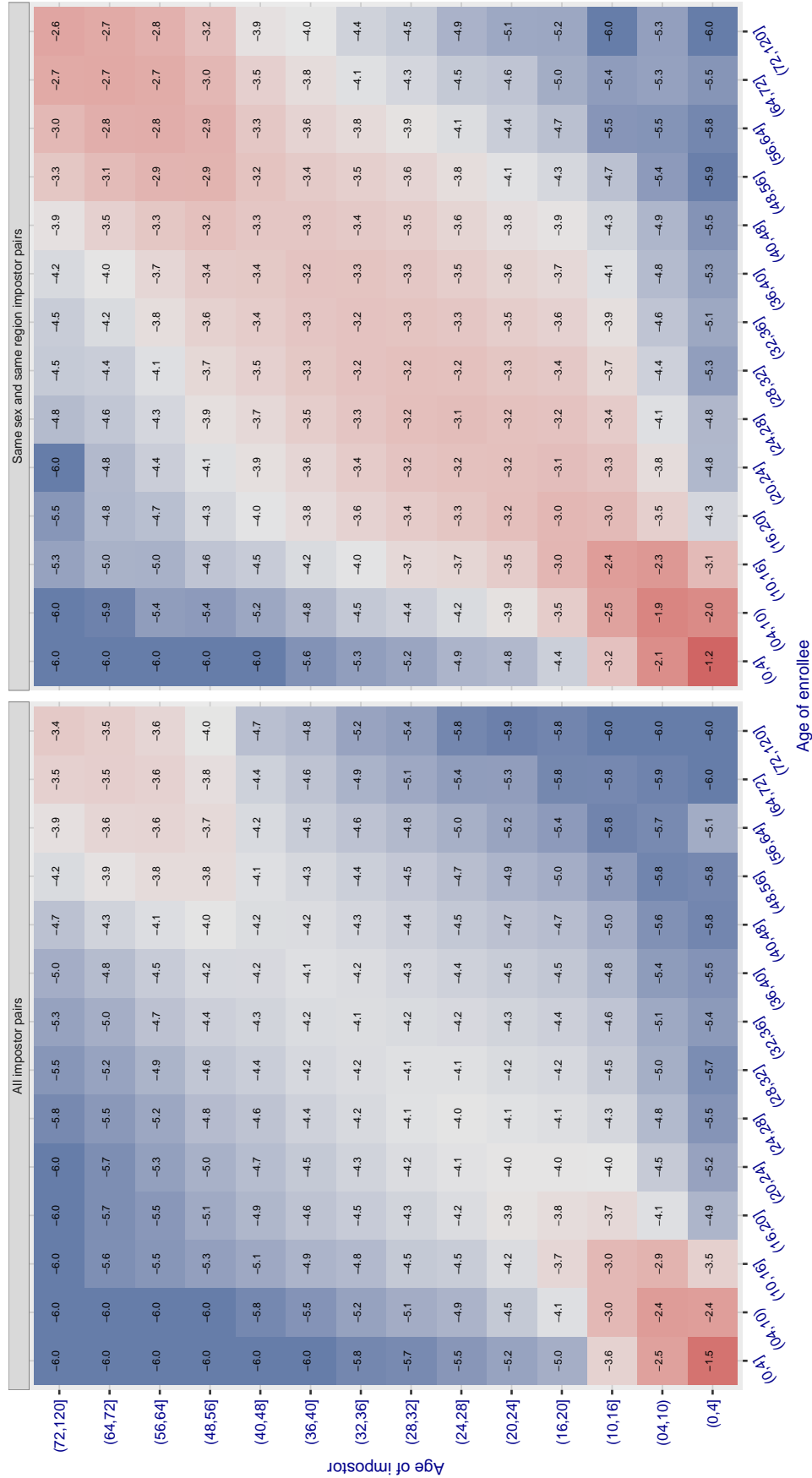


Figure 564: For algorithm isystems-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

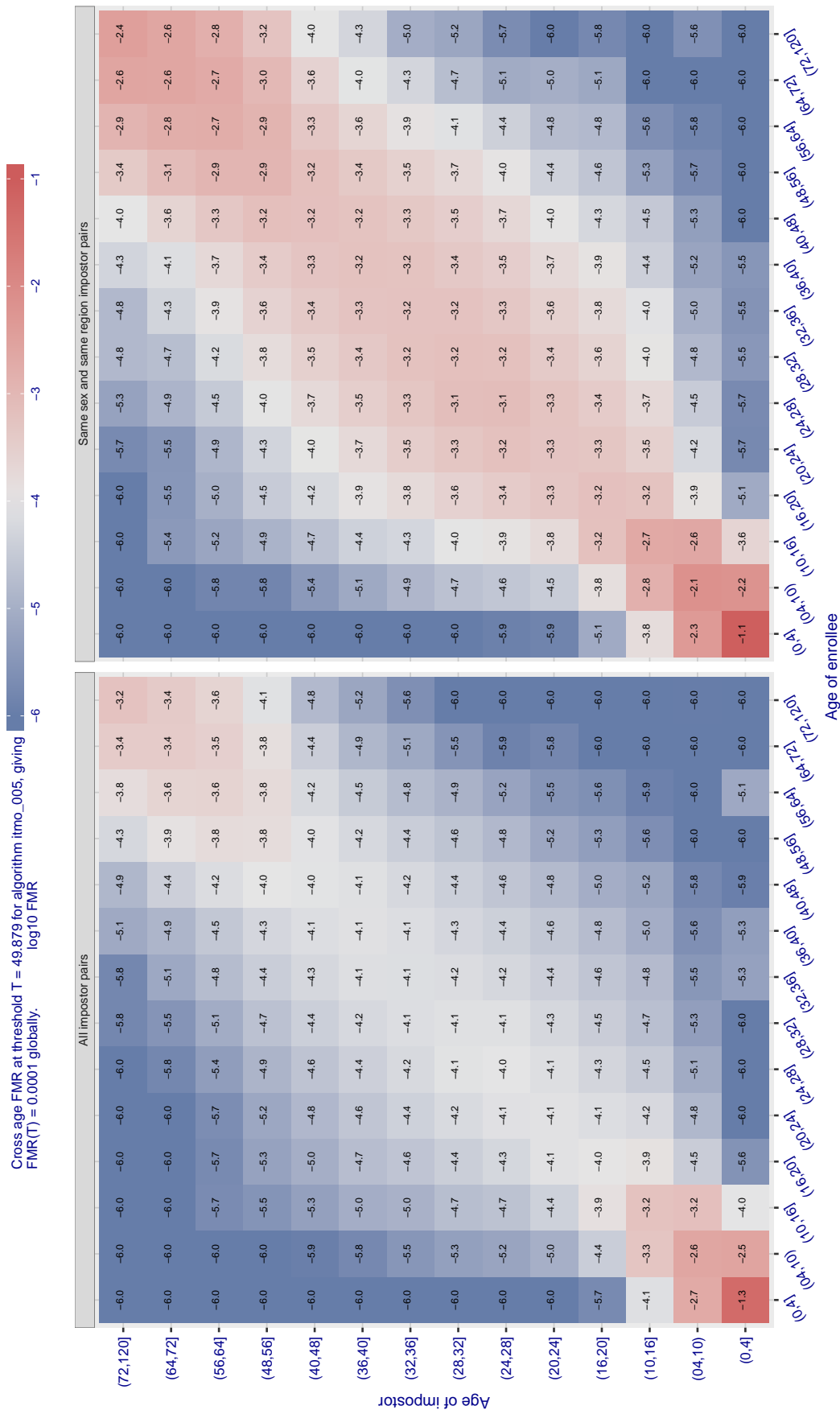


Figure 565: For algorithm itmo-005 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

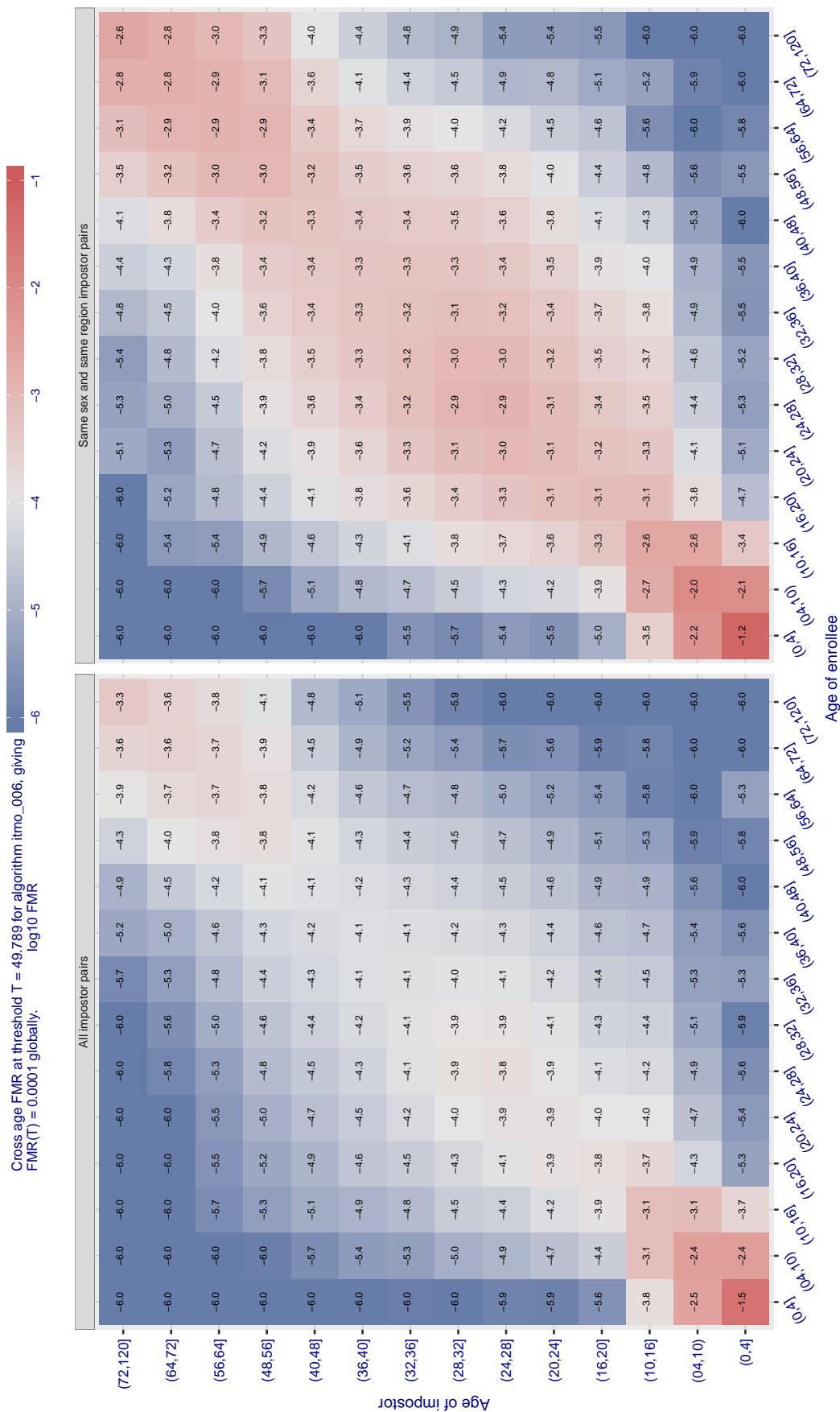


Figure 566: For algorithm itmo-006 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.



Cross age FMR at threshold  $T = 1.301$  for algorithm kakao\_001, giving  $FMR(T) = 0.0001$  globally.

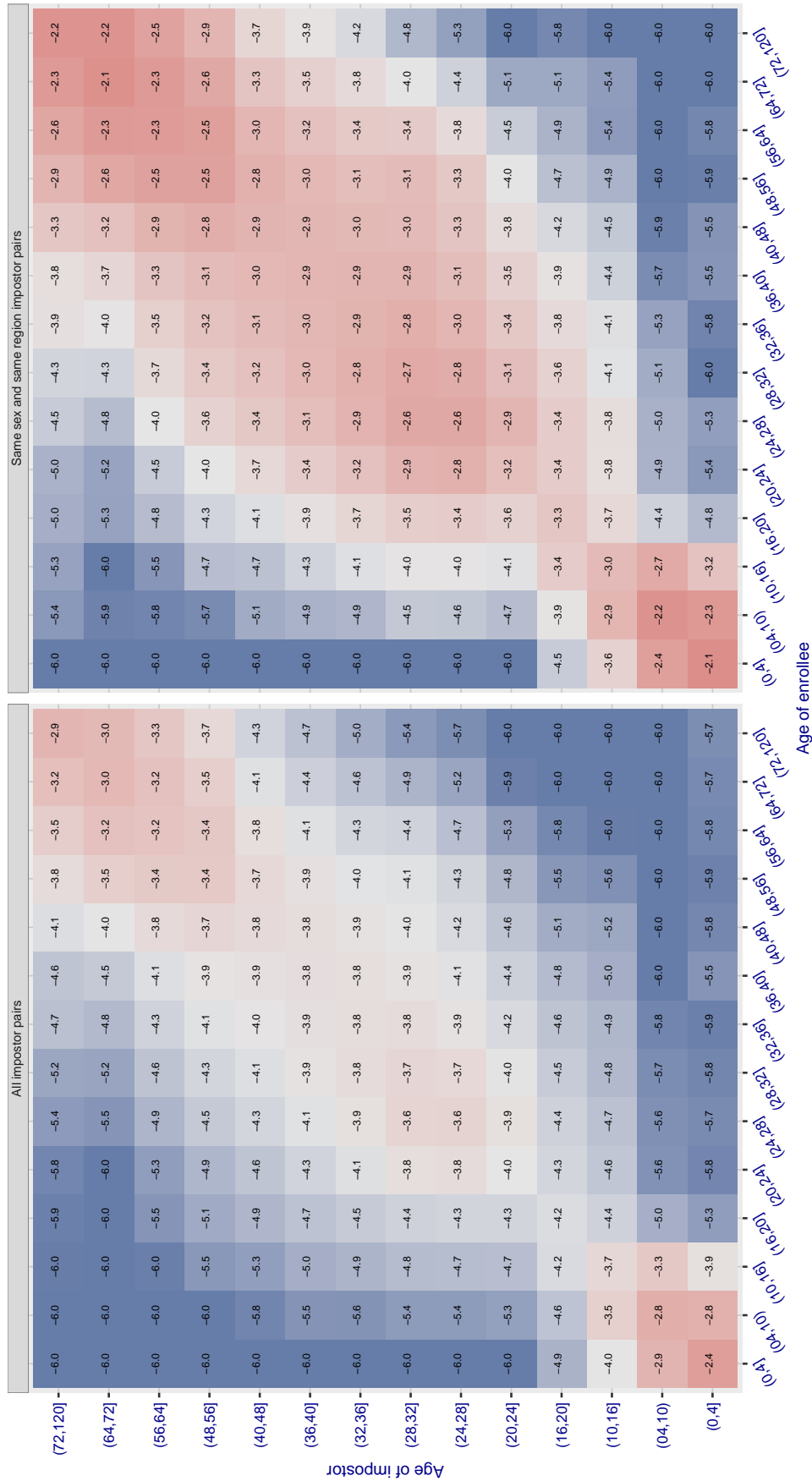


Figure 567: For algorithm kakao-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.929$  for algorithm kakao\_002, giving  $\log_{10} \text{FMR}(T) = 0.0001$  globally.

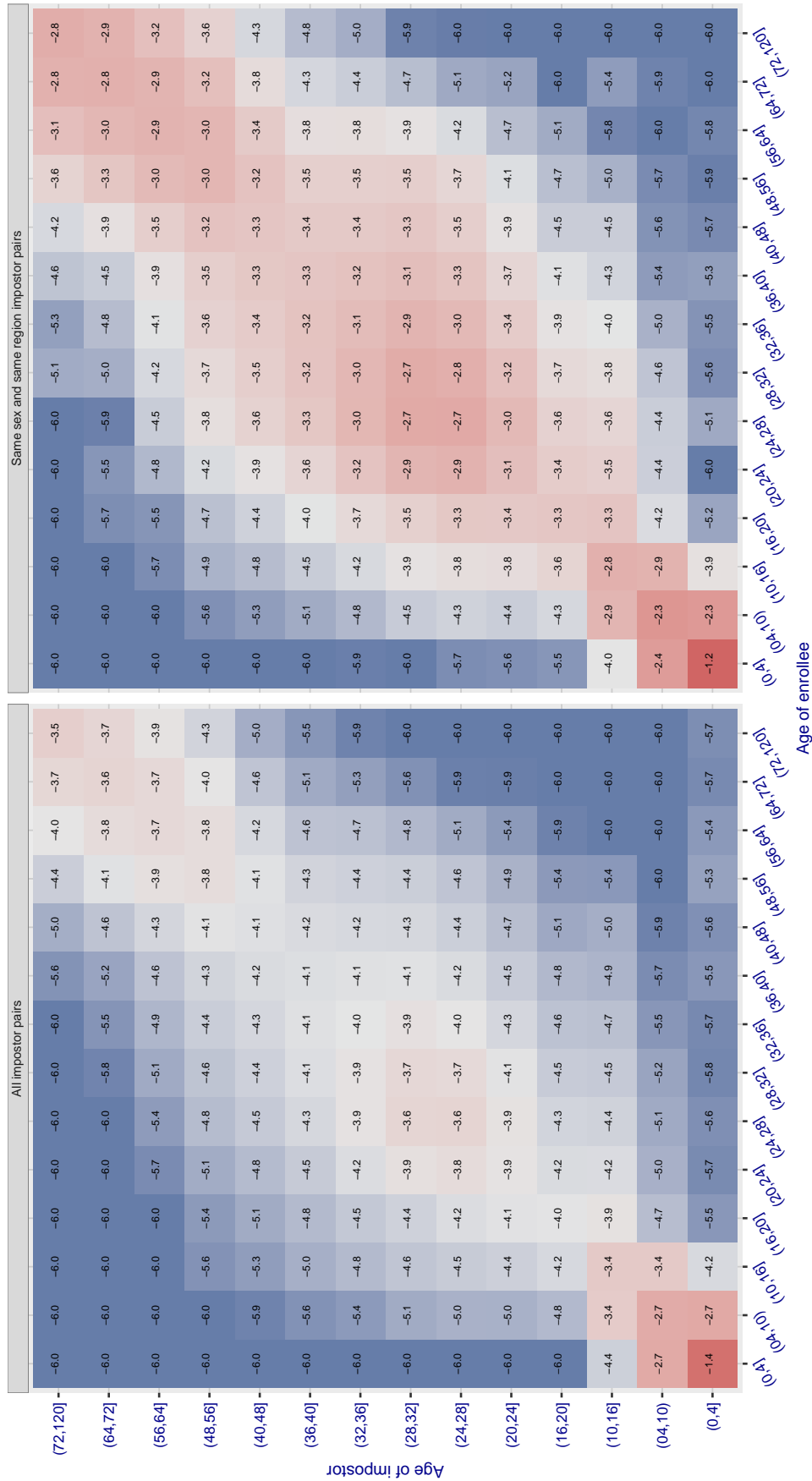


Figure 568: For algorithm kakao-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

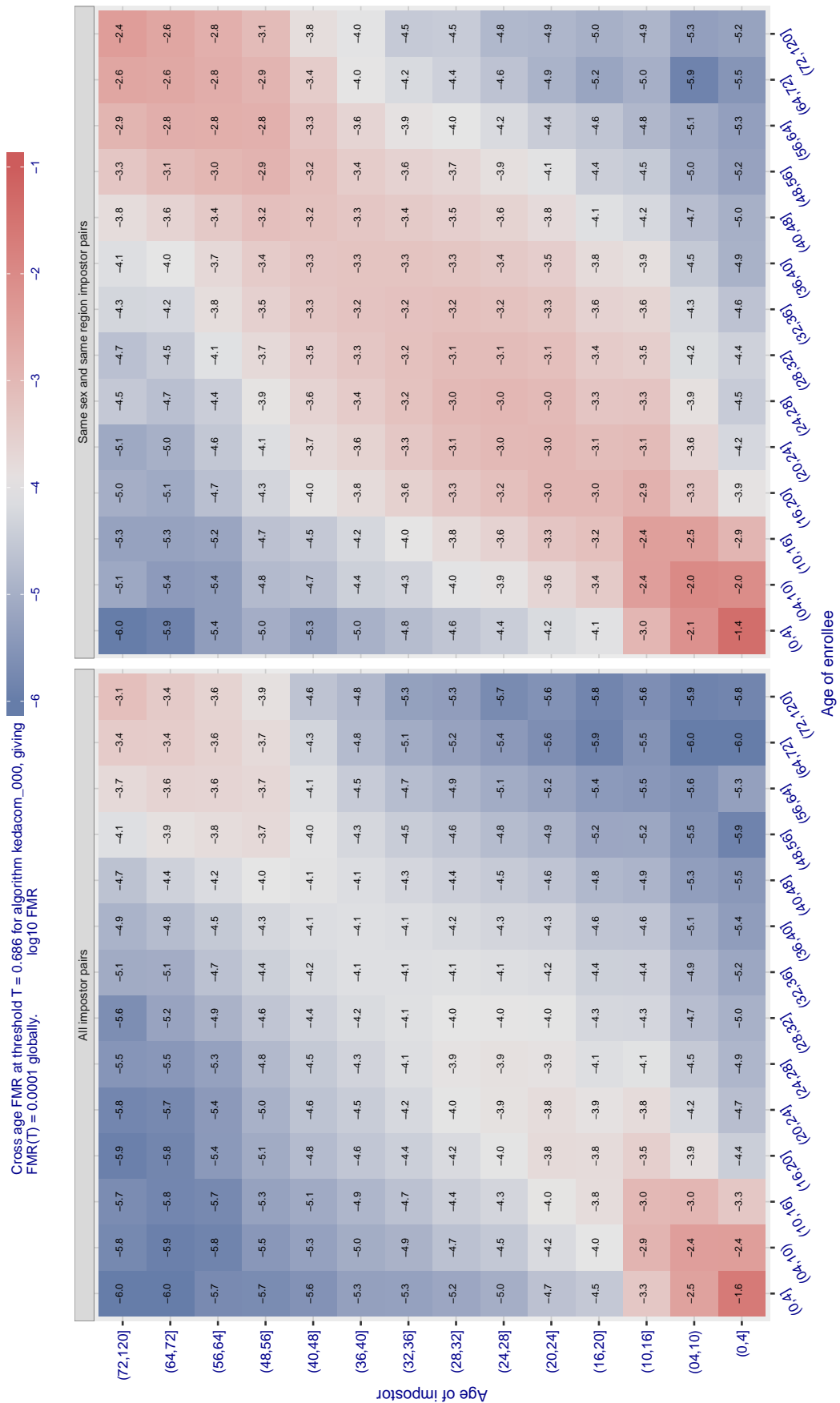


Figure 569: For algorithm kedacom-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.500$  for algorithm kneron\_003, giving  $FMR(T) = 0.0001$  globally.

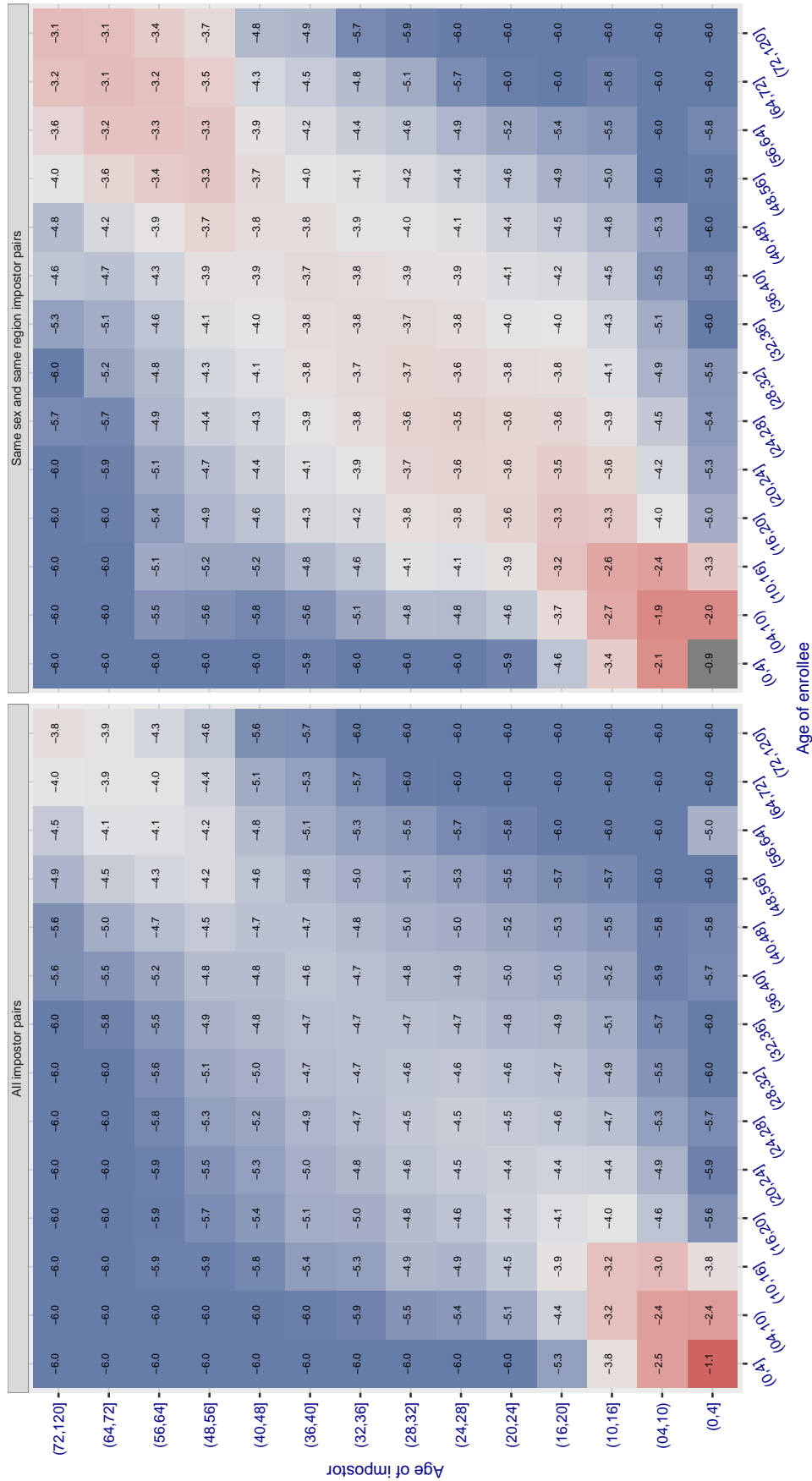


Figure 570: For algorithm kneron-003 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.701$  for algorithm lookman\_002, giving  $\log_{10} \text{FMR}(T) = 0.0001$  globally.

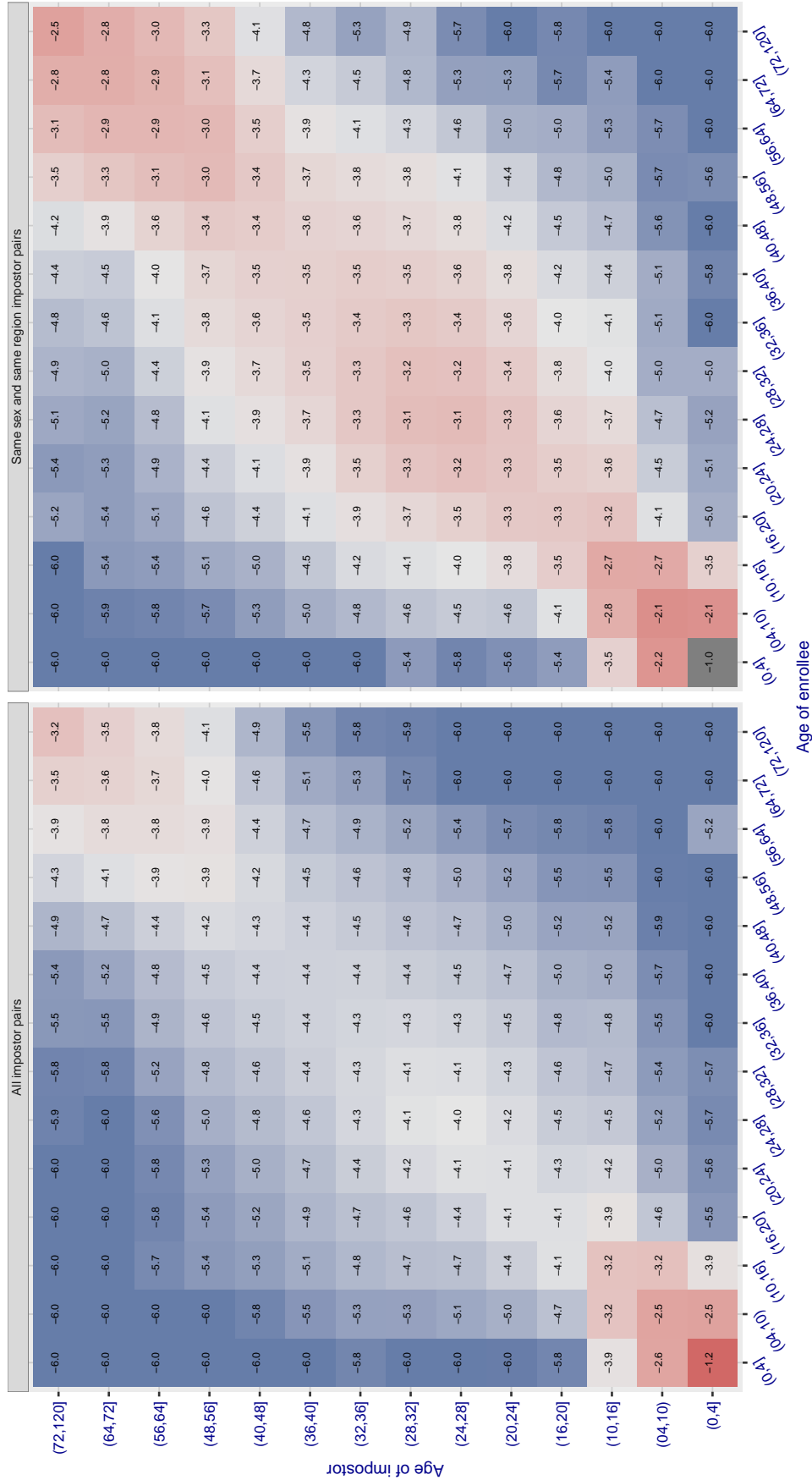


Figure 571: For algorithm lookman-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.733$  for algorithm lookman\_004, giving  $\log_{10} \text{FMR}(T) = 0.0001$  globally.

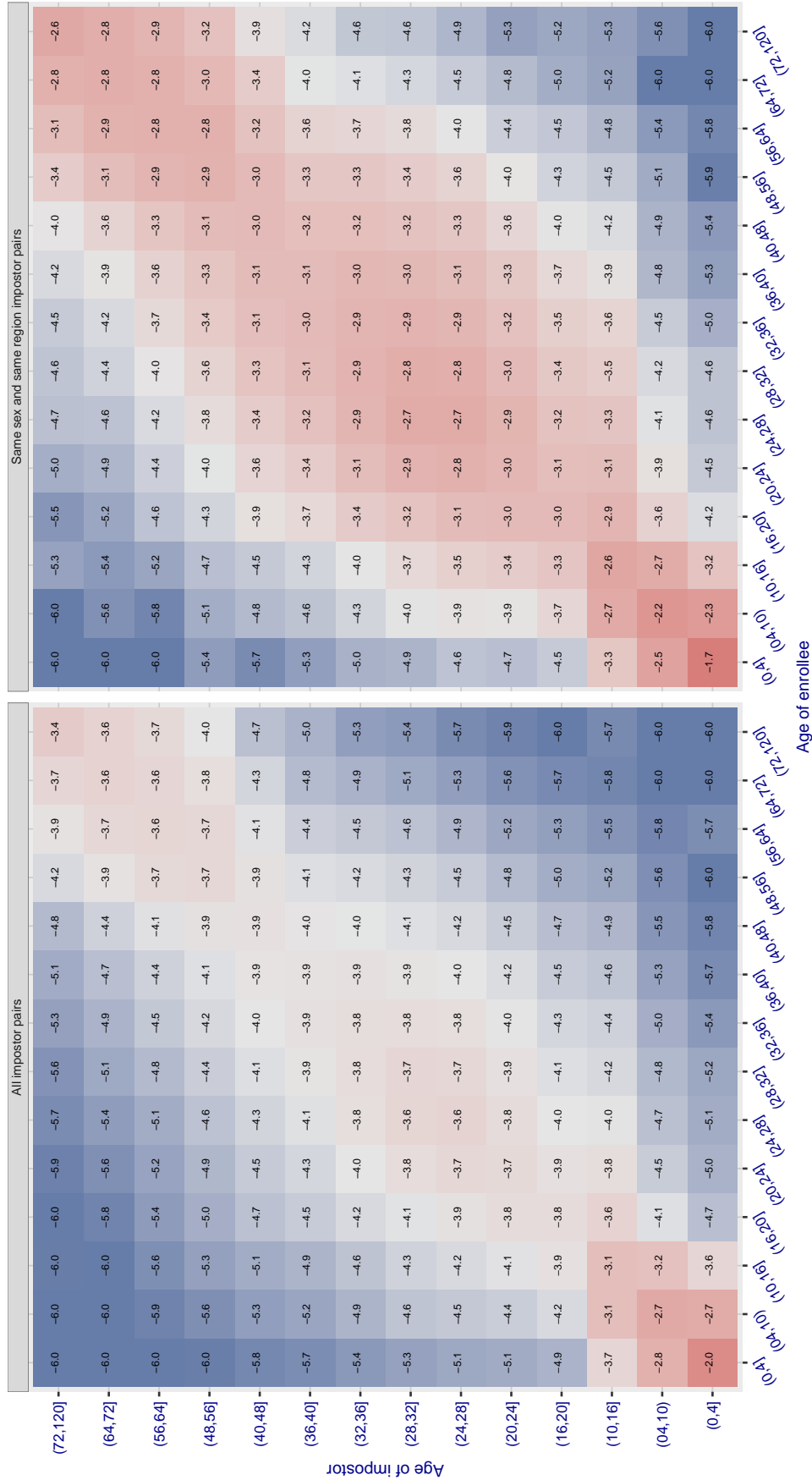


Figure 572: For algorithm lookman-004 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

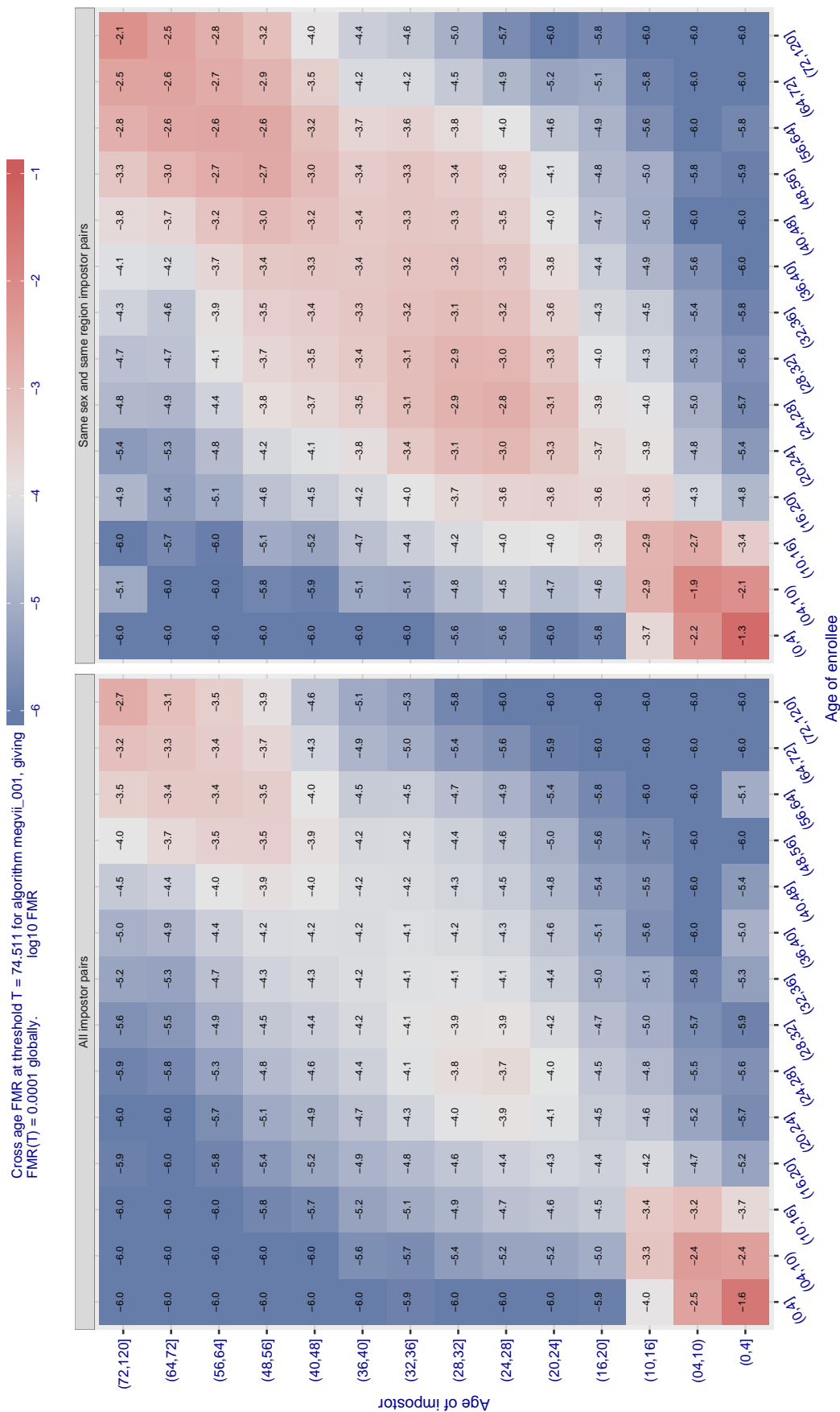


Figure 573: For algorithm megvii-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

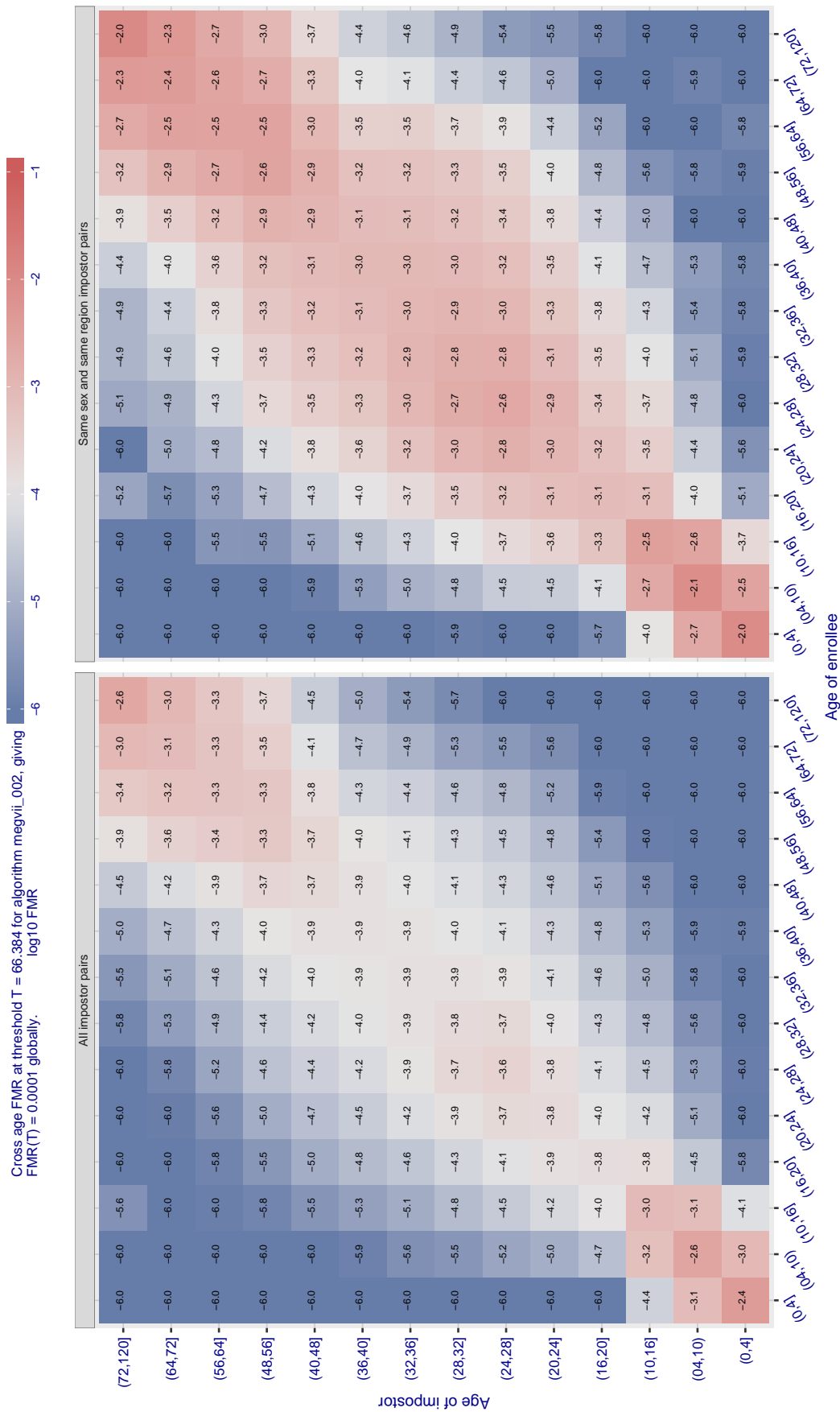


Figure 574: For algorithm megvii-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.



Cross age FMR at threshold  $T = 0.425$  for algorithm meiya\_001, giving  $FMR(T) = 0.0001$  globally.

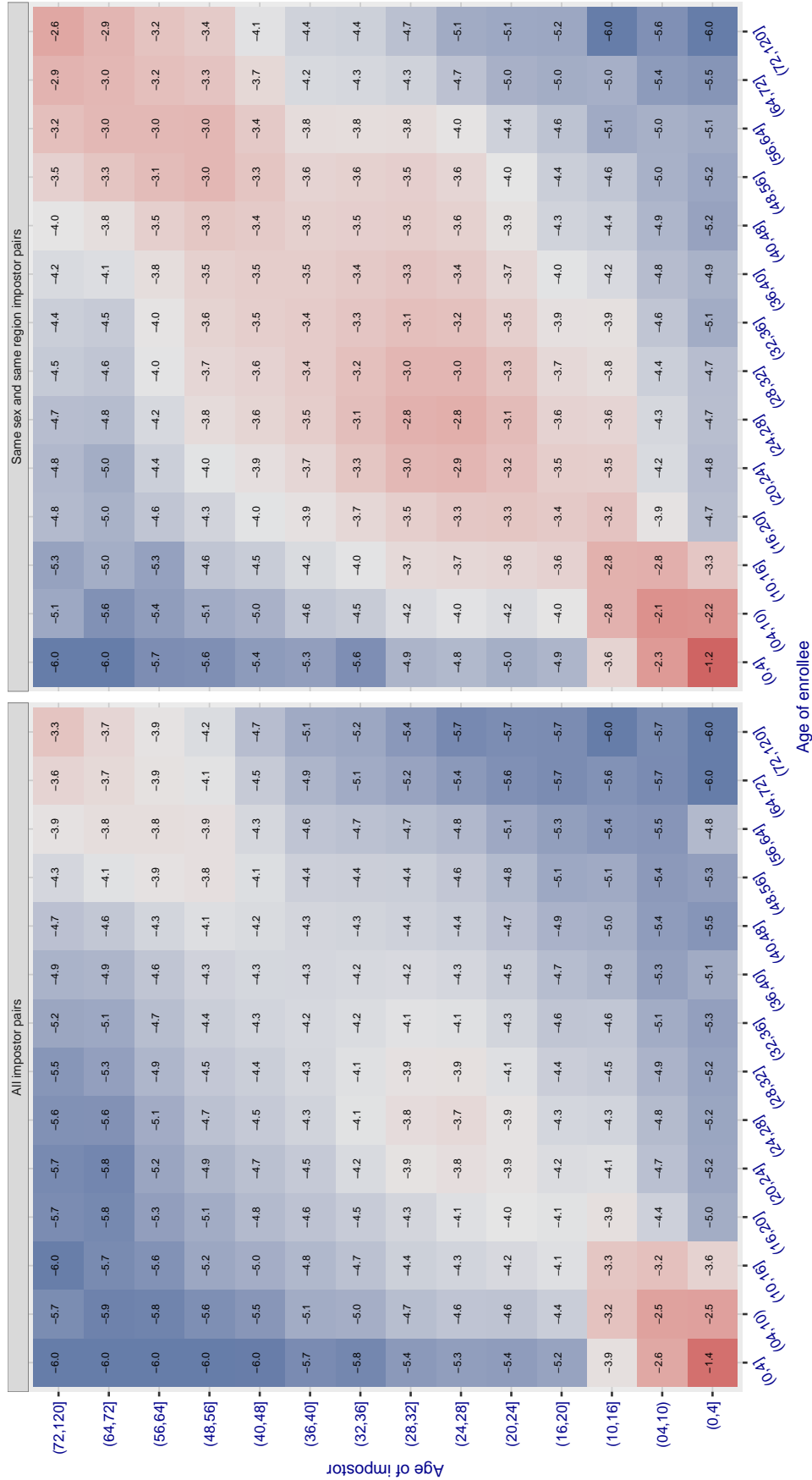


Figure 575: For algorithm meiya-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

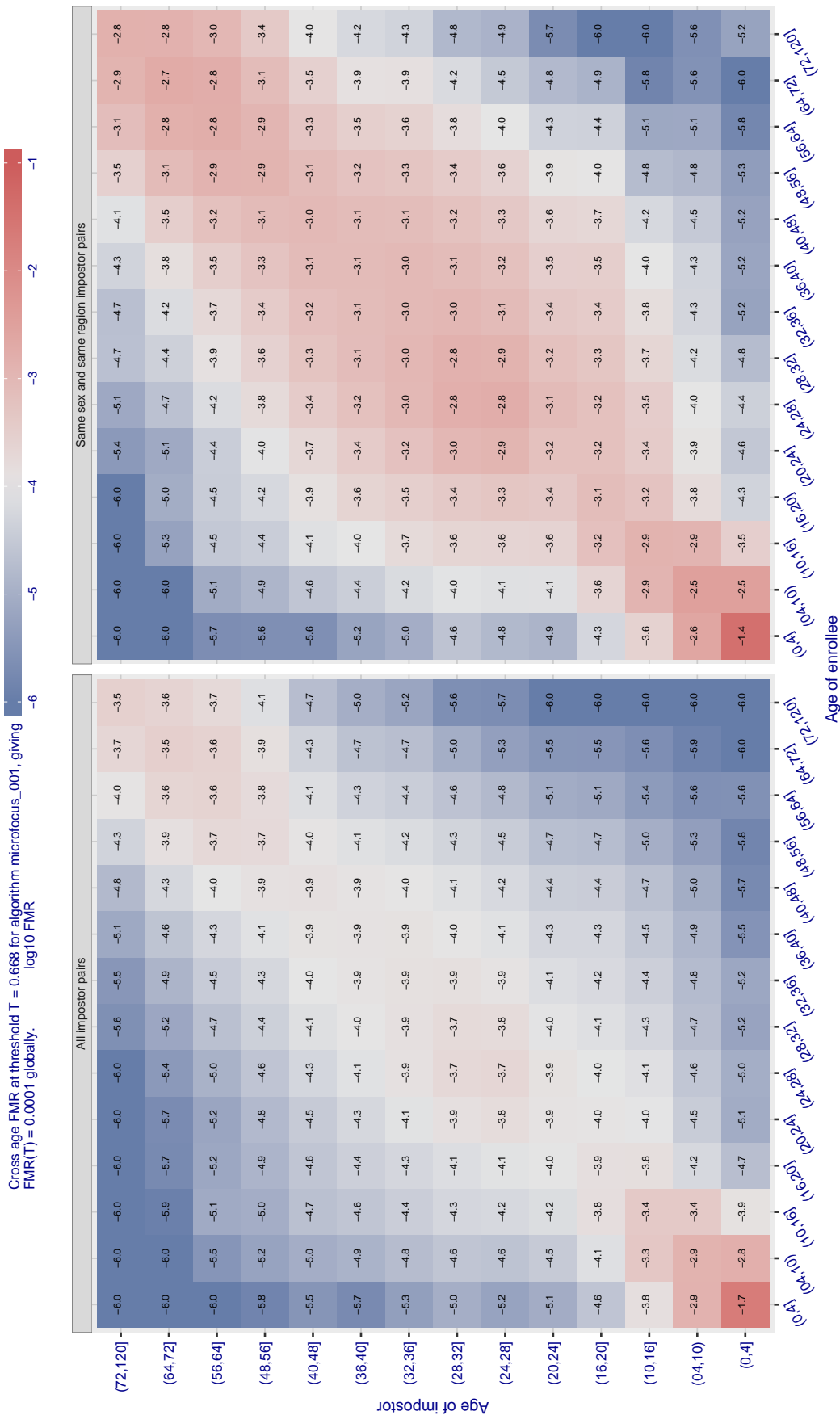


Figure 576: For algorithm microfocus-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

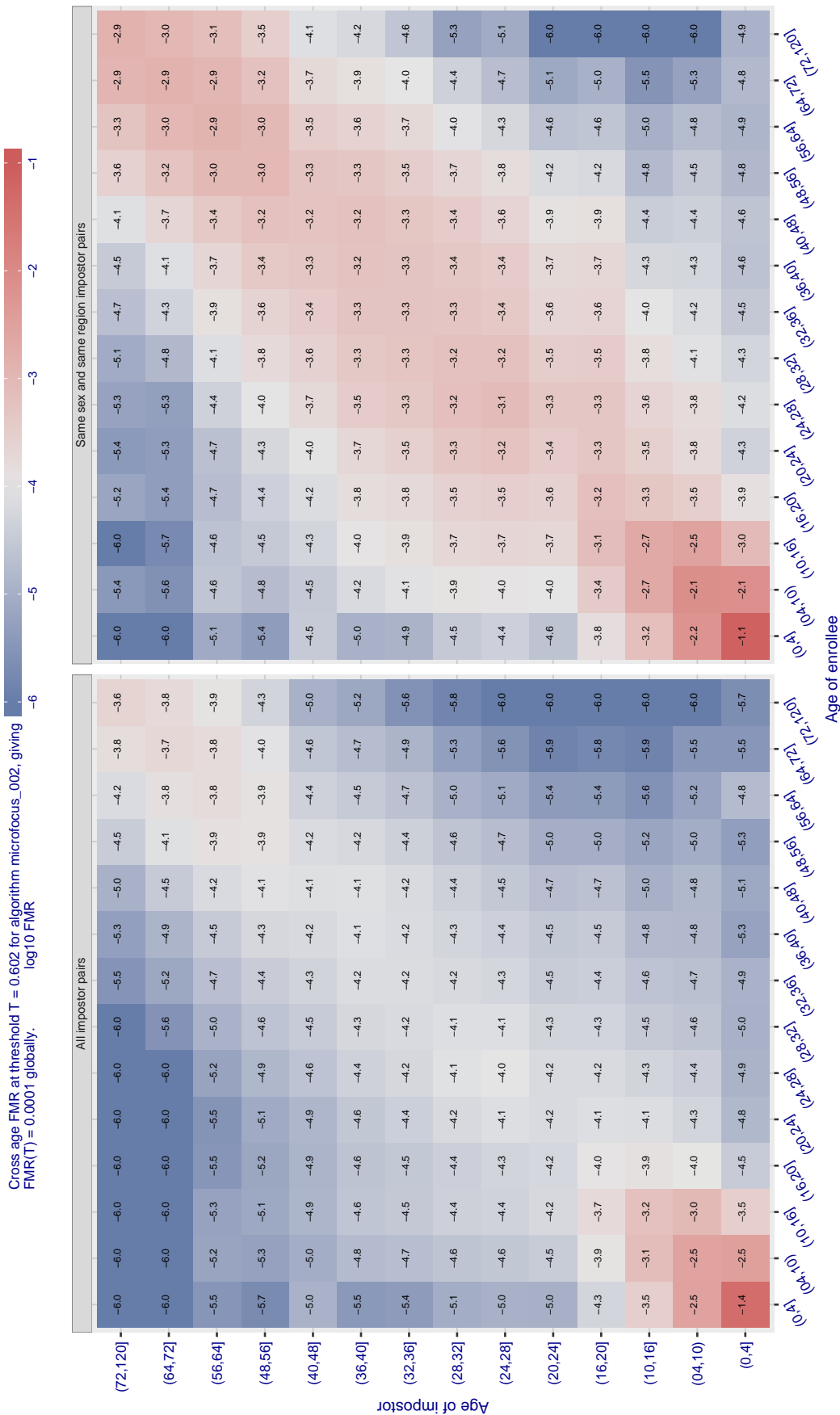


Figure 577: For algorithm microfocus-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

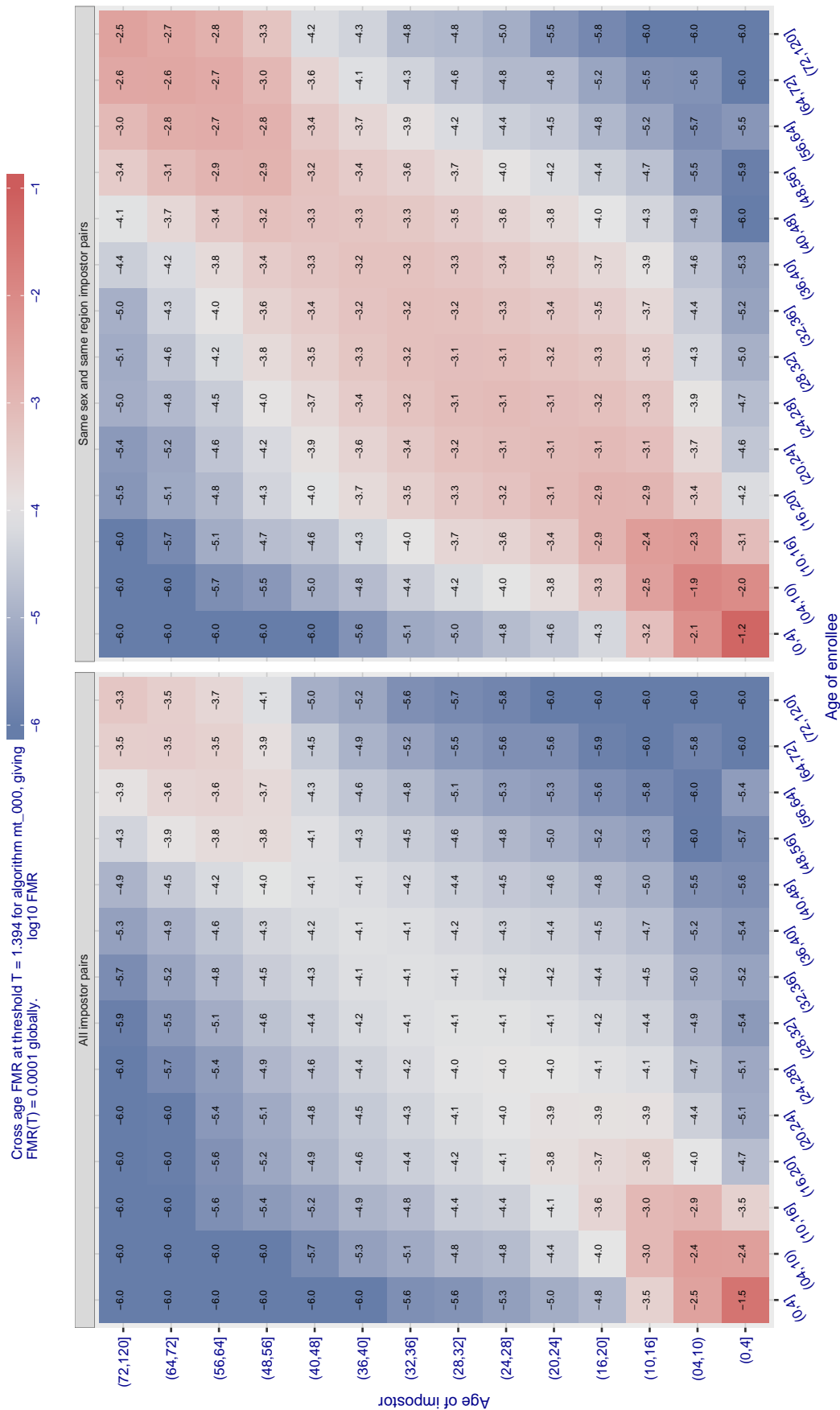


Figure 578: For algorithm mt-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

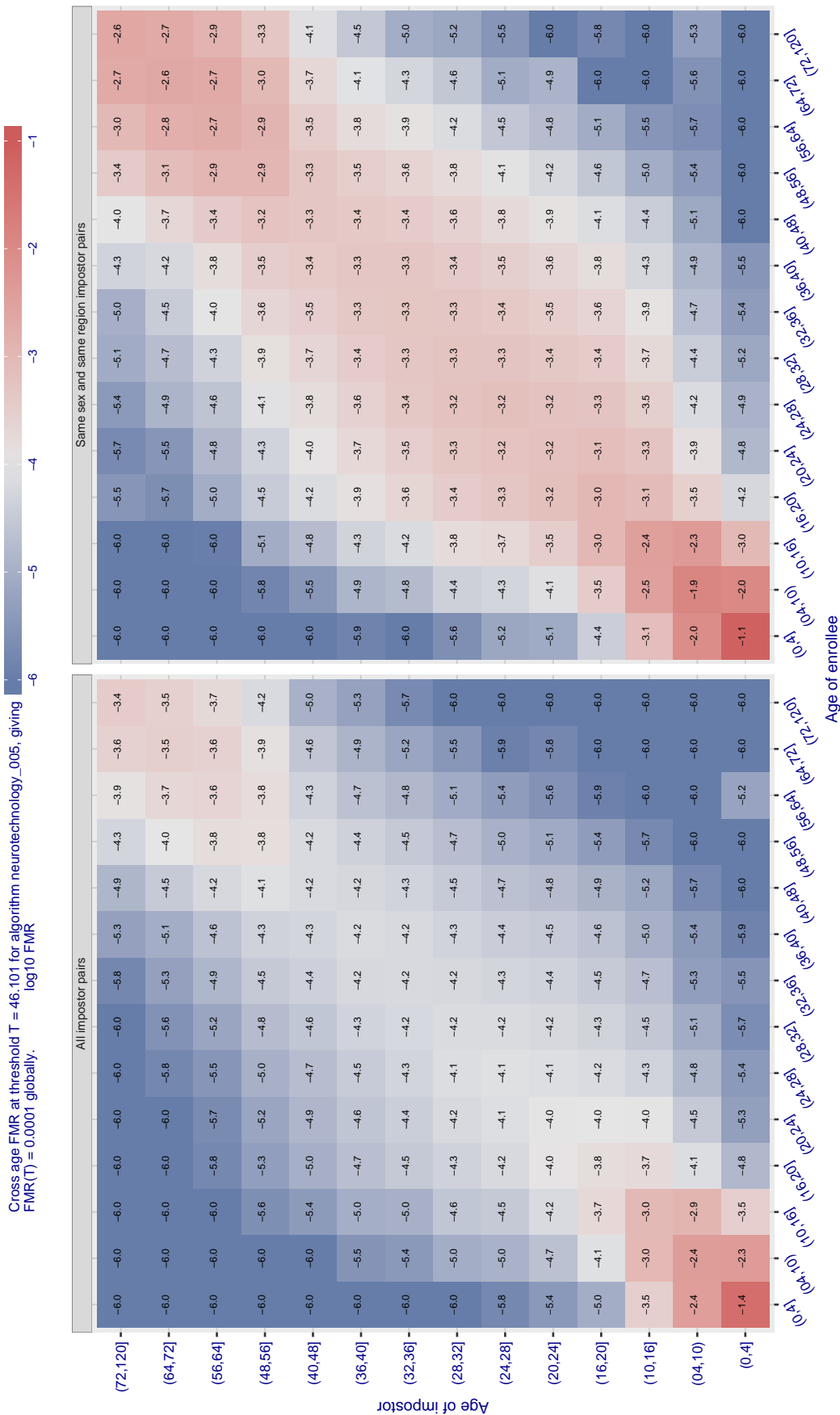


Figure 579: For algorithm neurotechnology-005 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

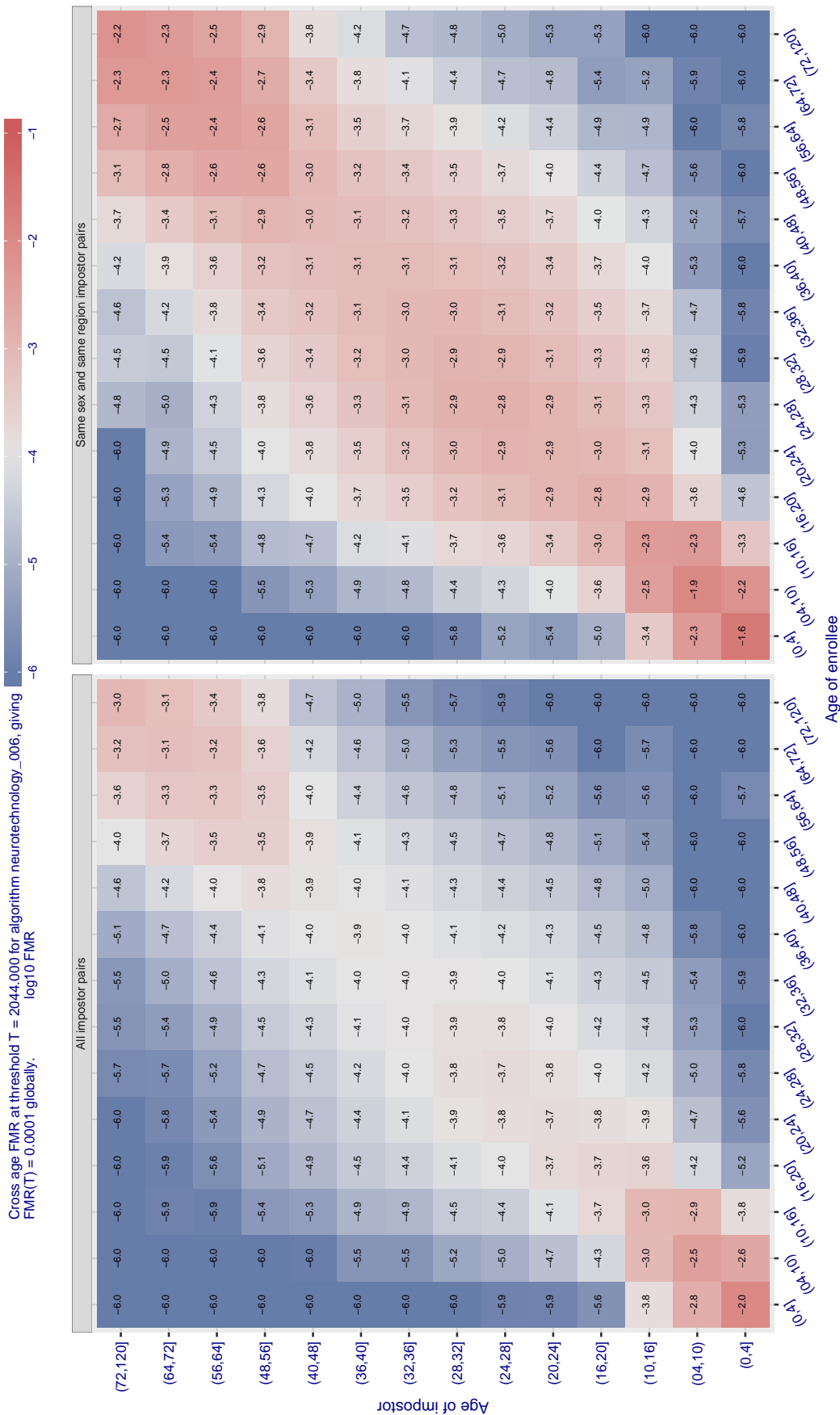


Figure 580: For algorithm neurotechnology-006 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 1.000$  for algorithm nodeflux\_001, giving  $FMR(T) = 0.0001$  globally.

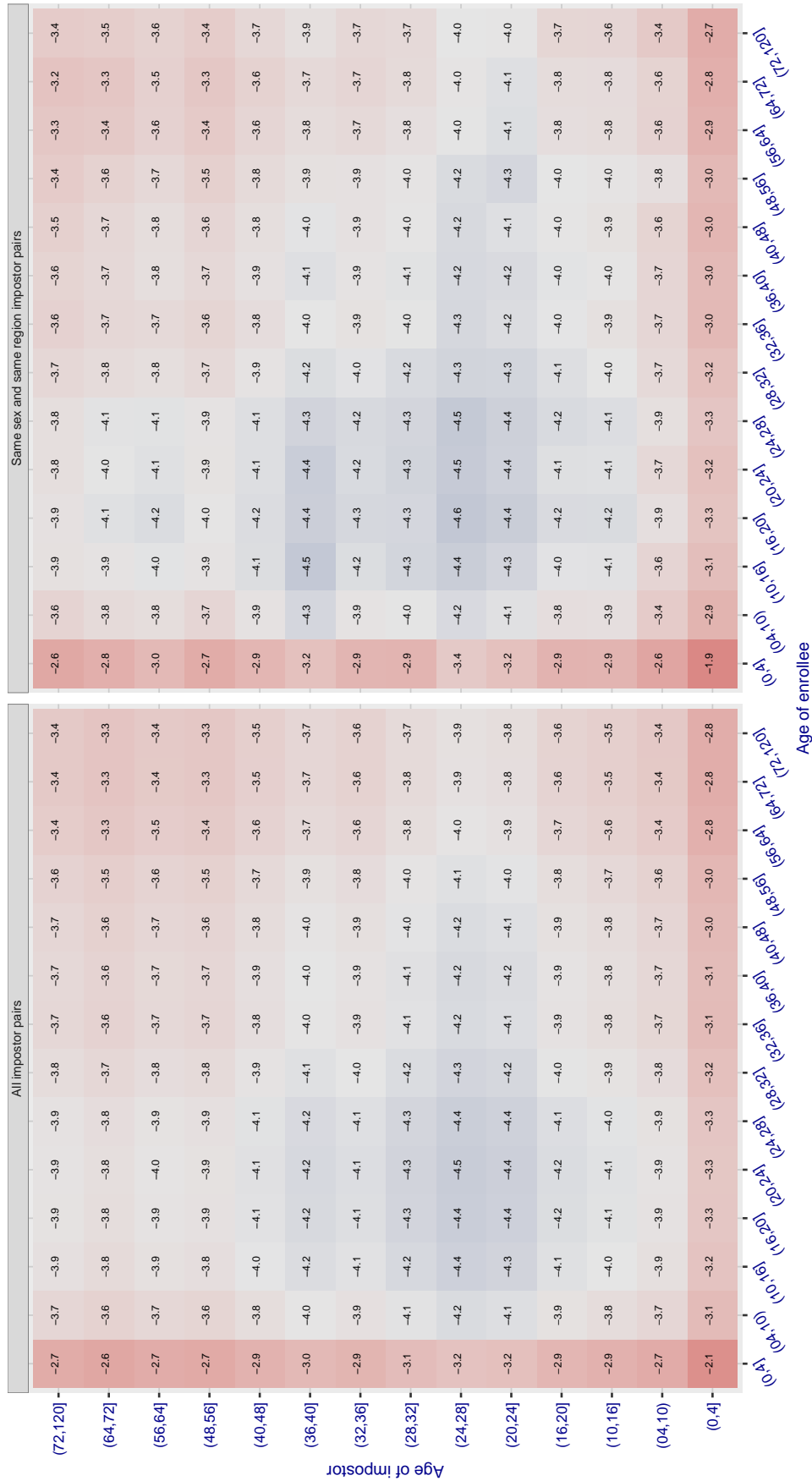


Figure 581: For algorithm nodeflux-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

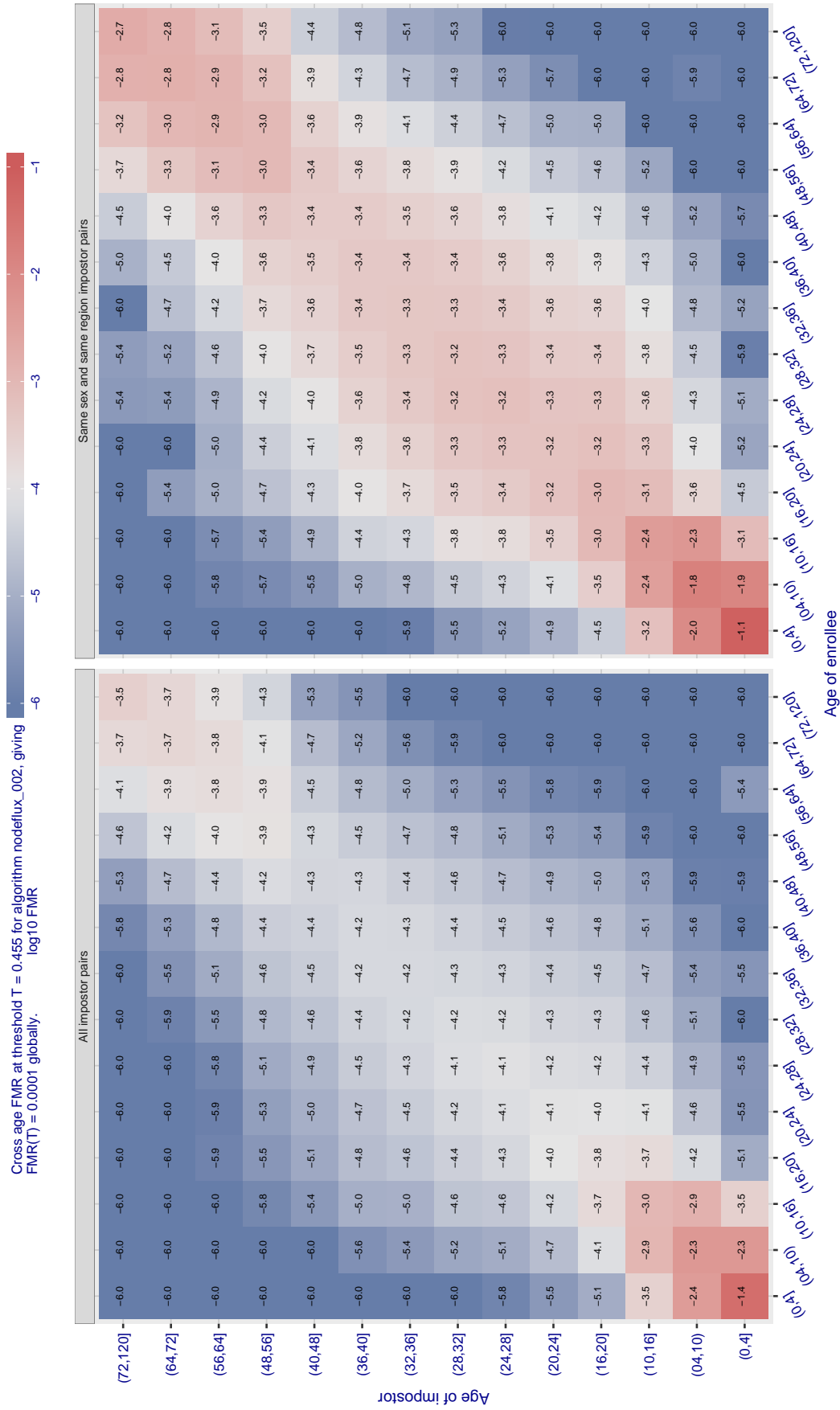


Figure 582: For algorithm nodeflux-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.



78728508749508306738122785099180495252950144487468954605214391819635563576348021983576872062648638901233947118338438420271161854018147318546067599795435142378710012068708547335424481767

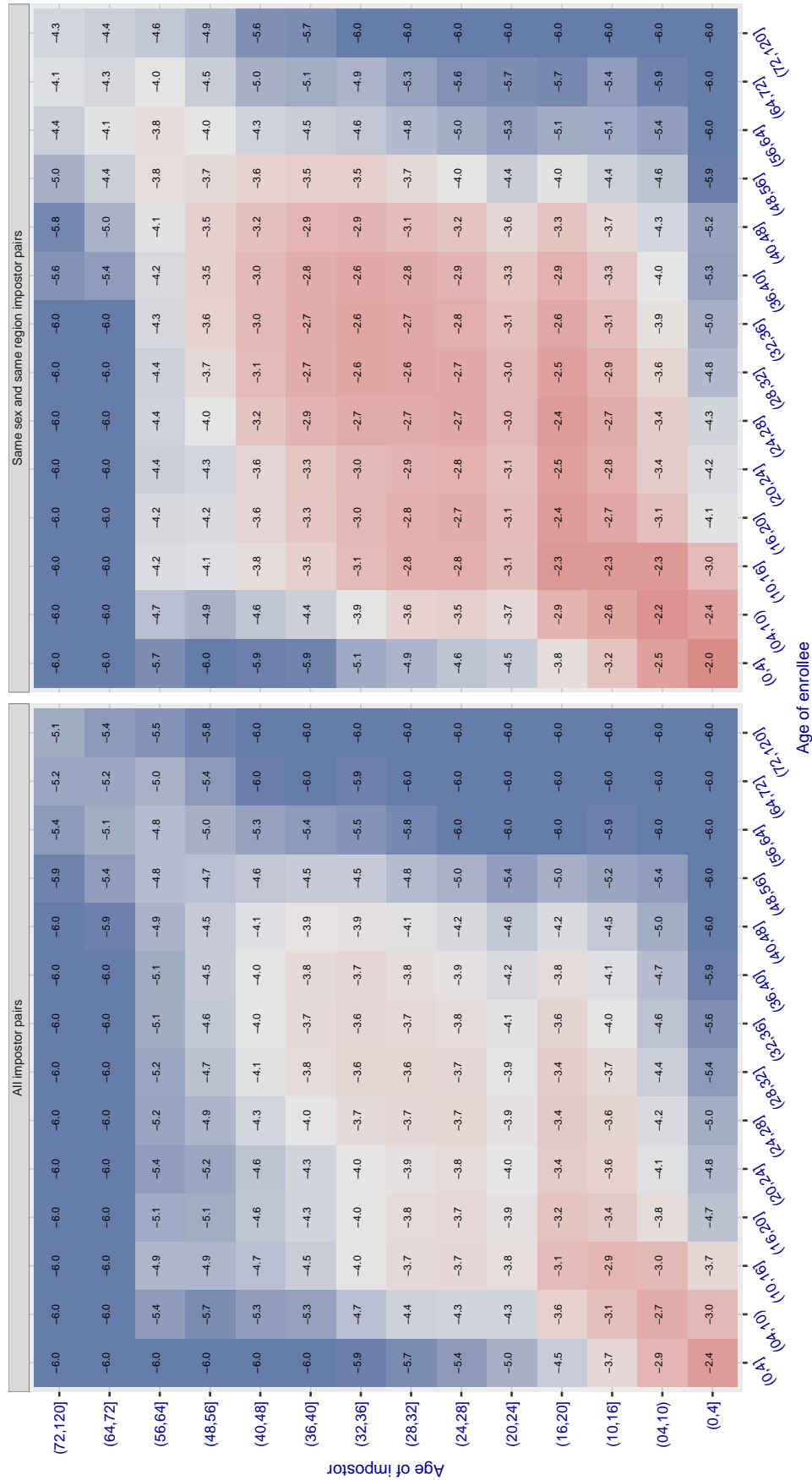


Figure 583: For algorithm notontag-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give FMR = 0.0001 over all on the order of 10<sup>10</sup> impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

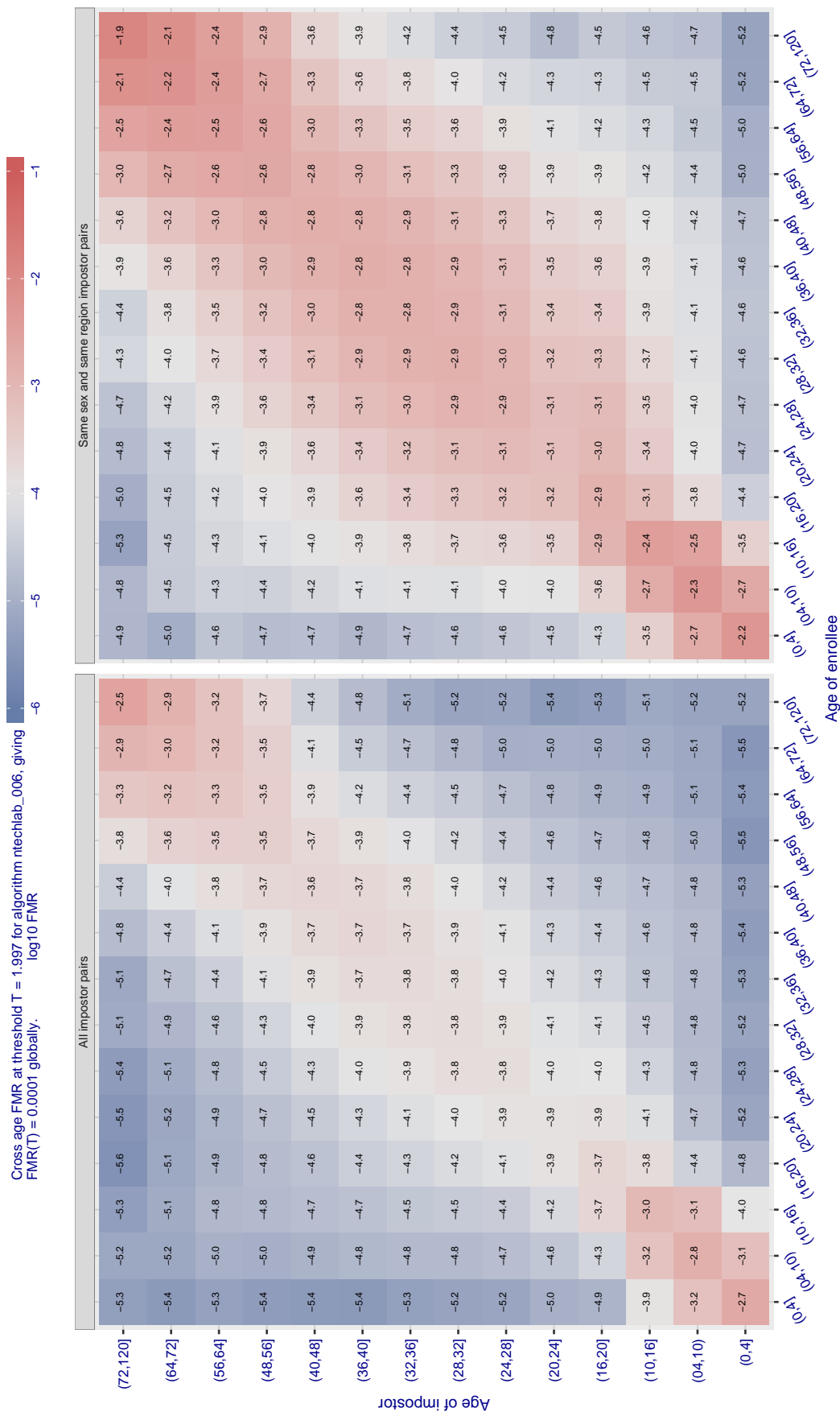


Figure 584: For algorithm ntechlab-006 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 1.416$  for algorithm nteclab\_007, giving  $\log_{10} \text{FMR}(T) = 0.0001$  globally.

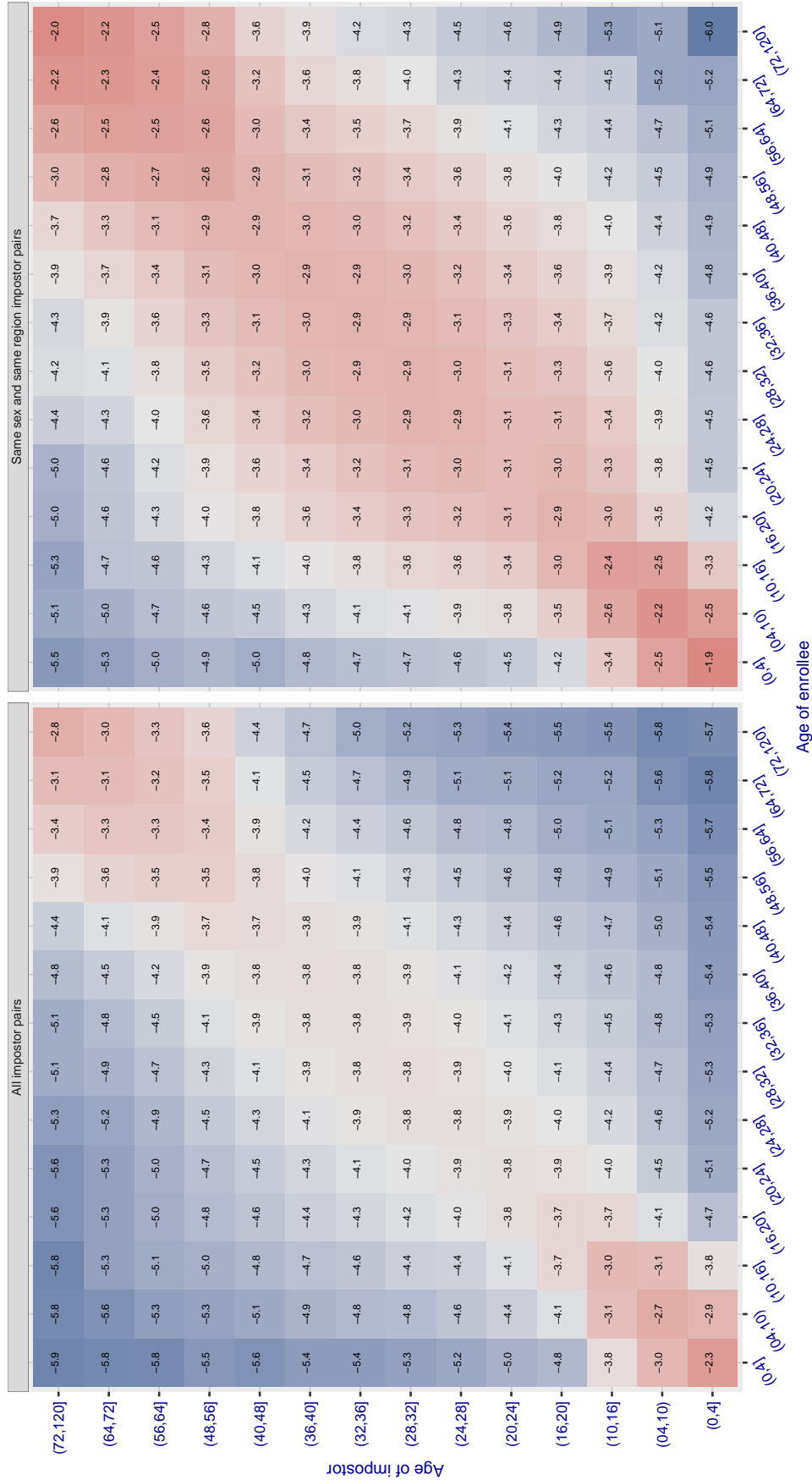


Figure 585: For algorithm nteclab-007 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.428$  for algorithm pixelall\_002, giving  $FMR(T) = 0.0001$  globally.

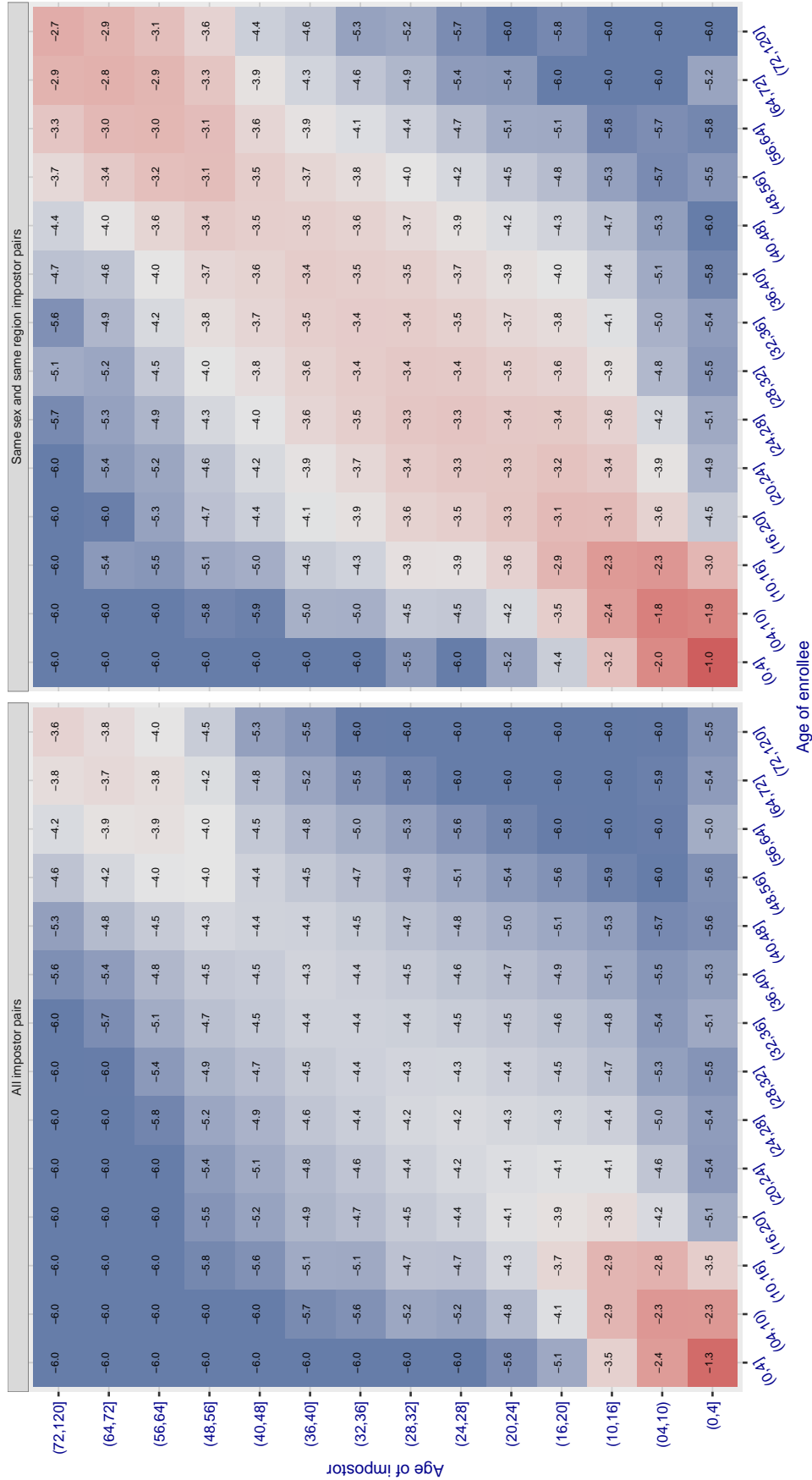


Figure 586: For algorithm pixelall-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.389$  for algorithm pixelall\_003, giving  $FMR(T) = 0.0001$  globally.

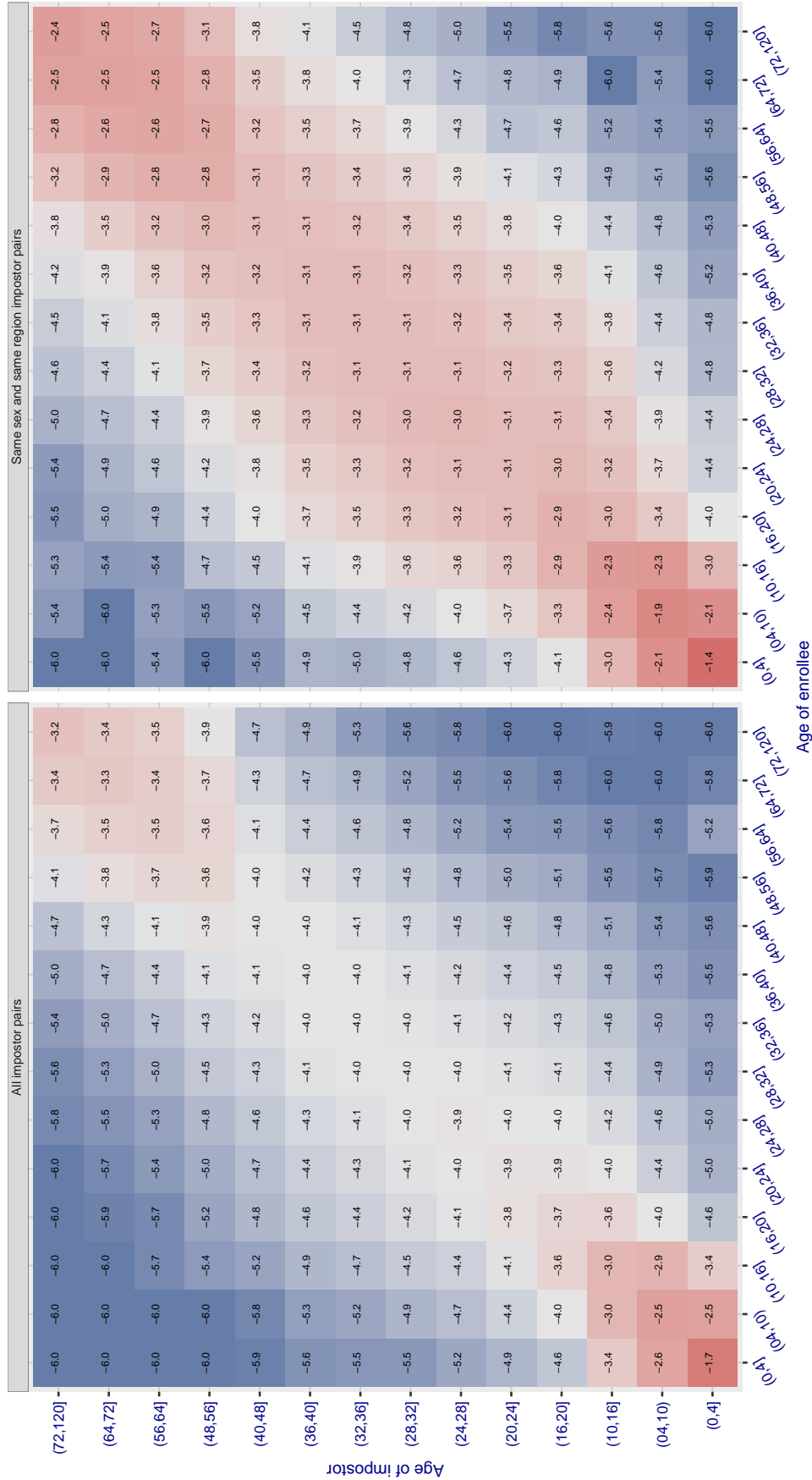


Figure 587: For algorithm pixelall-003 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

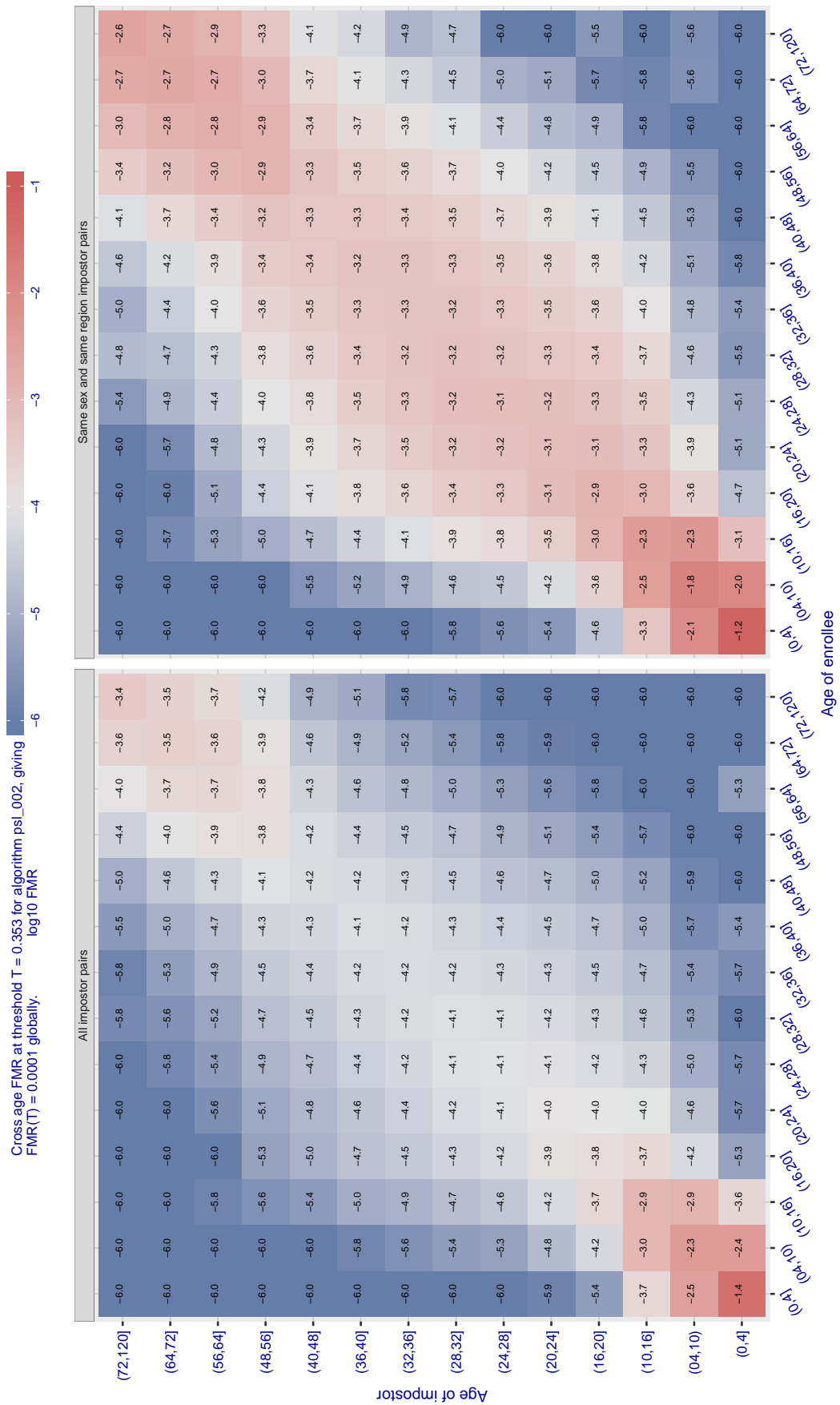


Figure 588: For algorithm `psl-002` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

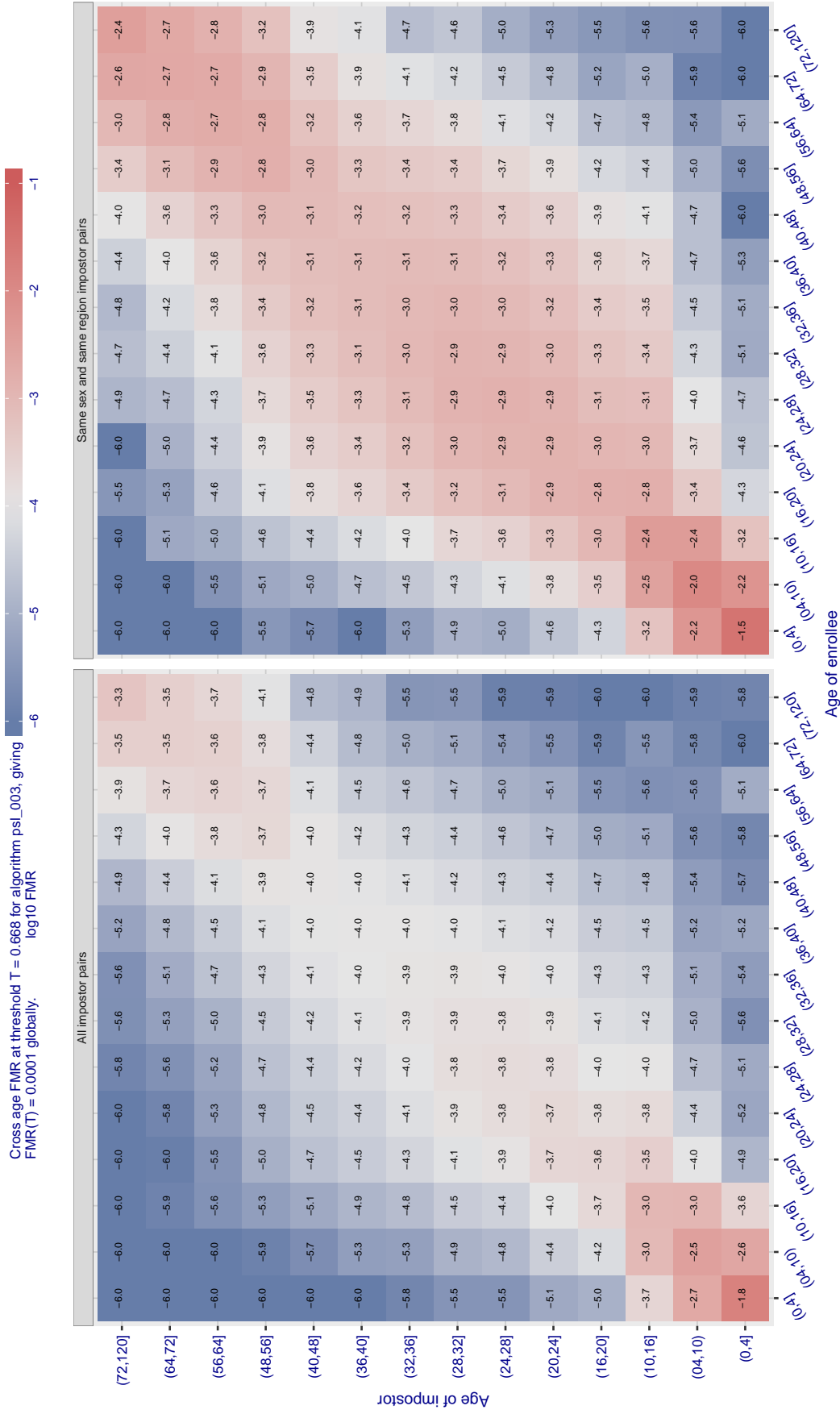


Figure 589: For algorithm `psl-003` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

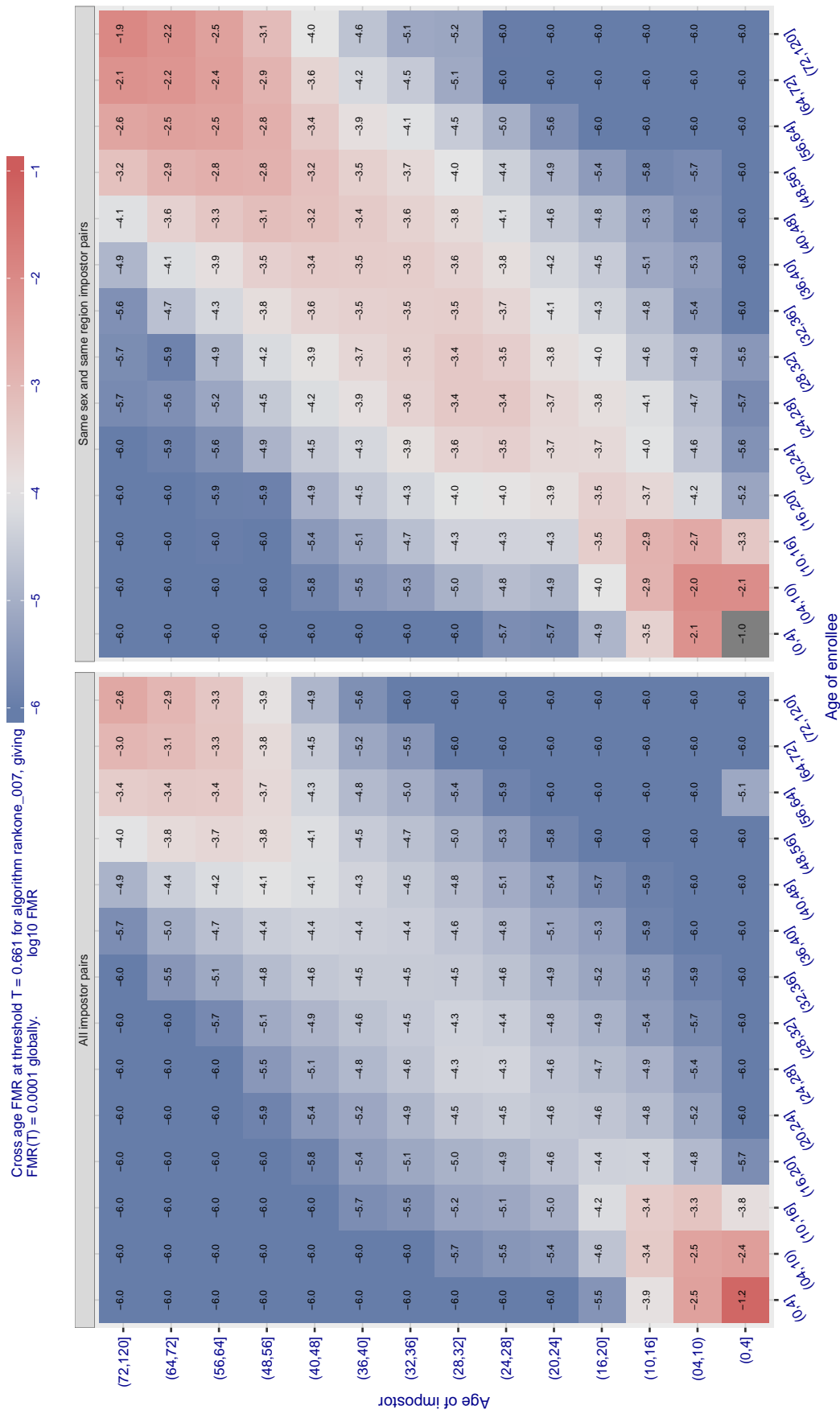


Figure 590: For algorithm rankone-007 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.



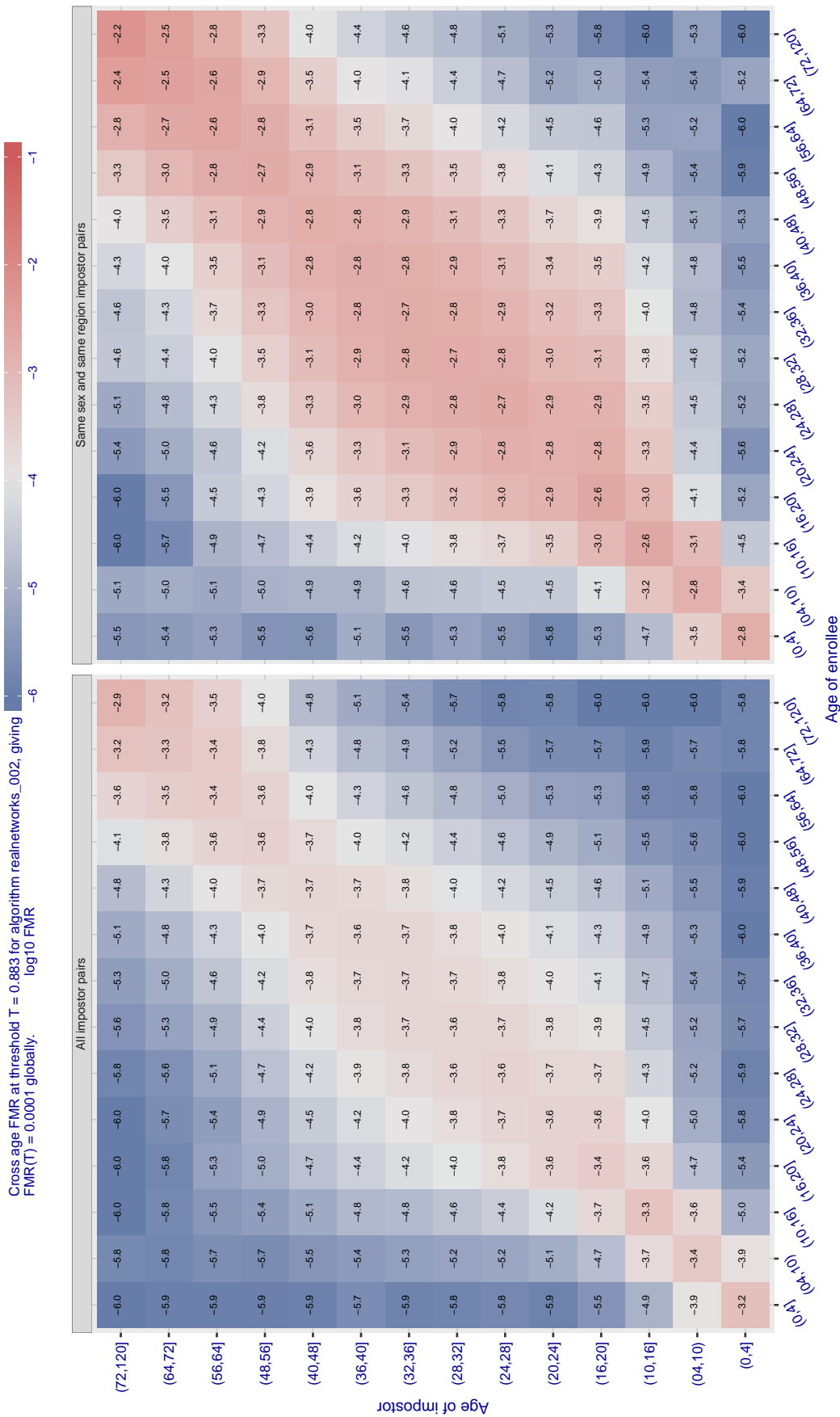


Figure 591: For algorithm reainetworks-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

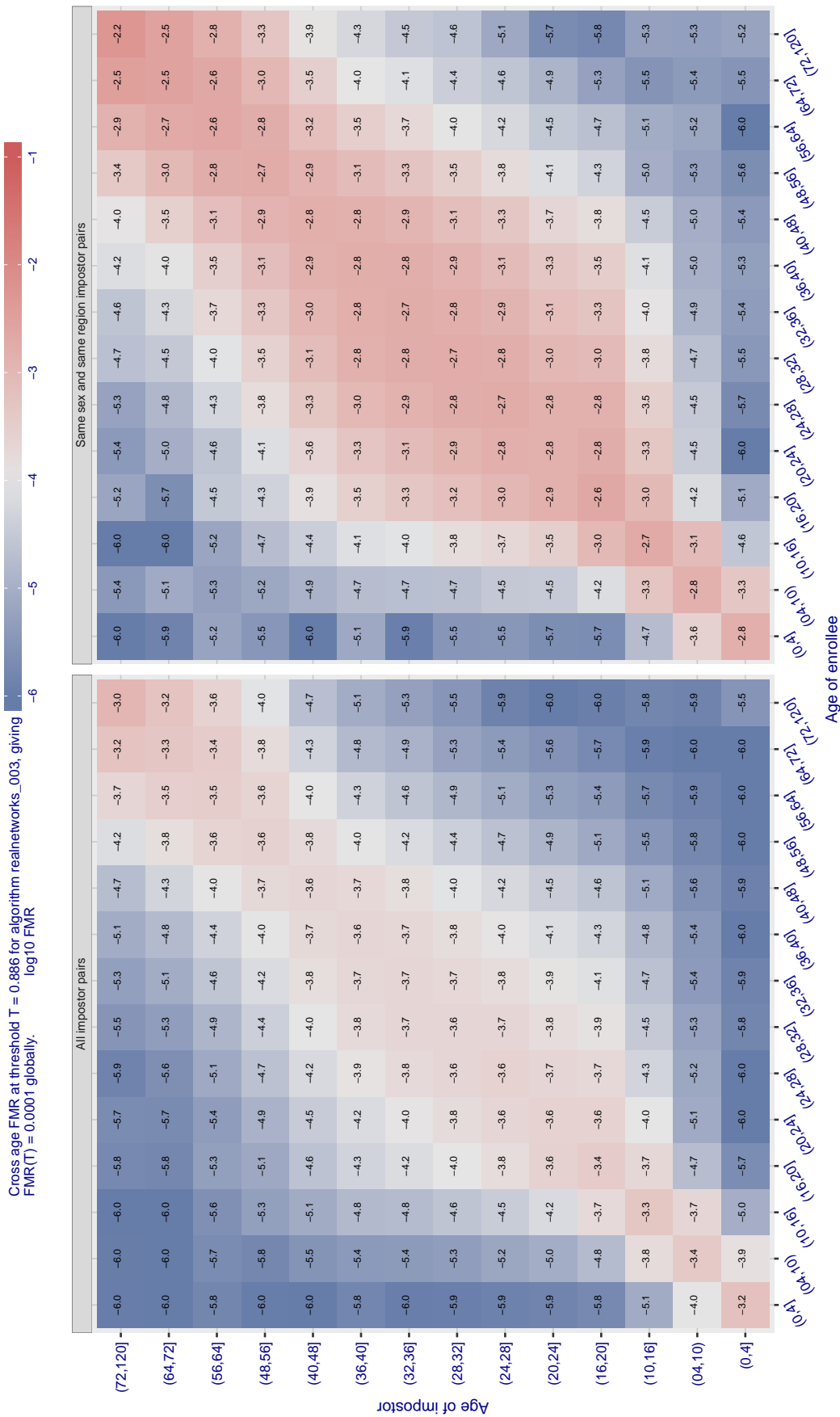


Figure 592: For algorithm reainetworks-003 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

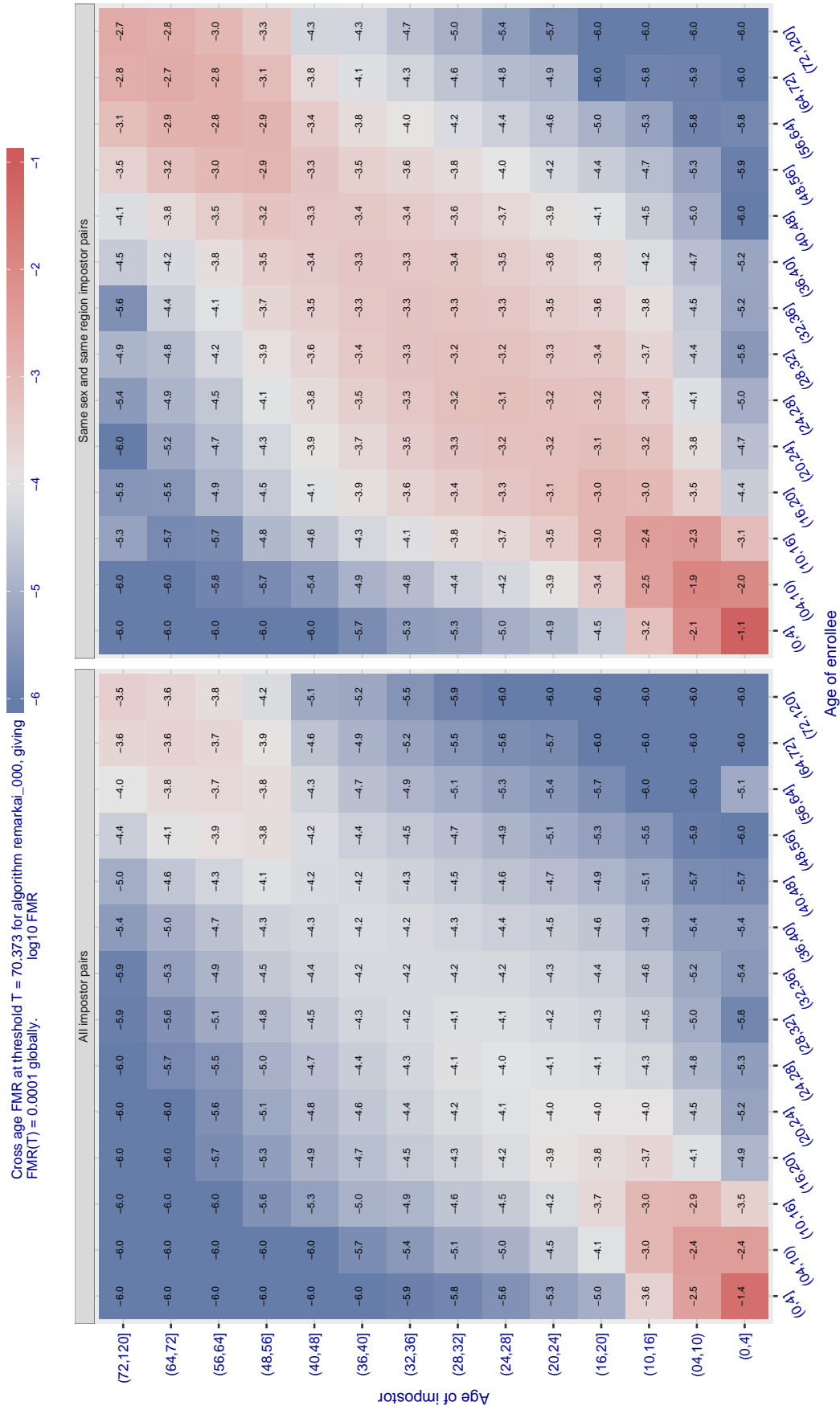


Figure 593: For algorithm remarkai-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

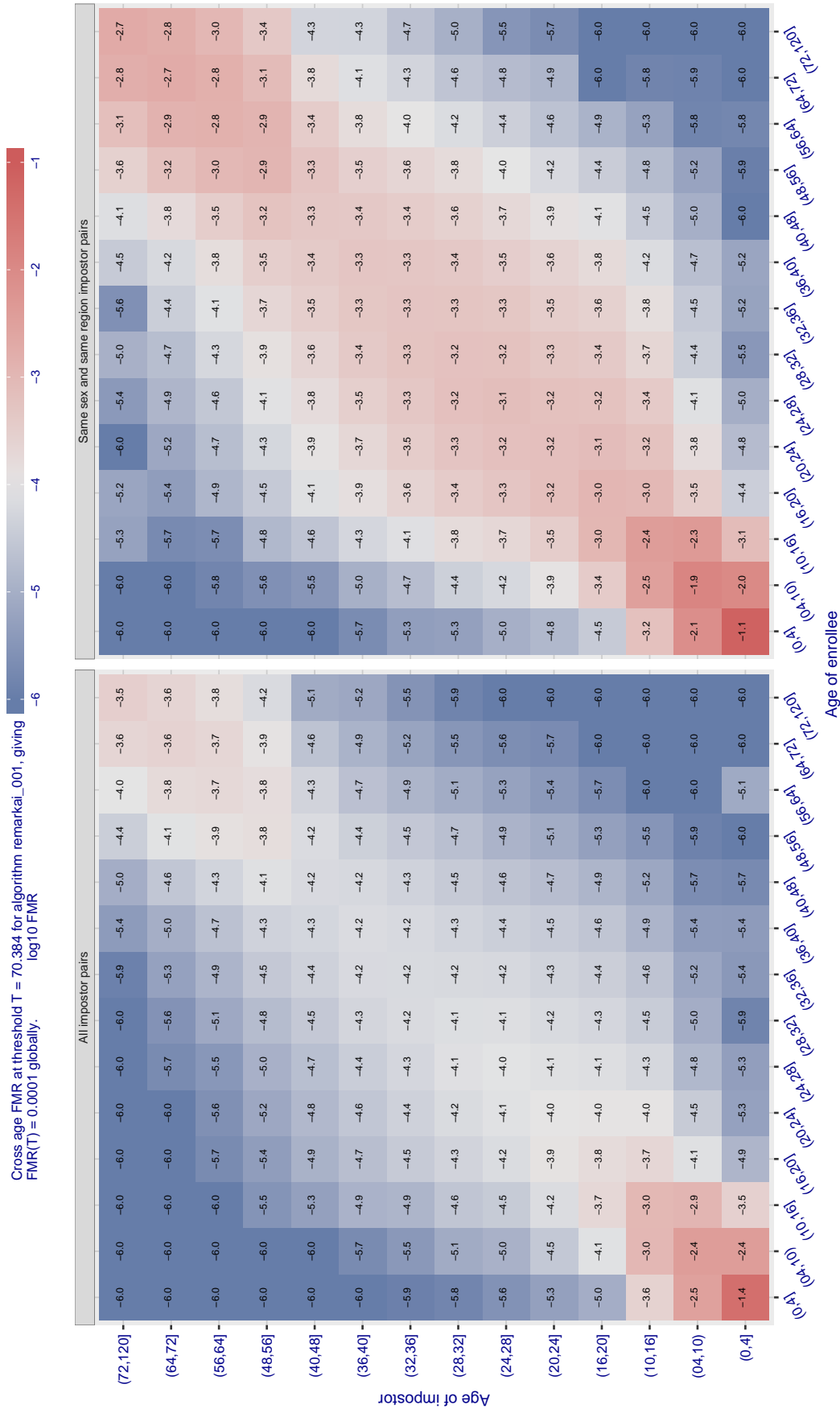


Figure 594: For algorithm remarkai-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

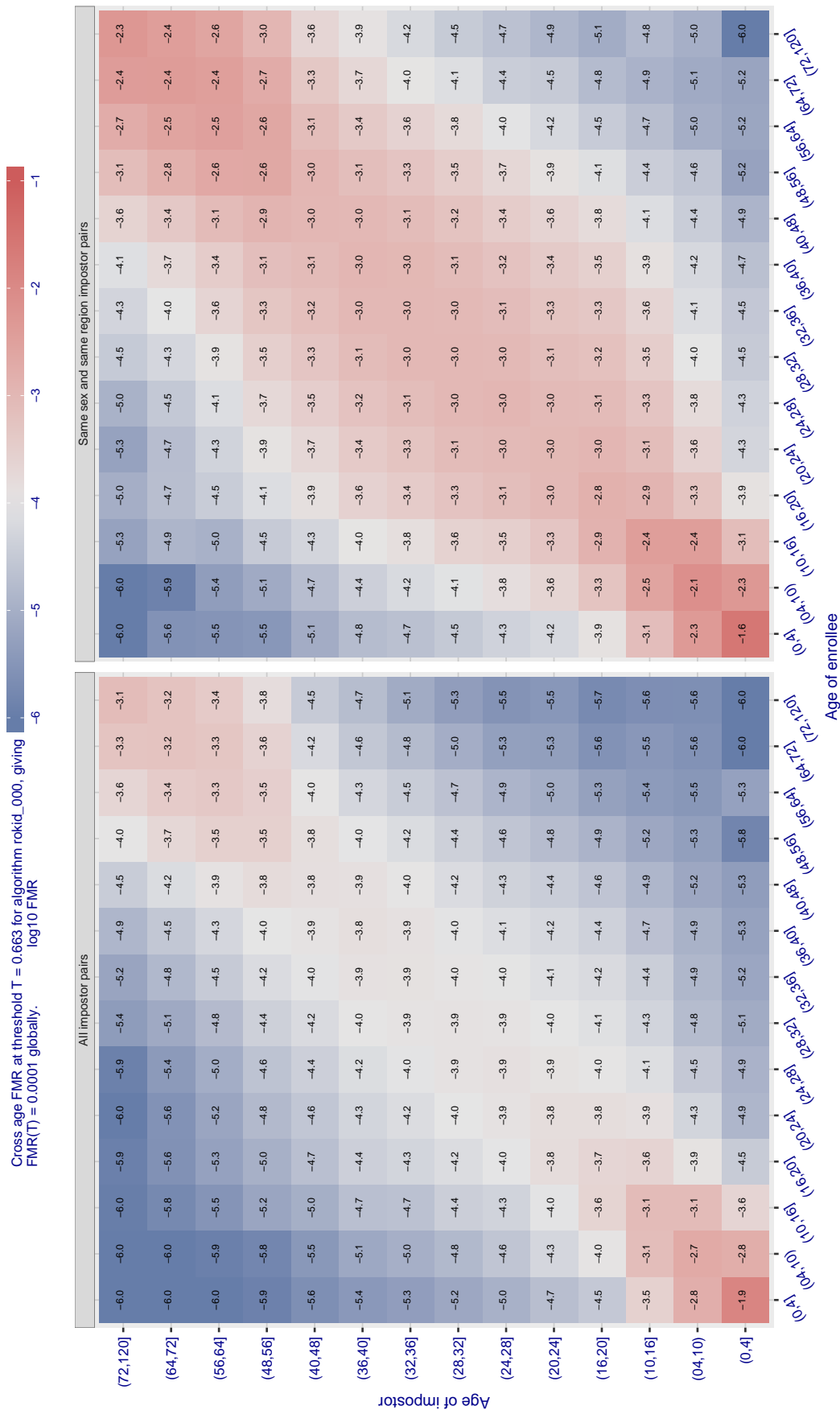


Figure 595: For algorithm rokid-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

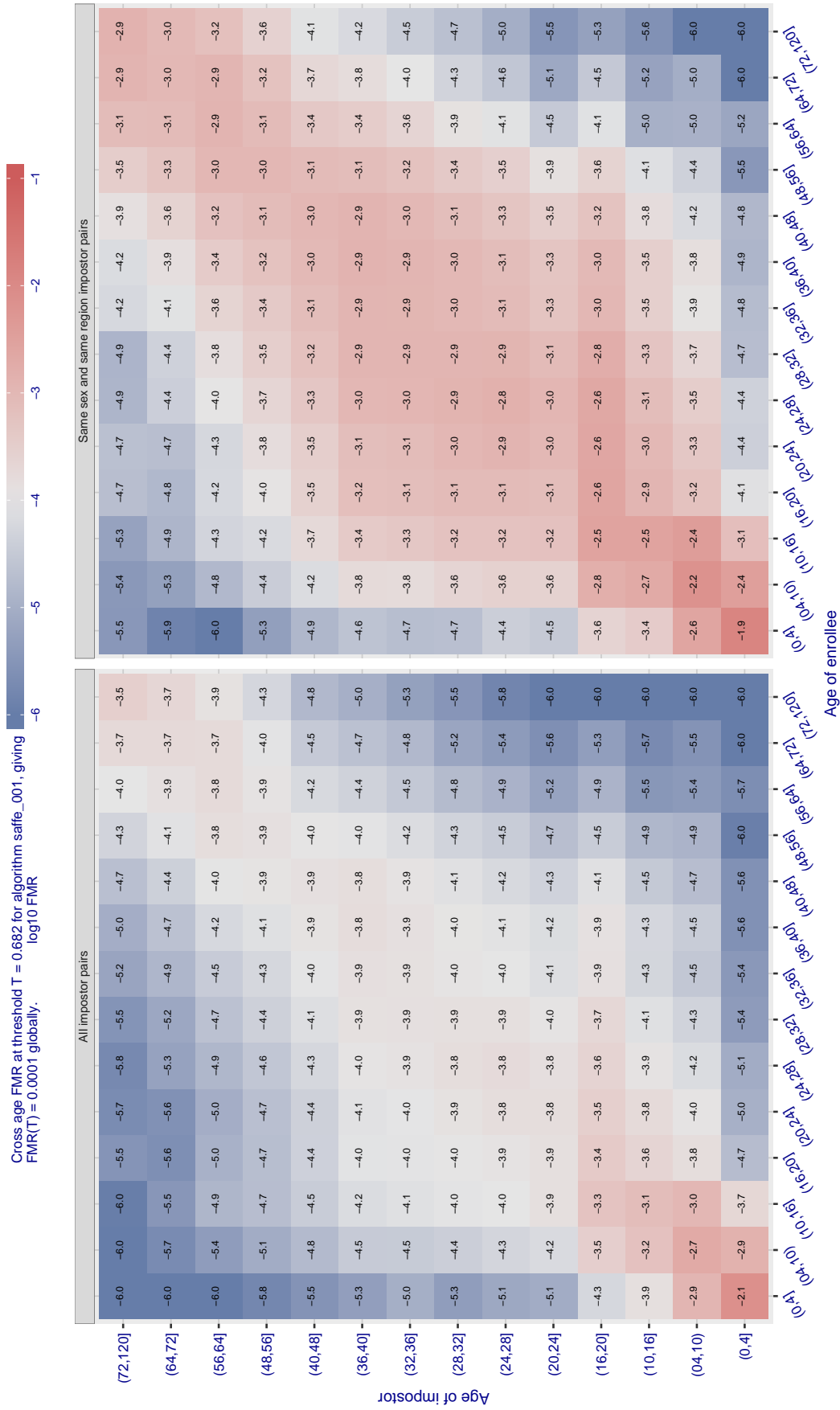


Figure 59c: For algorithm saffe-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

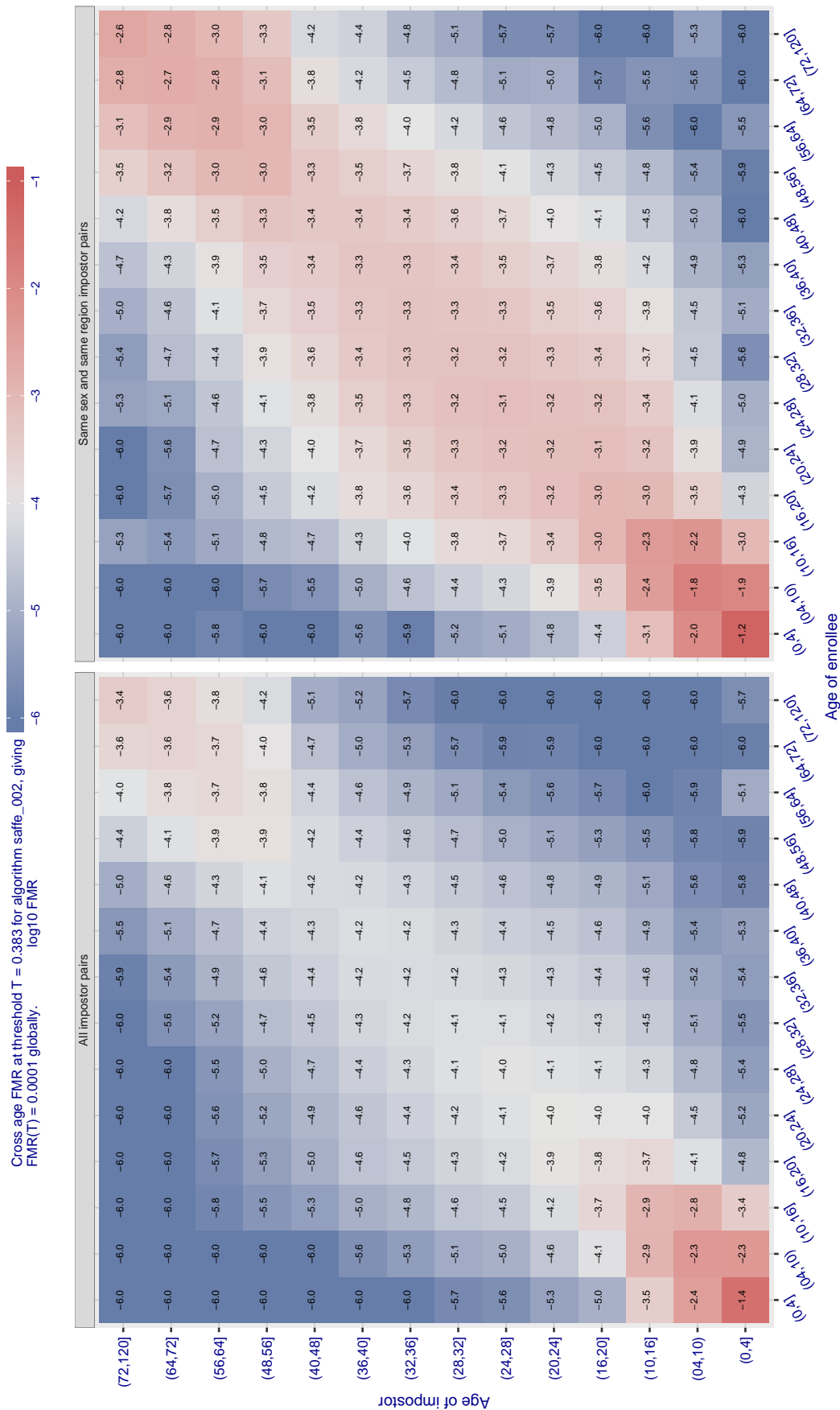


Figure 597: For algorithm saffe-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

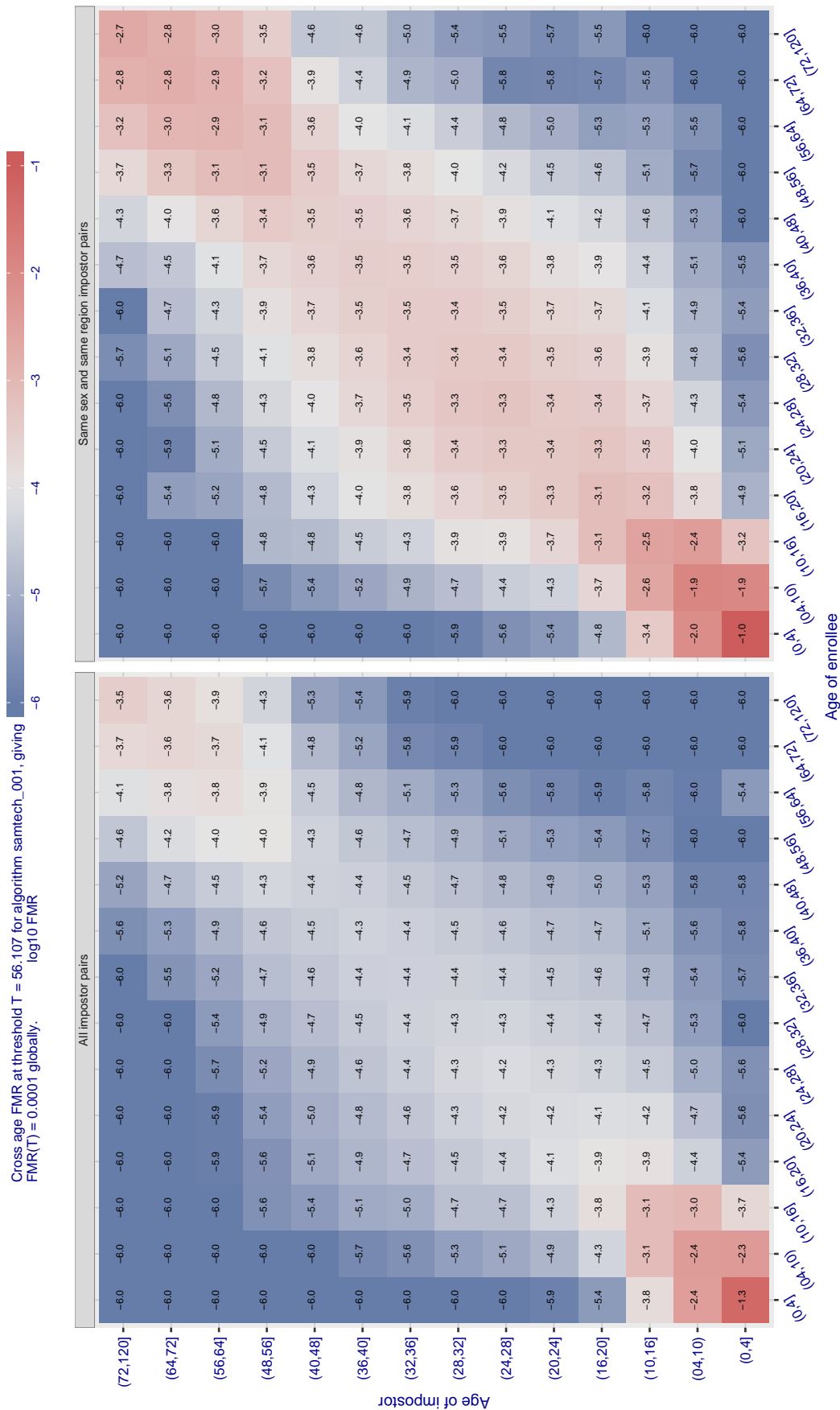


Figure 598: For algorithm samtech-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.



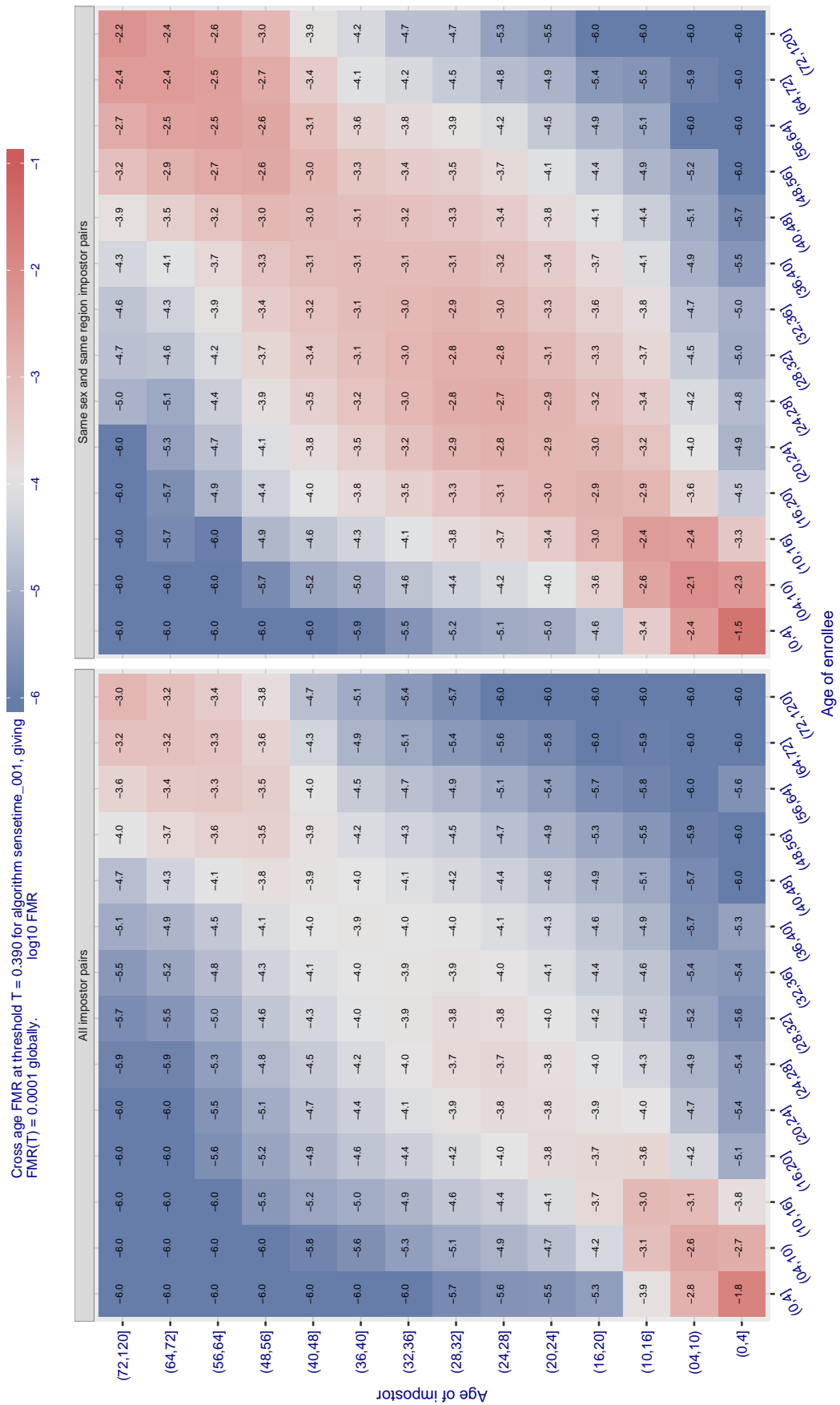


Figure 599: For algorithm `sensetime-001` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

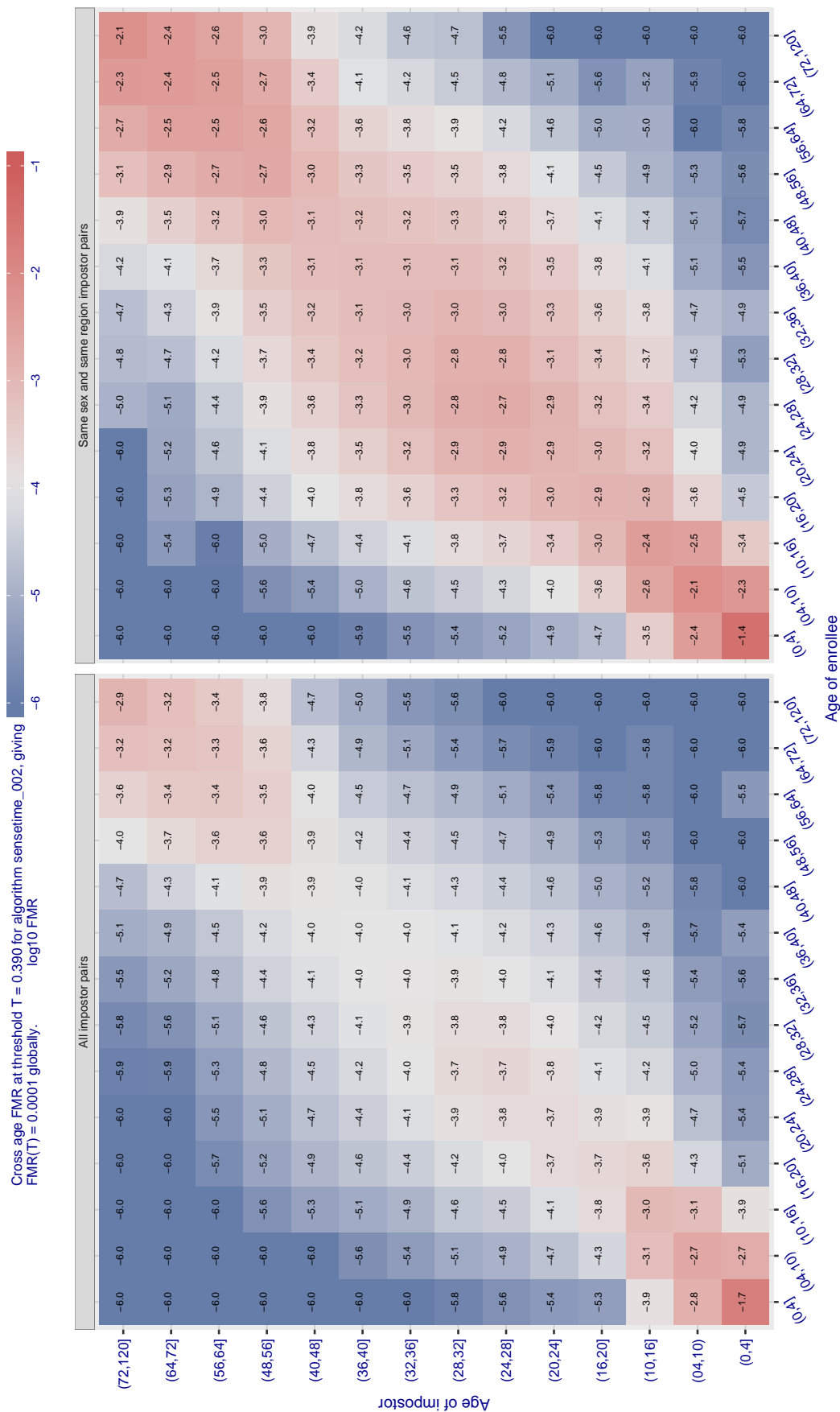


Figure 600: For algorithm `sensetime-002` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

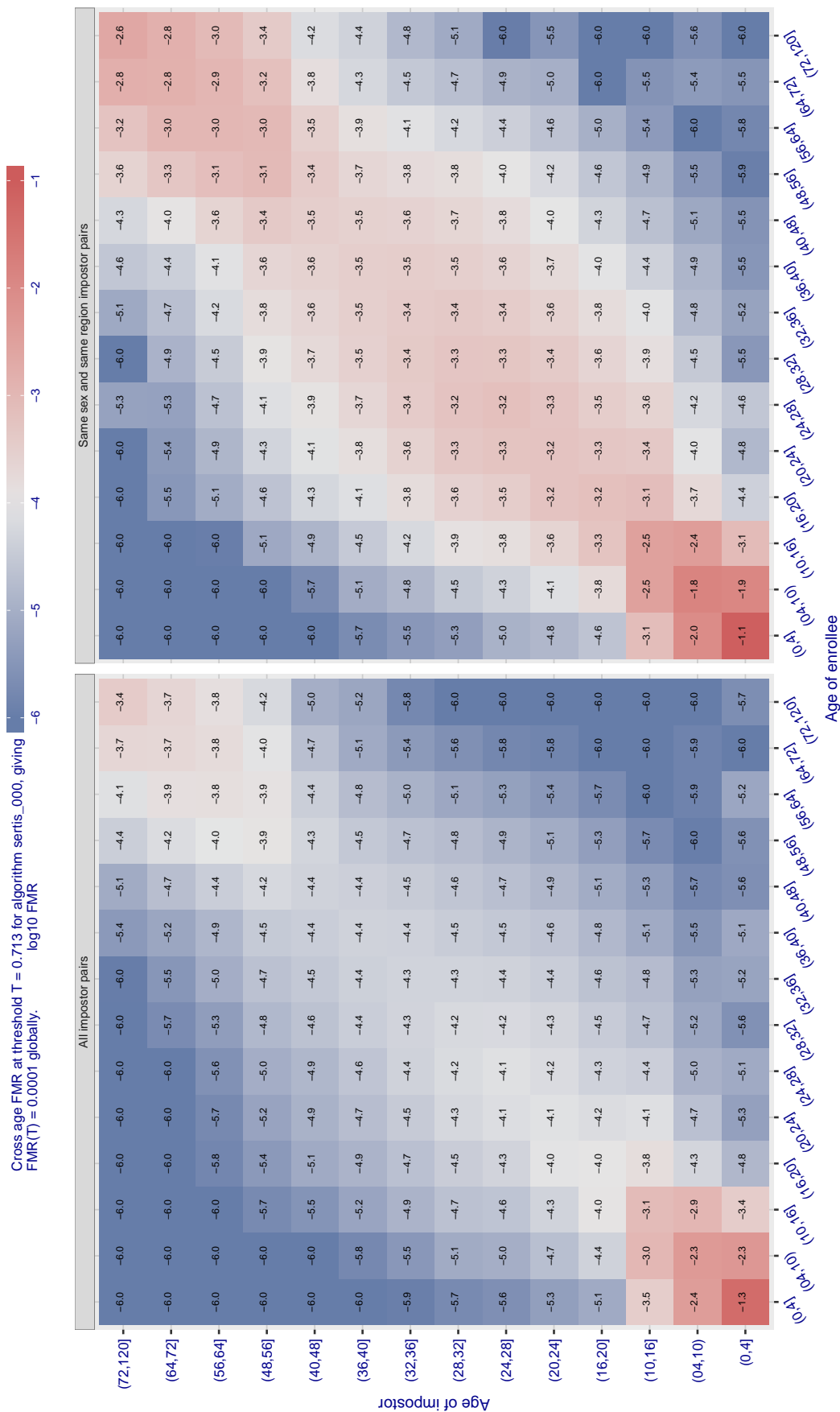


Figure 601: For algorithm `sertis-000` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

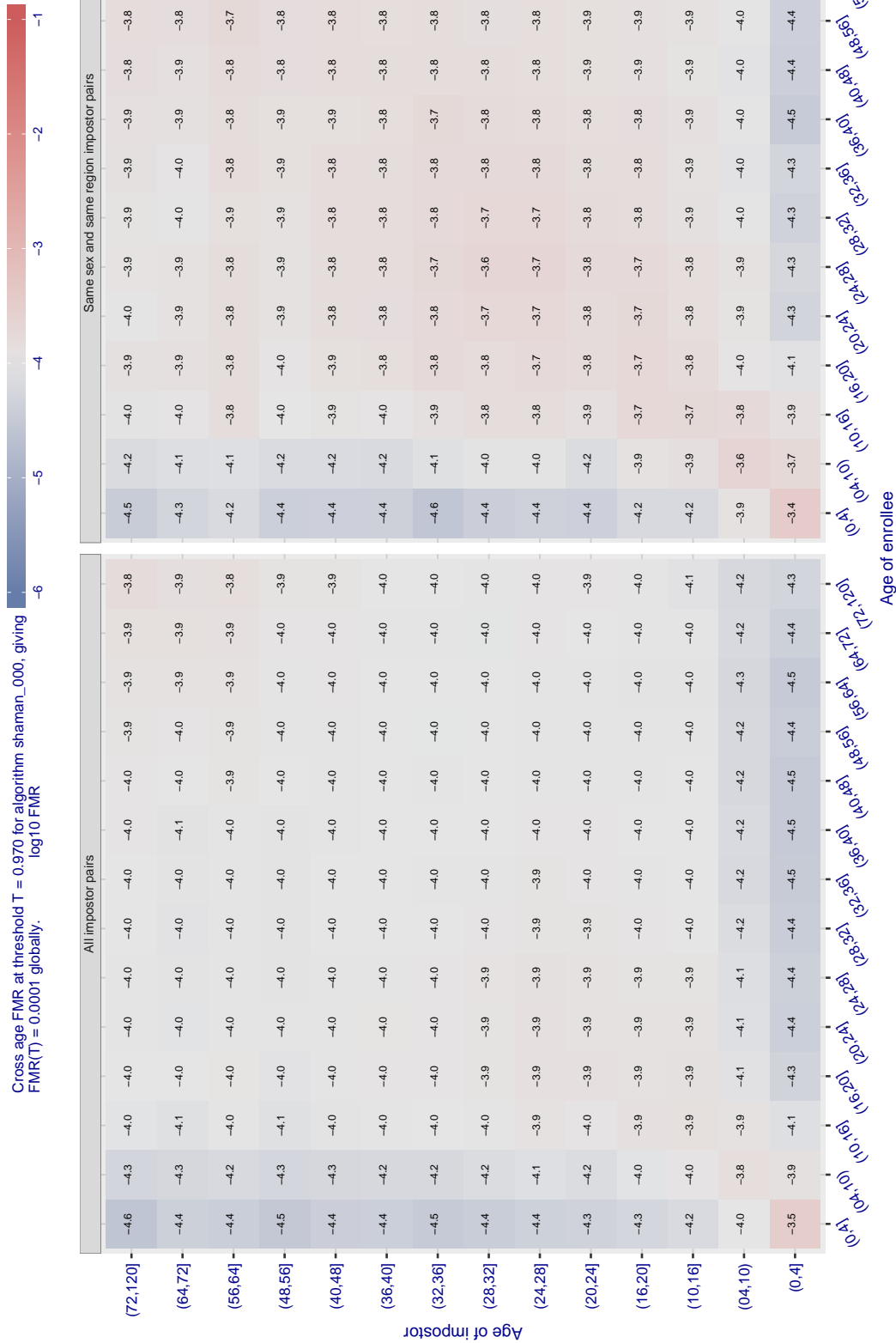


Figure 602: For an algorithm shaman-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

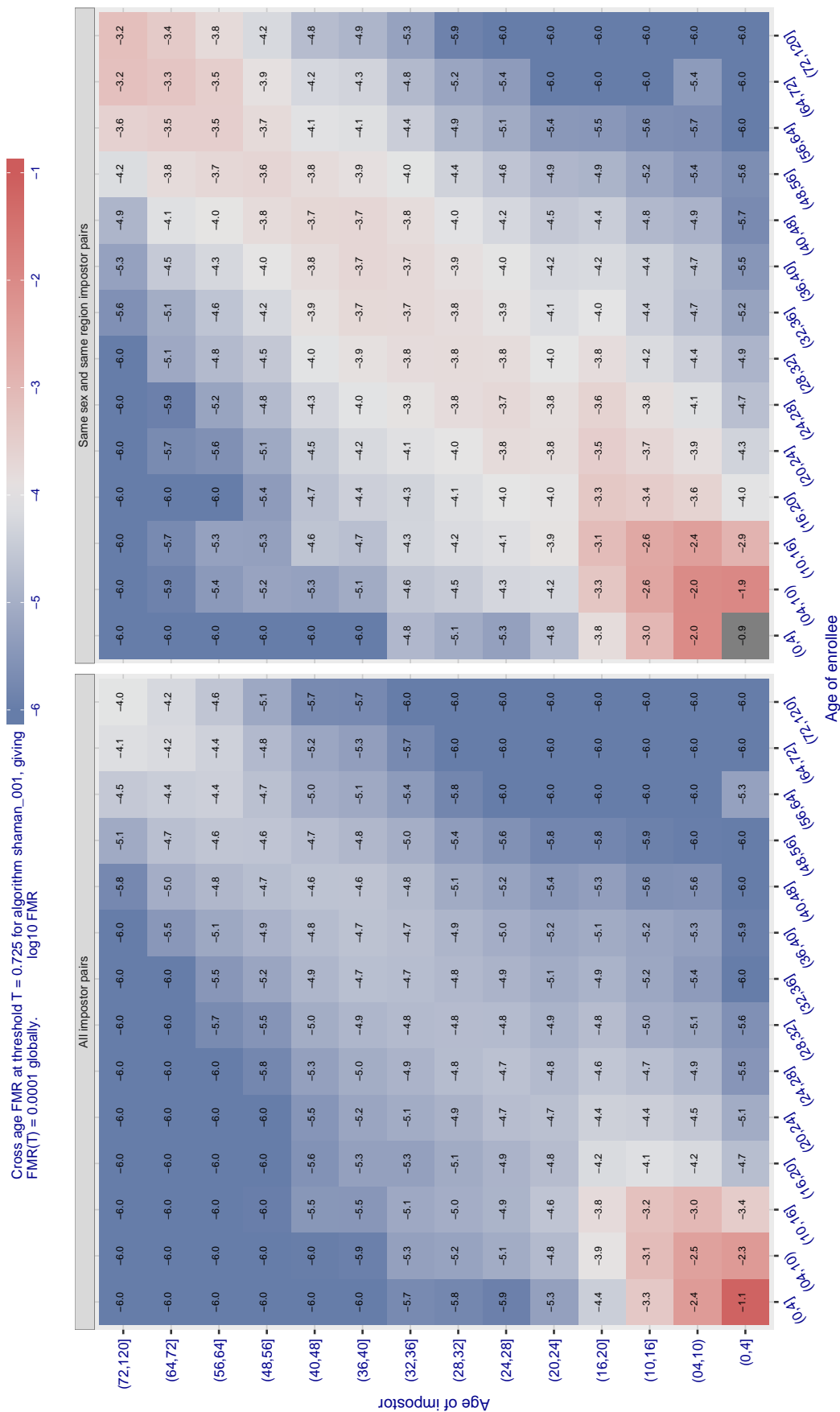


Figure 603: For algorithm shaman-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

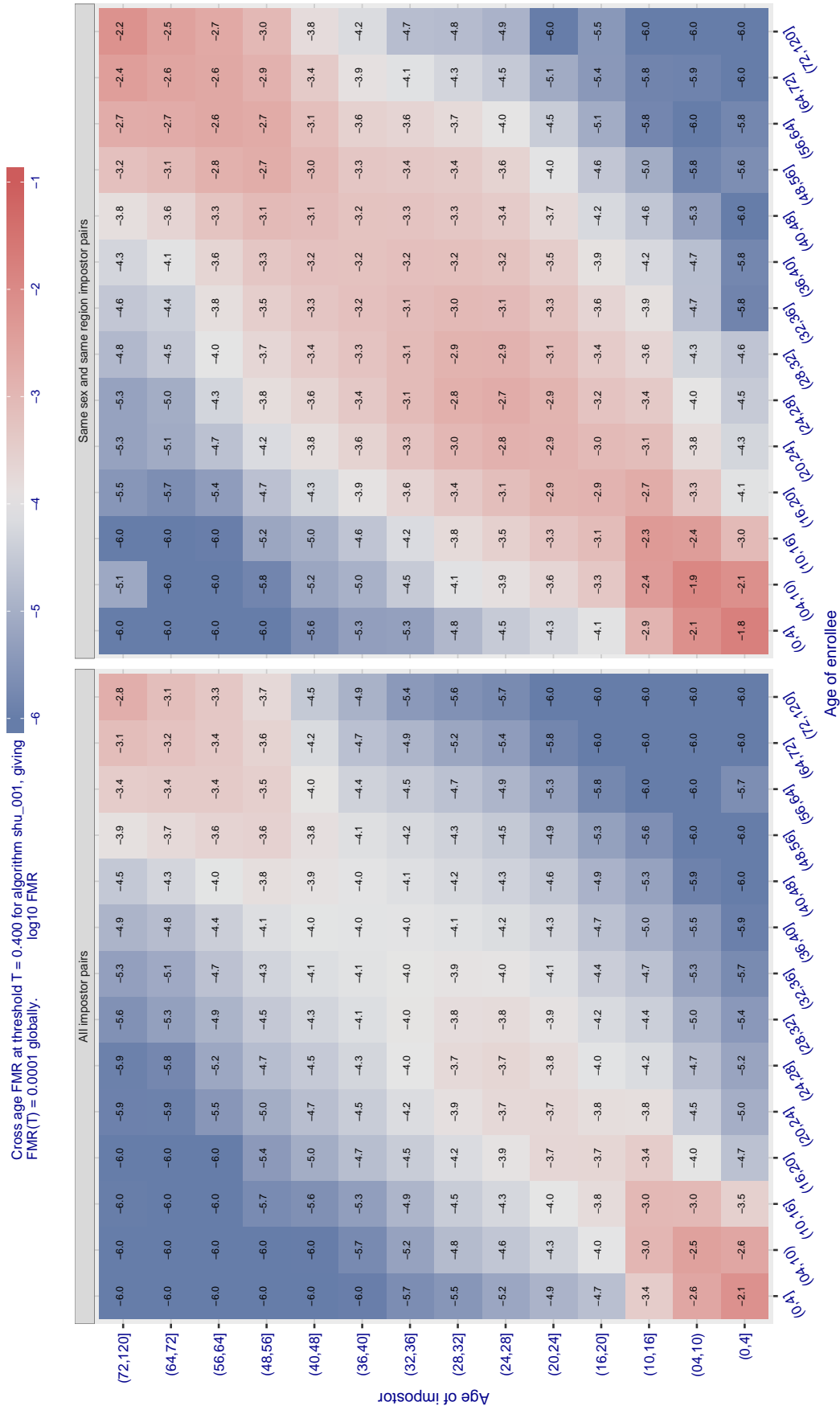


Figure 604: For algorithm shu-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

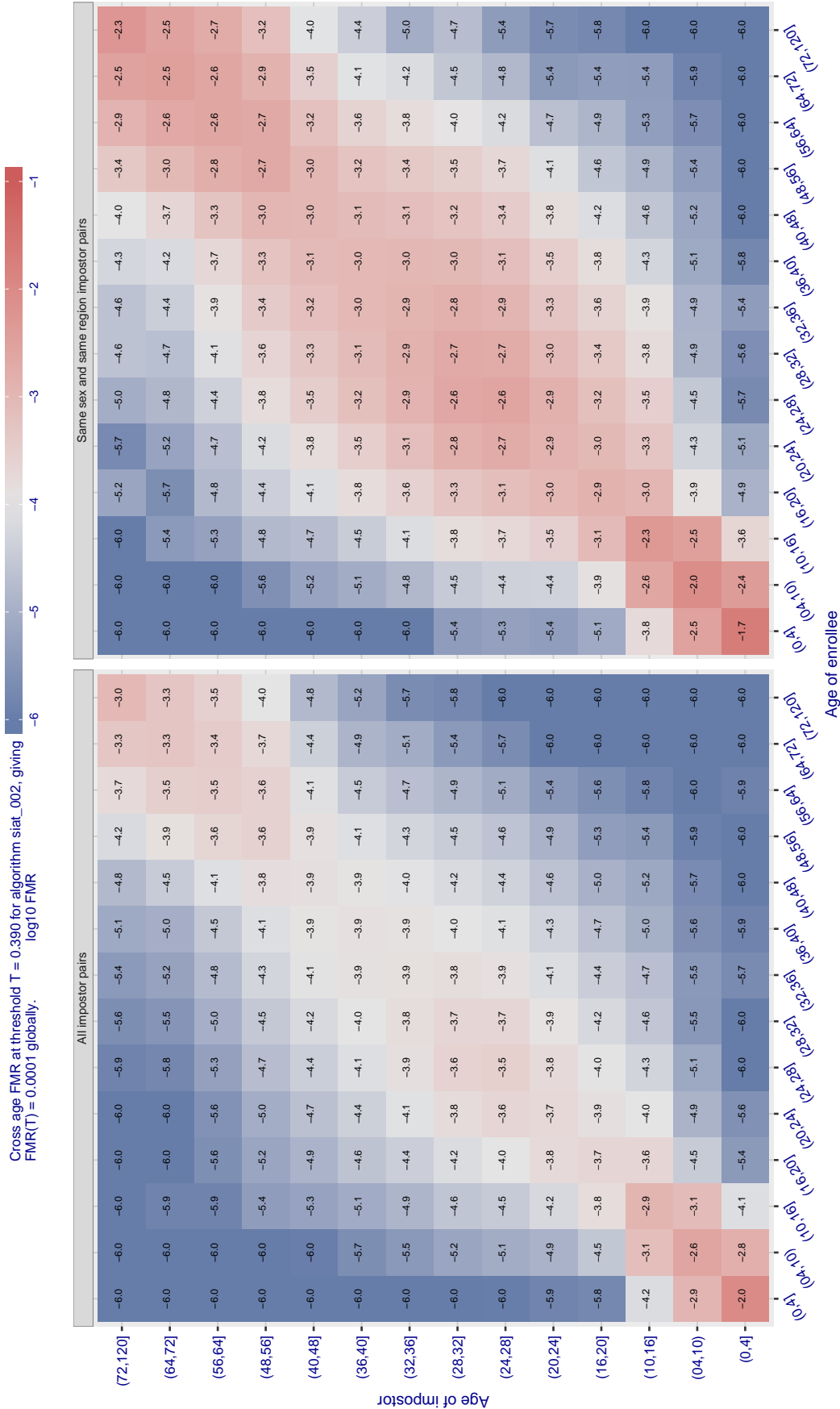


Figure 605: For algorithm `siat-002` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

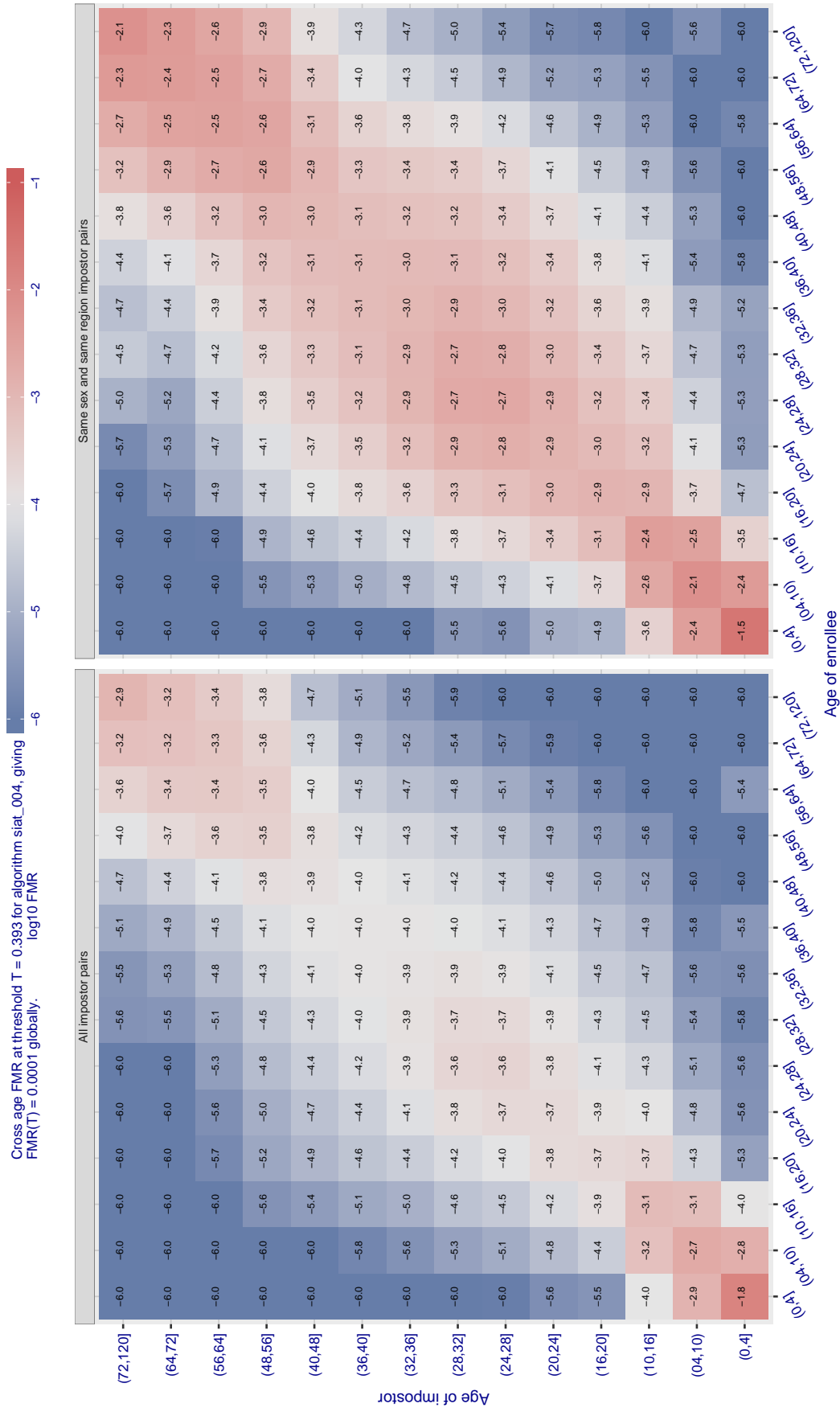


Figure 606: For algorithm `siat-004` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.



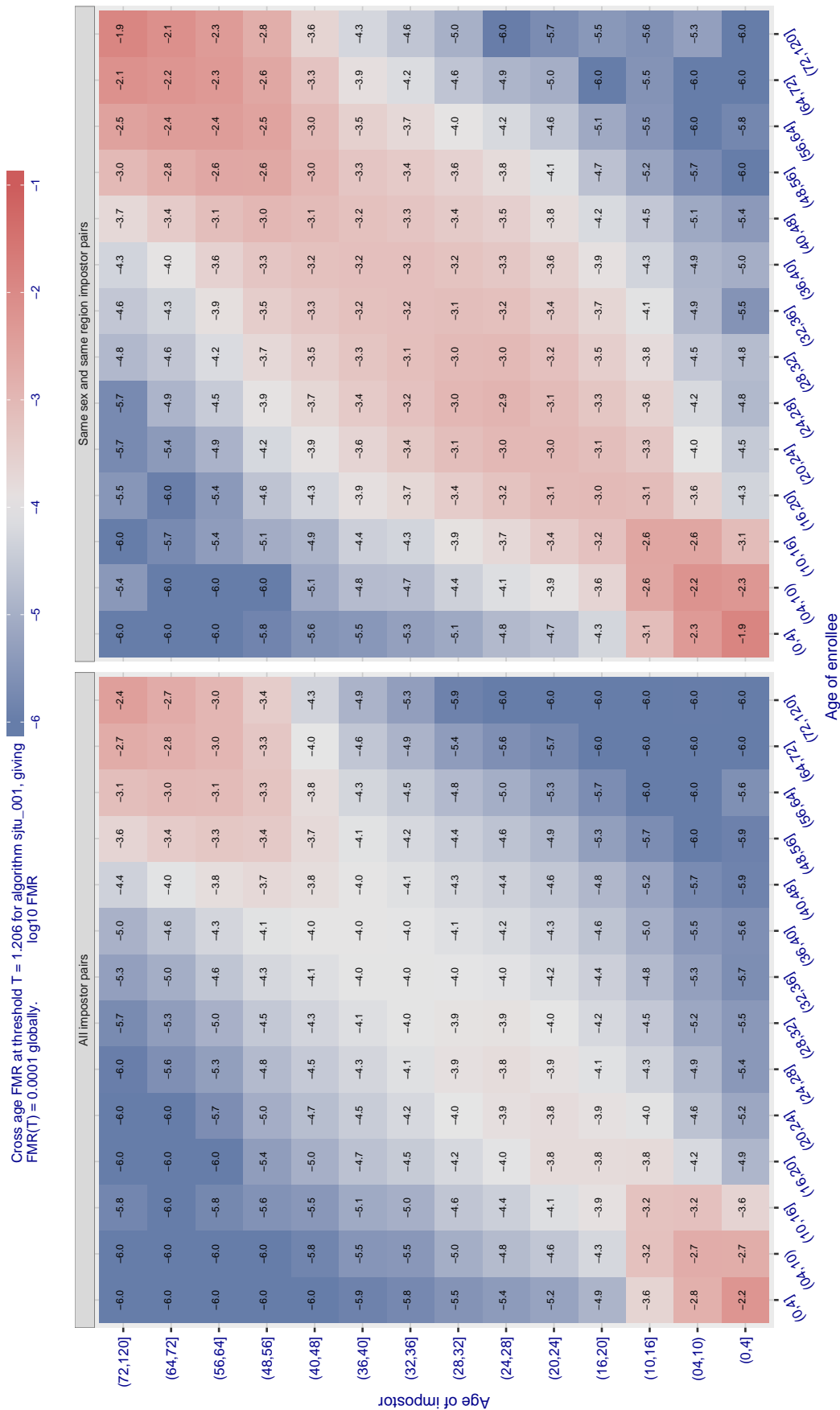


Figure 607: For algorithm `situ_001` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.598$  for algorithm smilart\_002, giving  $FMR(T) = 0.0001$  globally.

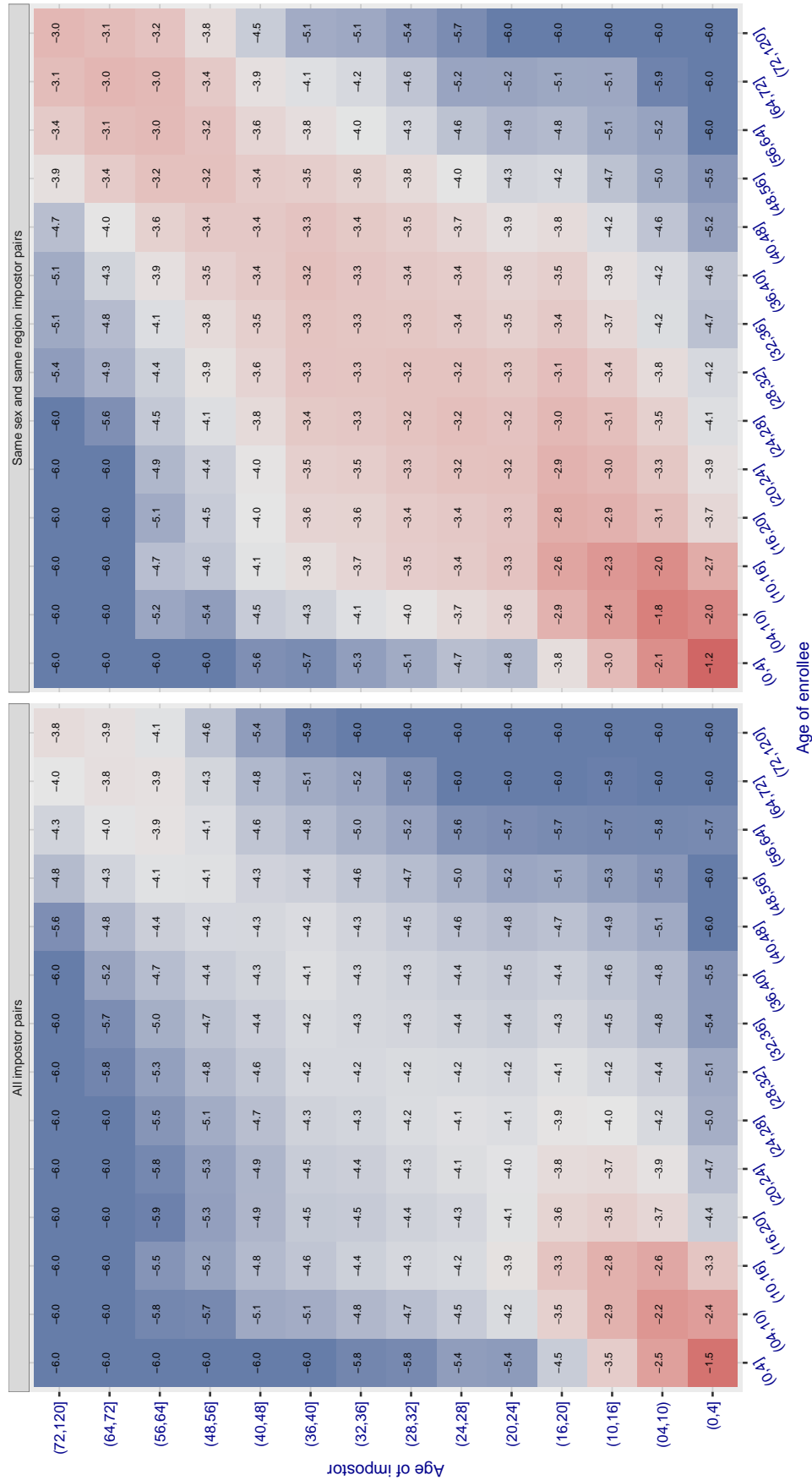


Figure 608: For algorithm smilart-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.654$  for algorithm smilart\_003, giving  $\log_{10} \text{FMR}(T) = 0.0001$  globally.

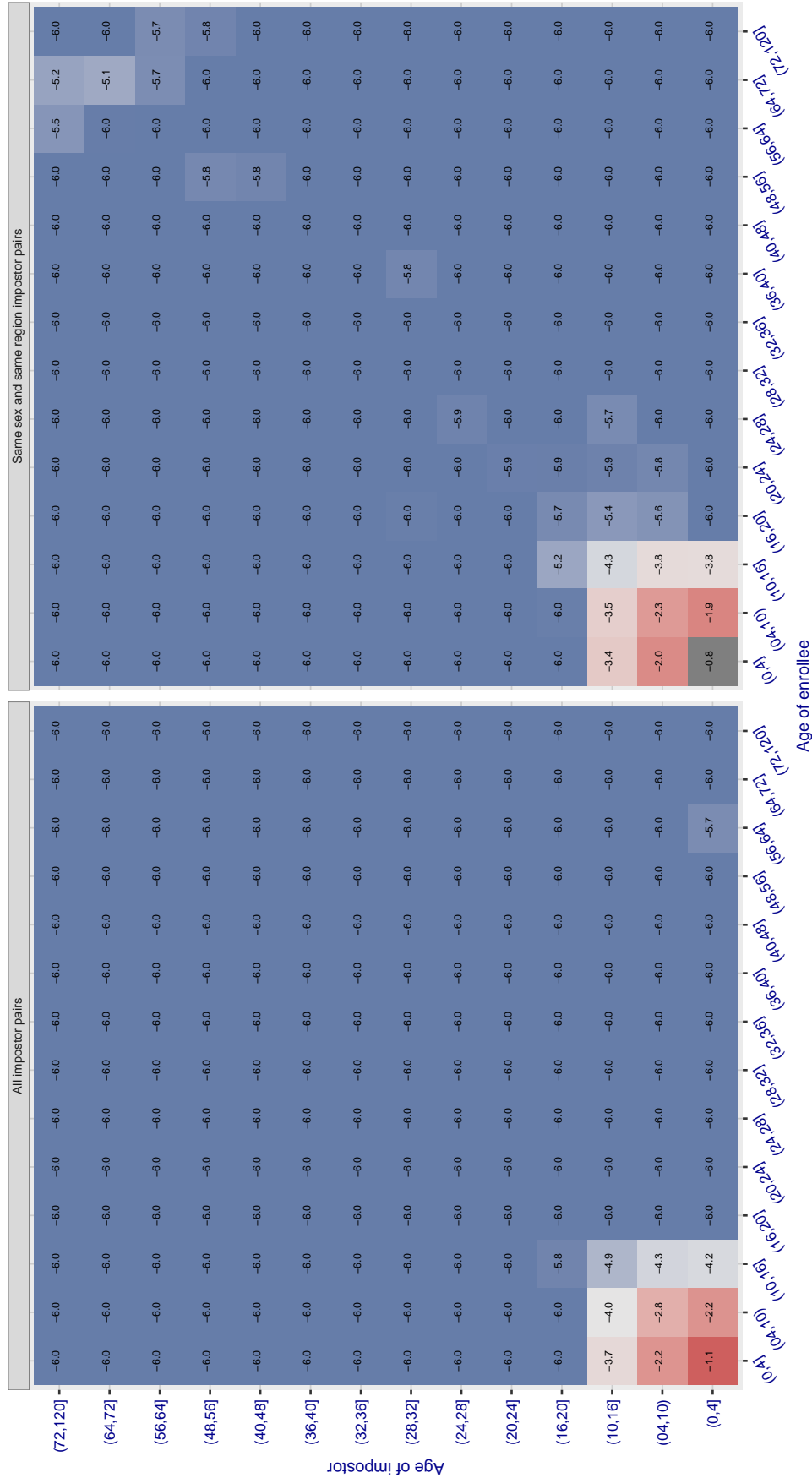


Figure 609: For algorithm smilart-003 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.314$  for algorithm starhybrid\_001, giving  $FMR(T) = 0.0001$  globally.

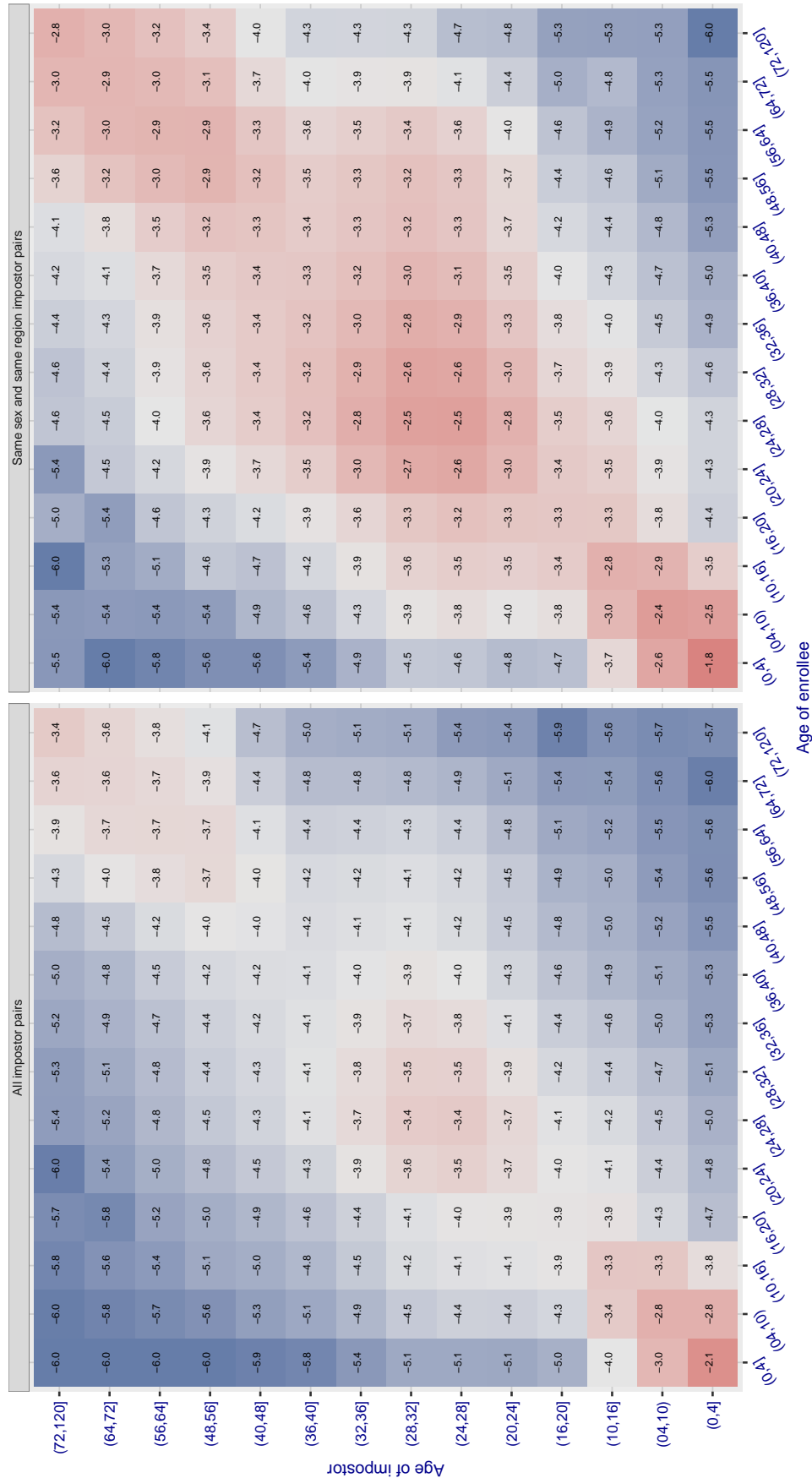


Figure 610: For algorithm starhybrid-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

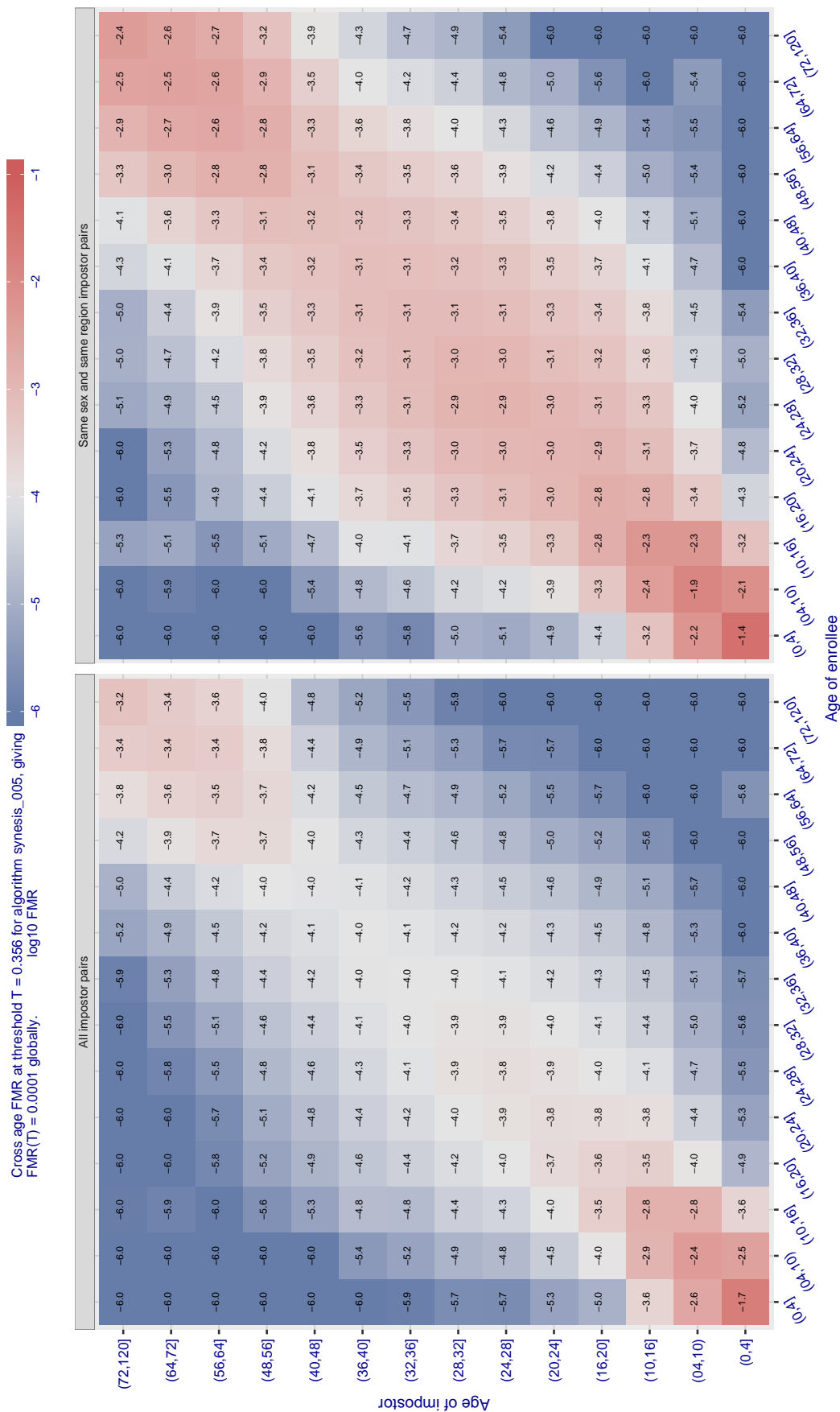


Figure 611: For algorithm synthesis-005 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

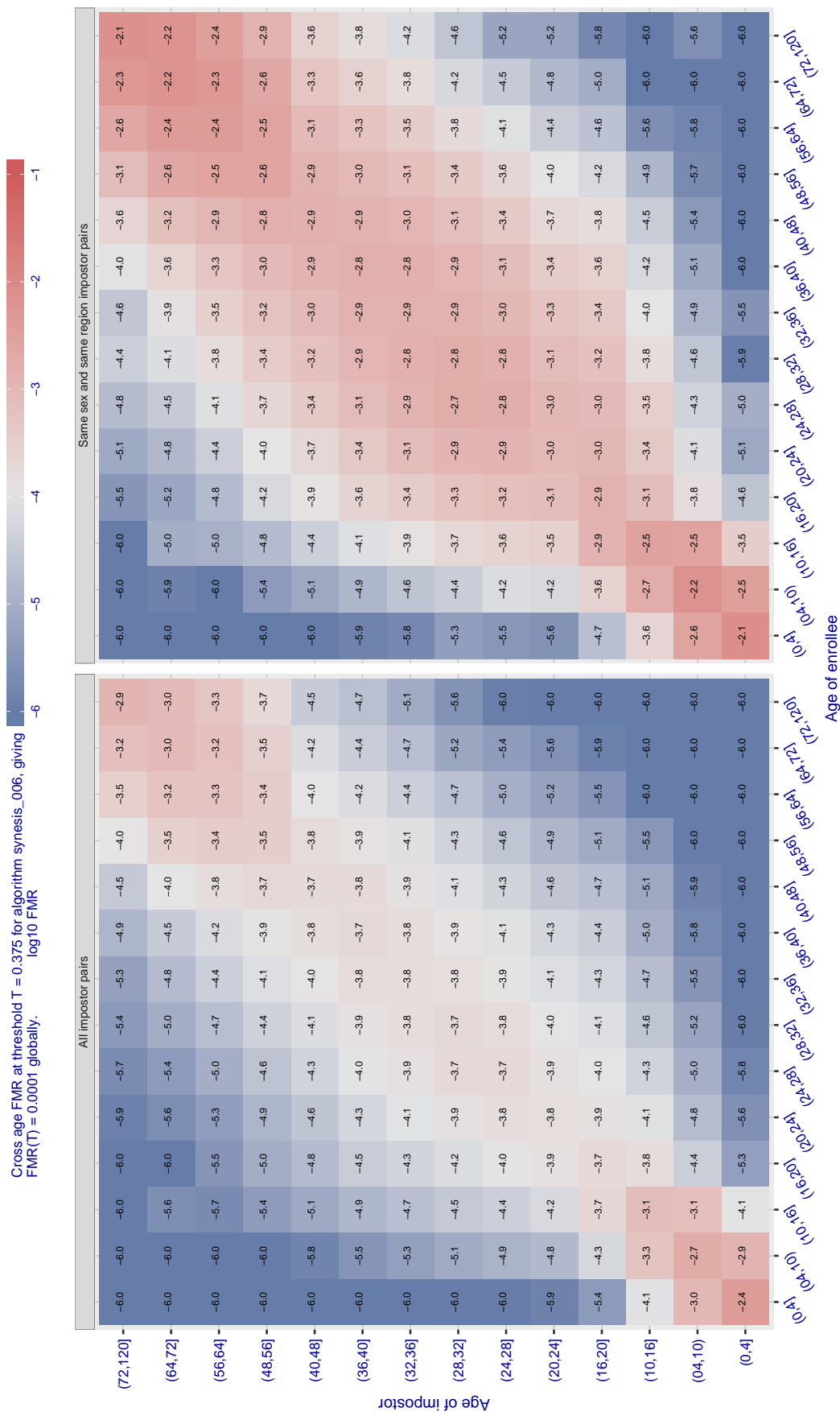


Figure 612: For algorithm synthesis-006 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

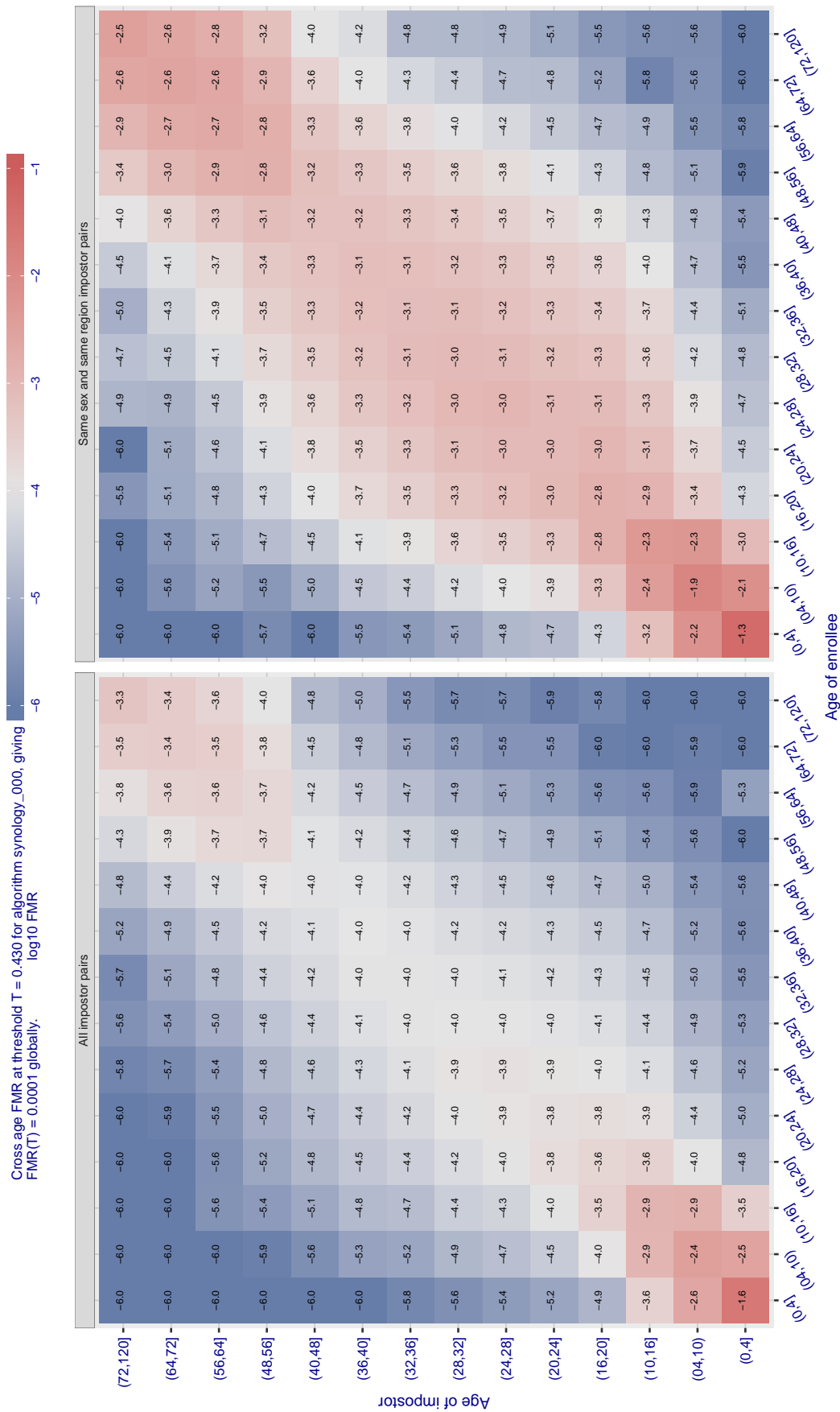


Figure 613: For algorithm `synology-000` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

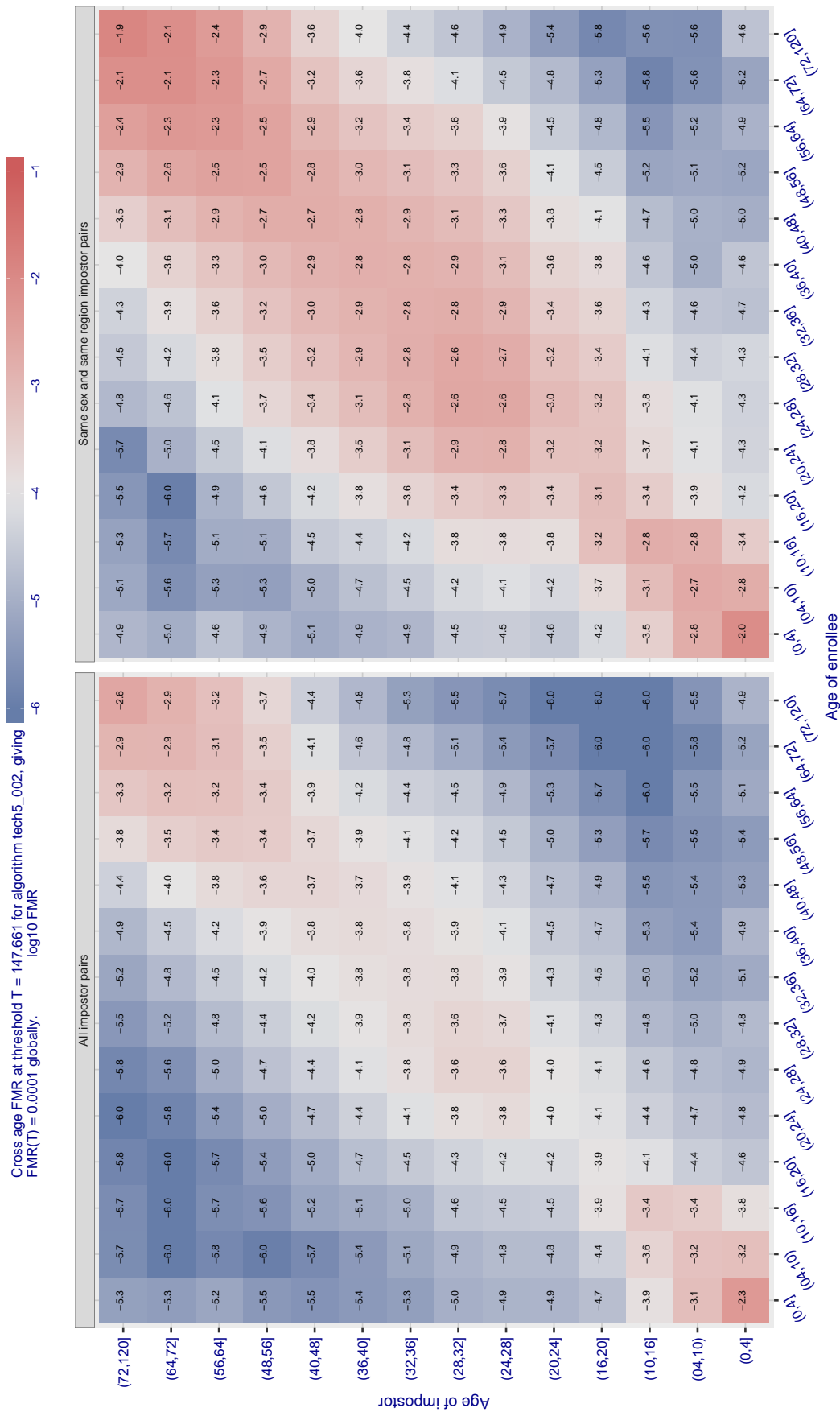


Figure 614: For algorithm tech5-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.



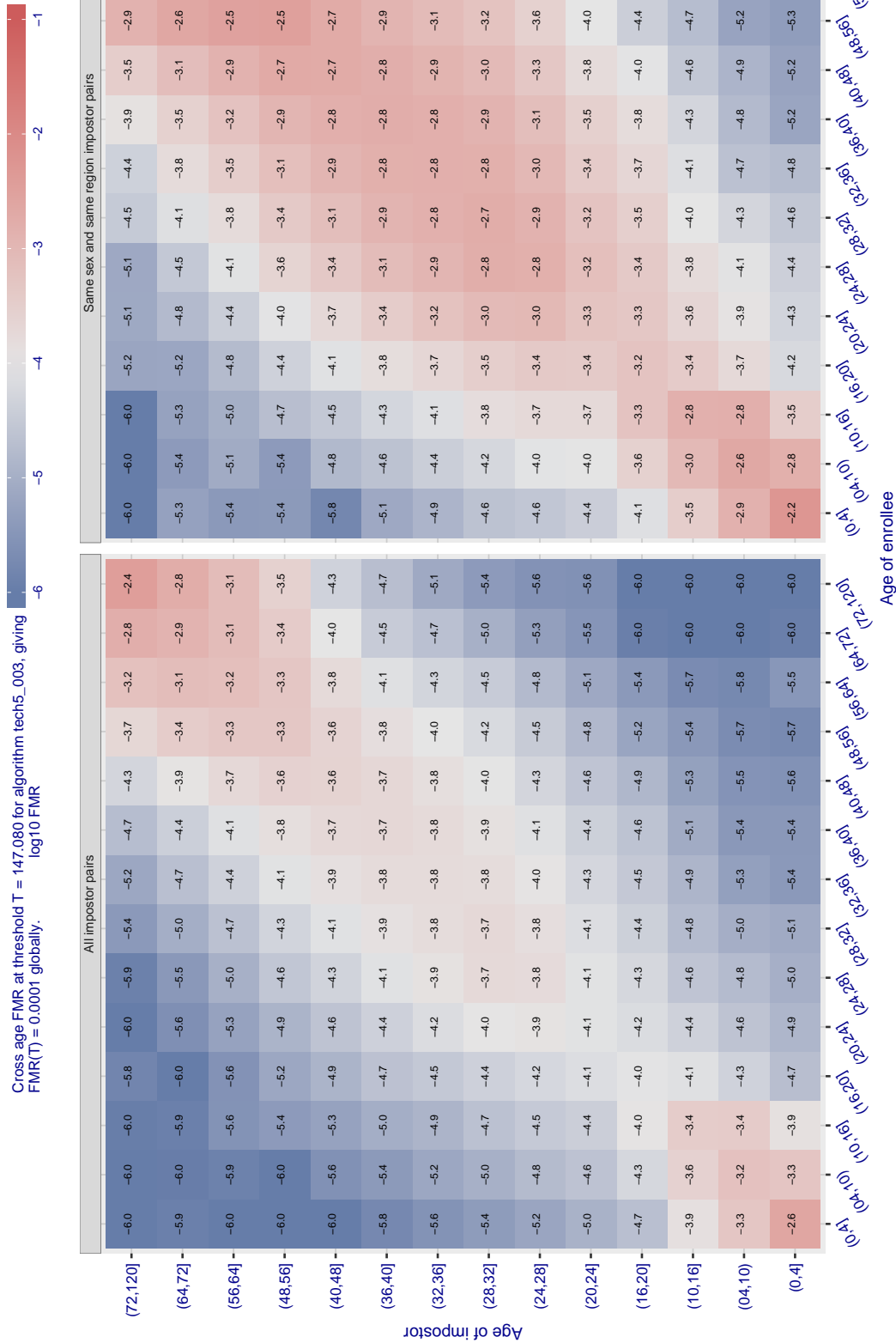


Figure 615: For algorithm tech5-003 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.896$  for algorithm teviaan\_004, giving  $FMR(T) = 0.0001$  globally.

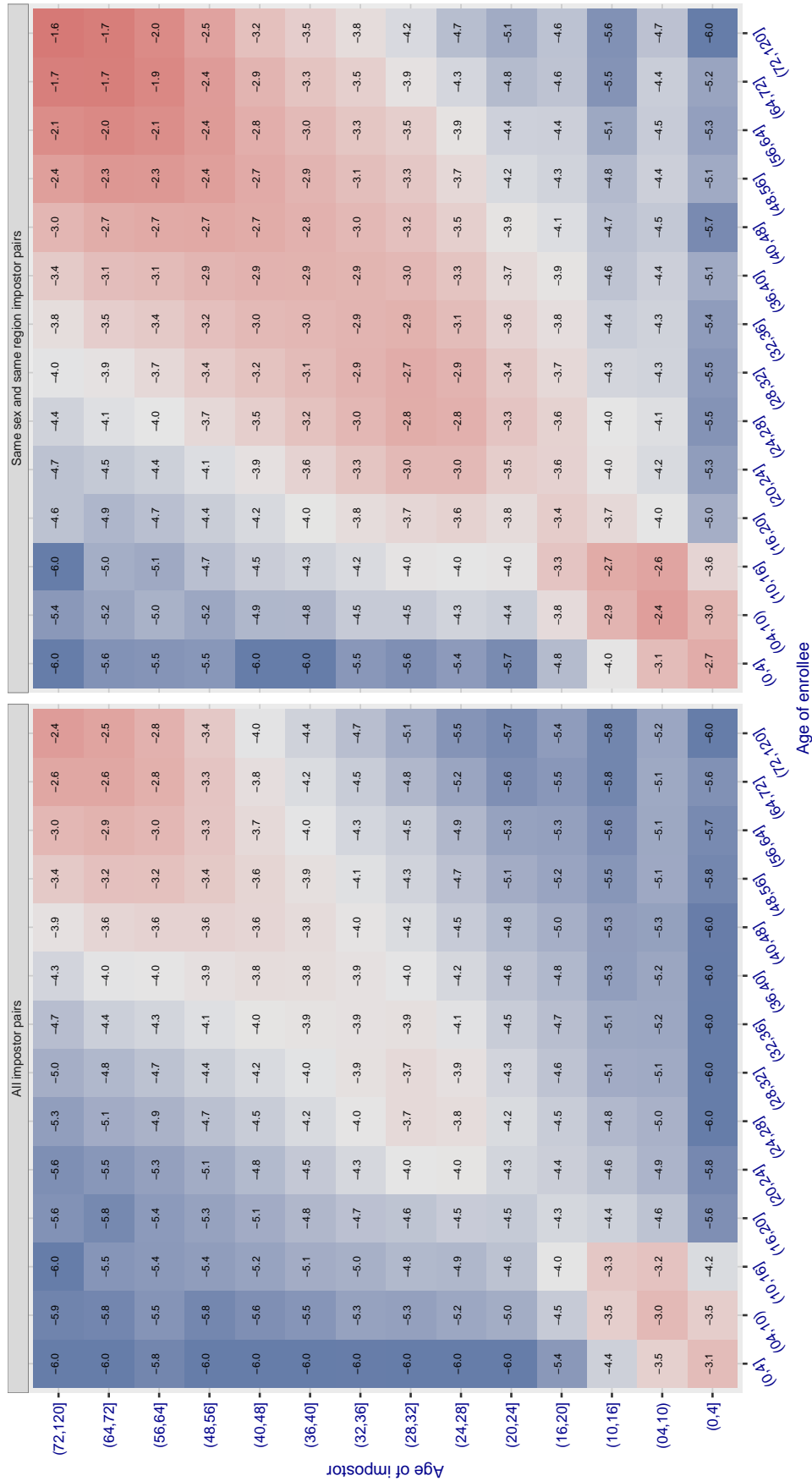


Figure 616: For algorithm teviaan-004 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.854$  for algorithm teviaan\_005, giving  $FMR(T) = 0.0001$  globally.

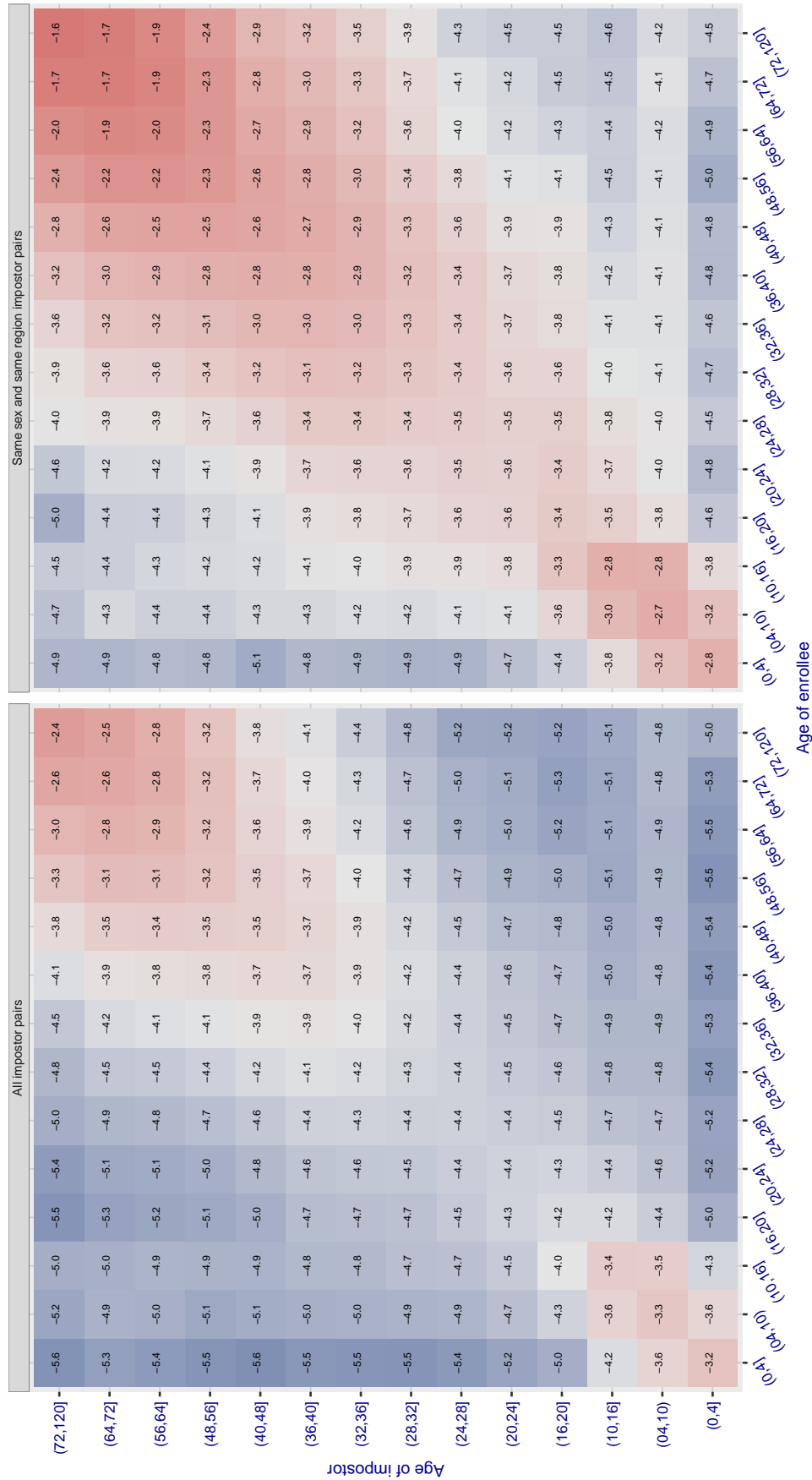


Figure 617: For algorithm teviaan-005 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 151.011$  for algorithm tiger\_002, giving  $FMR(T) = 0.0001$  globally.

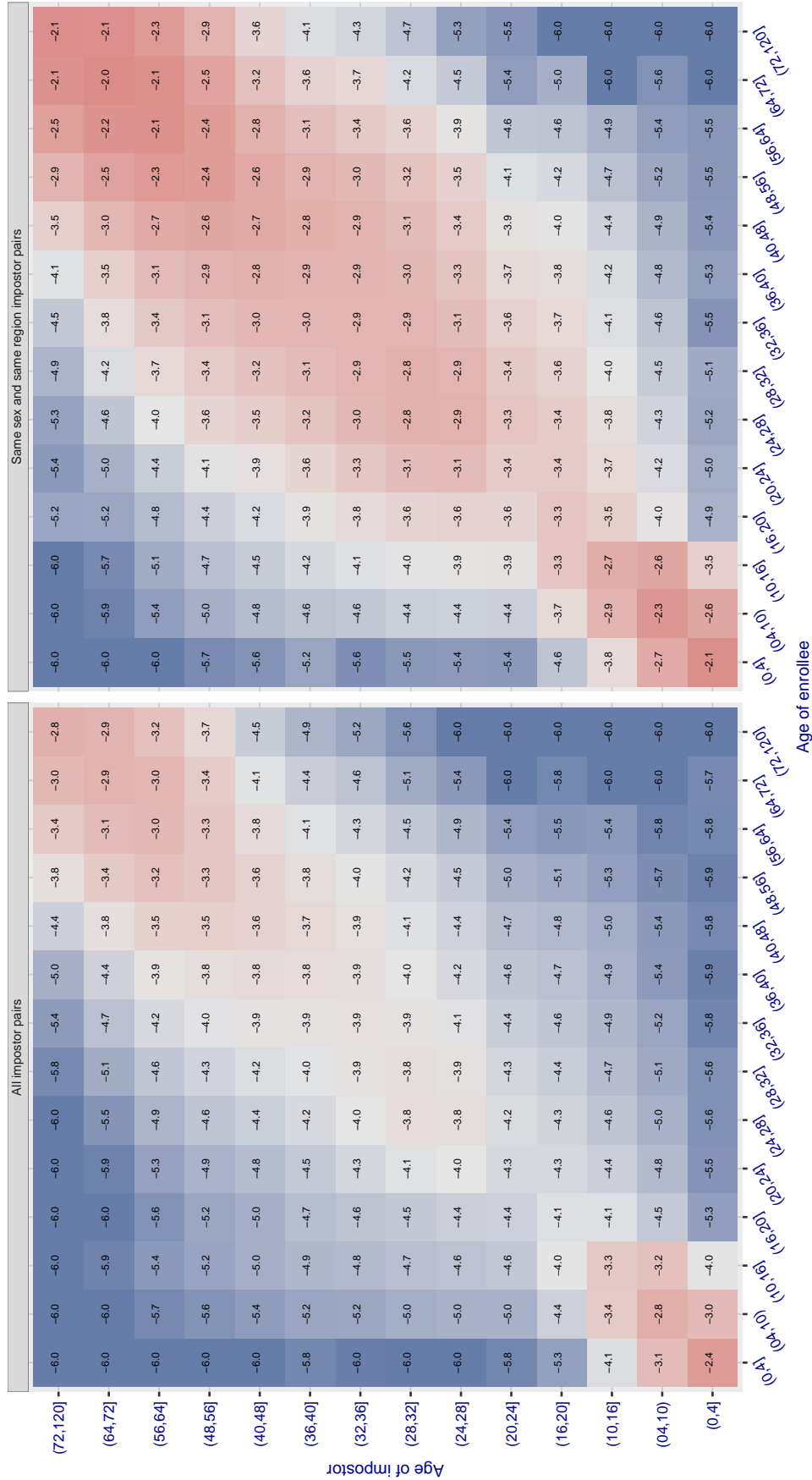


Figure 618: For algorithm tiger-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 149.313$  for algorithm tiger\_003, giving  $FMR(T) = 0.0001$  globally.

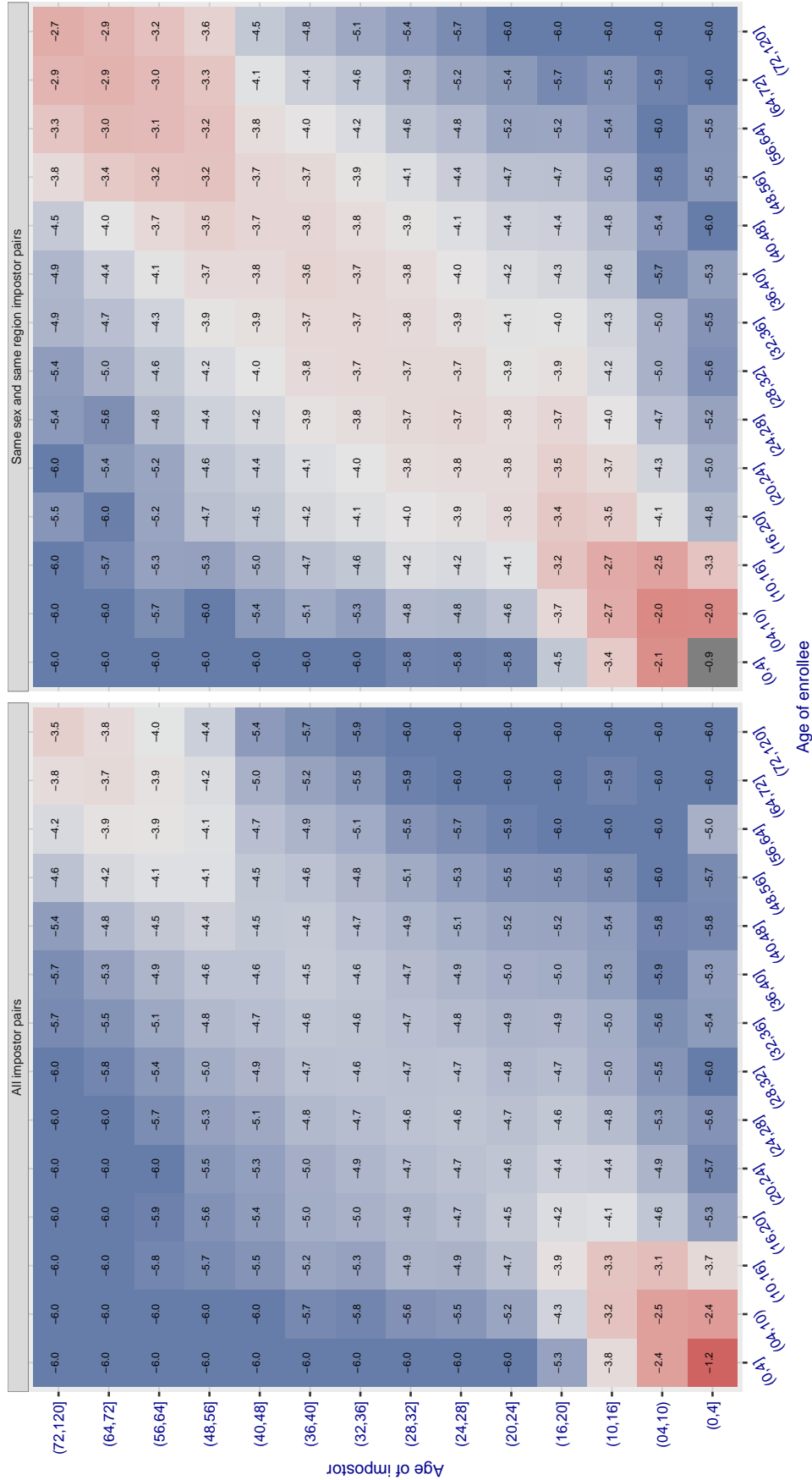


Figure 619: For algorithm tiger-003 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 43.677$  for algorithm tongyi\_005, giving  $FMR(T) = 0.0001$  globally.

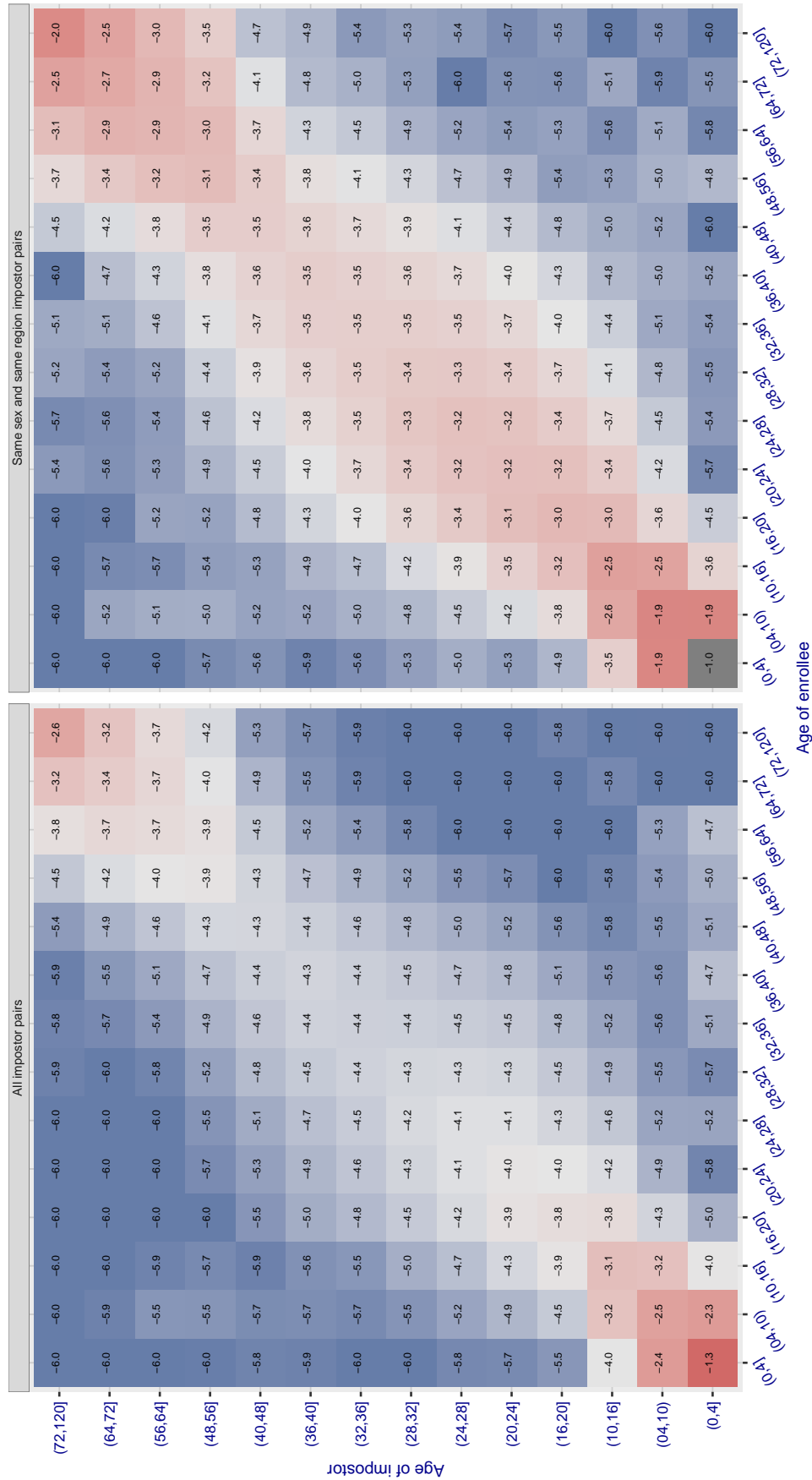


Figure 620: For algorithm tongyi-005 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.628$  for algorithm toshiba\_002, giving  $FMR(T) = 0.0001$  globally.

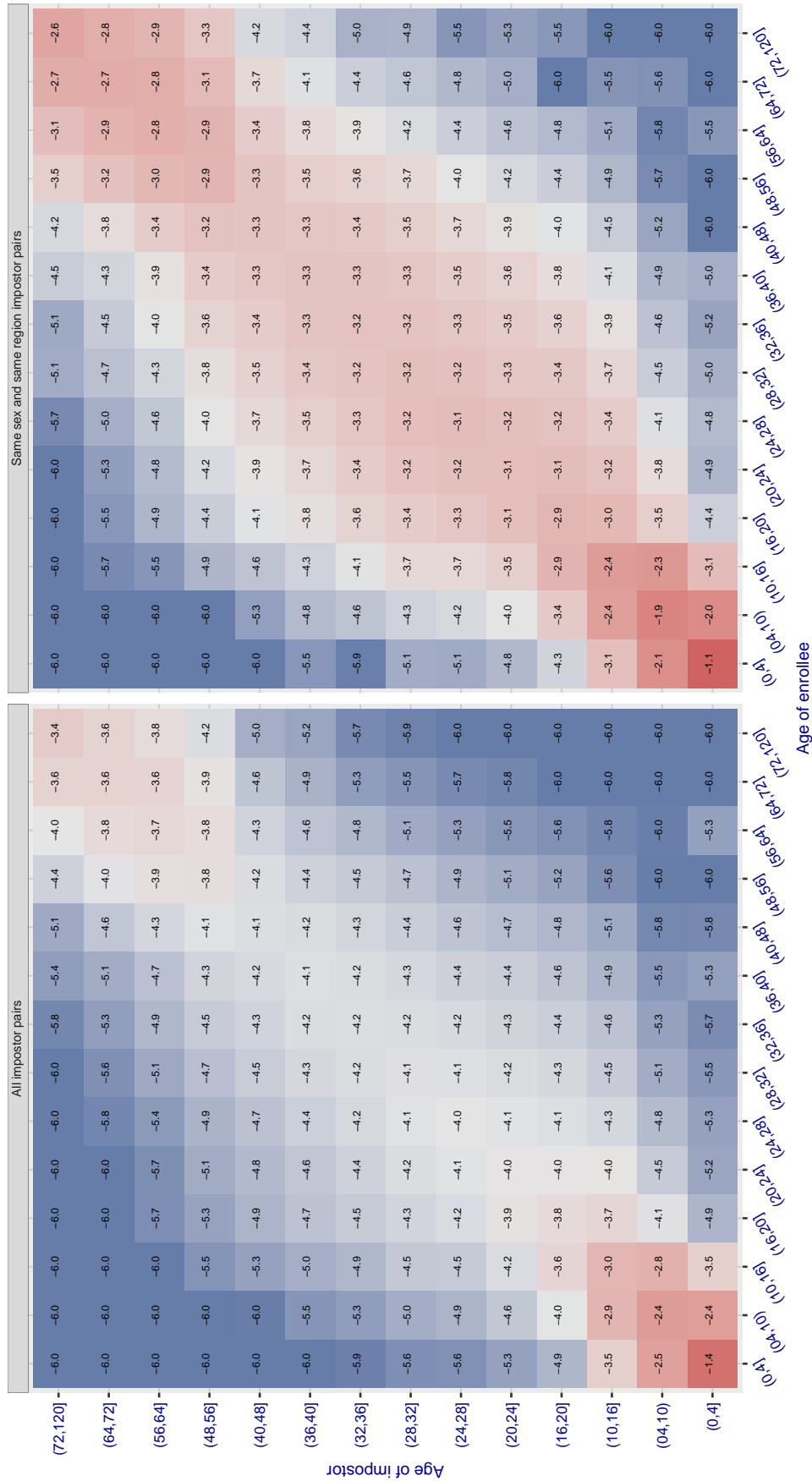


Figure 621: For algorithm toshiba-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.626$  for algorithm toshiba\_003, giving  $FMR(T) = 0.0001$  globally.

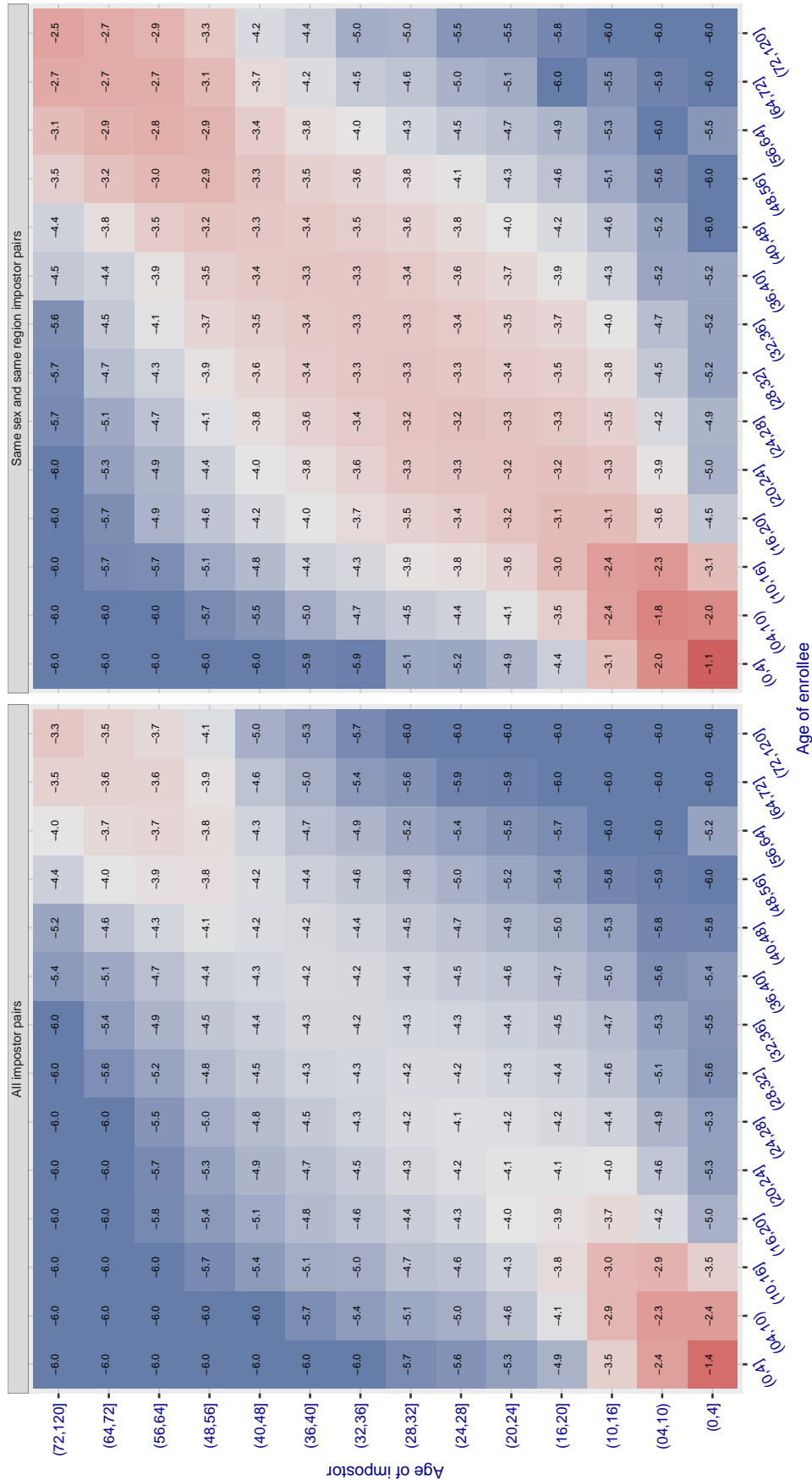


Figure 622: For algorithm toshiba-003 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.



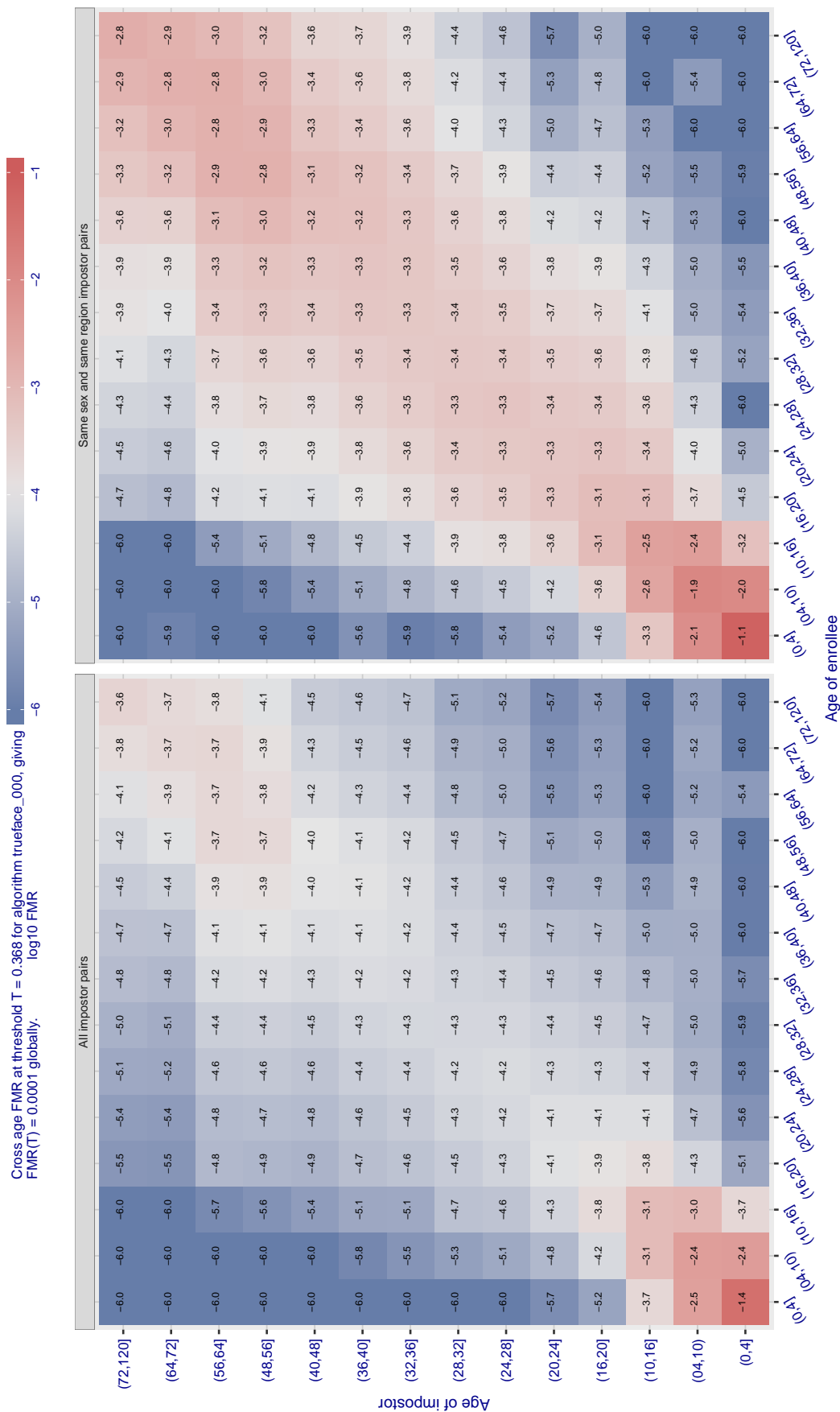


Figure 623: For algorithm trueface-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

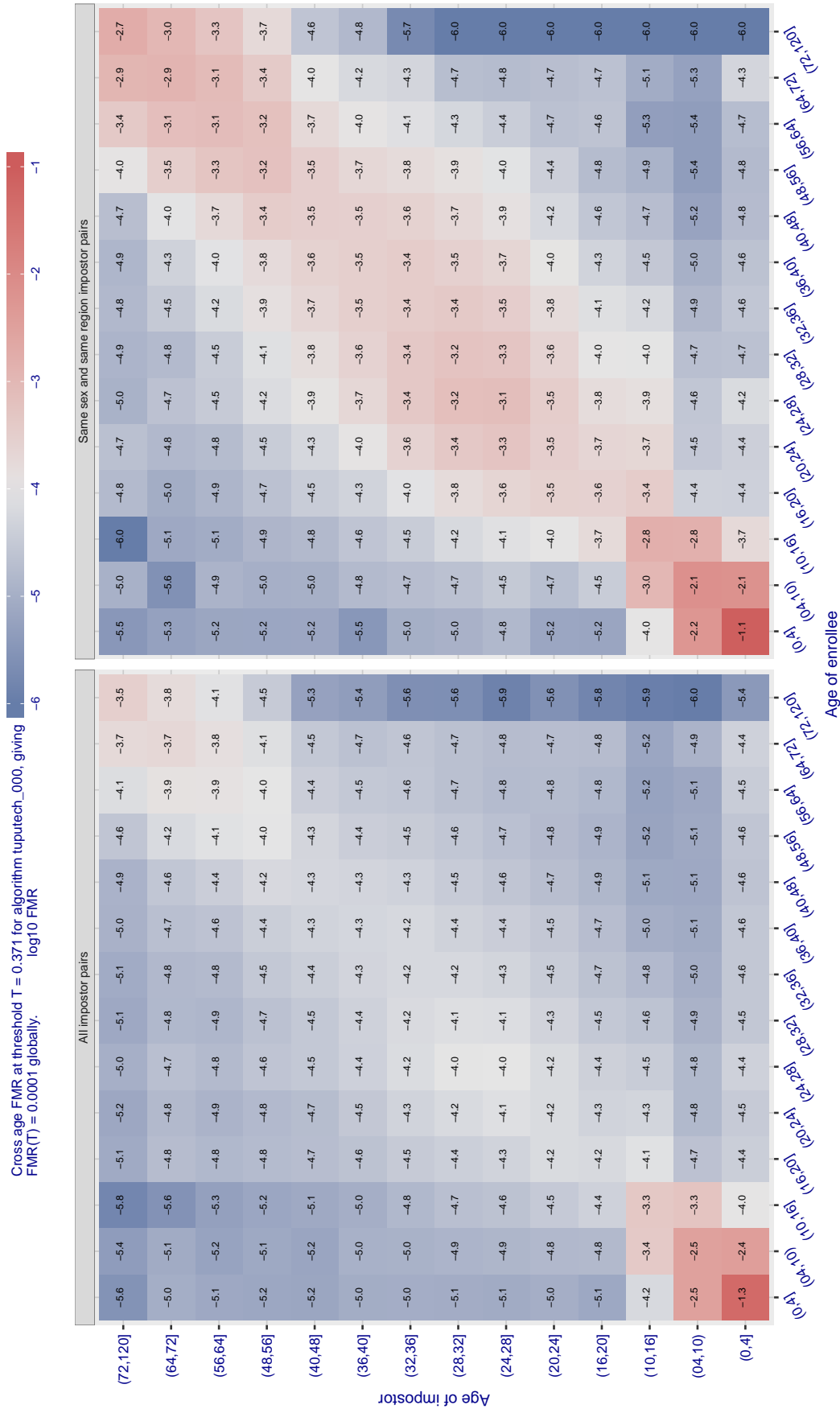


Figure 624: For algorithm tuputech-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.151$  for algorithm ulsee\_001, giving  $FMR(T) = 0.0001$  globally.

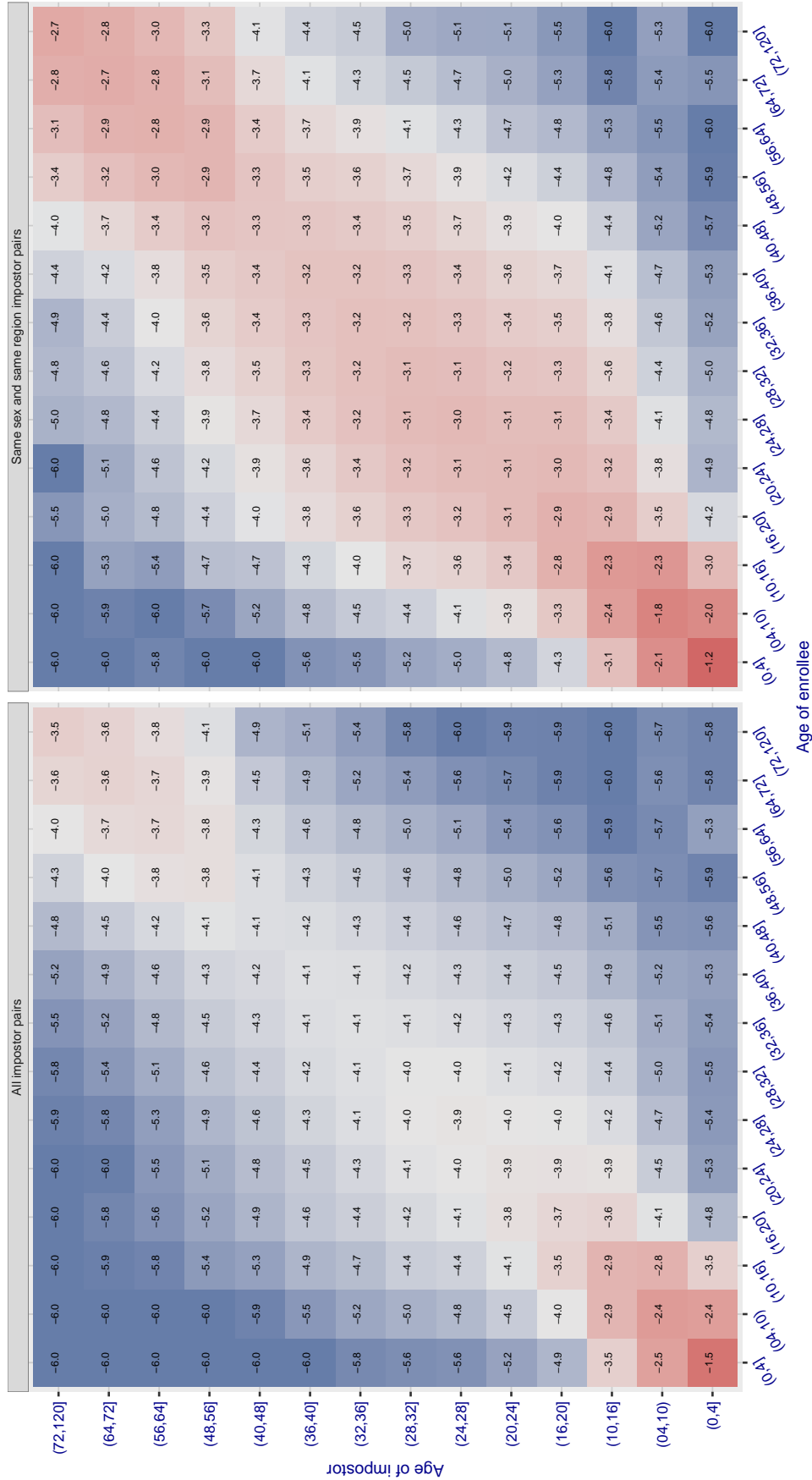


Figure 625: For algorithm ulsee-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.771$  for algorithm uliface\_002, giving  $FMR(T) = 0.0001$  globally.

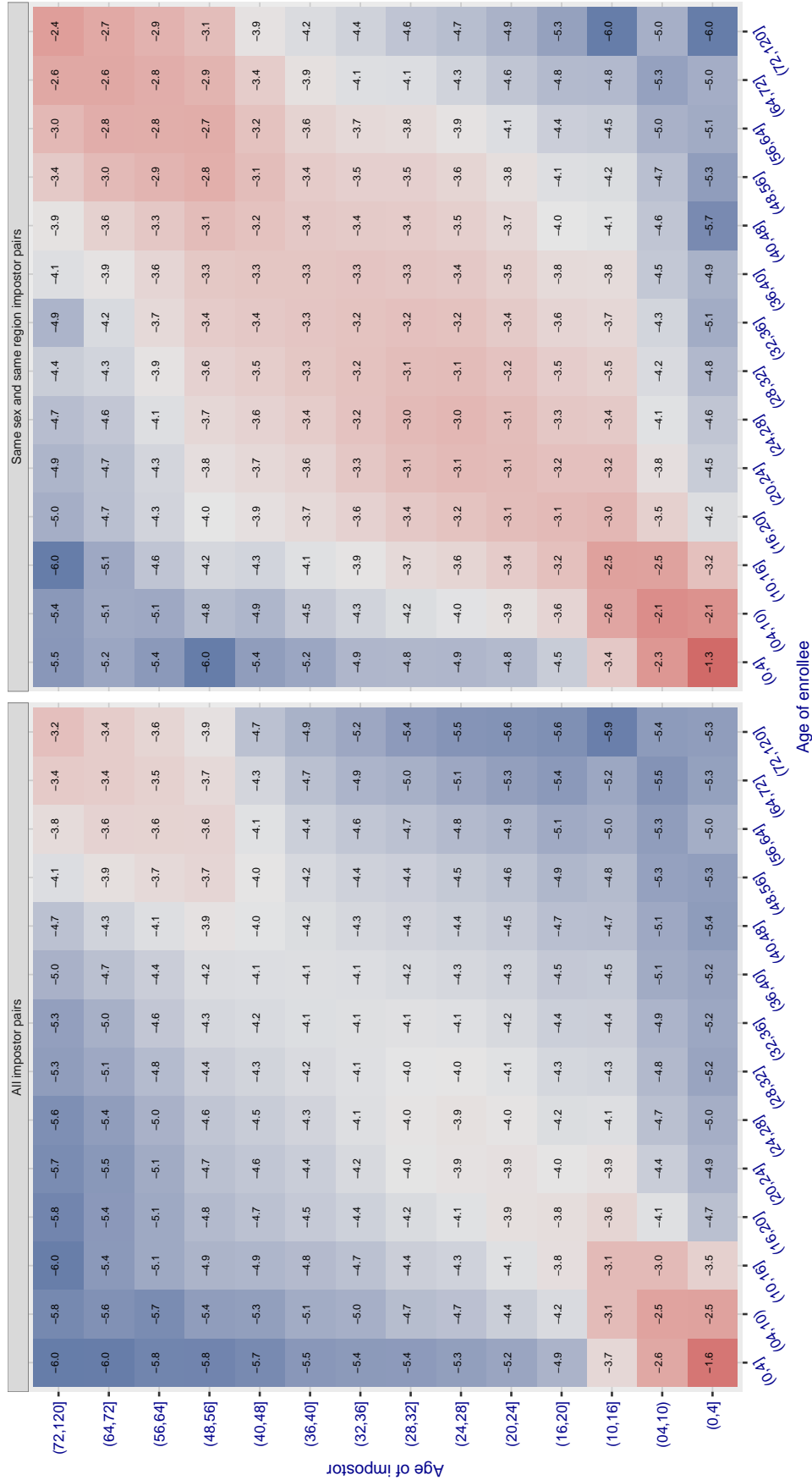


Figure 626: For algorithm uliface-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

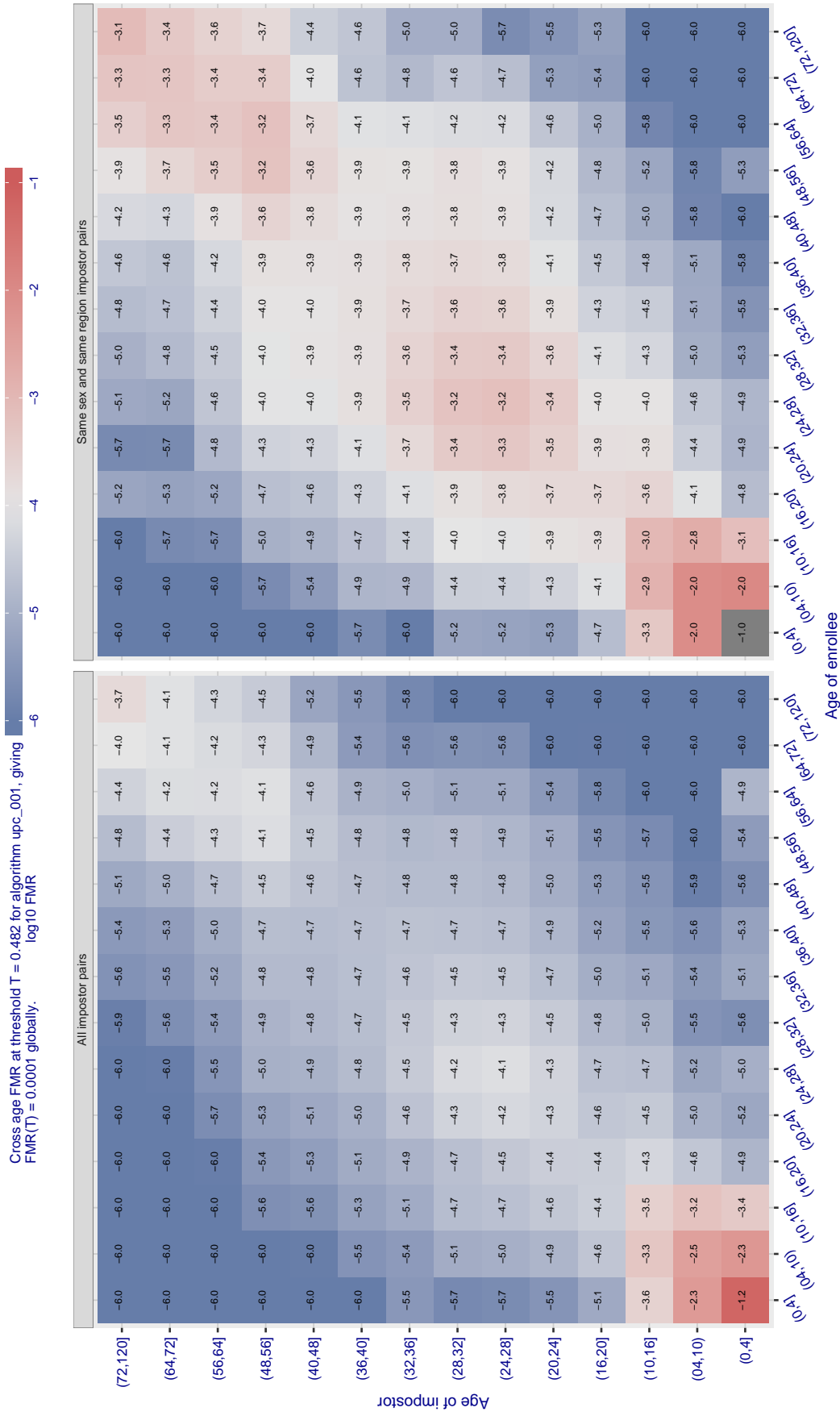


Figure 627: For algorithm upc-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.428$  for algorithm vcog\_002, giving  $FMR(T) = 0.0001$  globally.

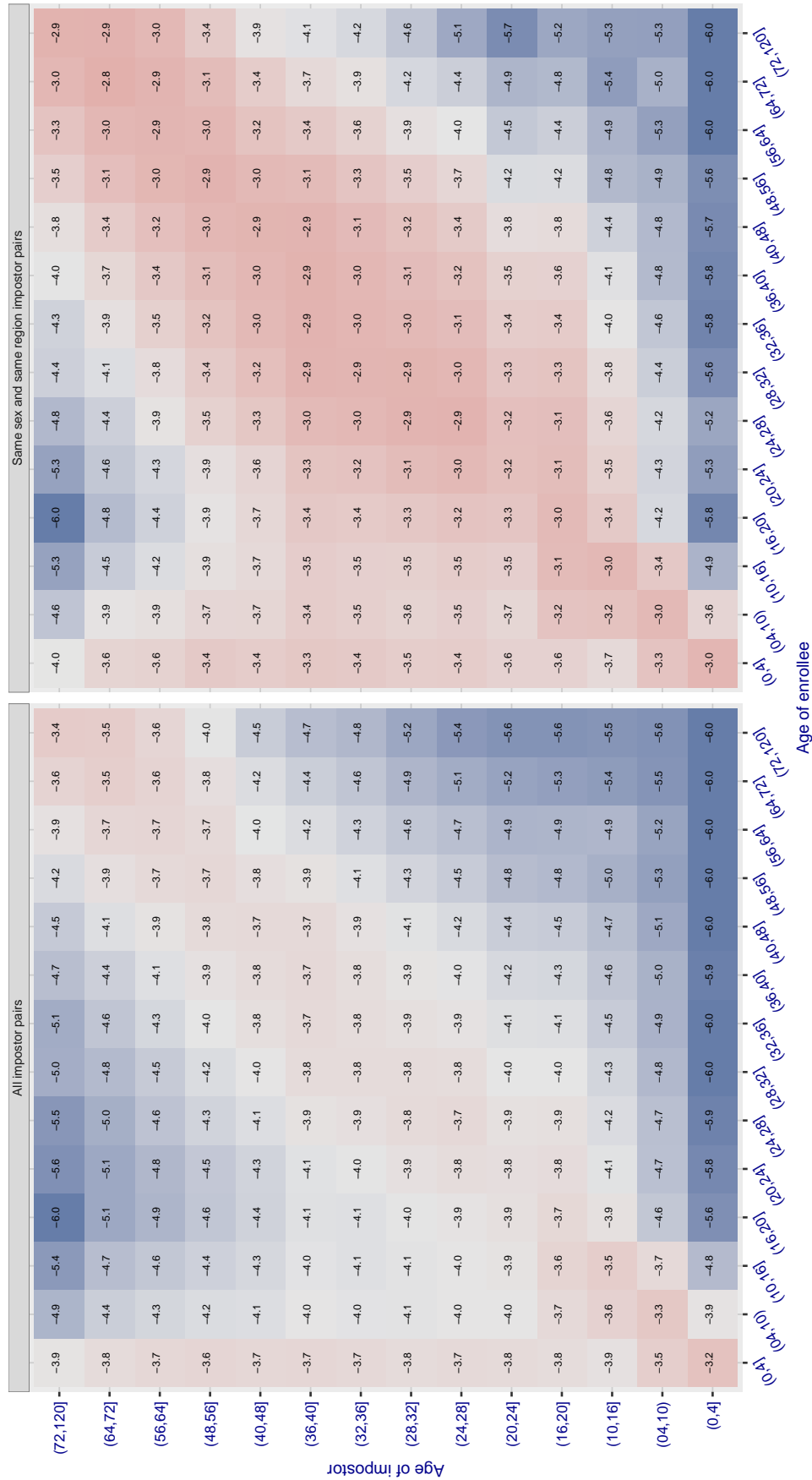


Figure 628: For algorithm vcog-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

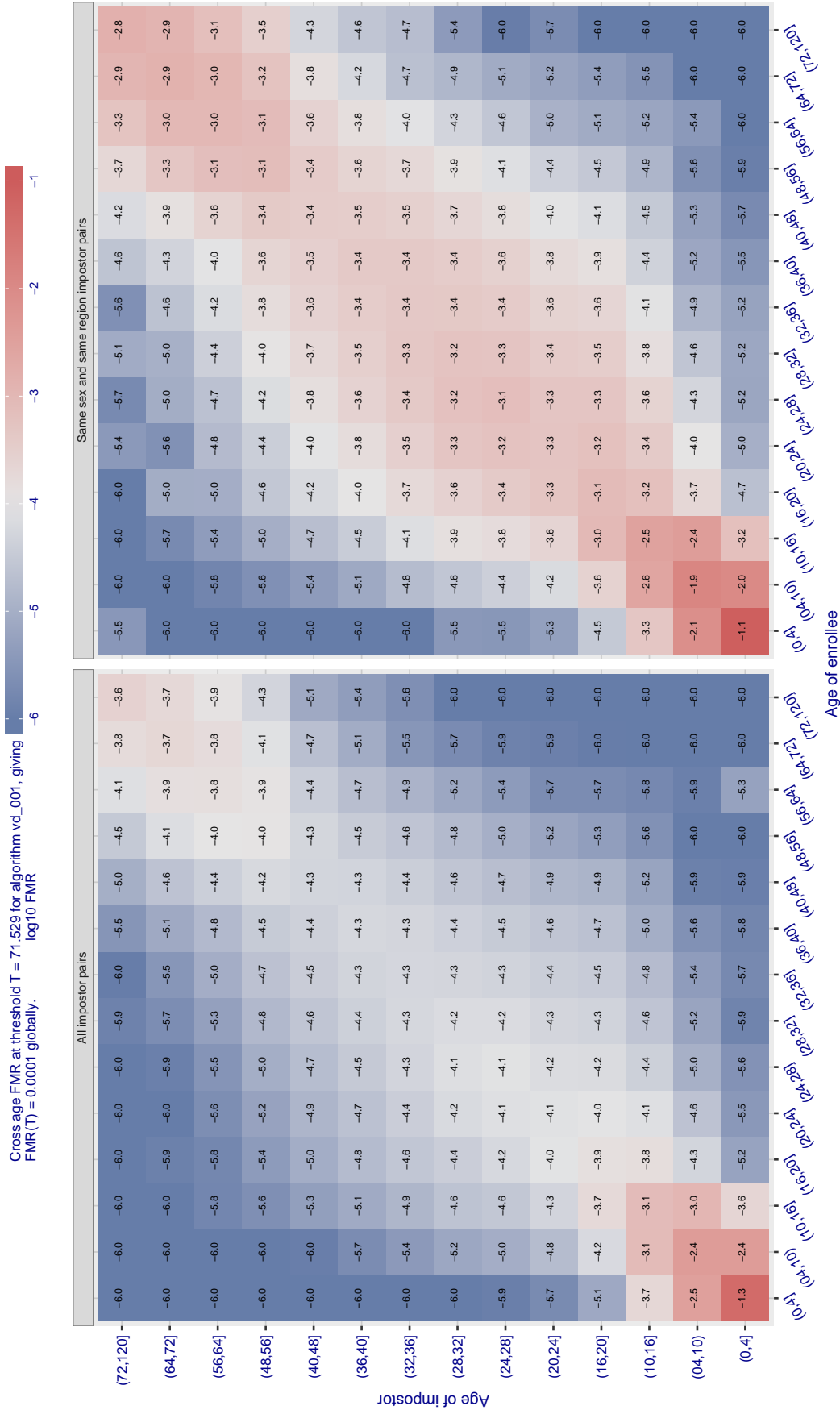


Figure 629: For algorithm vd-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

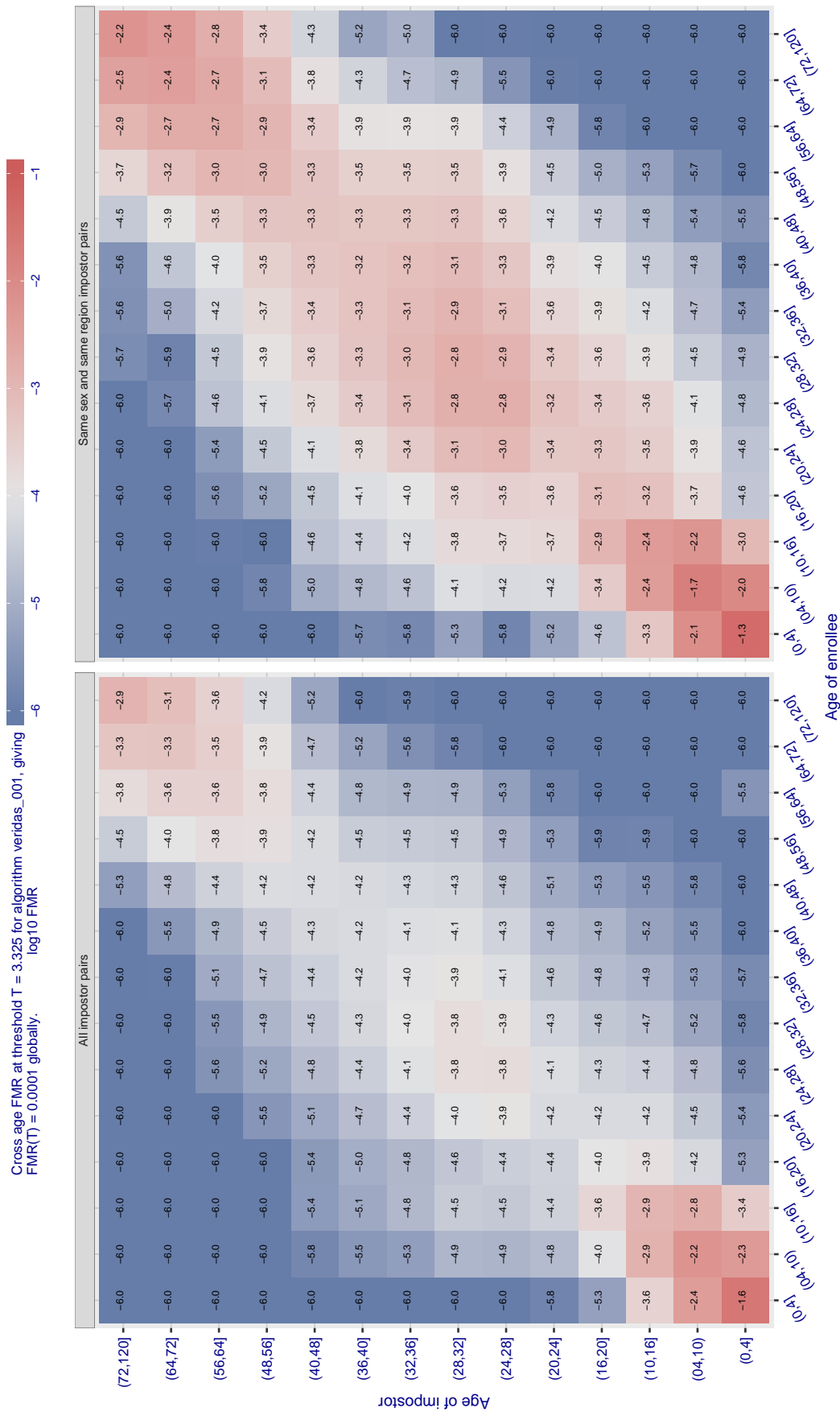


Figure 630: For algorithm veridas-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.



Cross age FMR at threshold  $T = 3.389$  for algorithm veridas\_002, giving  $FMR(T) = 0.0001$  globally.

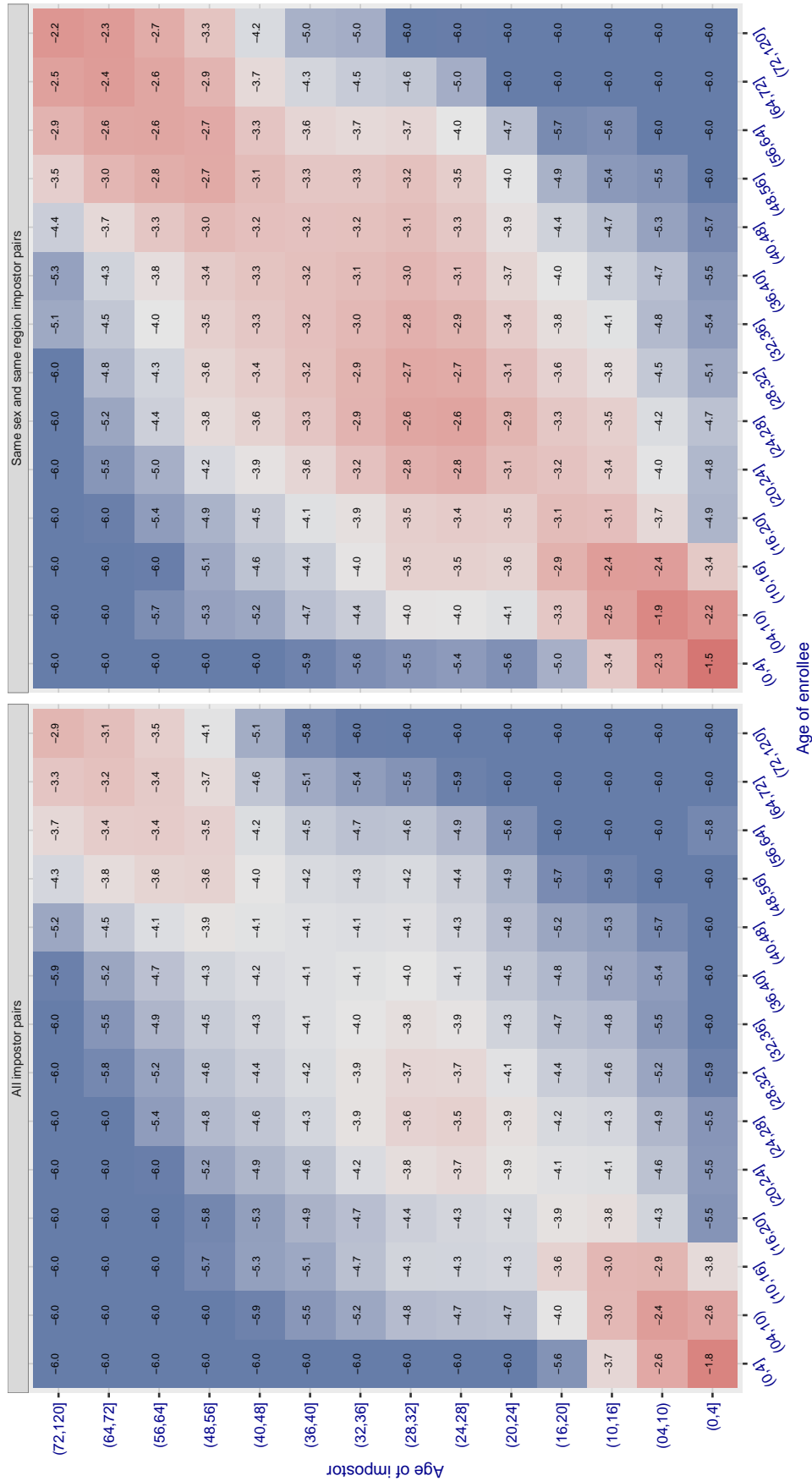


Figure 631: For algorithm veridas-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

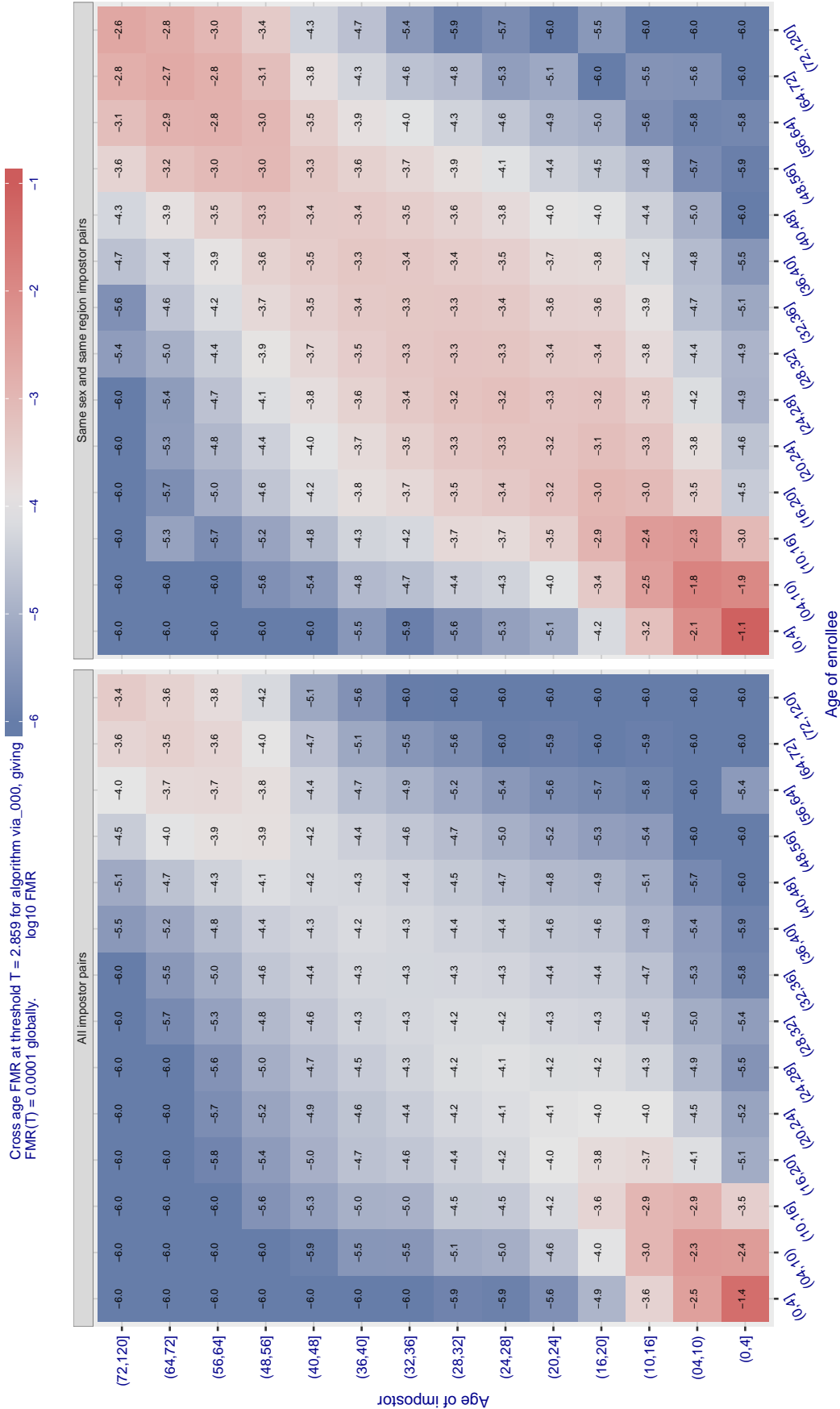


Figure 632: For algorithm via-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

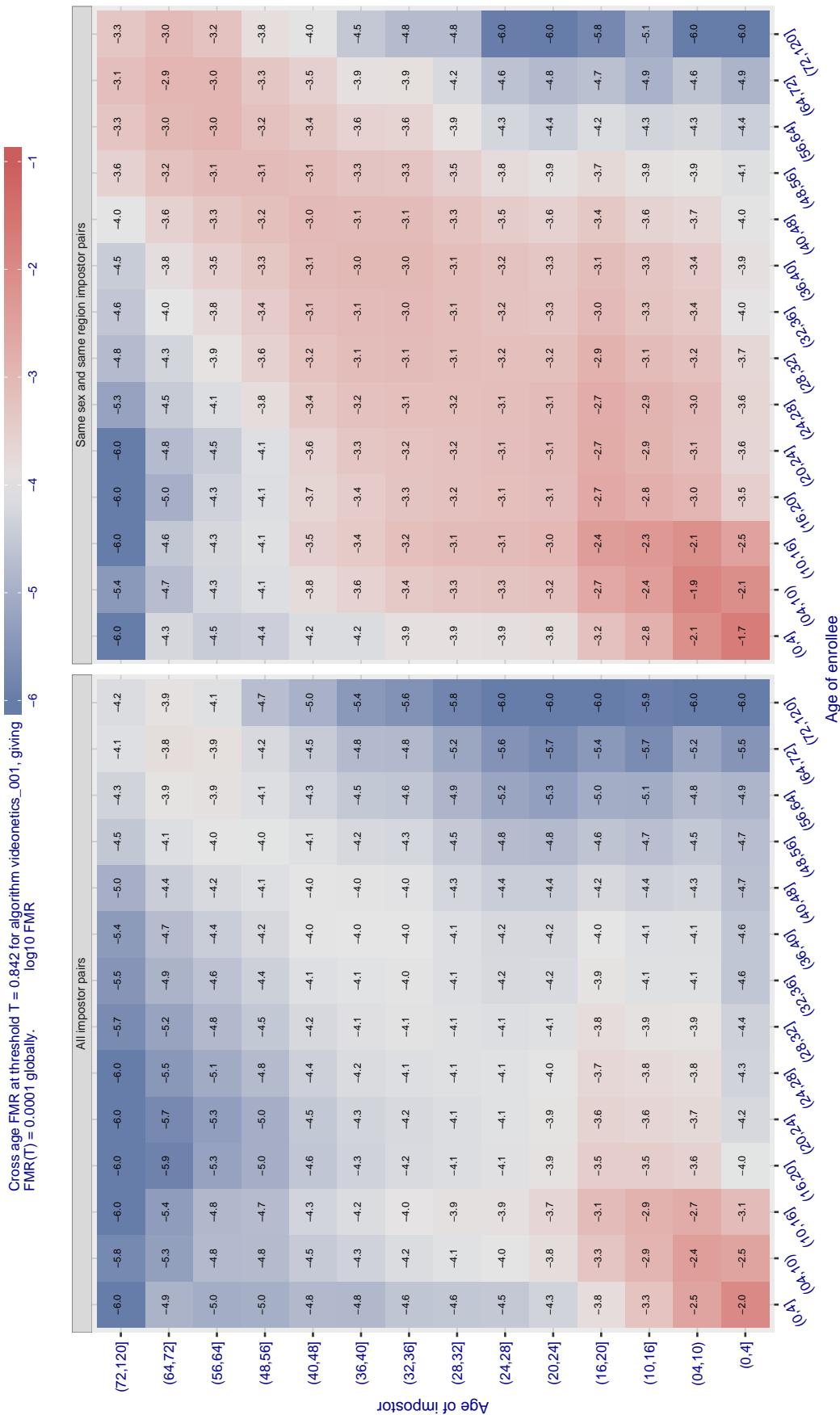


Figure 633: For algorithm videonetrics-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

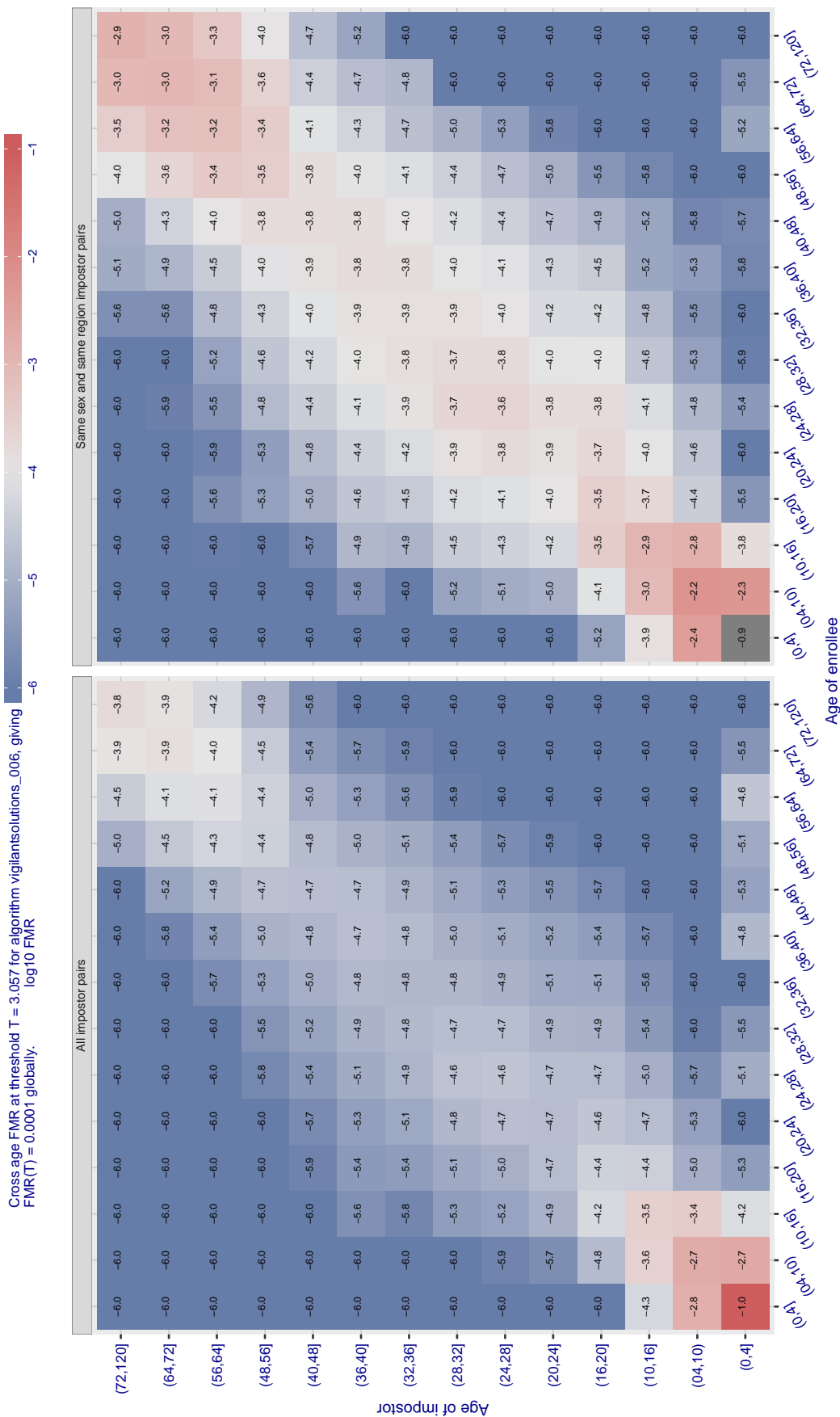


Figure 634: For algorithm `vigilantsolutions-006` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

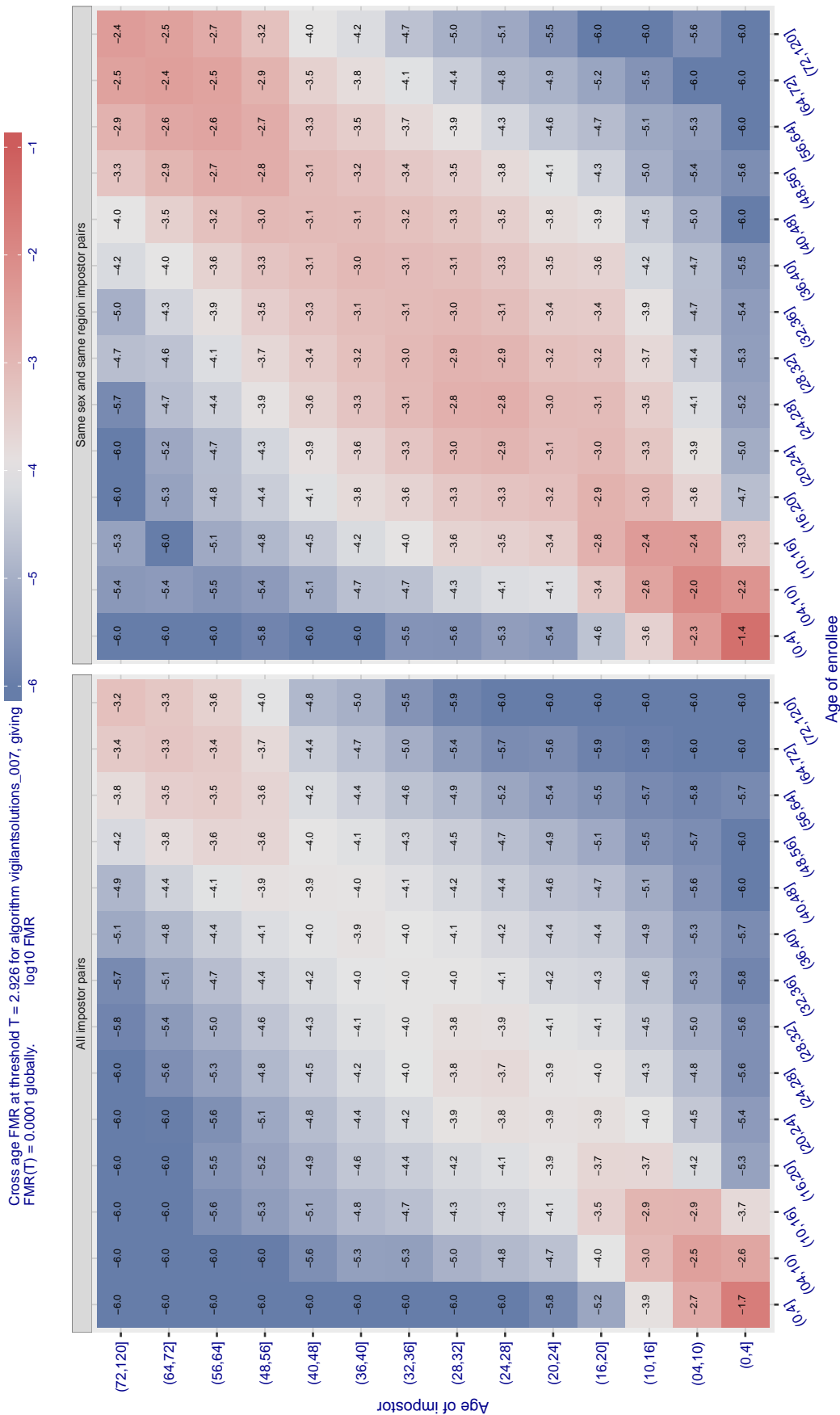


Figure 635: For algorithm `vigilantsolutions-007` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

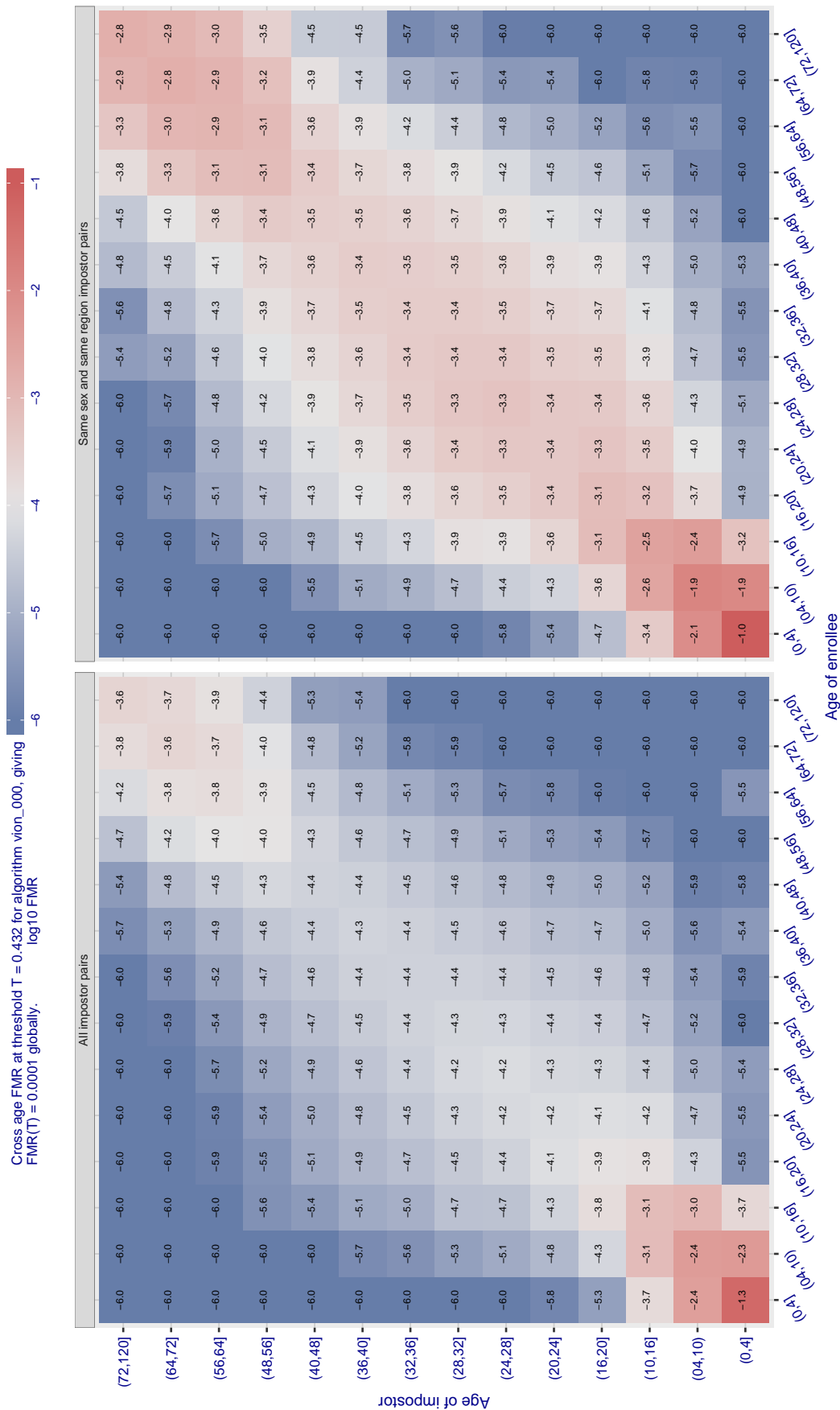


Figure 636: For algorithm  $\text{vion-000}$  operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

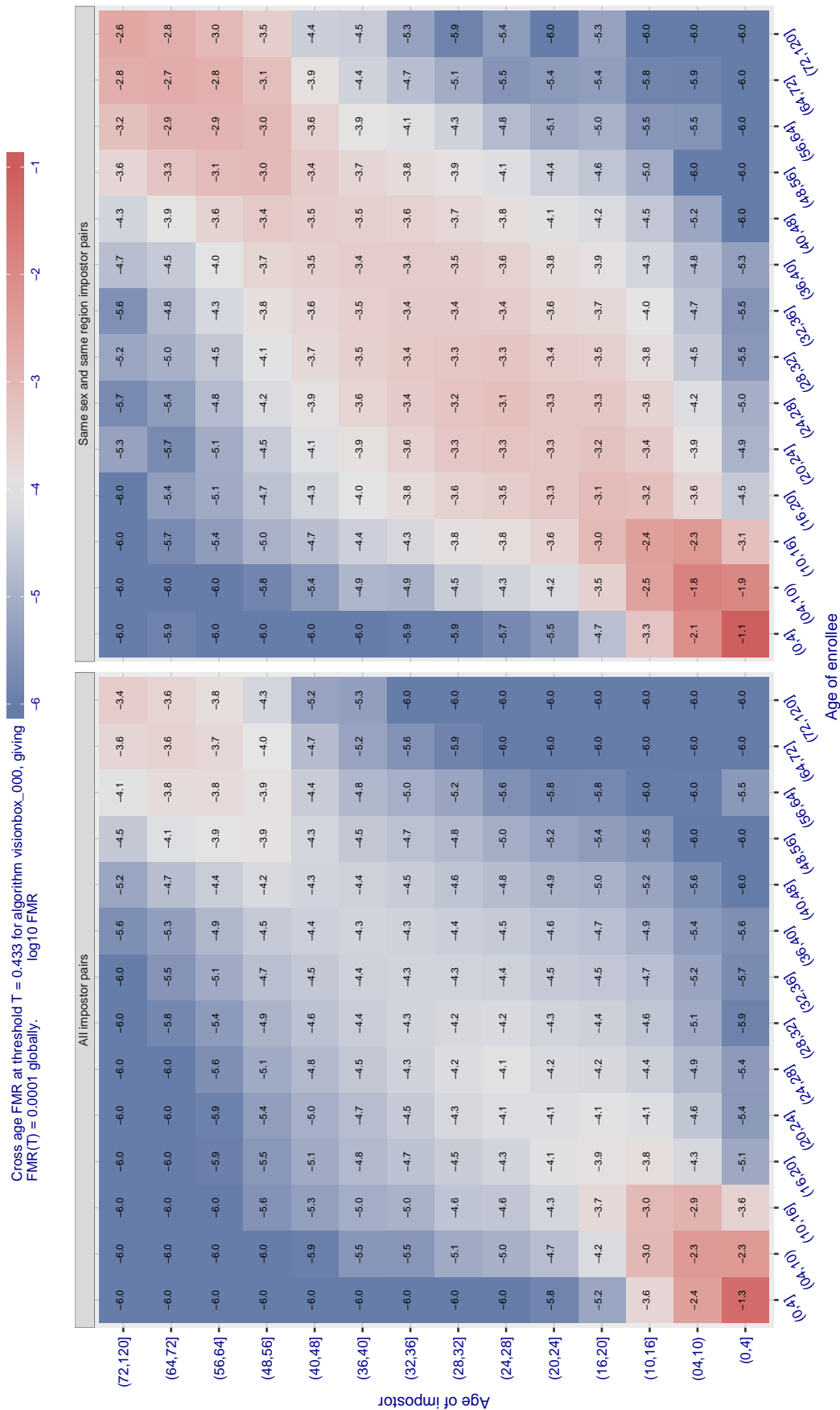


Figure 637: For algorithm visionbox-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.382$  for algorithm visionbox\_001, giving  $FMR(T) = 0.0001$  globally.

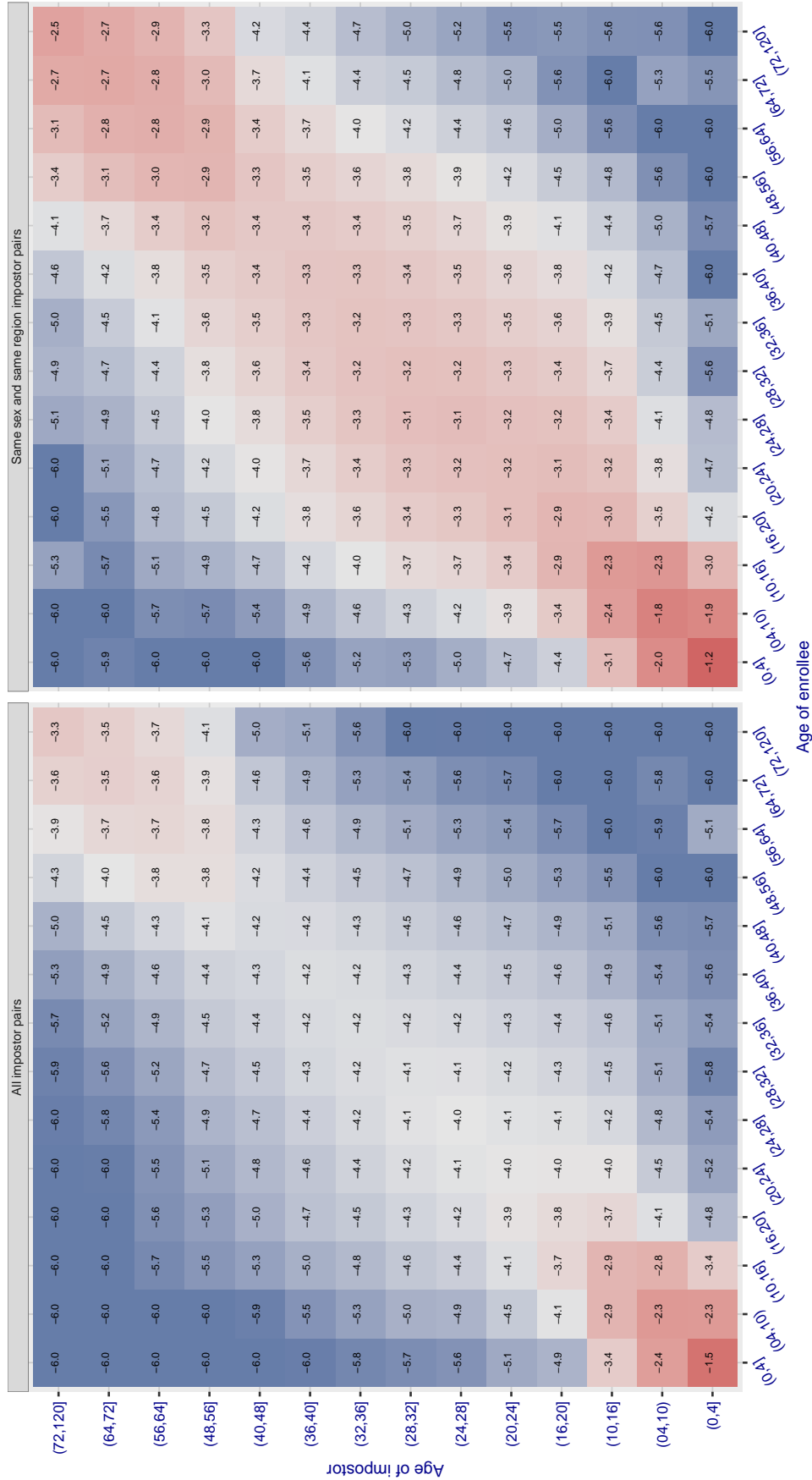


Figure 638: For algorithm visionbox-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.



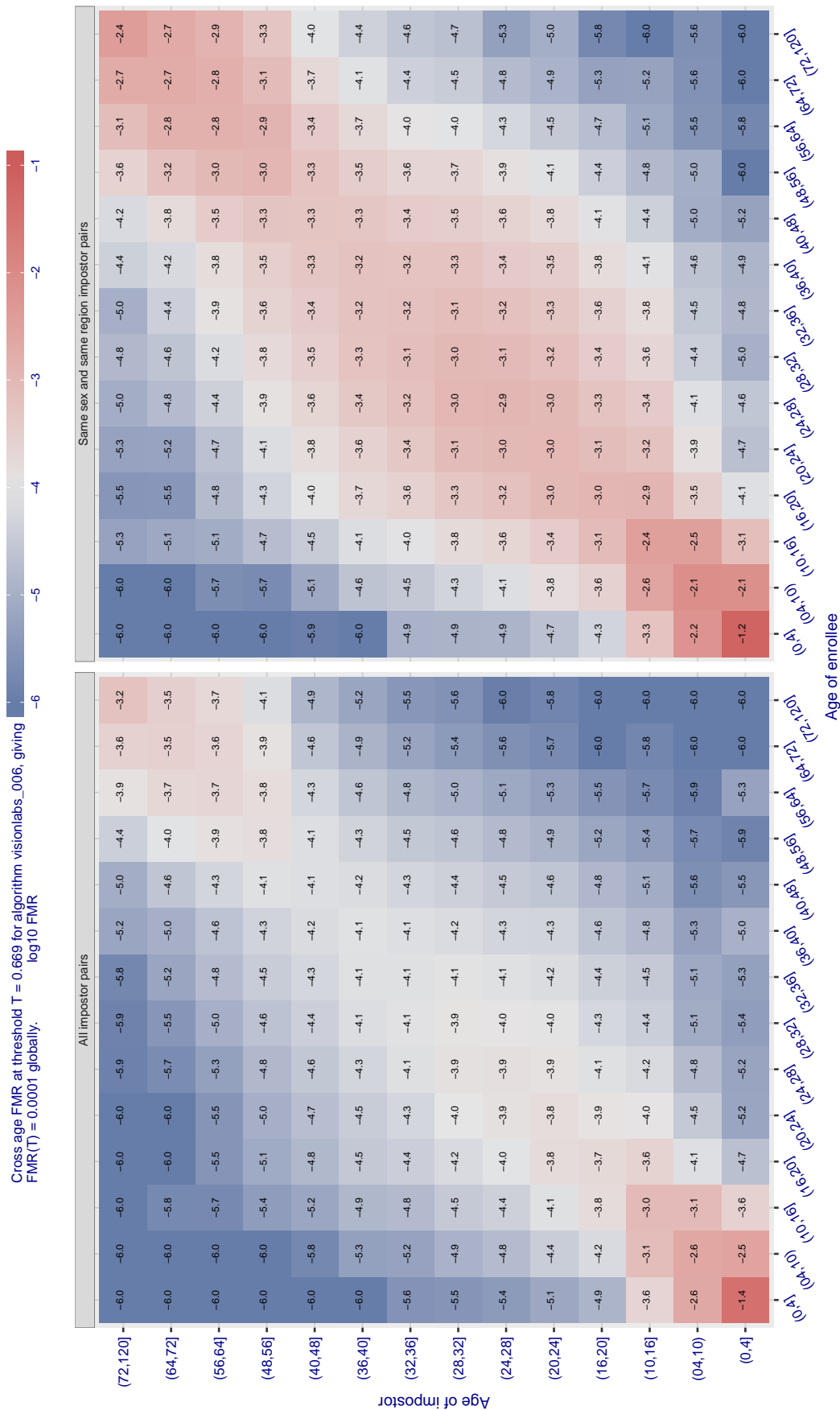


Figure 639: For algorithm visionlabs-006 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.657$  for algorithm visionlabs\_007, giving  $FMR(T) = 0.0001$  globally.

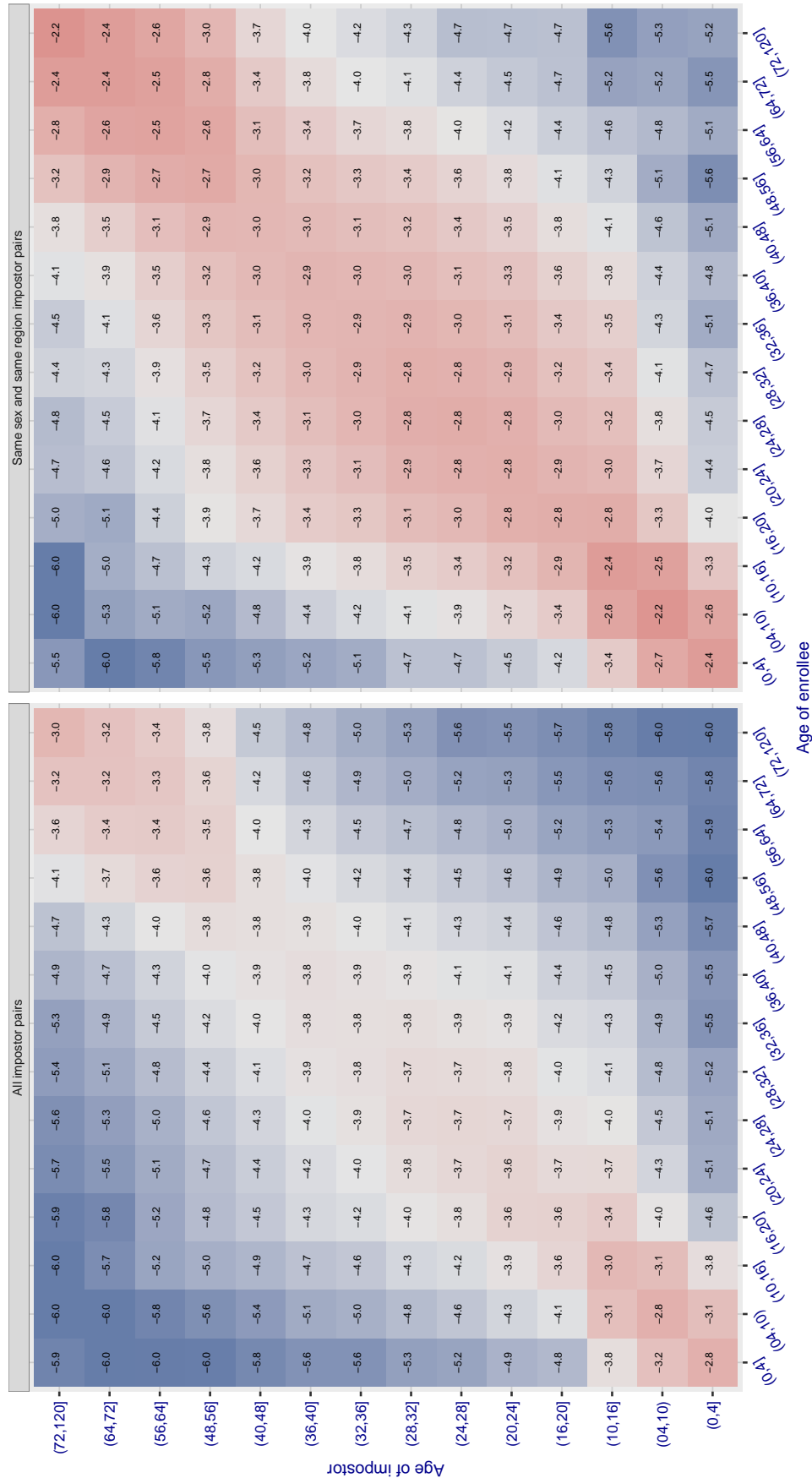


Figure 640: For algorithm visionlabs-007 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

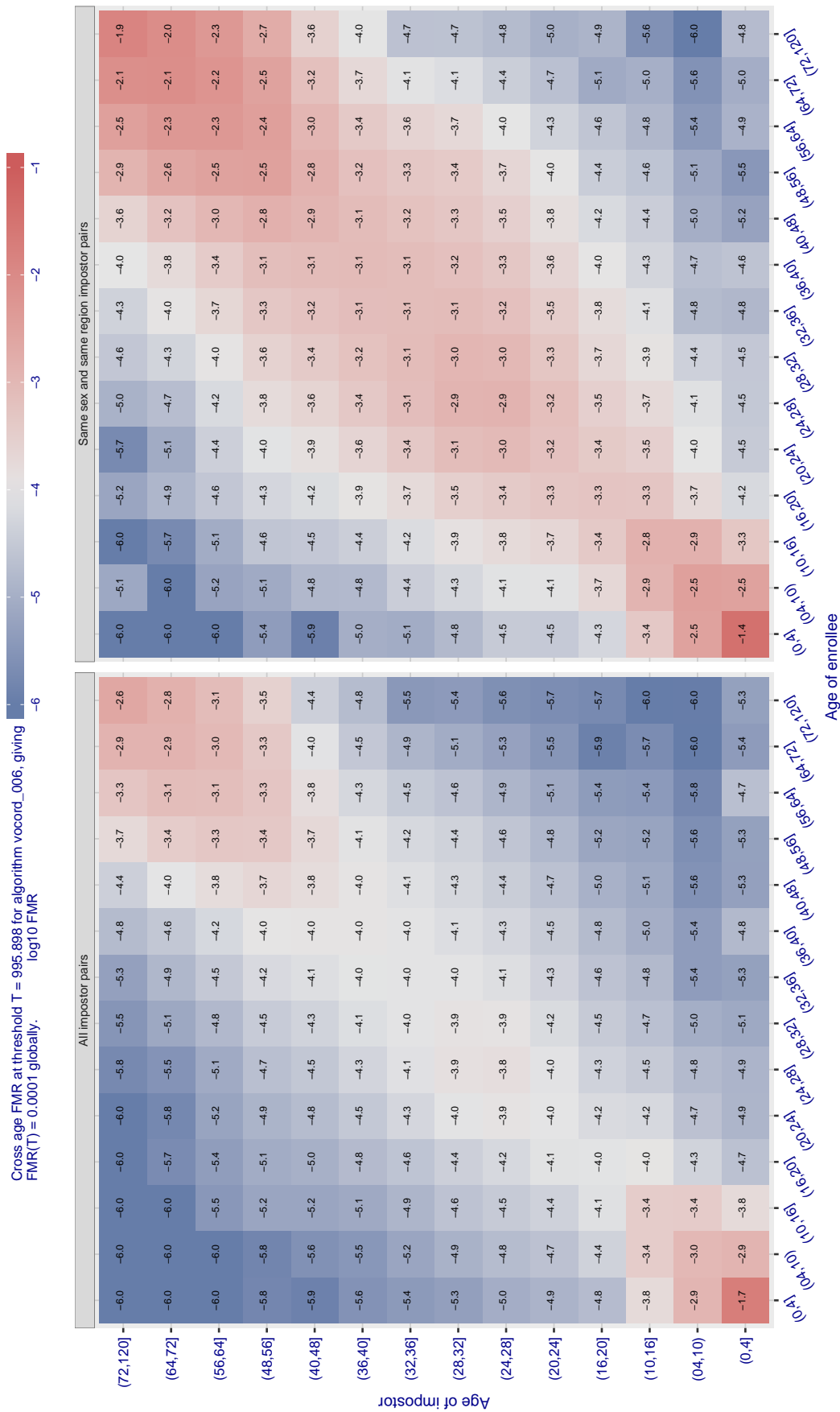


Figure 64: For algorithm vocord-006 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

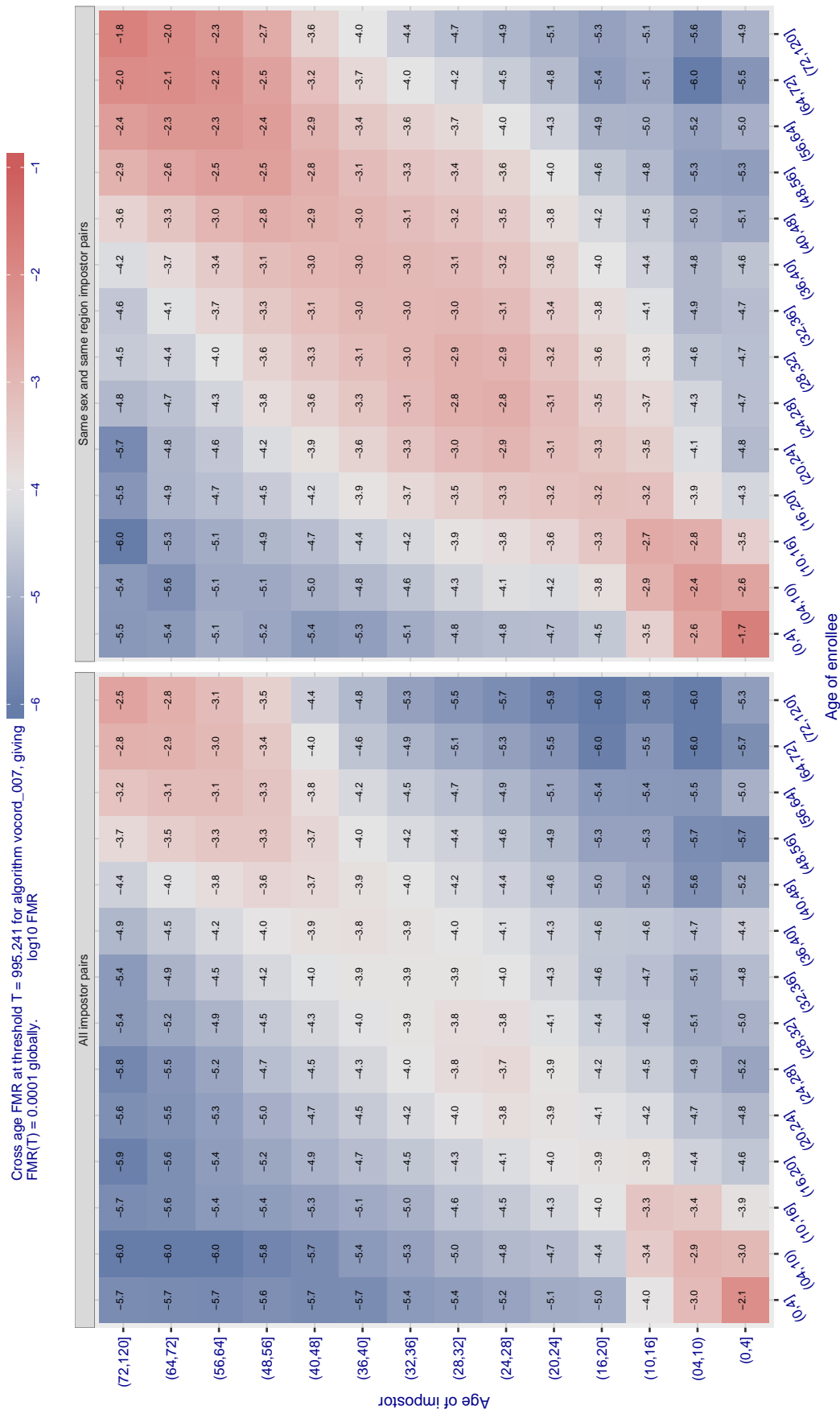


Figure 642: For algorithm vocord-007 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.400$  for algorithm  $winsense\_000$ , giving  $FMR(T) = 0.0001$  globally.

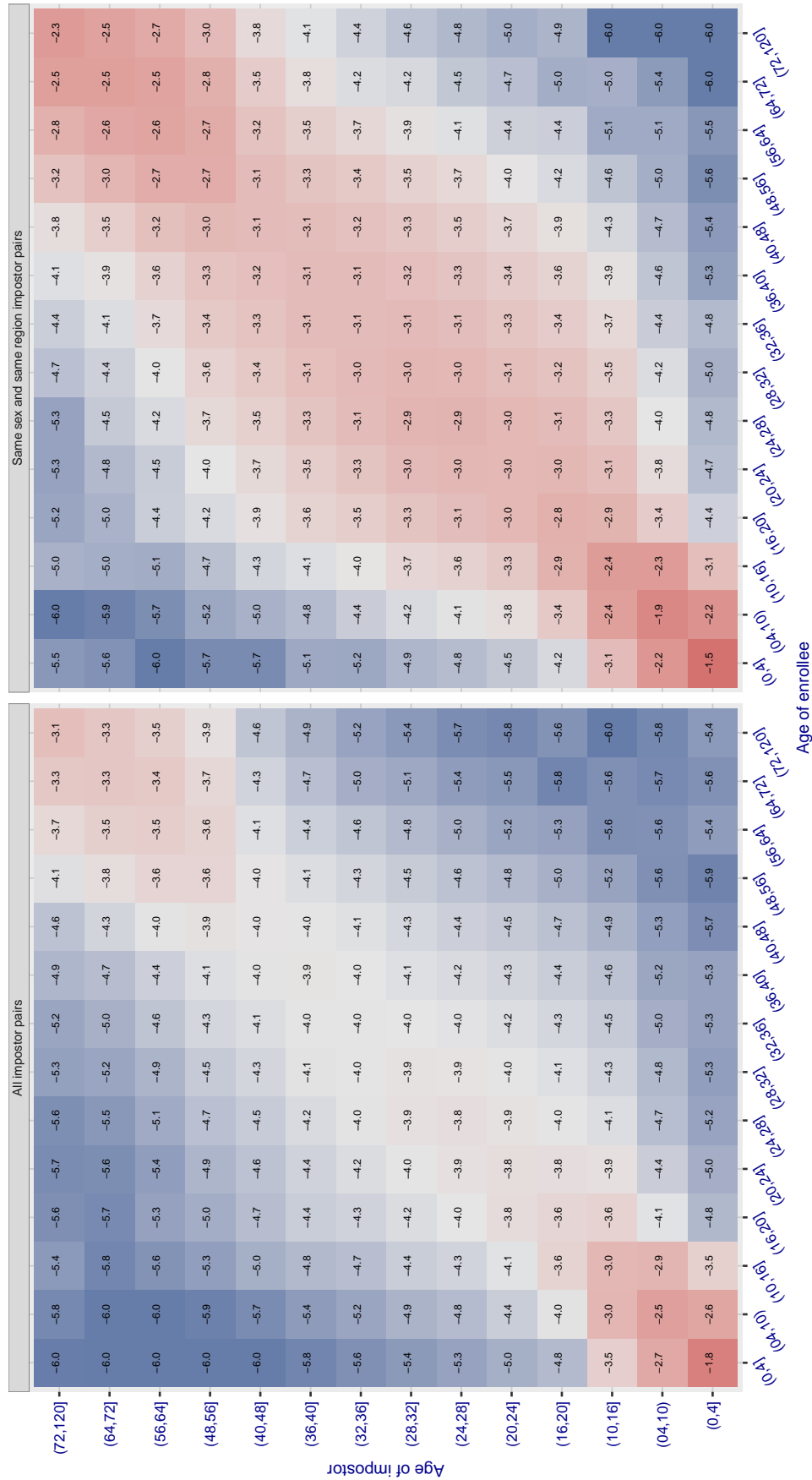


Figure 643: For algorithm  $winsense\_000$  operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 0.322$  for algorithm winsense\_001, giving  $FMR(T) = 0.0001$  globally.

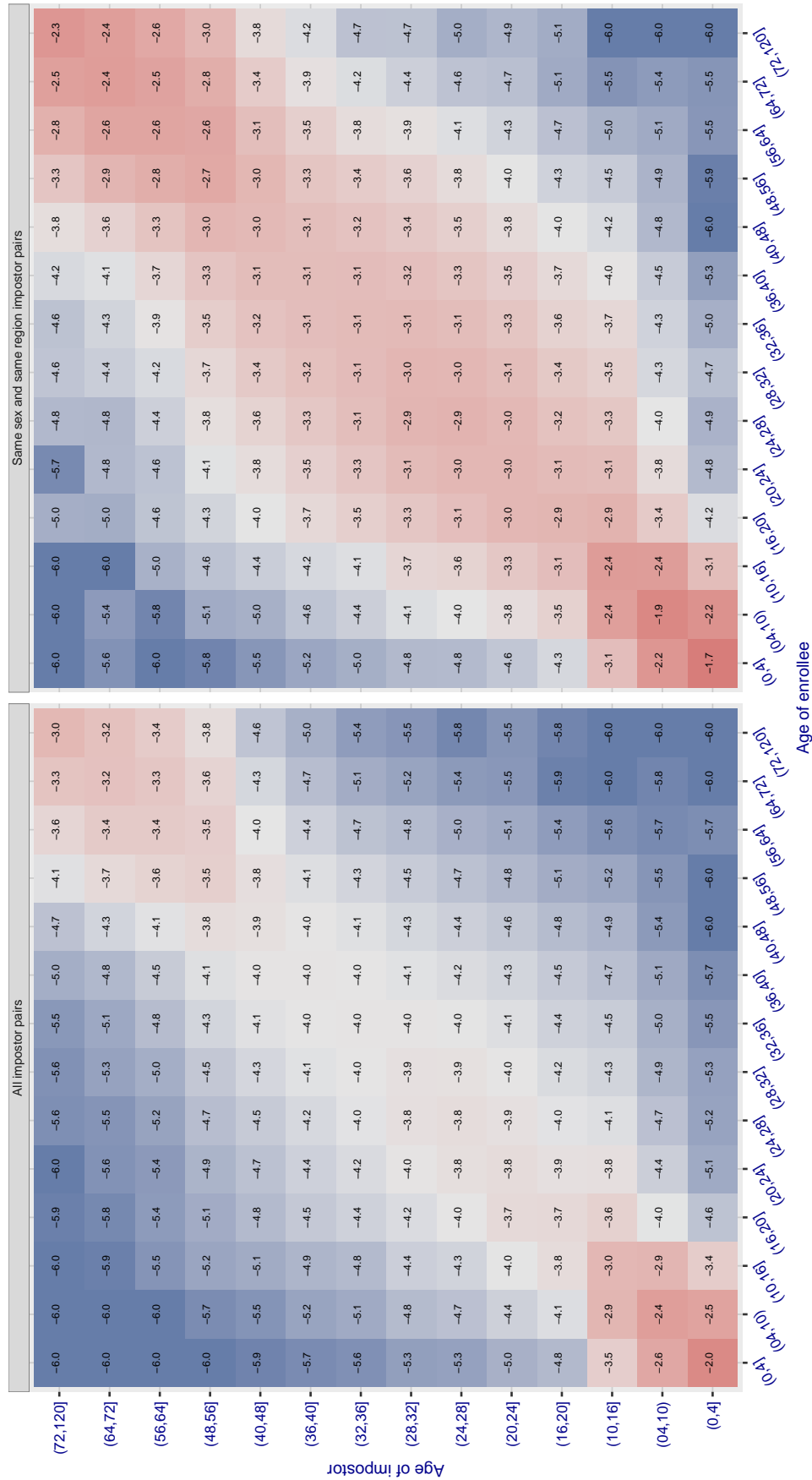


Figure 644: For algorithm winsense-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

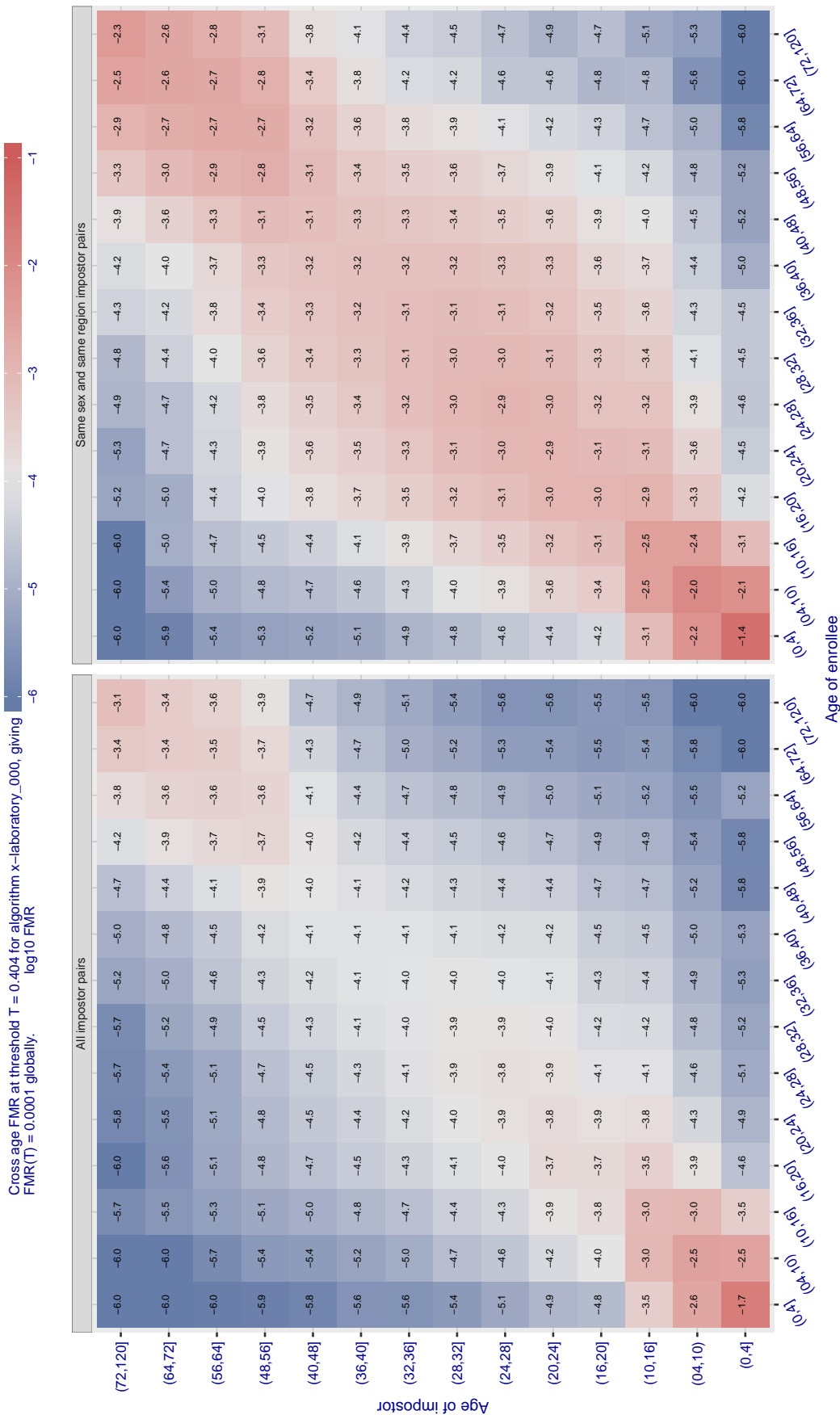


Figure 645: For algorithm x-laboratory-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $\text{FMR} = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold  $T = 5.544$  for algorithm yisheng\_004, giving  $FMR(T) = 0.0001$  globally.

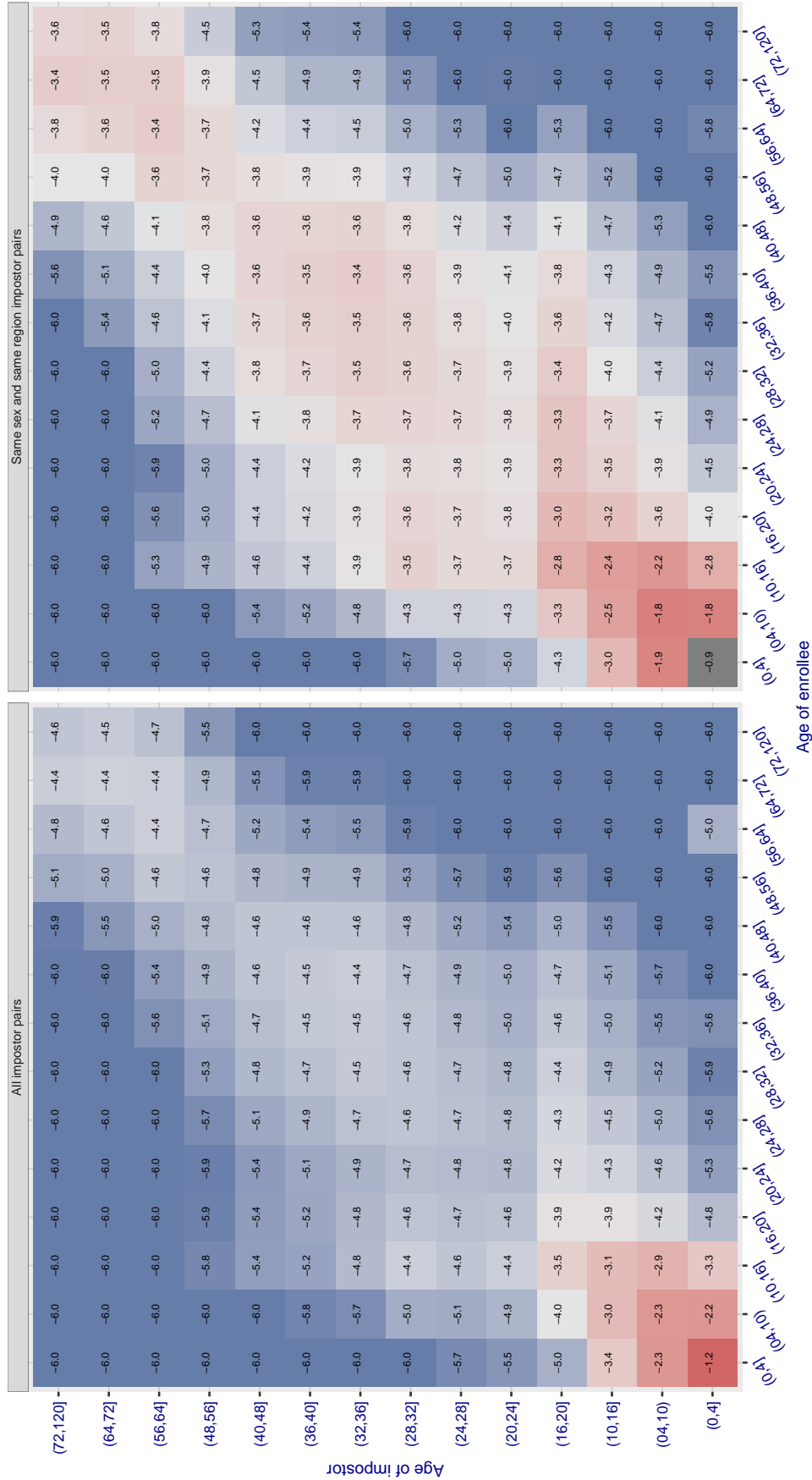


Figure 646: For algorithm yisheng-004 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.



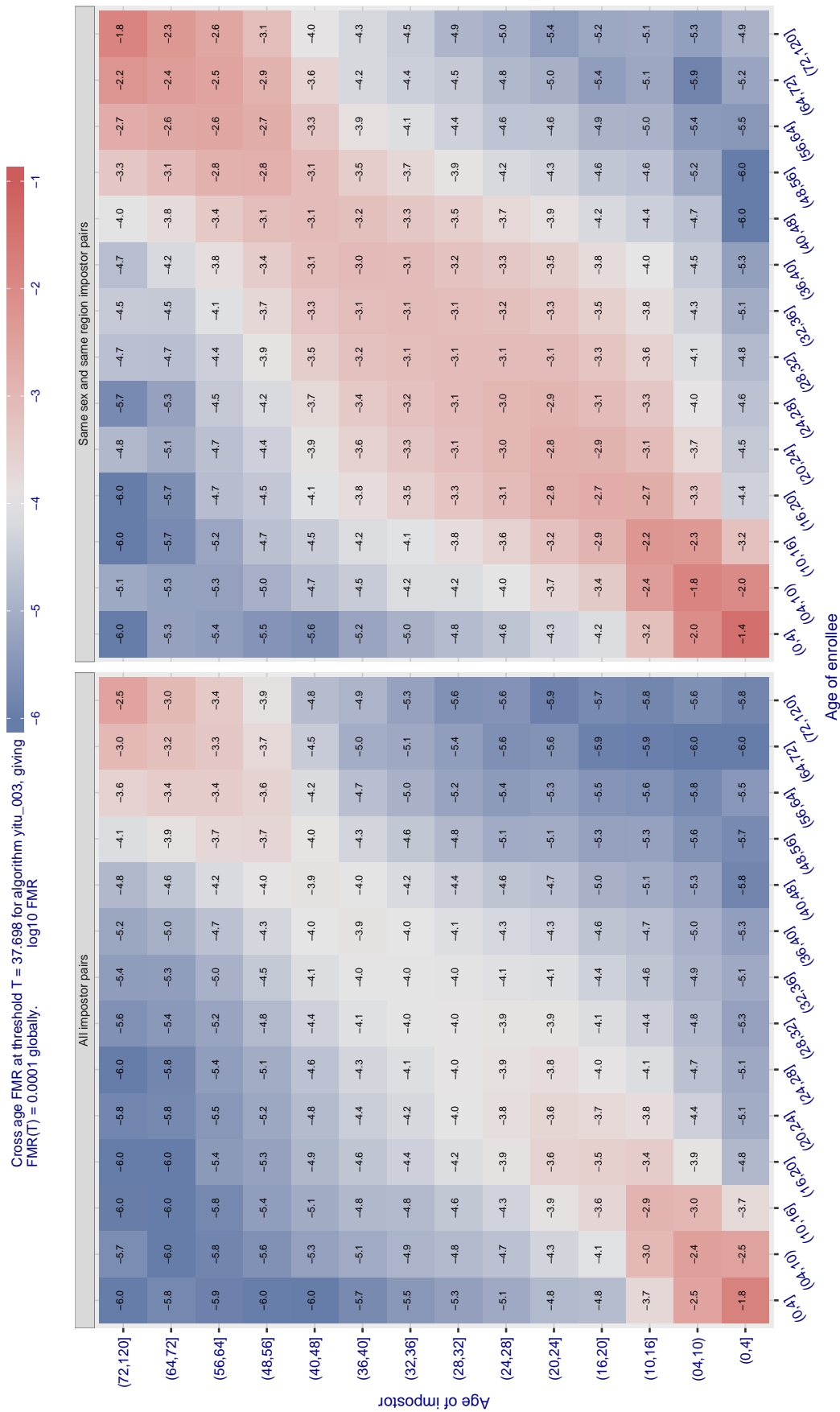


Figure 647: For algorithm yitu-003 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give  $FMR = 0.0001$  over all on the order of  $10^{10}$  impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

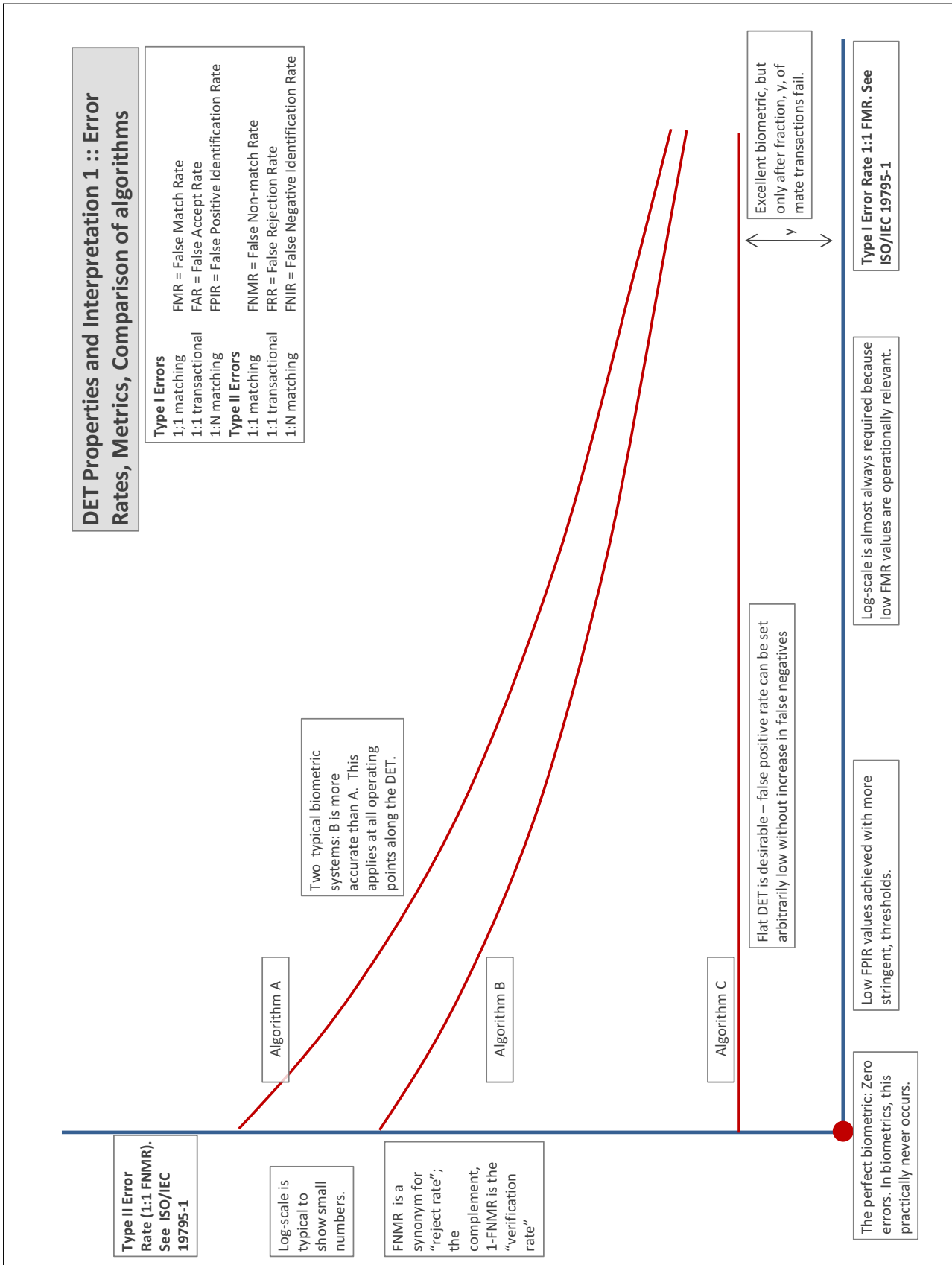
## Accuracy Terms + Definitions

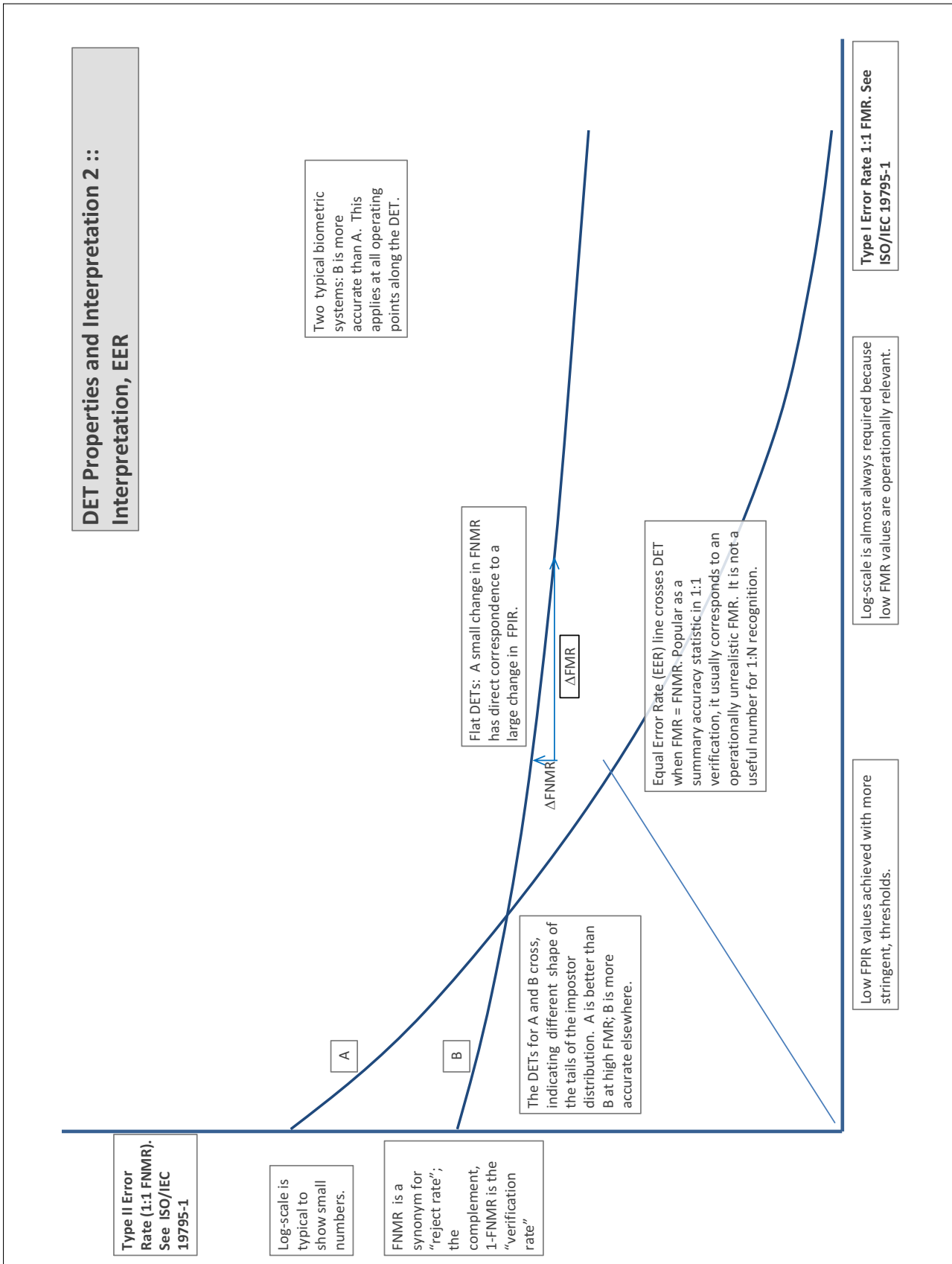
In biometrics, Type II errors occur when two samples of one person do not match – this is called a **false negative**. Correspondingly, Type I errors occur when samples from two persons do match – this is called a **false positive**. Matches are declared by a biometric system when the native comparison score from the recognition algorithm meets some **threshold**. Comparison scores can be either **similarity scores**, in which case higher values indicate that the samples are more likely to come from the same person, or **dissimilarity scores**, in which case higher values indicate different people. Similarity scores are traditionally computed by **fingerprint** and **face** recognition algorithms, while dissimilarities are used in **iris recognition**. In some cases, the dissimilarity score is a distance; this applies only when **metric** properties are obeyed. In any case, scores can be either **mate** scores, coming from a comparison of one person's samples, or **nonmate** scores, coming from comparison of different persons' samples. The words **genuine** or **authentic** are synonyms for mate, and the word **impostor** is used a synonym for nonmate. The words mate and nonmate are traditionally used in identification applications (such as law enforcement search, or background checks) while genuine and impostor are used in verification applications (such as access control).

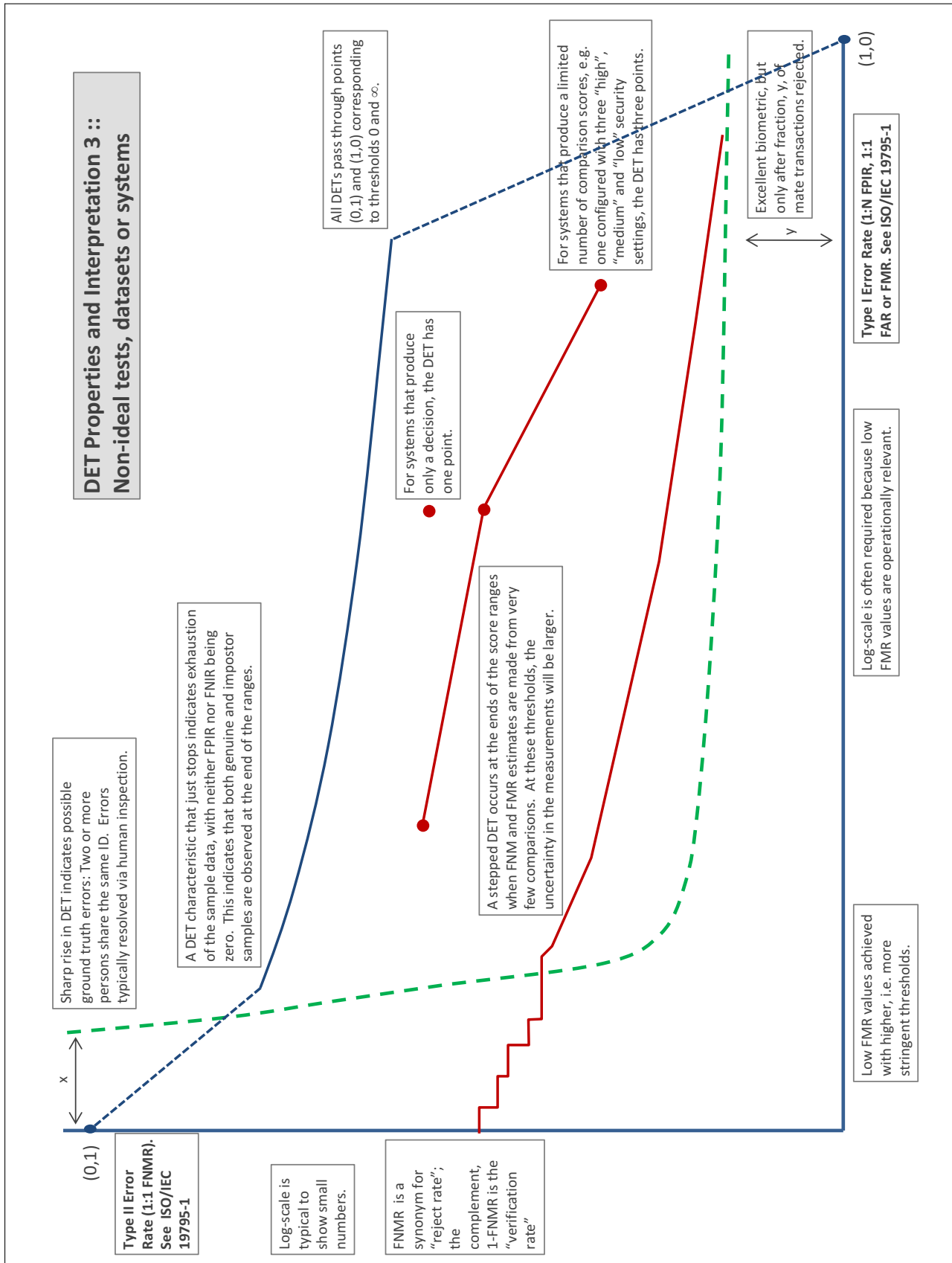
A **error tradeoff** characteristic represents the tradeoff between Type II and Type I classification errors. For verification this plots false non-match rate (FNMR) vs. false match rate (FMR) parametrically with T.

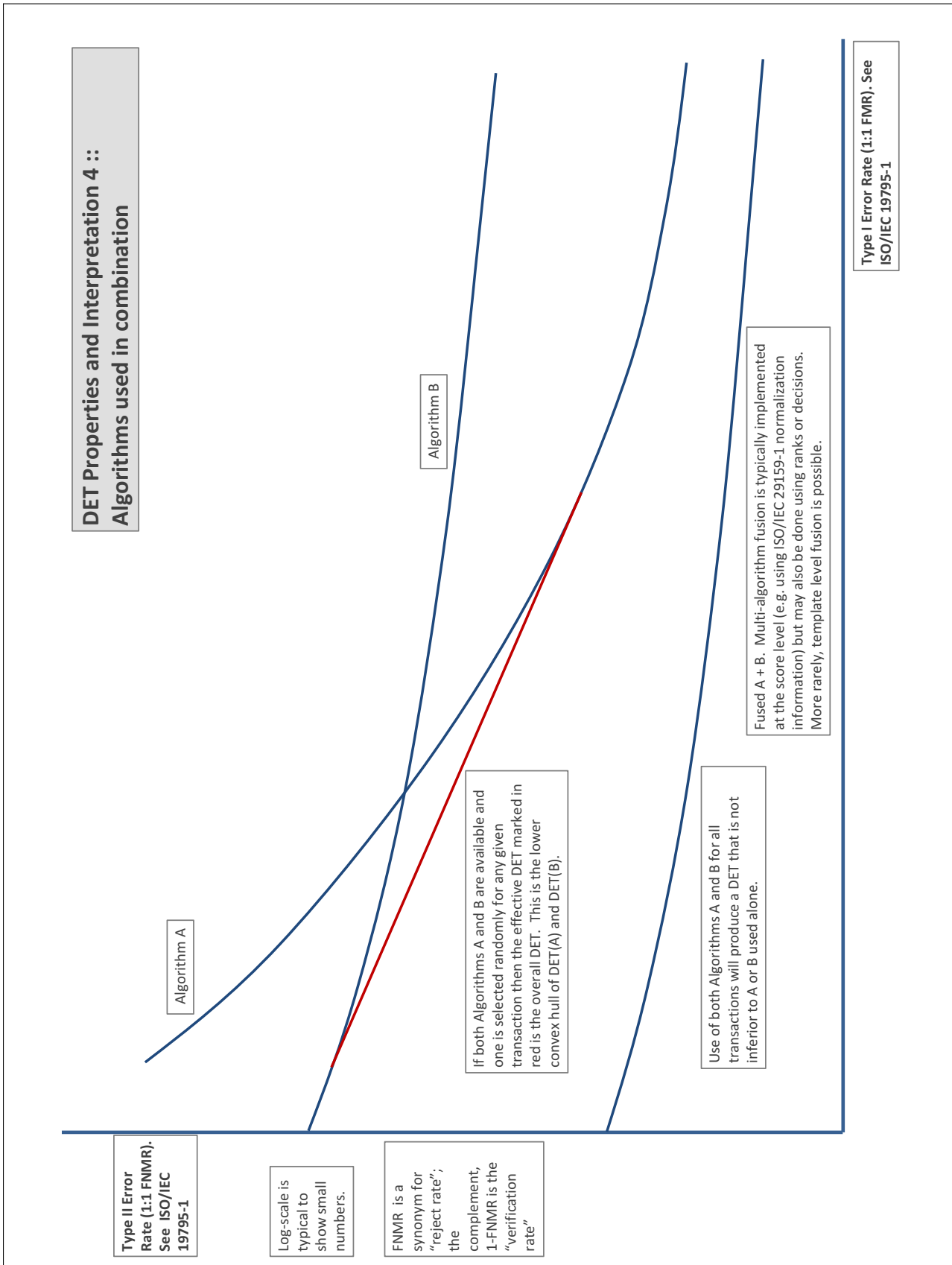
The error tradeoff plots are often called **detection error tradeoff (DET)** characteristics or **receiver operating characteristic (ROC)**. These serve the same function but differ, for example, in plotting the complement of an error rate (e.g.  $TMR = 1 - FNMR$ ) and in transforming the axes most commonly using logarithms, to show multiple decades of FMR. More rarely, the function might be the inverse Gaussian function.

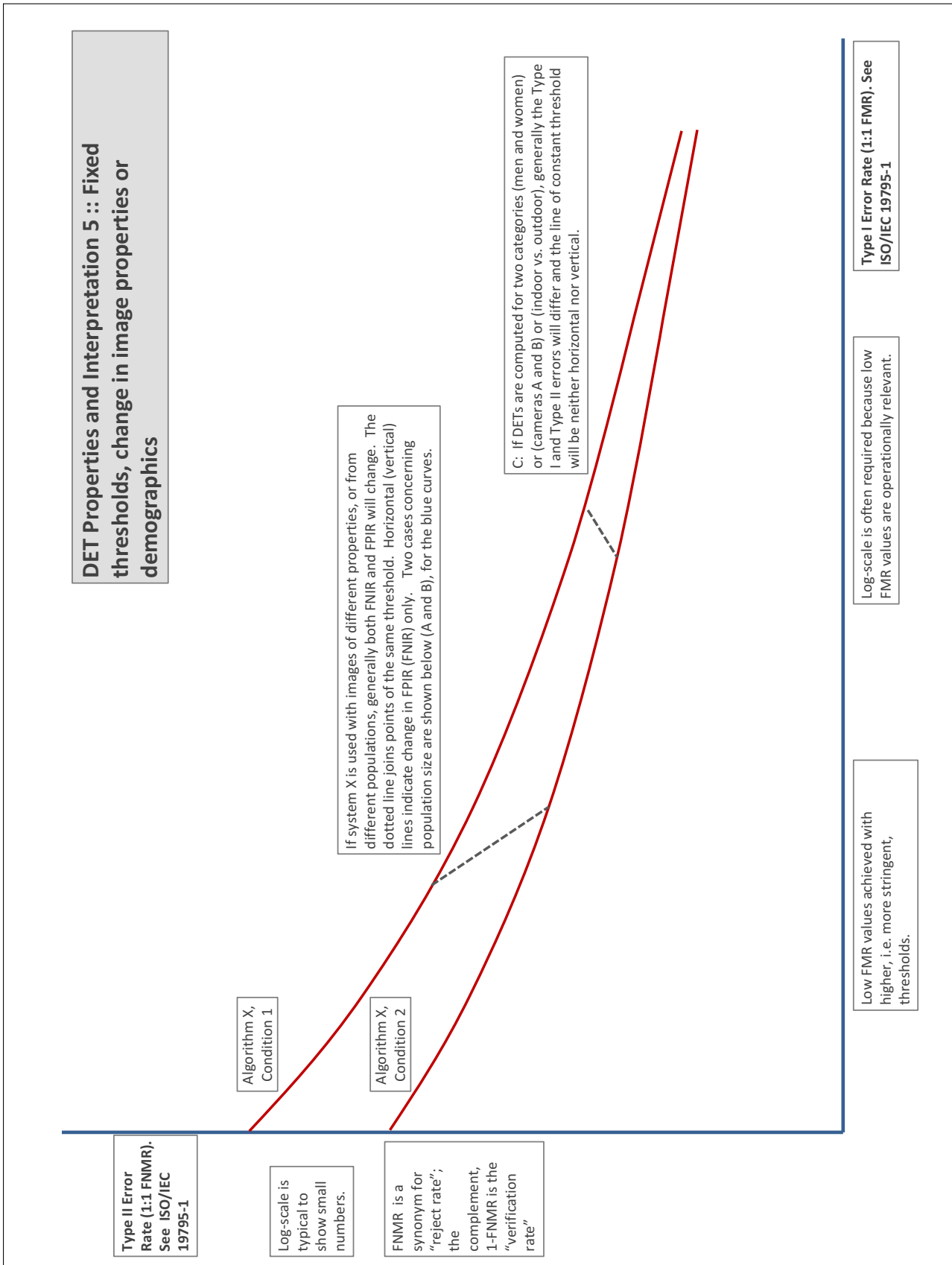
More detail and generality is provided in formal biometrics testing standards, see the various parts of [ISO/IEC 19795 Biometrics Testing and Reporting](#). More terms, including and beyond those to do with accuracy, see [ISO/IEC 2382-37 Information technology -- Vocabulary -- Part 37: Harmonized biometric vocabulary](#)











## References

- [1] P. Jonathon Phillips, Amy N. Yates, Ying Hu, Carina A. Hahn, Eilidh Noyes, Kelsey Jackson, Jacqueline G. Cavazos, Géraldine Jeckeln, Rajeev Ranjan, Swami Sankaranarayanan, Jun-Cheng Chen, Carlos D. Castillo, Rama Chellappa, David White, and Alice J. O'Toole. Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms. *Proceedings of the National Academy of Sciences*, 115(24):6171–6176, 2018.