The ISO/IEC 30107-3 standard for testing of Presentation Attack Detection

Christoph Busch / Michael Thieme
CASED and EAB / Novetta

Contributions from:
Carsten Gottschlich, Josef Bigun and Martin Olsen

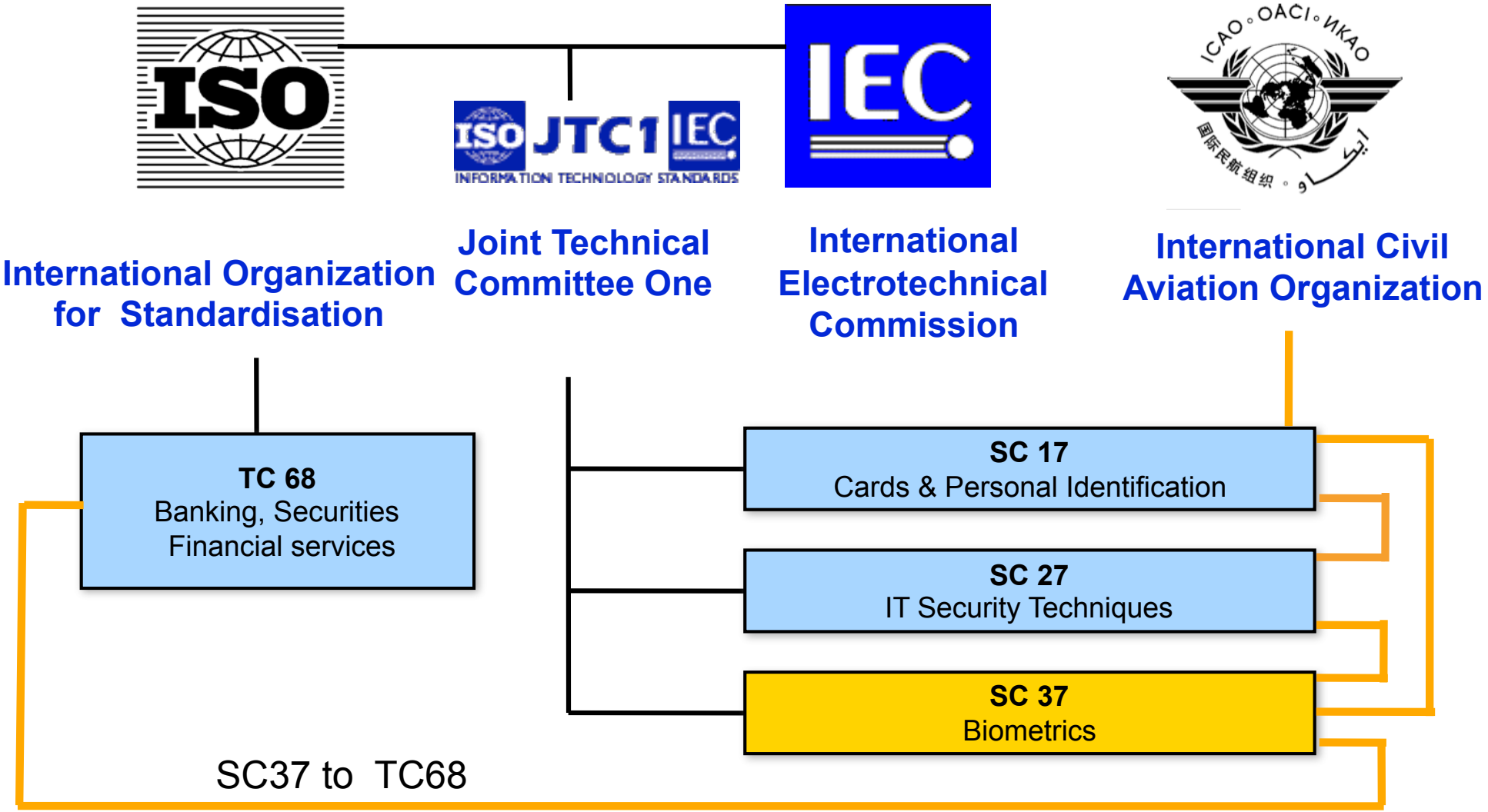
NIST IBPC 2016
2016-05-04

Presentation Attack Detection

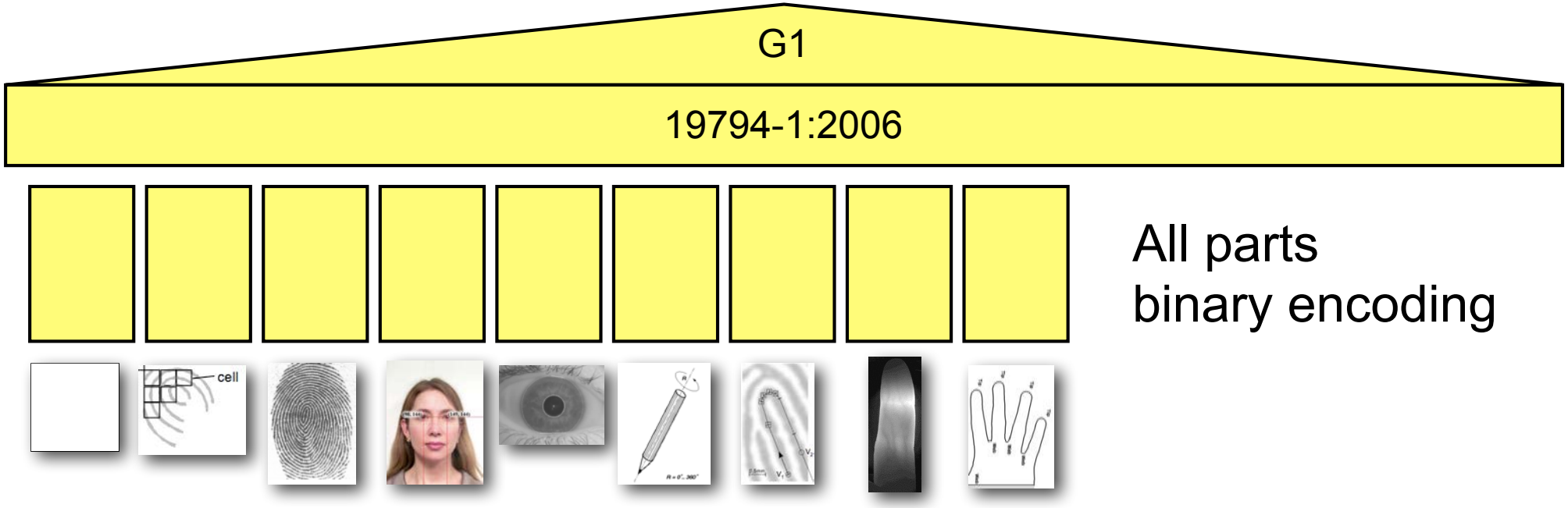
Outline

- Introduction to International Standardisation on PAD
- ISO/IEC 30107
- Application areas

Biometric Standardisation



First Generation Format Standards



All parts
binary encoding

The 19794-Family: Biometric data interchange formats

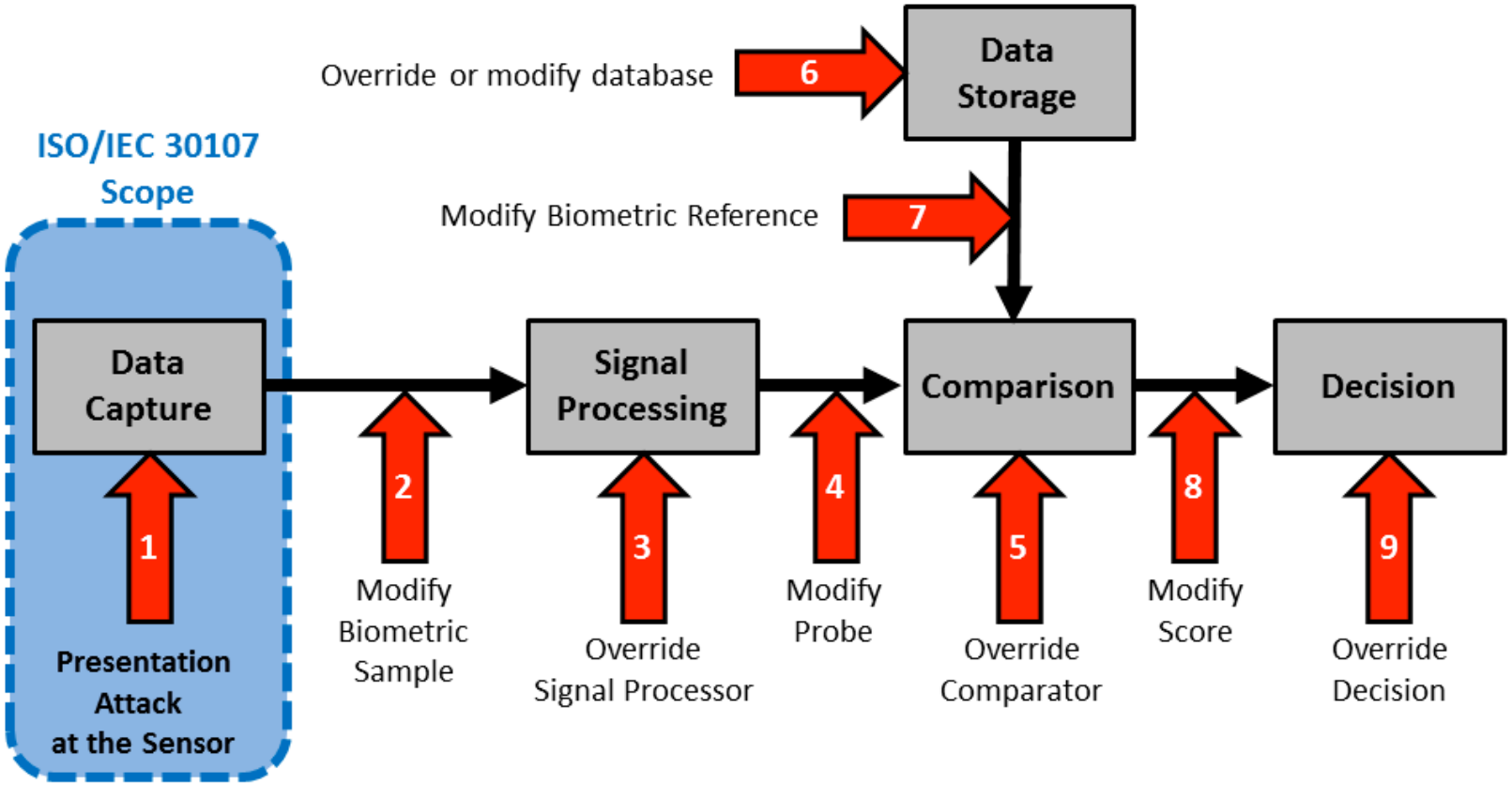
Presentation Attack Detection

ISO/IEC 30107 - Overview and Part 1

System Perspective - Framework

ISO/IEC 30107-1:2016 Presentation Attack Detection

- Attacks on Biometric Systems



Source: ISO/IEC 30107-1
Inspired by N.K. Ratha, J.H. Connell, R.M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Systems Journal, Vol 40. NO 3, 2001.

Presentation Attack Detection

ISO/IEC 30107 - Scope

- terms and definitions that are useful in the specification, characterization and evaluation of presentation attack detection methods;
- a common data format for conveying the type of approach used and the assessment of presentation attack in data formats;
- principles and methods for performance assessment of presentation attack detection algorithms or mechanisms; and
- a classification of known attacks types (in an informative annex).

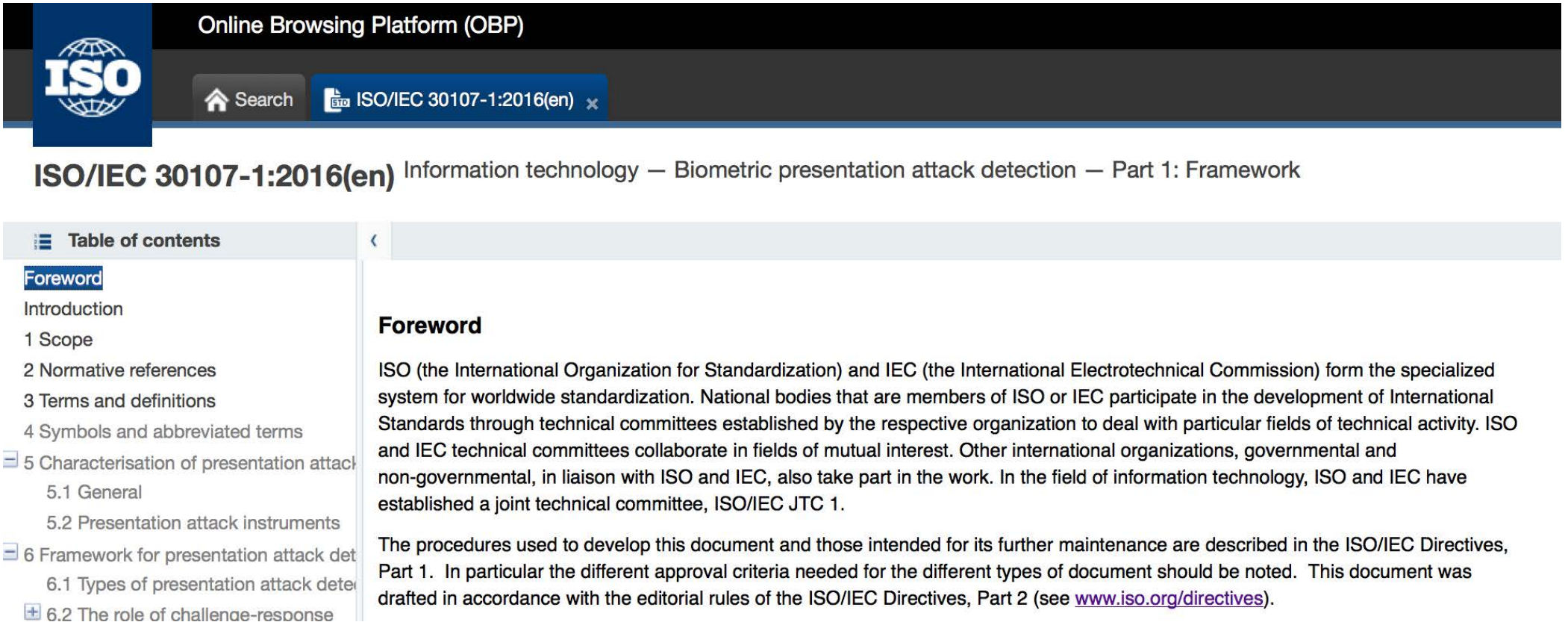
Outside the scope are

- standardization of specific PAD detection methods;
- detailed information about countermeasures (i.e. anti-spoofing techniques), algorithms, or sensors;
- overall system-level security or vulnerability assessment.

Presentation Attack Detection - Framework

ISO/IEC IS 30107-1 Standard

- now available in the ISO-Portal
  https://www.iso.org/obp/ui/#!iso:std:53227:en
- SC37 has initiated to make this standard freely available



Presentation Attack Detection

Definitions in ISO/IEC 30107 PAD - Part 1: Framework

- **presentation attack**
  presentation to the biometric capture subsystem with the goal of interfering with the operation of the biometric system
- **presentation attack detection (PAD)**
  automated determination of a presentation attack

Definitions in ISO/IEC 2382-37: Vocabulary

http://www.christoph-busch.de/standards.html

- **impostor**
  subversive biometric capture subject who attempts to being matched to someone else's biometric reference
- **identity concealer**
  subversive biometric capture subject who attempts to avoid being matched to their own biometric reference

Presentation Attack Detection

ISO/IEC 30107 - Definitions

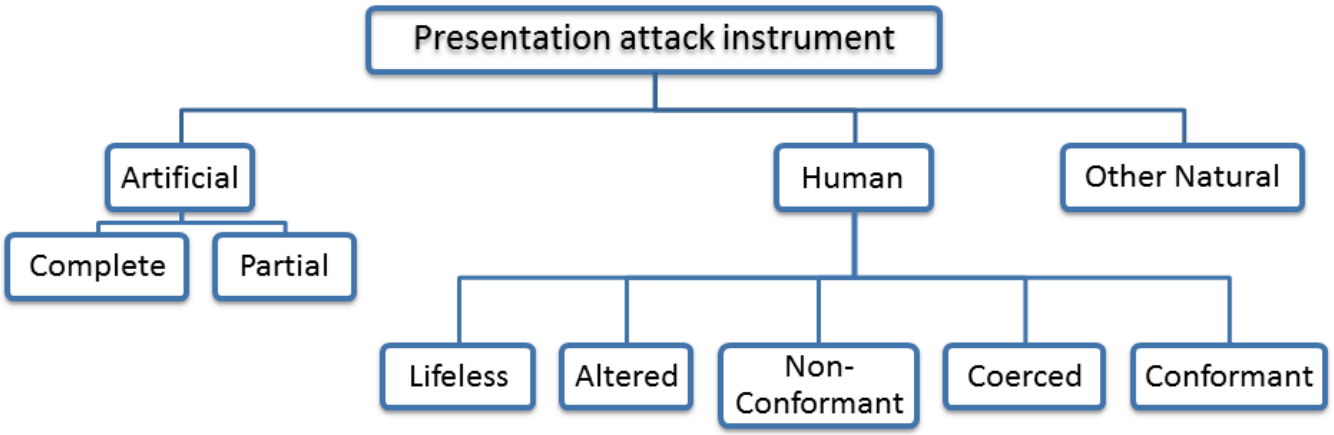
- **presentation attack instrument (PAI)**
  biometric characteristic or object used in a presentation attack
- **artefact**
  artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns

Types of presentation attacks

(General Noun)

(Adjectives describing categories)

(Qualifying adjectives)



Source: ISO/IEC 30107-1

Presentation Attack Detection

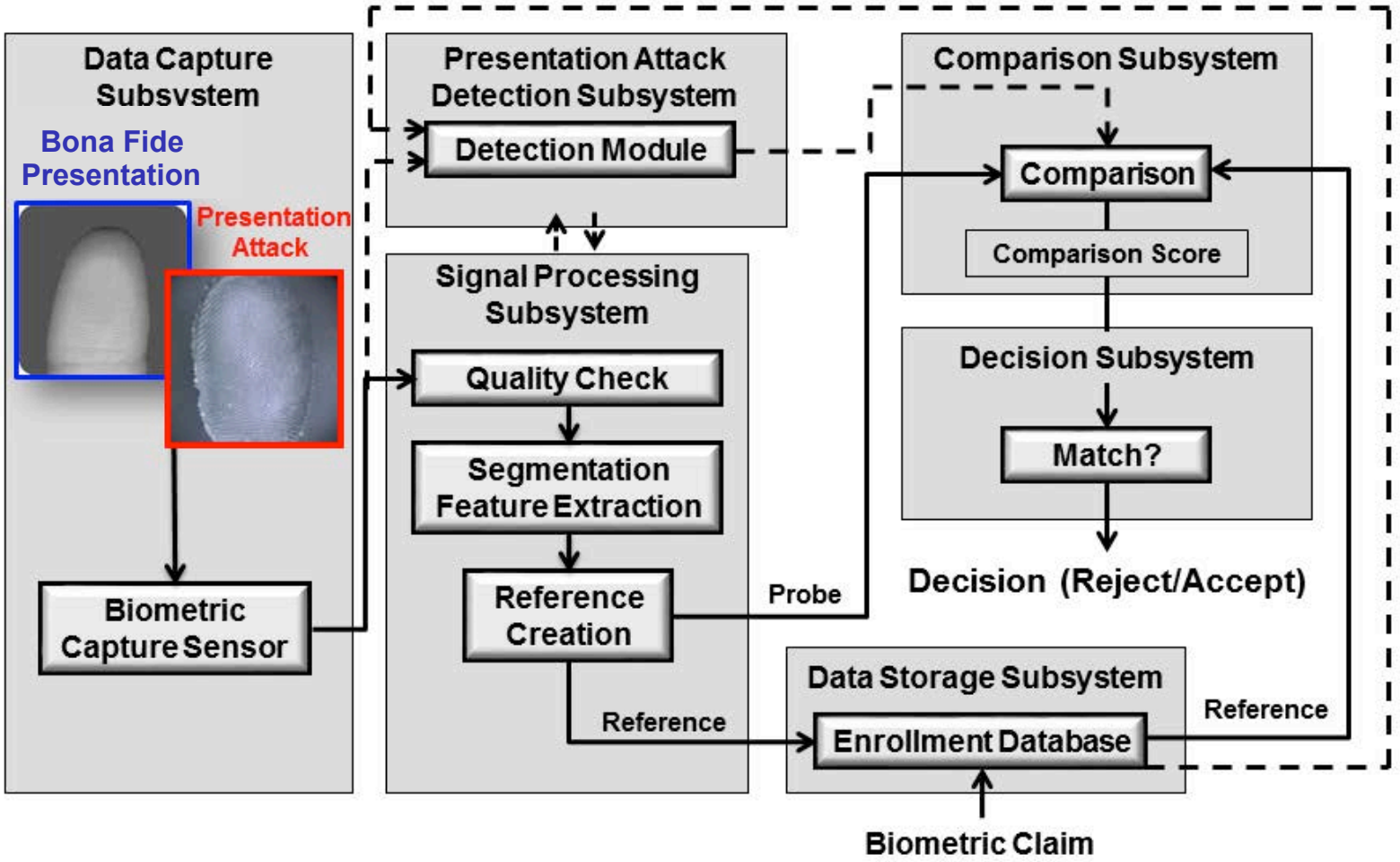
ISO/IEC 30107-1: Examples of Artificial and Human Presentation Attack Instruments

Artificial	*Complete*	gummy finger, video of face
	Partial	glue on finger, sunglasses, artificial/patterned contact lens
Human	*Lifeless*	cadaver part, severed finger/hand
	Altered	mutilation, surgical switching of fingerprints between hands and/or toes
	Non-Conformant	facial expression/extreme, tip or side of finger
	Coerced[1]	unconscious, under duress
	Conformant	zero effort impostor attempt

Source: ISO/IEC 30107-1

Presentation Attack Detection

Biometric framework with PAD



Source: ISO/IEC 30107-1

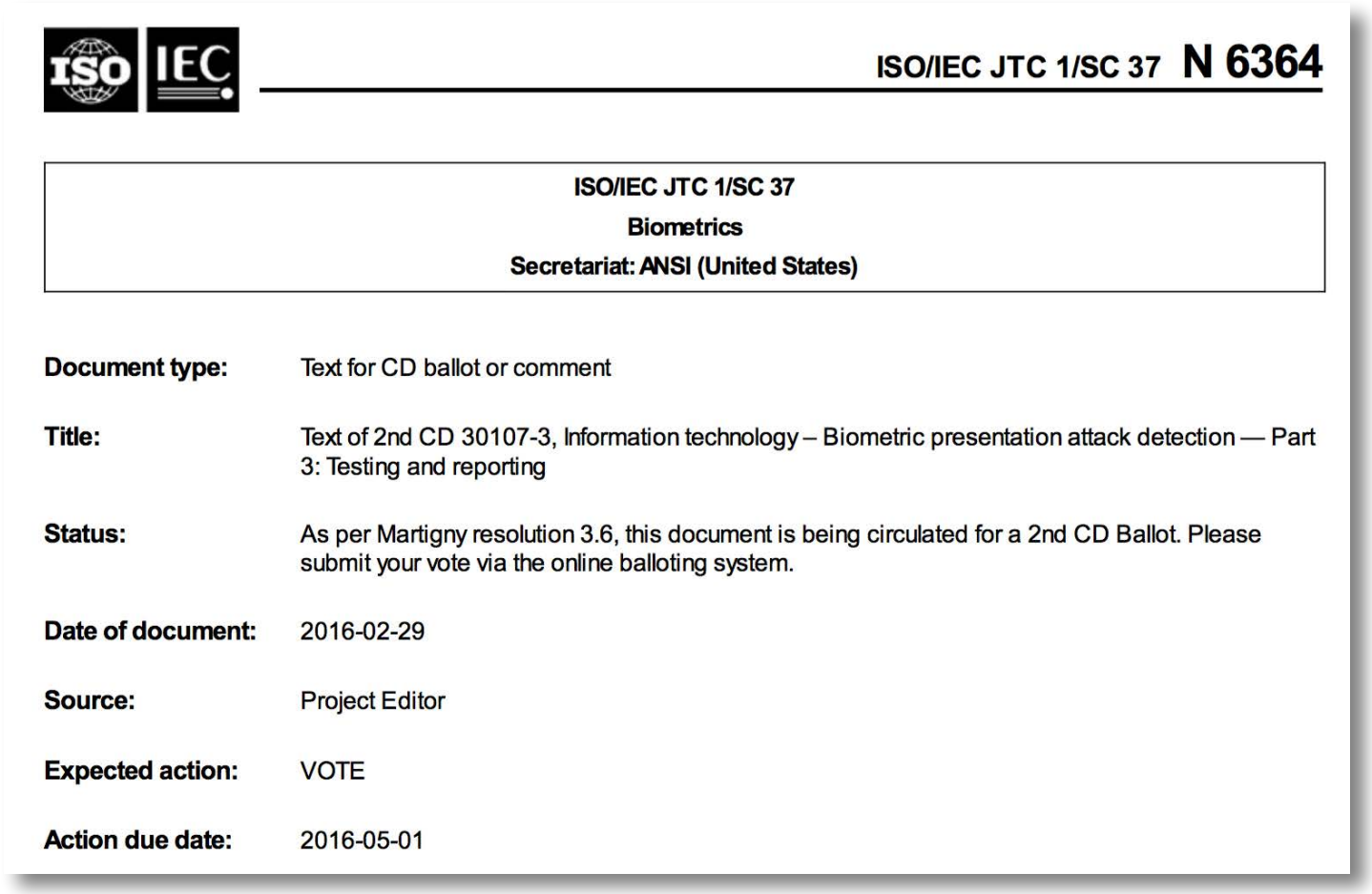
Presentation Attack Detection

ISO/IEC 30107 - Part 3

Presentation Attack Detection - Metrics

ISO/IEC CD 30107-3

- available as draft
  http://isotc.iso.org/livelink/livelink?func=ll&objId=17578675&objAction=Open&viewType=1



ISO IEC

ISO/IEC JTC 1/SC 37 N 6364

ISO/IEC JTC 1/SC 37
Biometrics
Secretariat: ANSI (United States)

Document type:	Text for CD ballot or comment
Title:	Text of 2nd CD 30107-3, Information technology – Biometric presentation attack detection — Part 3: Testing and reporting
Status:	As per Martigny resolution 3.6, this document is being circulated for a 2nd CD Ballot. Please submit your vote via the online balloting system.
Date of document:	2016-02-29
Source:	Project Editor
Expected action:	VOTE
Action due date:	2016-05-01

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-3

- Testing the full system:

- **Attack presentation match rate (APMR)**
  in a full-system evaluation of a verification system, the proportion of presentation attacks in which the target reference is matched

  Source: ISO/IEC 30107-3

- **Attack presentation non-match rate (APNMR)**
  in a full-system evaluation of a verification system, the proportion of presentation attacks in which the target reference is not matched.

  Source: ISO/IEC 30107-3

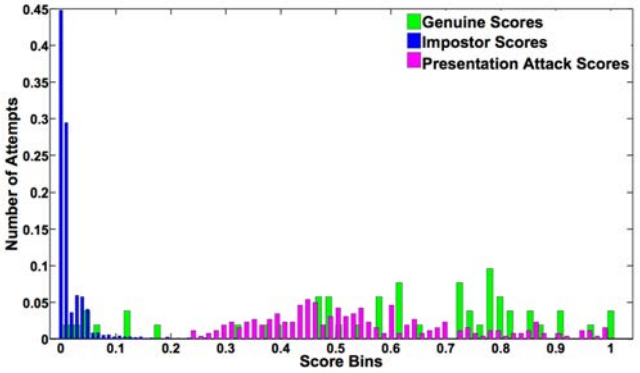


Image Source: K. Raja, R. Raghavendra, C. Busch: "Video Presentation Attack Detection in Visible Spectrum Iris Recognition Using Magnified Phase Information", in IEEE TIFS, June 2015

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-3

- Testing the PAD subsystem:

- **Attack presentation non-response rate (APNRR)**
  proportion of presentation attacks that cause no response at the PAD subsystem or data capture subsystem

- **Bona Fide presentation non-response rate (BPNRR)**
  proportion of bona fide presentations that cause no response at the PAD subsystem or data capture subsystem
  - *NOTE An example of a non-response is a data capture subsystem "time out" if a presentation is not registered within a certain amount of time.*

Source: ISO/IEC 30107-3

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-3

- Testing the PAD subsystem:

- **Attack presentation classification error rate (APCER)**
  proportion of attack presentations incorrectly classified as Bona Fide presentations at the component level in a specific scenario

- **Bona Fide presentation classification error rate (BPCER)**
  proportion of Bona Fide presentations incorrectly classified as attack presentations at the component level in a specific scenario

Source: ISO/IEC 30107-3

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-3

- Testing the PAD subsystem:

- **PAI species**
  class of presentation attack instruments created using a common production method and based on different biometric characteristic
- **Attack potential**
  measure of the effort to be expended in attacking a TOE, expressed in terms of an attacker's expertise, resources and motivation
- **target of evaluation (TOE)**
  within Common Criteria, the product or system that is the subject of the evaluation

Source: ISO/IEC 30107-3

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-3

- Testing the PAD subsystem:

- **Attack presentation classification error rate (APCER)**
  proportion of attack presentations incorrectly classified as Bona Fide presentations at the component level in a specific scenario

$$APCER_{PAIS} = \frac{1}{N_{PAIS}} \sum_{i=1}^{N_{PAIS}} (1 - Res_i)$$

Source: ISO/IEC 30107-3

- N_{PAIS} *is the number of attack presentations for the given PAI species*
- Res_i *takes value 1 if the* i^{th} *presentation is classified as an attack presentation, and value 0 if classified as a bona fide presentation*

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-3

- Testing the PAD subsystem with different species:

- **Attack presentation classification error rate (APCER)** *the highest APCER (i.e. that of the most successful PAI) should be used as follows:*

$$APCER_{at\ attack\ potential\ AP} = \max_{PAIS \in \mathcal{A}_{AP}} (APCER_{PAIS})$$

Source: ISO/IEC 30107-3

Where $\mathcal{A}_{AP}$ is a subset of PAI species with attack potential at or below *AP*.s

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-3

- Testing the PAD subsystem with different species:

- **Bona Fide presentation classification error rate (BPCER)**
  BPCER shall be calculated as follows:

$$BPCER = \frac{\sum_{i=1}^{N_{BF}} RES_i}{N_{BF}}$$

Source: ISO/IEC 30107-3

- N_{BF} *is the number of bona fide presentations*
- Res_i *takes value 1 if the* it^h *presentation is classified as an attack presentation, and value 0 if classified as a bona fide presentation*

Presentation Attack Detection

Application area - Mobile Biometric Transactions

PAD-Standard and FIDO

FIDO - on 9th September 2015

What about rubber fingers?

- Protection methods in FIDO
  1. Attacker needs access to the Authenticator and have swipe rubber finger on it. This makes it a non-scalable attack.
  2. Authenticators might implement presentation attack detection methods.

Remember:

Creating hundreds of millions of rubber fingers + stealing the related authenticators is expensive. Stealing hundreds of millions of passwords from a server is not.

Source: R. Lindemann (NokNok) - 2015

Presentation Attack Detection

Application area - Identity Concealer

Altered Fingerprint Detection - Testing

Example for fingerprint alterations

- Z-shaped alteration (Finger of Jose Izquierdo, 1997)

Image Source: S. Yoon, J. Feng, and A. Jain, “Altered fingerprints: Analysis and detection,”
IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 34, no. 3, pp. 451–464, Mar. 2012

Altered Fingerprint Detection - Testing

Example for fingerprint alterations

- Left middle finger of Gus Winkler (Bank robber in the 1930s)

Image Source: H. Cummins, “Attempts to alter and obliterate finger-prints,” Journal of Criminal Law and Criminology, vol. 25, pp. 982–991, May 1935.

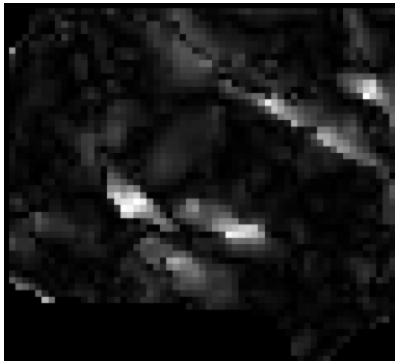
Altered Fingerprint Detection - Algorithms

- Feature: OFA and DOFTS
- Orientation Field Analysis (OFA)
  - Altered areas cause discontinuities in the OF [YoonJain2012]
- Differentials of Orientation Fields by Tensors in Scale (DOFTS)
  - Complex valued structure tensor [MikBig2014]

BonaFide fingerprint

Error map

Altered fingerprint



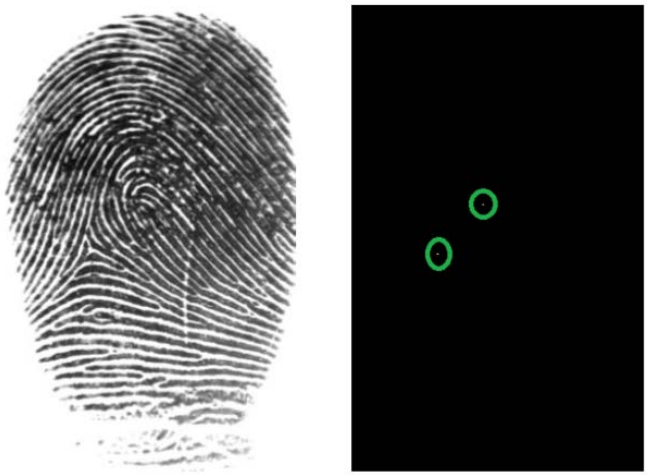
Error map

[YoonJain2012] S. Yoon, J. Feng, and A. Jain, “Altered fingerprints: Analysis and detection,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 34, no. 3, Mar. 2012

[MikBig2014] A. Mikaelyan and J. Bigun, “Symmetry assessment by finite expansion: application to forensic fingerprints,” in Proc. BIOSIG, Darmstadt, Germany, pp. 75–86. , (2014)

Altered Fingerprint Detection - Algorithms

- Feature: SPDA
- Singular Point Density Analysis [Ellingsg2014]
- using the Poincare´ index to detect noisy friction ridge areas



BonaFide fingerprint

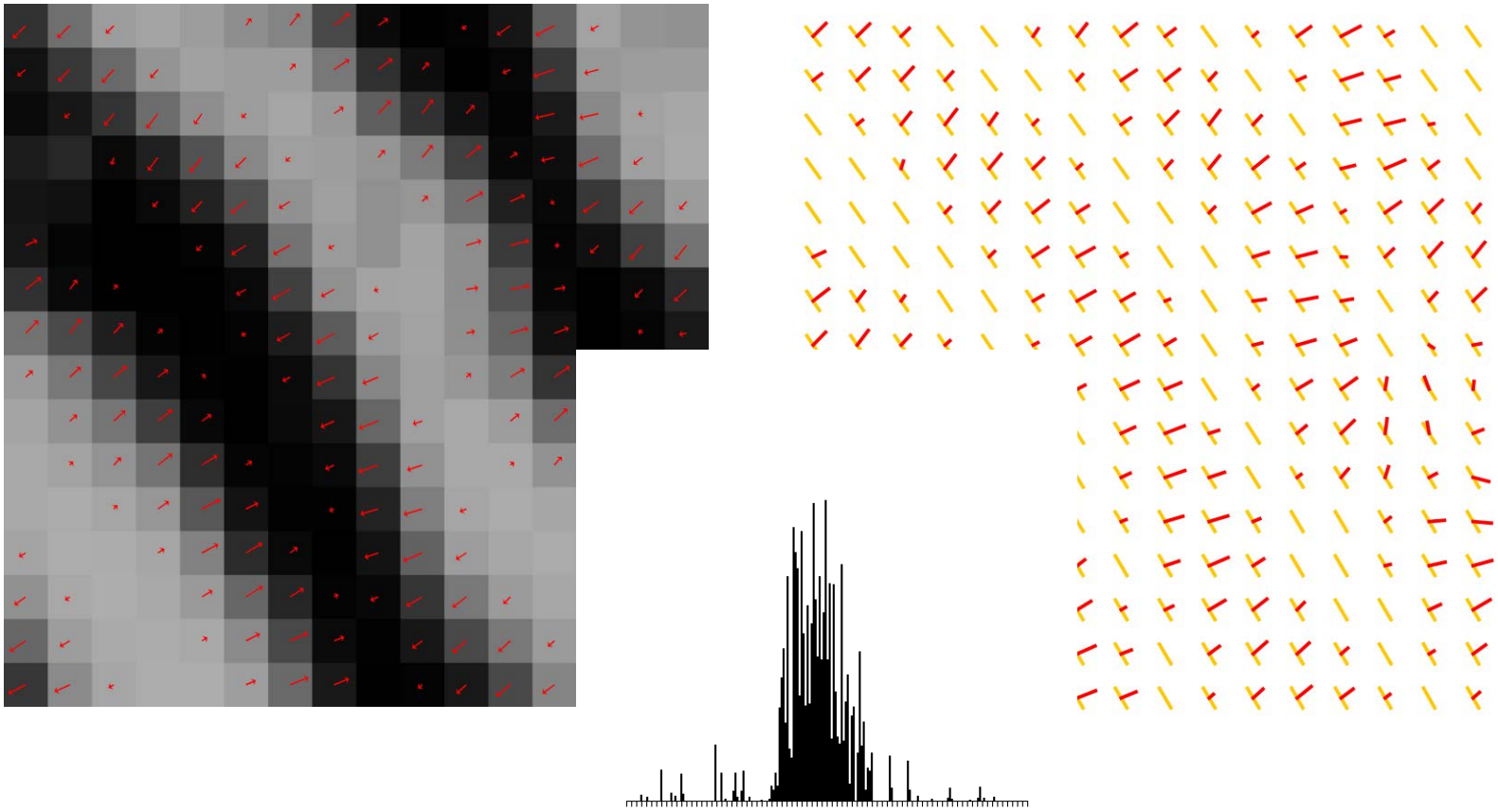
altered fingerprint

Poincare´ index response

[Ellingsg2014] J. Ellingsgaard, C. Sousedik, and C. Busch, “Detecting fingerprint alterations by orientation field and minutiae orientation analysis,” in Proc. IWBF, Valletta, Malta, (2014)

Altered Fingerprint Detection - Algorithms

- Feature: HIG
  - Histograms of invariant gradients [Gottschl2014]

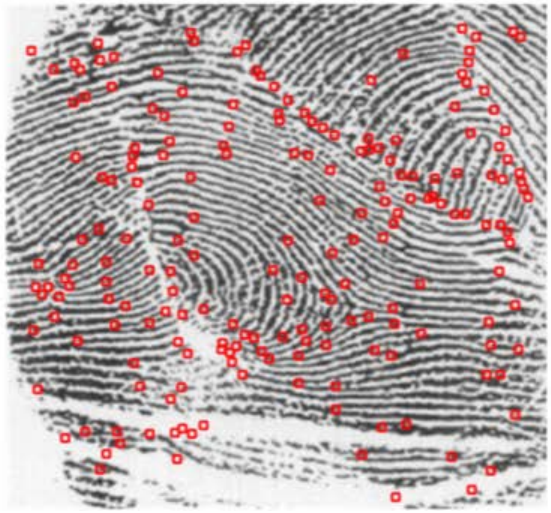


[Gottschl2014] C. Gottschlich, E. Marasco, A. Yang, and B. Cukic, “Fingerprint liveness detection based on histograms of invariant gradients,” in Proc. IJCB, Clearwater, USA, pp. 1–7. , (2014)

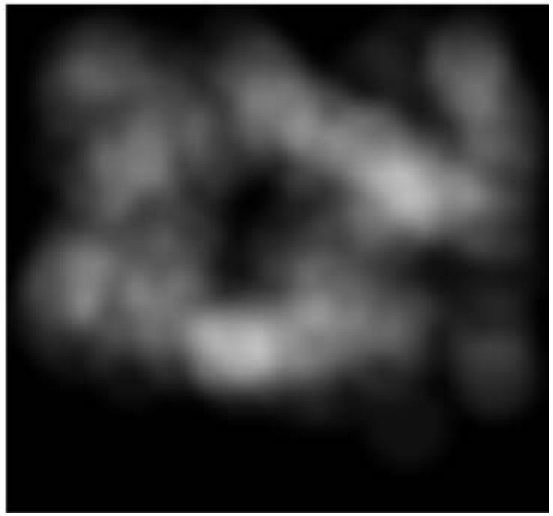
Altered Fingerprint Detection - Algorithms

- Feature: MDA
- Minutiae Distribution Analysis [YoonJain2012]

Altered fingerprint



minutia distribution



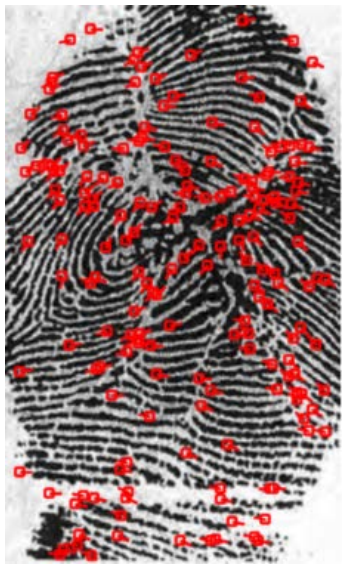
density map

[YoonJain2012] S. Yoon, J. Feng, and A. Jain, “Altered fingerprints: Analysis and detection,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 34, no. 3, Mar. 2012

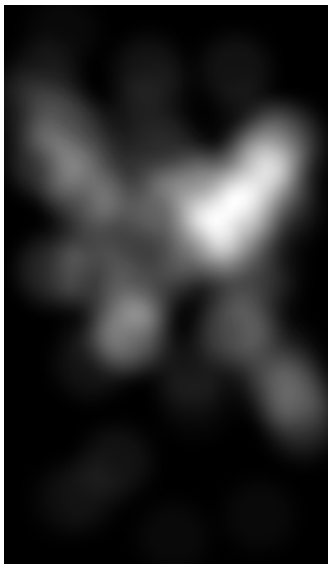
Altered Fingerprint Detection - Algorithms

- Feature: MOA
- Minutiae Orientation Analysis [Ellingsg2014]

Altered fingerprint



minutia distribution

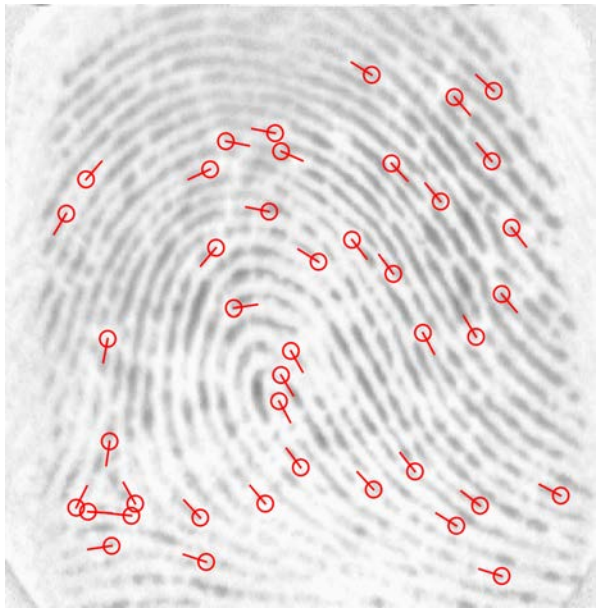


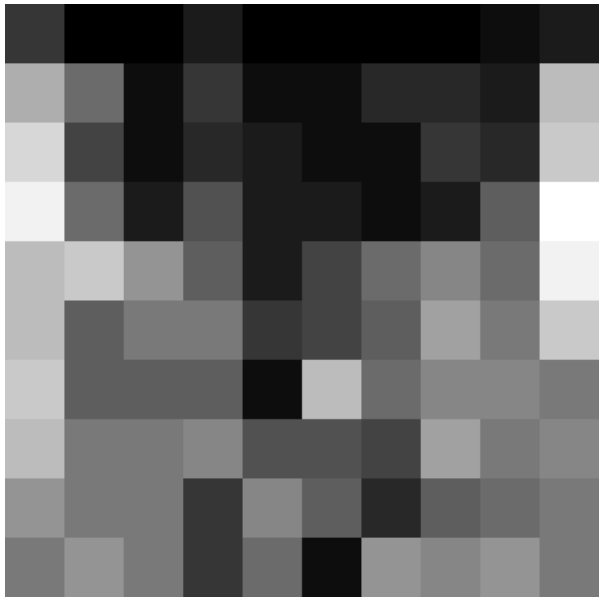
density map

[Ellingsg2014] J. Ellingsgaard, C. Sousedik, and C. Busch, “Detecting fingerprint alterations by orientation field and minutiae orientation analysis,” in Proc. IWBF, Valletta, Malta, (2014)

Altered Fingerprint Detection - Algorithms

- Feature: MH
- Minutiae Histograms by [GottHuck2014]
  - Distance bins are displayed from top to bottom, directional difference bins from left to right.
  - A high brightness value corresponds to a high number of occurrences in a bin.





[GottHuck2014] C. Gottschlich and S. Huckemann, “Separating the real from the synthetic: Minutiae histograms as fingerprints of fingerprints,” IET Biometrics, vol. 3, no. 4, (2014)

Altered Fingerprint Detection - Algorithms

- Feature: COH
  - Coherence Measure to what degree gradients share a similar orientation. [Gottschl2012]

normal/unaltered fingerprint

altered fingerprint

[Gottschl2012] C. Gottschlich and C.-B. Schönlieb, “Oriented diffusion filtering for enhancing low-quality fingerprint images,” IET Biometrics, vol. 1, no. 2, pp. 105–113, (2012)

Altered Fingerprint Detection - Testing

Database

- Dataset of Ellingsgaard et al. [Ellingsg2014]
  - Size: 116 altered fingerprints and 180 unaltered fingerprints
  - This data is not of sufficient size !

- Sources:
  - subset of GUC-100 (NTNU)
  - subset of Samischenko (Book)
  - subset of Brno (collection of fingerprints with dermatological diseases)
  - subset of NIST Special Database 14

[Ellingsg2014] J. Ellingsgaard, C. Sousedik, and C. Busch, “Detecting fingerprint alterations by orientation field and minutiae orientation analysis,” in Proc. IWBF, Valletta, Malta, (2014)

Altered Fingerprint Detection - Testing

Training and test protocol

- Cross-validation
  - Dataset randomly divided into training and test set 100 times
- Training set size:
  - 80 altered and 80 unaltered fingerprints
- Test set size:
  - 36 altered and 100 unaltered fingerprints

[Gottsch2015] C. Gottschlich, A. Mikaelyan, M. Olsen, J. Bigun, C. Busch: „Improving Fingerprint Alteration Detection", in 9th International Symposium on Image and Signal Processing and Analysis (ISPA 2015), Zagreb, (2015)

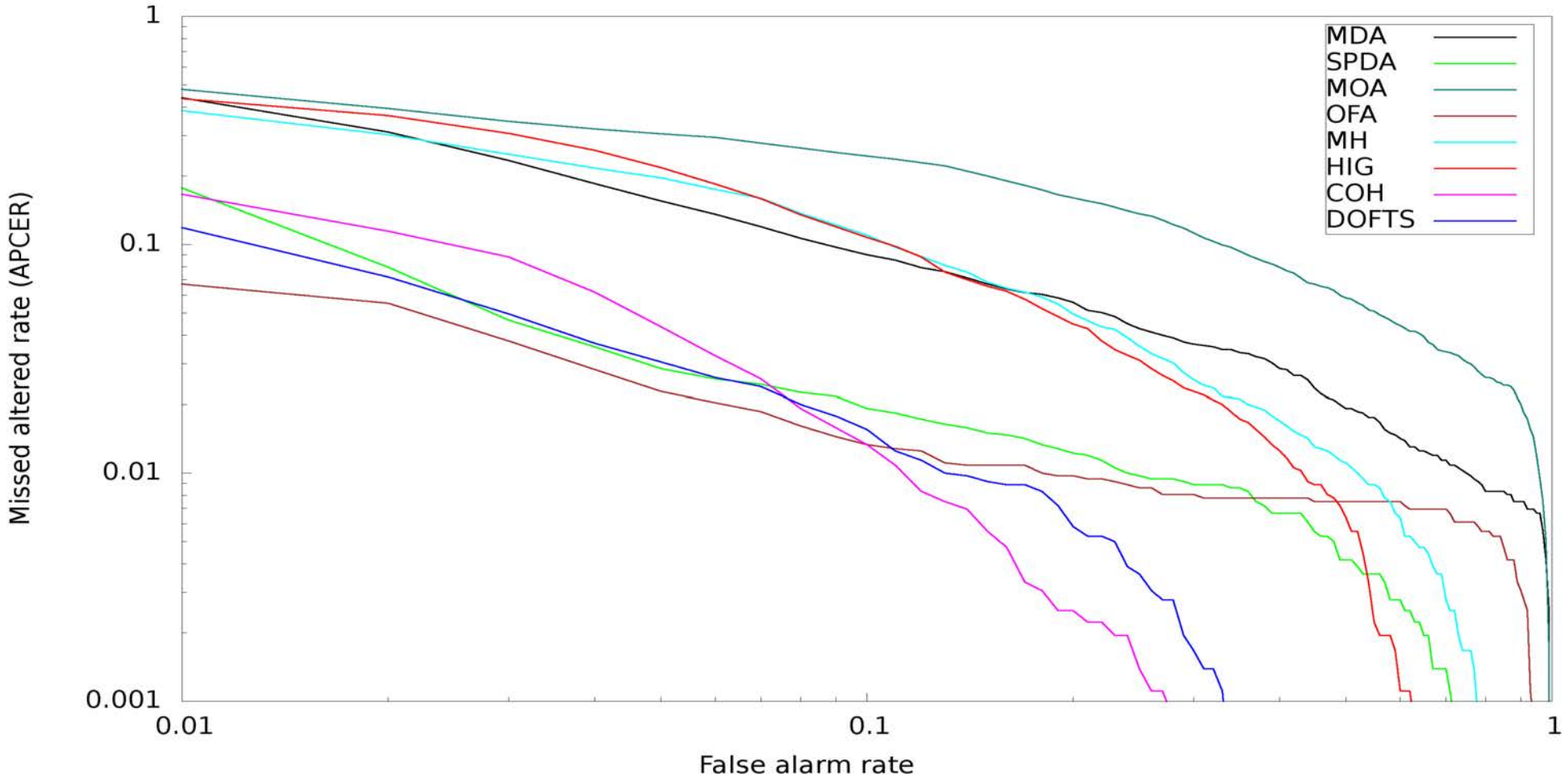
Altered Fingerprint Detection - Testing

Alteration Score

- Feature vector dimensions:
  - DOFTS = 189, COH = 189, HIG = 180, MH = 100
- Training sets and test set
  - Class labels:
    - 0 for normal, unaltered fingerprints
    - 1 for altered fingerprints
- Support Vector Machine
  - LIBSVM with linear kernel
  - Regression with values between 0 and 1 (alteration score)

Altered Fingerprint Detection - Testing

Results [Gottsch2015]



MDA = Minutia Distribution Analysis, SPDA = Singular Point Density Analysis, MOA = Minutia Orientation Analysis, OFA = Orientation Field Analysis, MH = Minutiae Histograms, HIG = Histograms of Invariant Gradients, COH = coherence, DOFTS = Differentials of Orientation Fields by Tensors in Scale,

Altered Fingerprint Detection - Testing

Conclusions

- We (biometrics community) need:
  - More research on fingerprint alteration
  - Larger databases
  - Publicly available datasets

- Aspects for future work:
  - Combination of multiple features
  - High speed and high accuracy (e.g. for border control)

Further Reading

References

- [ISO/IEC] ISO/IEC Standards http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=313770&published=on
- [YoonJain2012] S. Yoon, J. Feng, and A. Jain, “Altered fingerprints: Analysis and detection,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 34, no. 3, (2012)
- [MikBig2014] A. Mikaelyan and J. Bigun, “Symmetry assessment by finite expansion: application to forensic fingerprints,” in Proc. BIOSIG, Darmstadt, Germany, pp. 75–86. , (2014)
- [Ellingsg2014] J. Ellingsgaard, C. Sousedik, and C. Busch, “Detecting fingerprint alterations by orientation field and minutiae orientation analysis,” in Proc. IWBF, Valletta, Malta, (2014)
- [Gottsch2015] C. Gottschlich, A. Mikaelyan, M. Olsen, J. Bigun, C. Busch: „Improving Fingerprint Alteration Detection", in 9th International Symposium on Image and Signal Processing and Analysis (ISPA 2015), Zagreb, (2015)

Contact

Contact: