



# ANTI-SPOOFING EVALUATION OF DYNAMIC HANDWRITTEN SIGNATURE ALGORITHMS

R. Sanchez-Reillo, J. A. Amores-Duran, J.  
Liu-Jimenez, B. Fernandez-Saavedra  
University Group for Identification Technologies  
(GUTI)

Carlos III University of Madrid

<http://guti.uc3m.es>

[rsreillo@ing.uc3m.es](mailto:rsreillo@ing.uc3m.es)



# CONTENTS

- ◉ Handwritten Signature Toolbox
  - Features
  - Data Acquisition
  - Forgery Levels
- ◉ Algorithm to be Evaluated
- ◉ Results:
  - Forgery Level Impact
  - Forger Performance
  - Signature Robustness
- ◉ Addition of Anti-Spoofing Mechanisms
- ◉ Conclusions



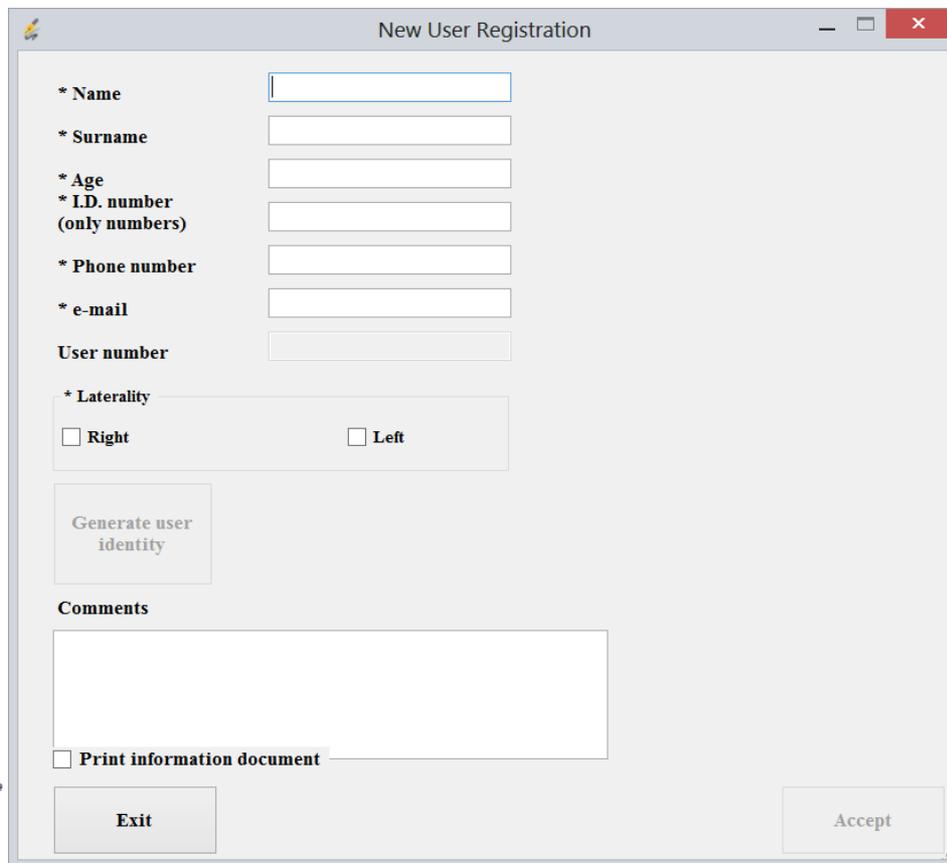
# HANDWRITTEN SIGNATURE TOOLBOX

- Genuine and Forgeries Acquisition Process
- 7 Levels of Knowledge when forging
  - Knowledge acquired controlled by the toolbox
- ISO/IEC 19794-7 2<sup>nd</sup> Generation for storing the samples acquired
- Files stored by:
  - Category (genuine/forgery)
  - User ID
  - Sample number
  - For forgeries, sample level
- Samples stored as individual files
- Availability expected by Q2-Q3 2013
  
- Requirements:
  - Microsoft Windows
  - Wacom STU-500 Tablet



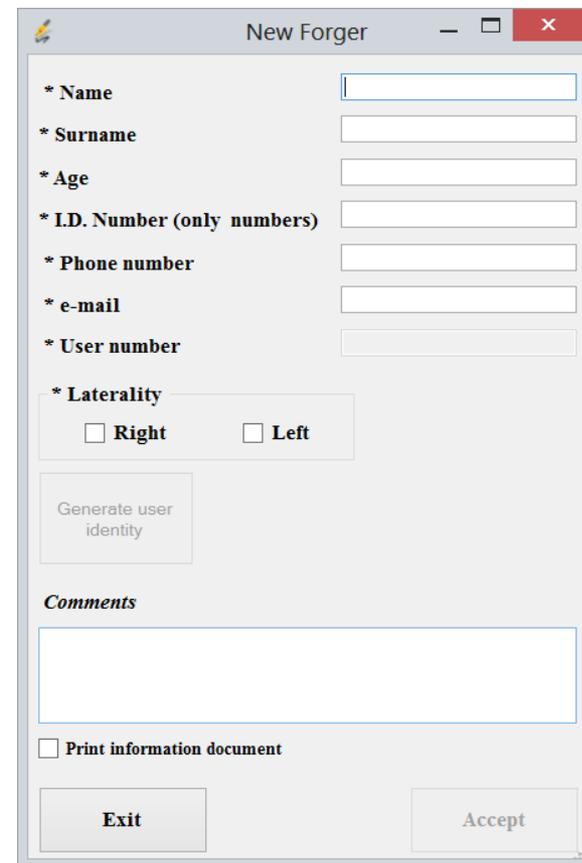
# GENUINE AND FORGER REGISTRATION

- ◉ Collects contacting information
- ◉ Allows Genuine, Forger or Both
- ◉ Personal data non attached to sample files



The 'New User Registration' window contains the following fields and controls:

- \* Name: Text input field
- \* Surname: Text input field
- \* Age: Text input field
- \* I.D. number (only numbers): Text input field
- \* Phone number: Text input field
- \* e-mail: Text input field
- User number: Text input field
- \* Laterality: Radio buttons for  Right and  Left
- Generate user identity: Button
- Comments: Text area
- Print information document: Check box
- Exit: Button
- Accept: Button



The 'New Forger' window contains the following fields and controls:

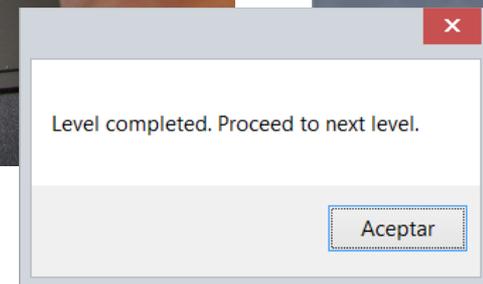
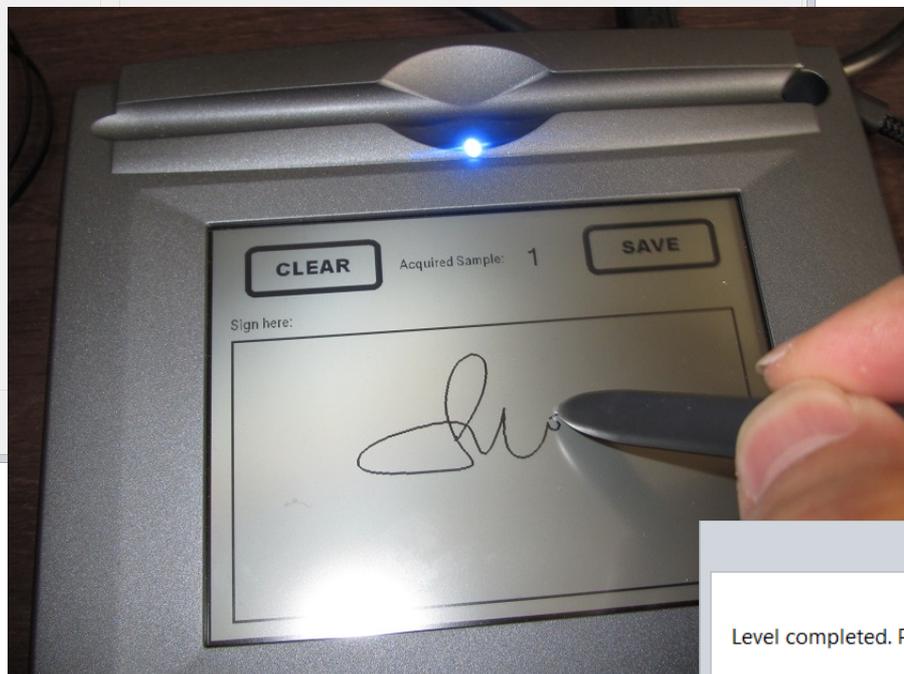
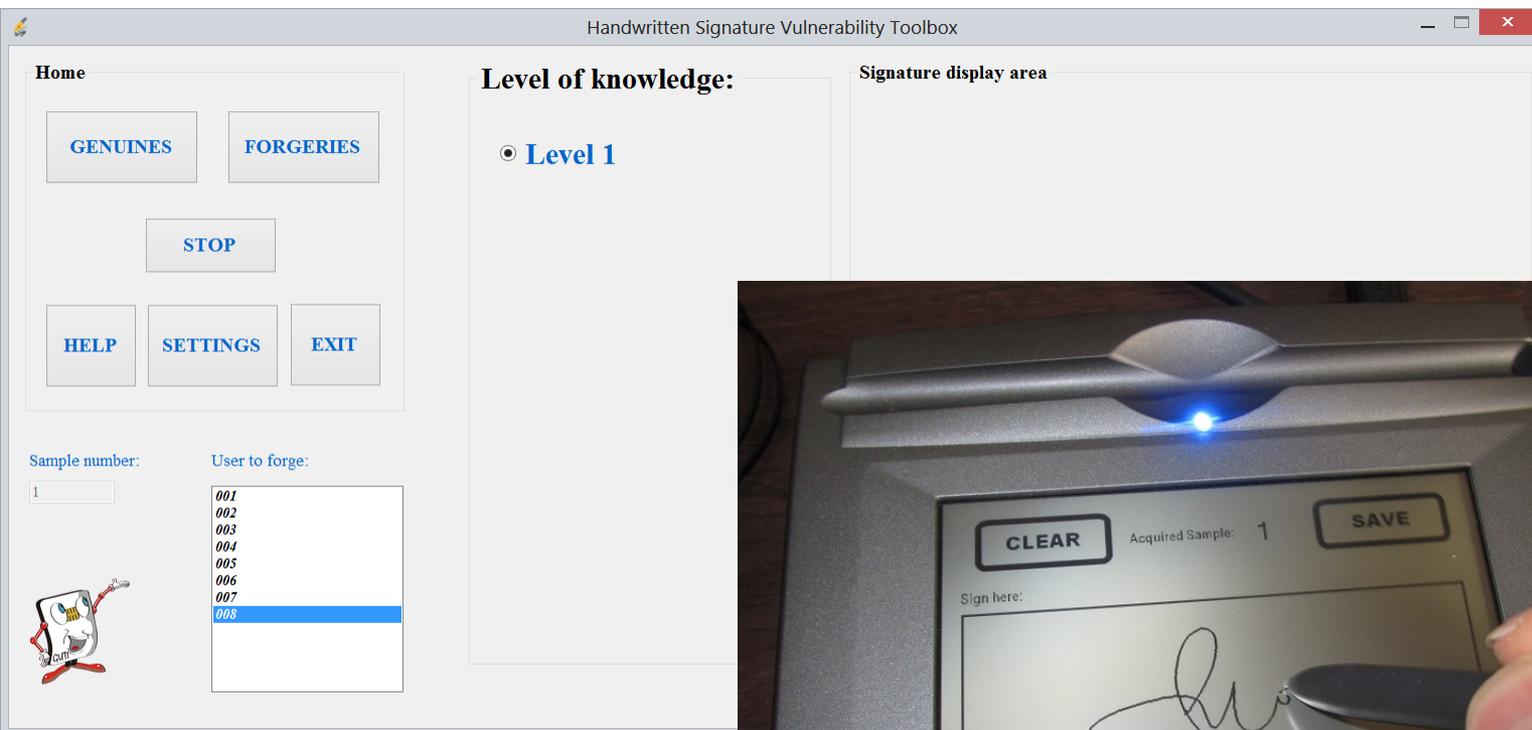
- \* Name: Text input field
- \* Surname: Text input field
- \* Age: Text input field
- \* I.D. Number (only numbers): Text input field
- \* Phone number: Text input field
- \* e-mail: Text input field
- \* User number: Text input field
- \* Laterality: Radio buttons for  Right and  Left
- Generate user identity: Button
- Comments: Text area
- Print information document: Check box
- Exit: Button
- Accept: Button



# FORGERIES: LEVEL 1

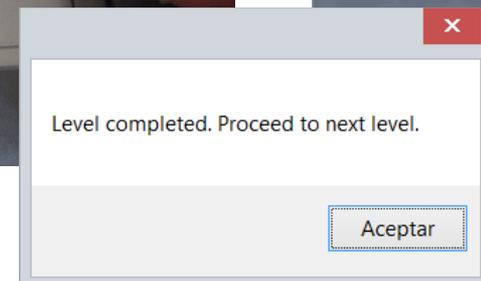
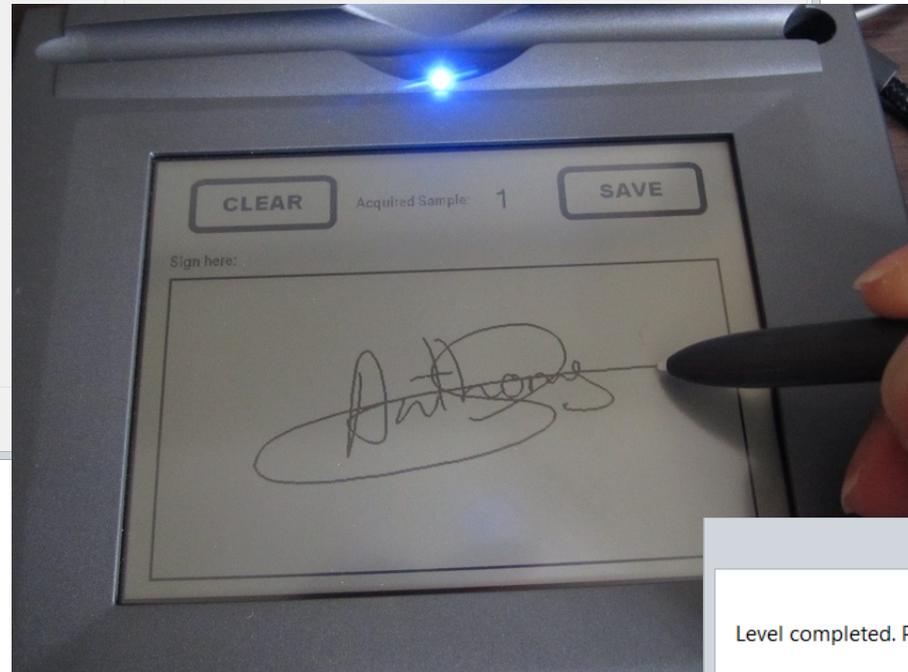
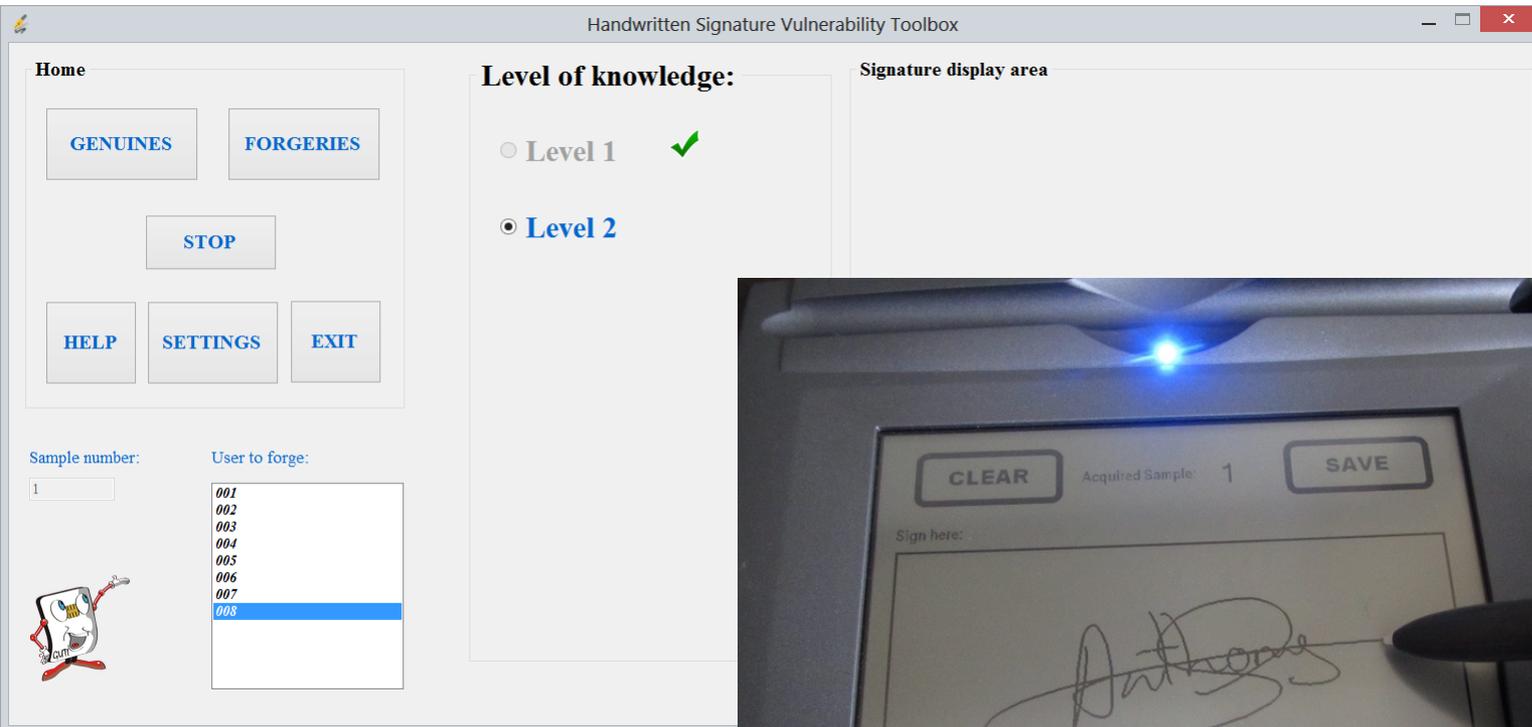


- ◉ No a-priory knowledge about the signature



# FORGERIES: LEVEL 2

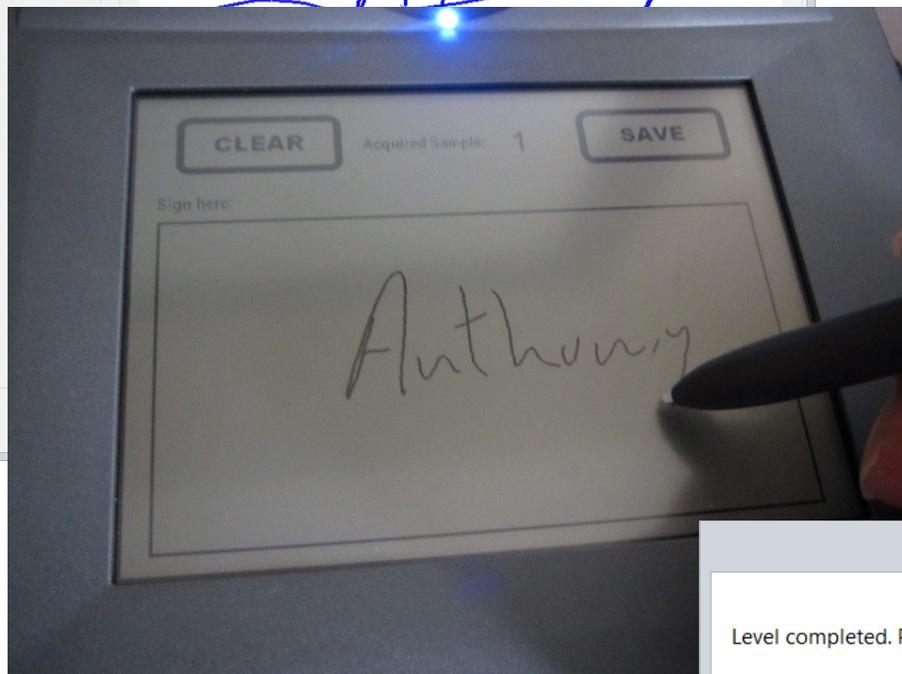
- ◉ Temporal knowledge about static signature (5s)



# FORGERIES: LEVEL 3



- ◉ Permanent knowledge about static signature



# FORGERIES: LEVEL 4



## ◉ "Carbon-copy"

The screenshot shows the 'Handwritten Signature Vulnerability Toolbox' application. The interface is divided into several sections:

- Home:** Contains buttons for 'GENUINES', 'FORGERIES', 'STOP', 'HELP', 'SETTINGS', and 'EXIT'.
- Level of knowledge:** A list of levels from 1 to 4. Levels 1, 2, and 3 are marked with green checkmarks, indicating they are completed. Level 4 is currently selected with a radio button.
- Signature display area:** A large empty space for displaying the signature.
- Sample number:** A text input field containing the number '1'.
- User to forge:** A list of user IDs from 001 to 008. User ID 008 is highlighted in blue.
- Cartoon character:** A small, smiling character with a camera lens for a head is located in the bottom left corner of the interface.



A small dialog box with a white background and a grey border. It contains the text 'Level completed. Proceed to next level.' and a button labeled 'Aceptar' at the bottom right.



# FORGERIES: LEVEL 5

- ◉ Temporal knowledge about dynamic signature (1 replay)

Handwritten Signature Vulnerability Toolbox

Home

GENUINES FORGERIES

STOP

HELP SETTINGS EXIT

Sample number: 1

User to forge:

- 001
- 002
- 003
- 004
- 005
- 006
- 007
- 008

Level of knowledge:

- Level 1 ✓
- Level 2 ✓
- Level 3 ✓
- Level 4 ✓
- Level 5

Signature display area

CLEAR Acquired Sample 1 SAVE

Sign here:

Level completed. Proceed to next level.

Aceptar

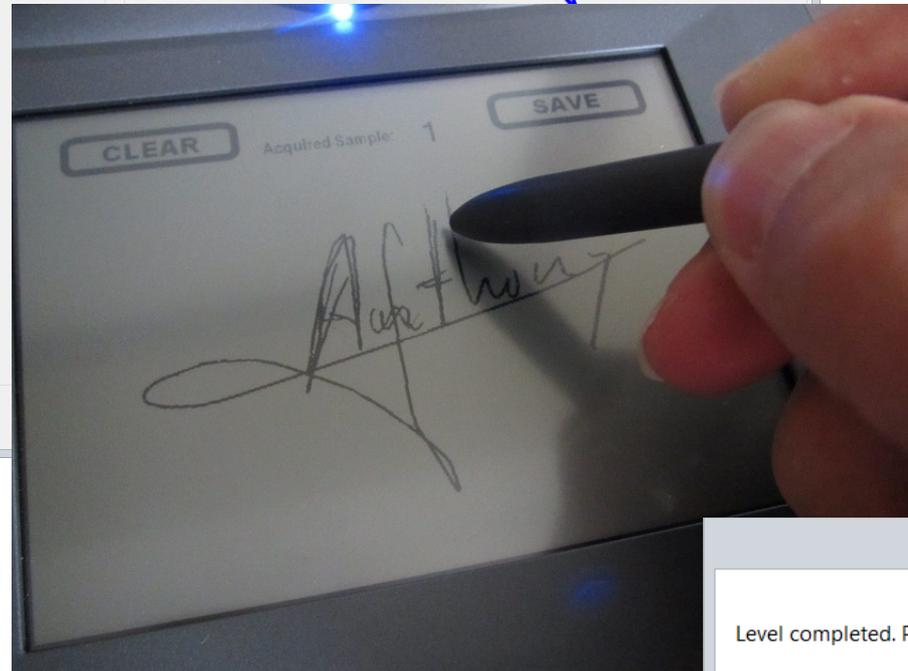
# FORGERIES: LEVEL 6

- Controlled knowledge about the dynamic signature

# FORGERIES: LEVEL 7

## ◉ Level 6 + Carbon-copy

The screenshot shows the 'Handwritten Signature Vulnerability Toolbox' window. On the left, a 'Home' panel contains buttons for 'GENUINES', 'FORGERIES', 'STOP', 'HELP', 'SETTINGS', and 'EXIT'. Below these are input fields for 'Sample number:' (containing '1') and 'User to forge:' (with a list of users: 001, 002, 003, 004, 005, 006, 007, 008, where 008 is selected). A cartoon character is visible at the bottom left. The main area is split into 'Level of knowledge:' and 'Signature display area'. The 'Level of knowledge:' section lists levels 1 through 7, with levels 1-5 and 7 marked with green checkmarks, and level 6 selected with a radio button. The 'Signature display area' shows a blue digital signature of 'A. Altho'.



A small dialog box with a white background and a grey border. It contains the text 'Level completed. Proceed to next level.' and a button labeled 'Aceptar'.



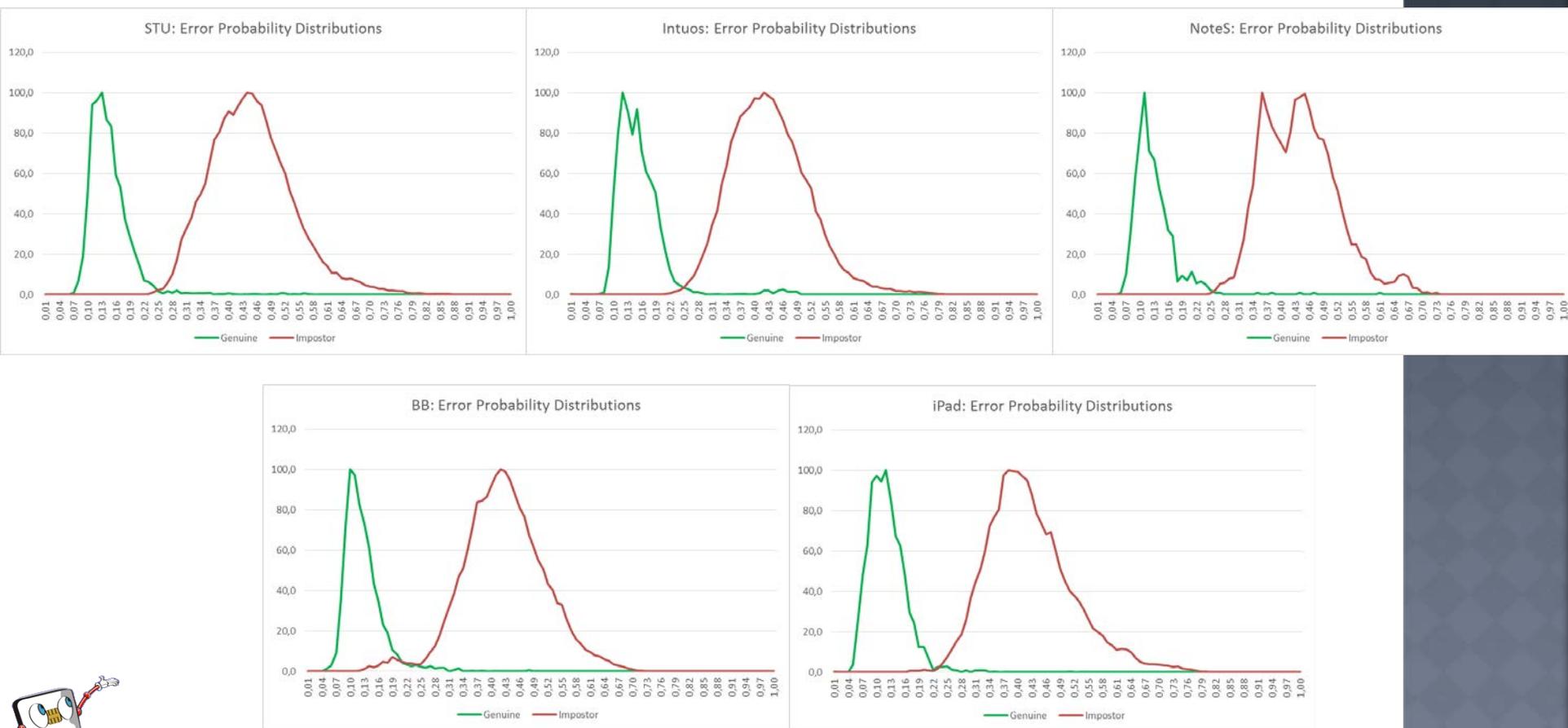
# BASELINE: GENUINE DATABASE

- ◉ Real Signatures
- ◉ Multi-device:
  - STU
  - Intuos
  - BlackBerry
  - iPad
  - Note (stylus)
- ◉ 49 people
- ◉ 60 signatures per device
- ◉ Biometric reference with the 3 first samples



# BASELINE: GENUINE DATABASE

- EERs: STU (1.4%), Intuos (2.3%), Note-S (0.6%), iPad (0.8%), BB (2.3%)



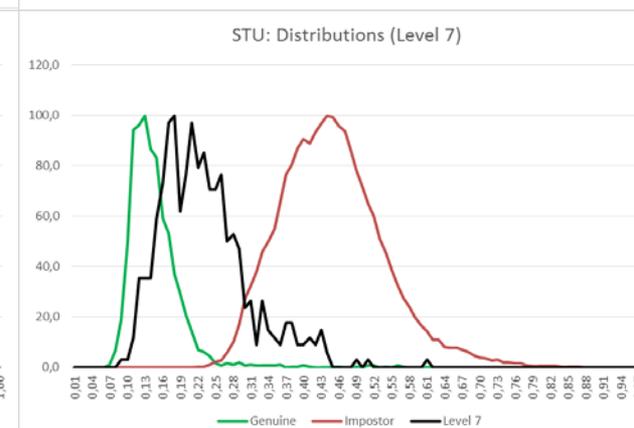
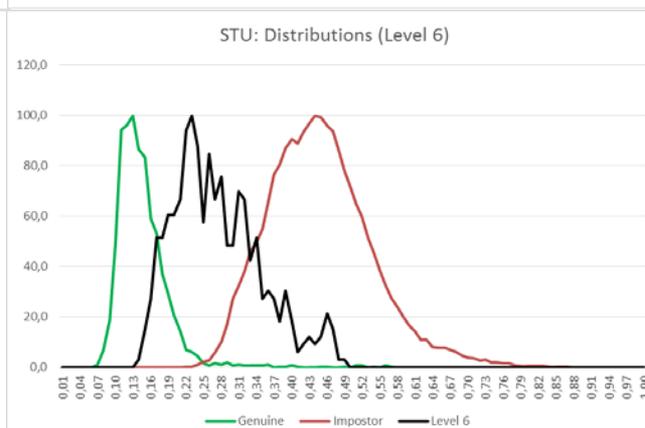
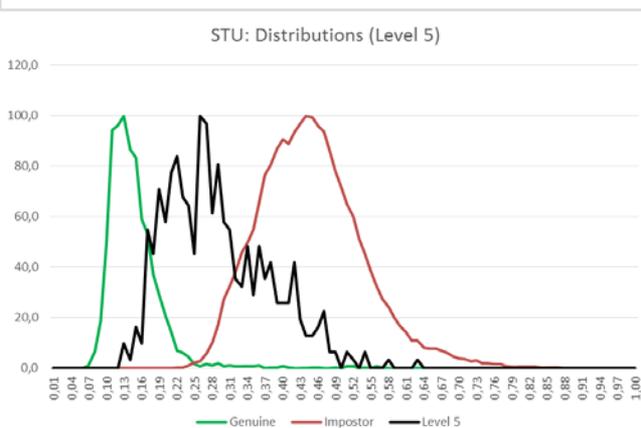
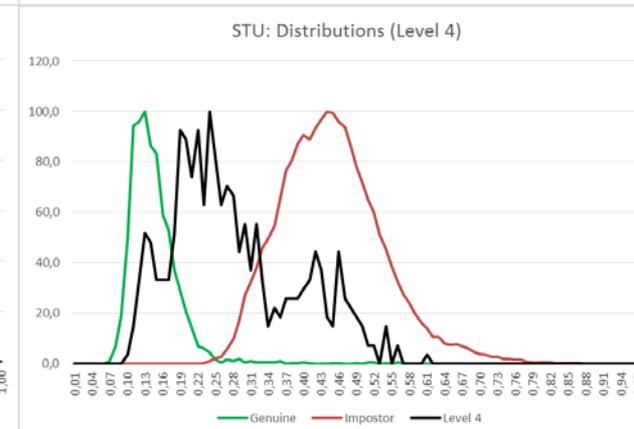
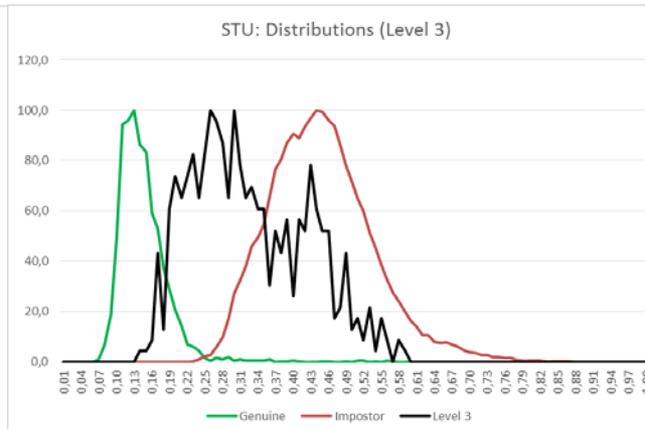
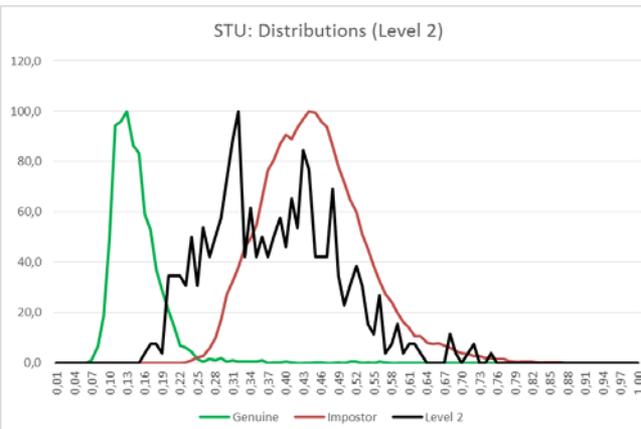
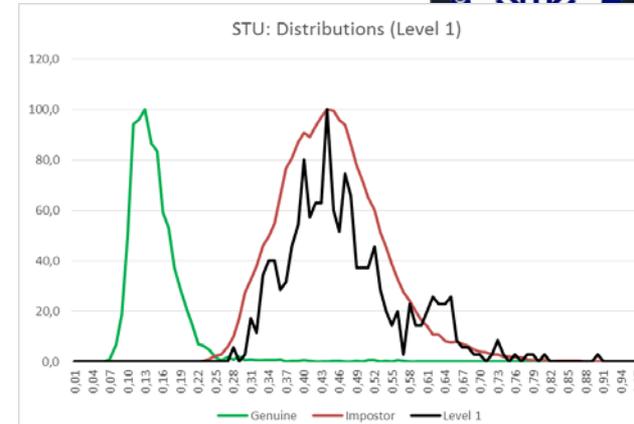
# FORGERY LEVEL IMPACT

- ◉ Forgers had to forge, at least, 10 unknown users
- ◉ For each level, the forger had to validate 5 forgeries.
  - For each forgery the forger is allowed to use as many attempts as possible
  - No feedback is provided to the forger about each of those attempts.
- ◉ Threshold at EER:
  - FPADER (False Presentation Attack Detection Error Rate) = % of forgeries considered as genuine



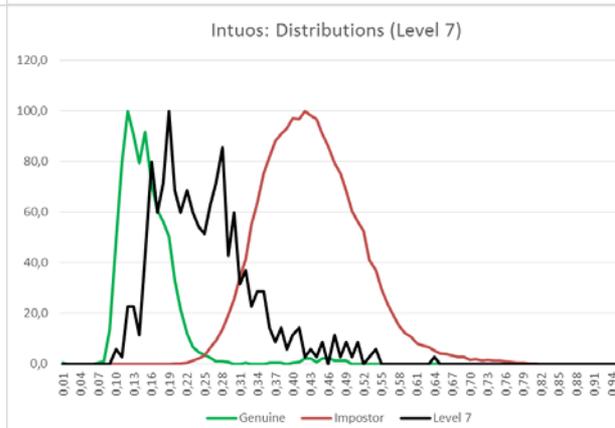
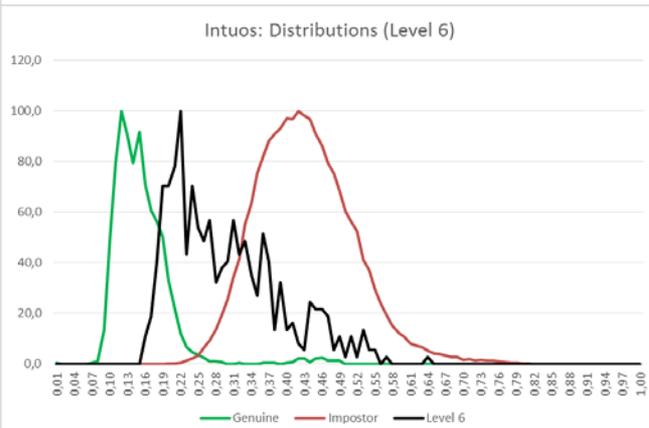
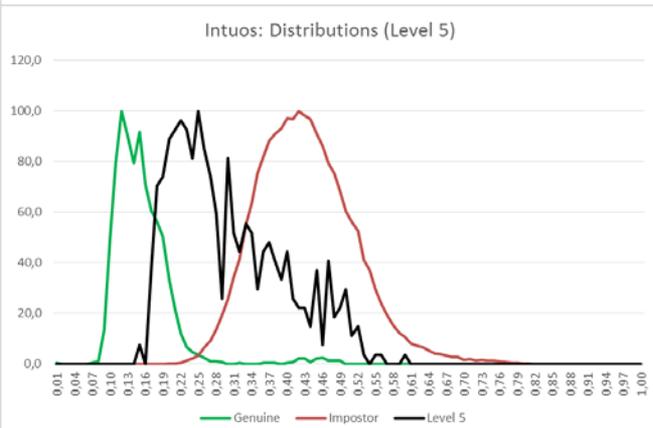
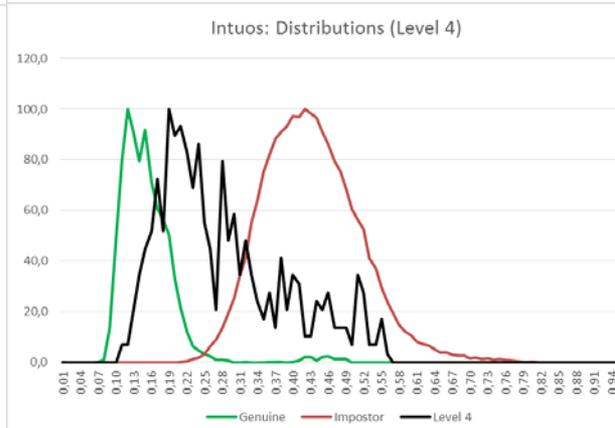
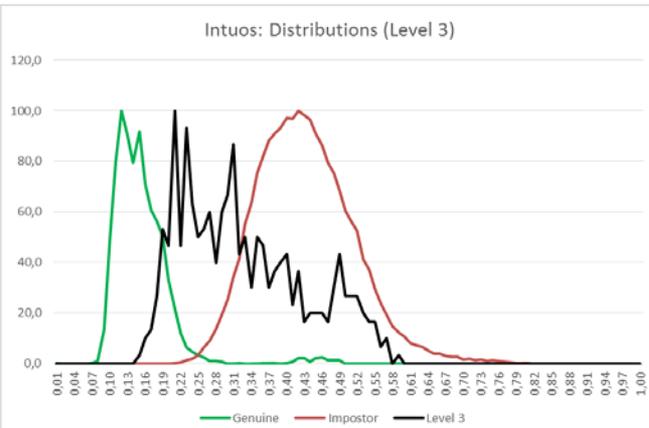
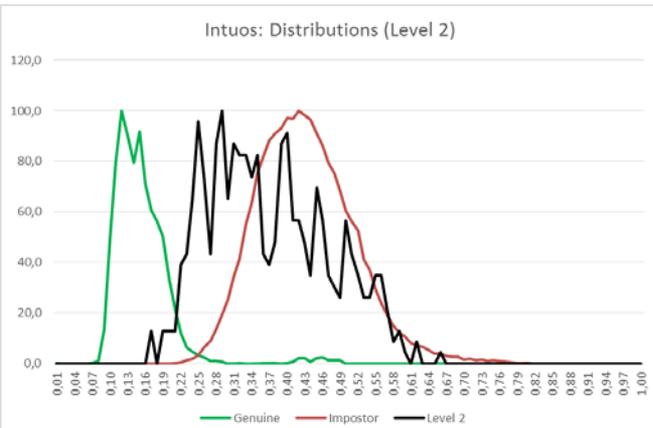
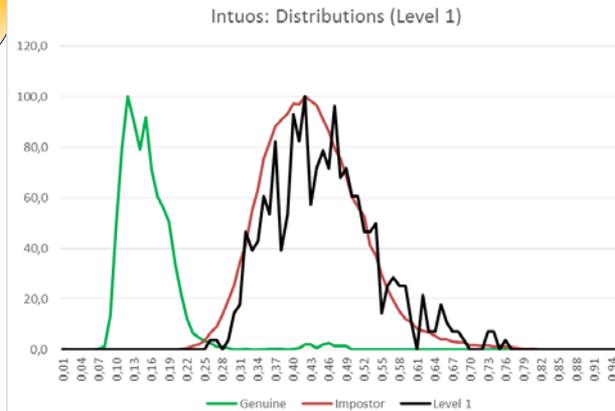
# FORGERY LEVELS (STU)

- L1 (0.4%), L2 (20.6%), L3 (40.8%), L4 (60.9%), L5 (55.1%), L6 (61.3%), L7 (81.3%)



# FORGERY LEVELS (INTUOS)

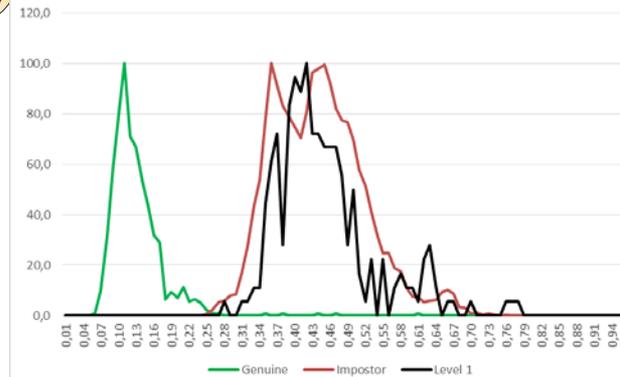
- L1 (0.4%), L2 (23.7%), L3 (40.7%), L4 (60.0%), L5 (53.5%), L6 (52.9%), L7 (72.2%)



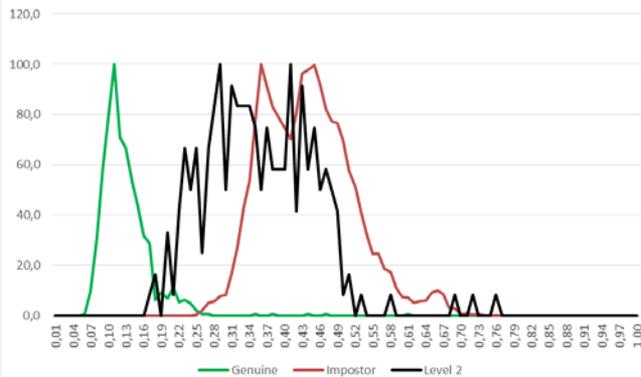
# FORGERY LEVELS (NOTE-S)

- ◉ L1 (0.0%), L2 (19.5%), L3 (42.8%), L4 (56.2%), L5 (56.2%), L6 (55.7%), L7 (78.4%)

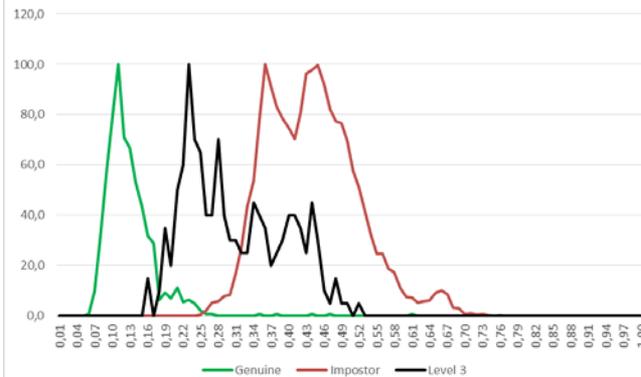
NoteS: Distributions (Level 1)



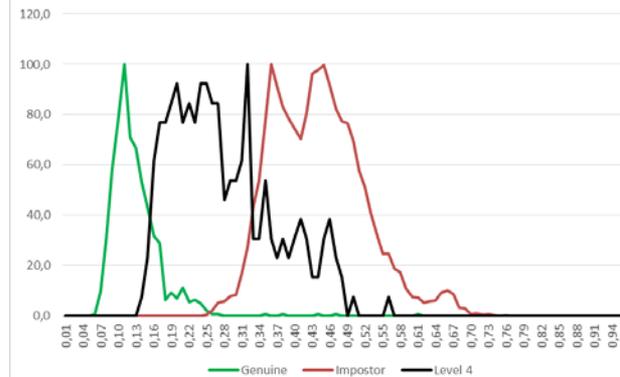
NoteS: Distributions (Level 2)



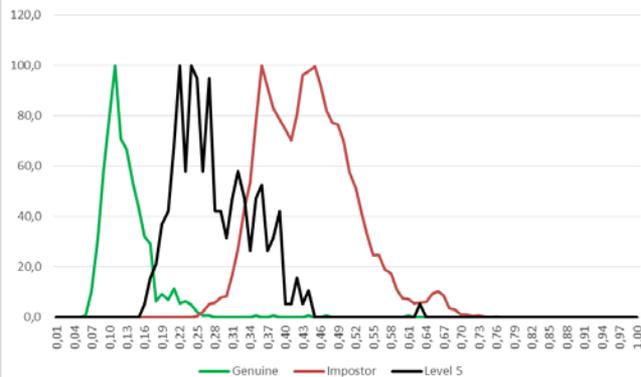
NoteS: Distributions (Level 3)



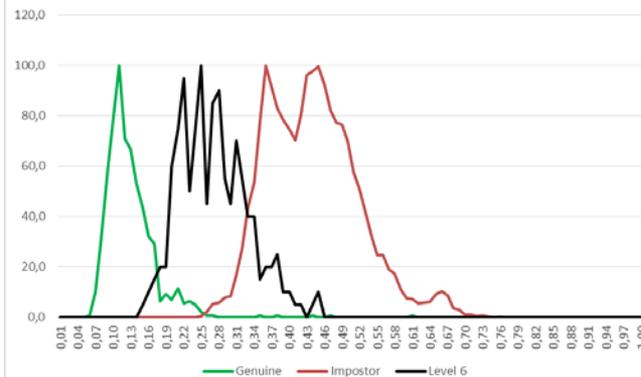
NoteS: Distributions (Level 4)



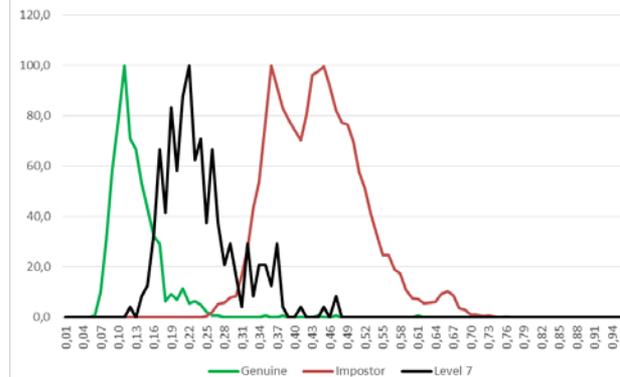
NoteS: Distributions (Level 5)



NoteS: Distributions (Level 6)

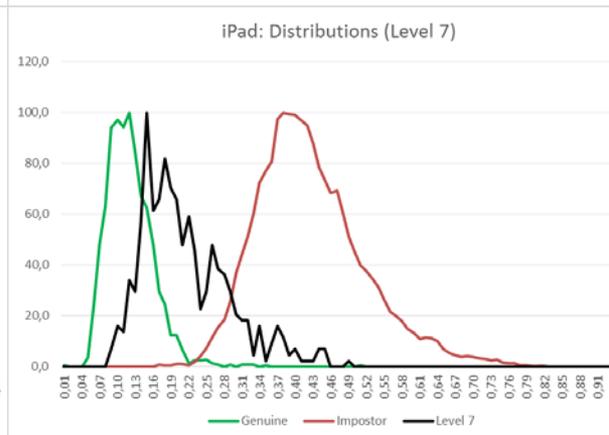
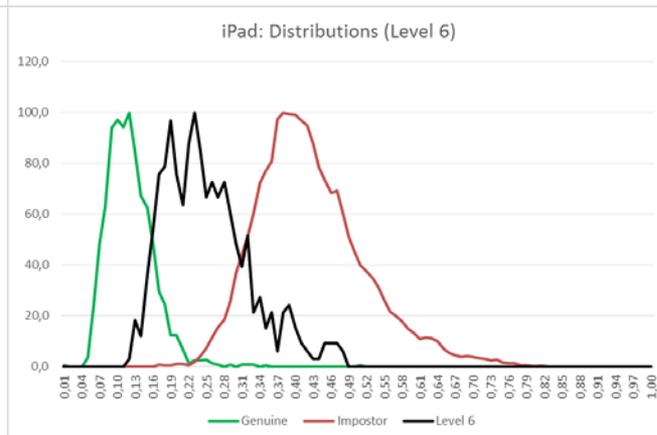
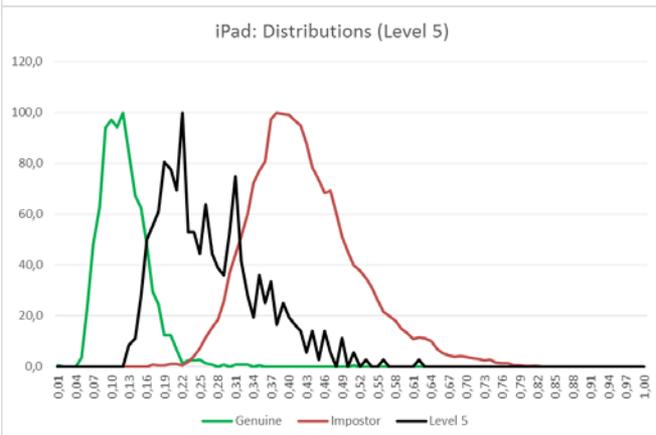
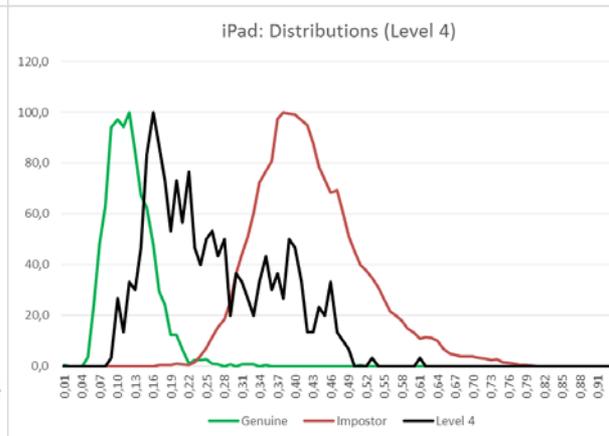
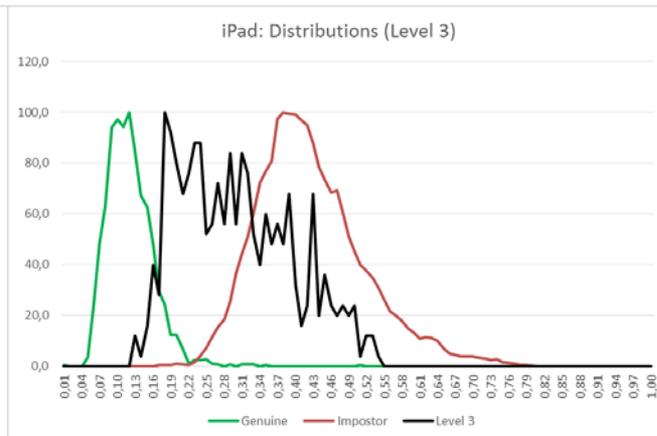
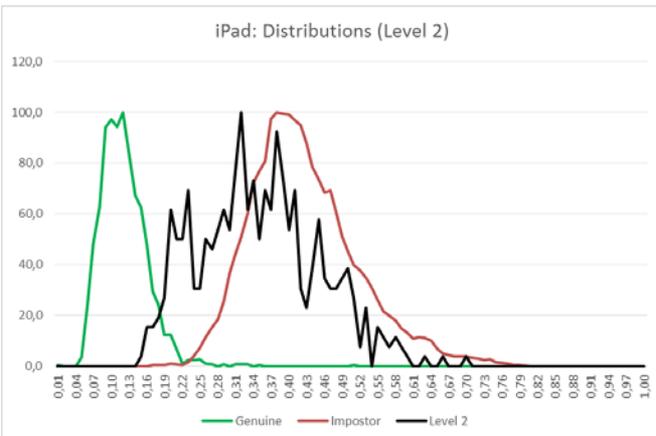
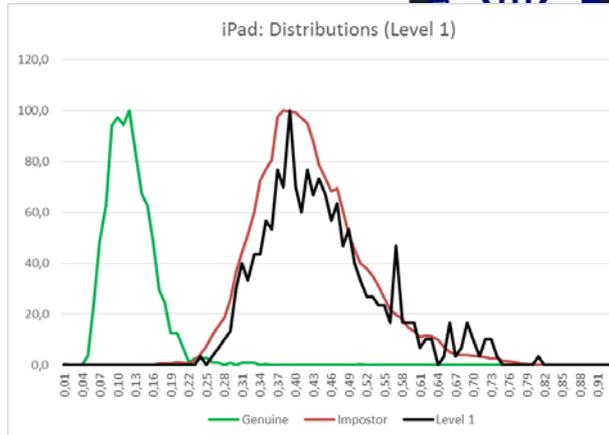


NoteS: Distributions (Level 7)



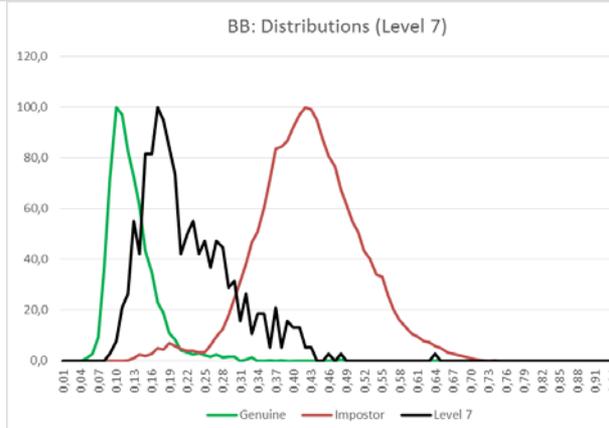
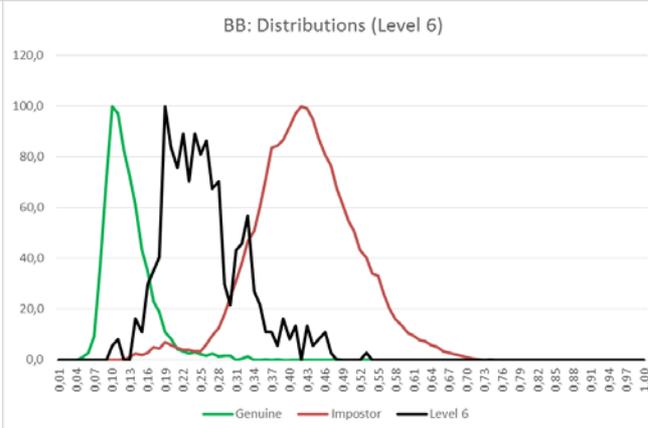
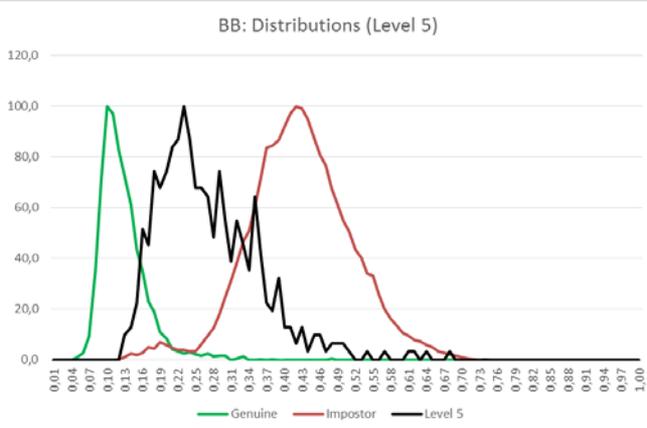
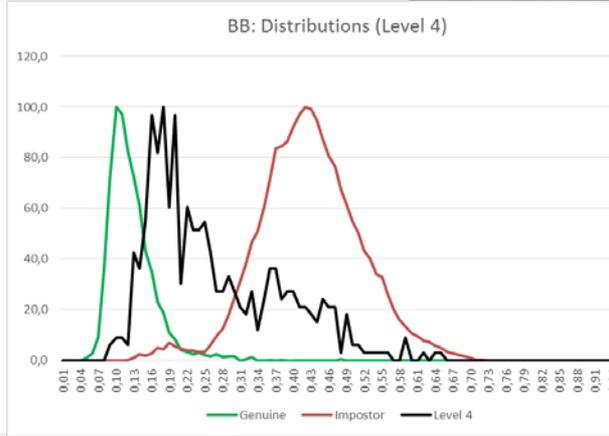
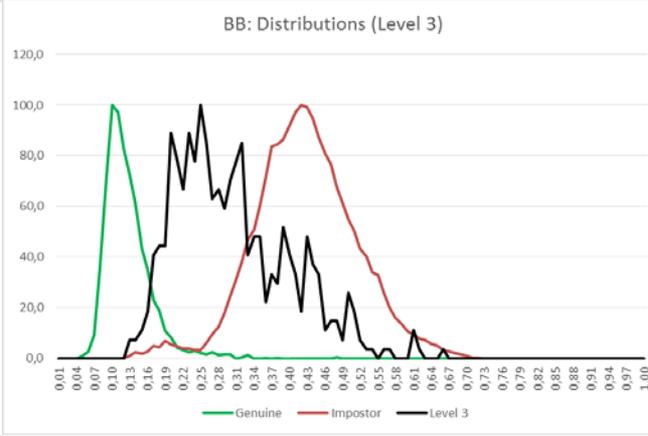
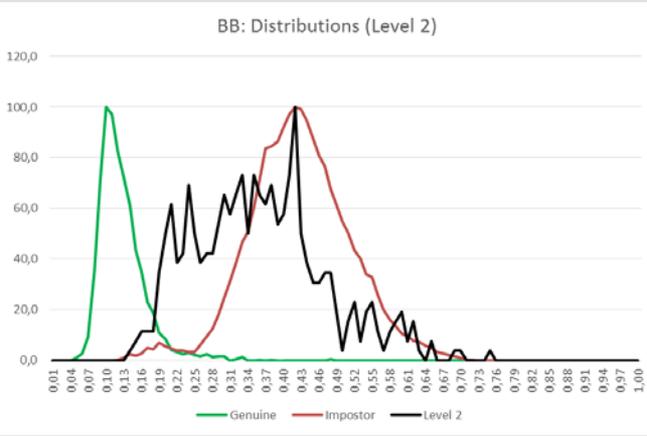
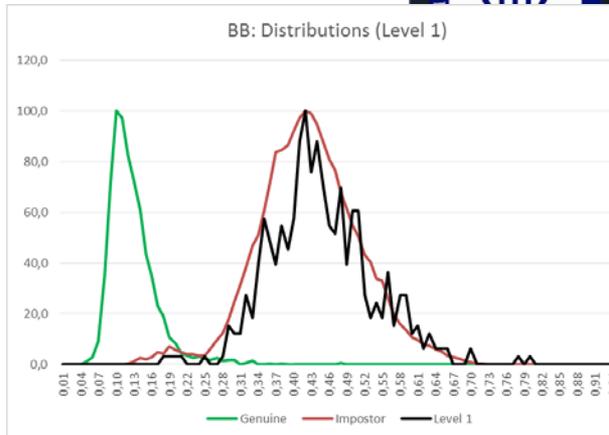
# FORGERY LEVELS (IPAD)

- L1 (0.2%), L2 (20.0%), L3 (38.4%), L4 (55.3%), L5 (51.4%), L6 (58.0%), L7 (72.7%)



# FORGERY LEVELS (BB)

- L1 (0.8%), L2 (14.6%), L3 (27.6%), L4 (50.5%), L5 (40.3%), L6 (43.0%), L7 (64.0%)



# FORGERY LEVEL IMPACT

- ◉ Behaviour is common to all devices:
  - Results seem to be dependent purely on the algorithm
  - Not dependency on whether the signature is done:
    - With a stylus or with the finger
    - In a professional Tablet, in a Smartphone or in a Tablet
- ◉ Major success in achieving forgeries when:
  - Having a static view of the signature
  - Using carbon copy
- ◉ Dynamic knowledge improves forgery
  - But not as much as expected
    - Is the algorithm really analysing the dynamics
  - But a non-professional forger obtain excellent results



# FORGER PERFORMANCE

## Level 3:

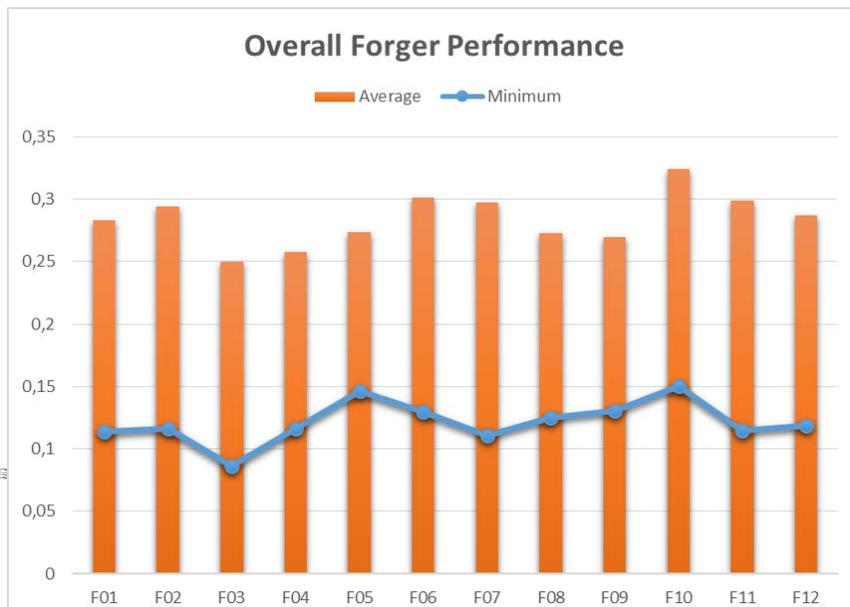
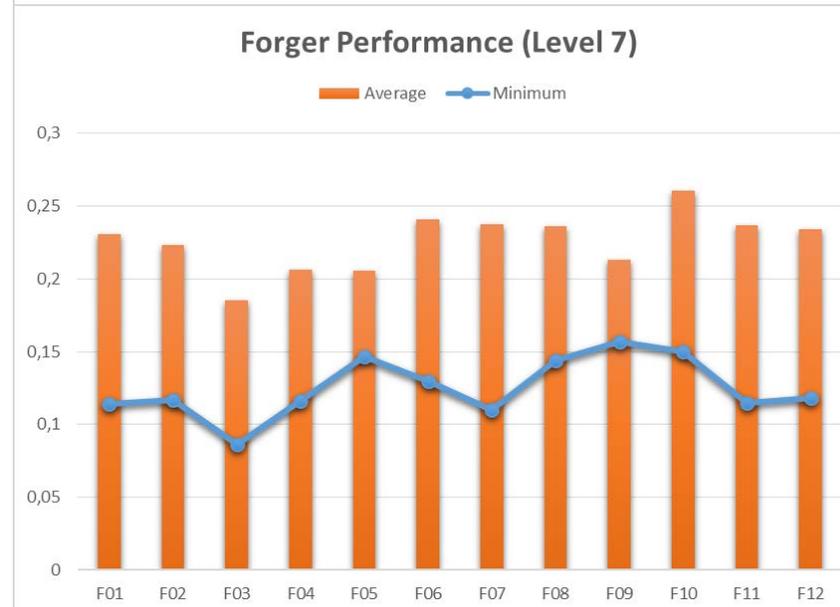
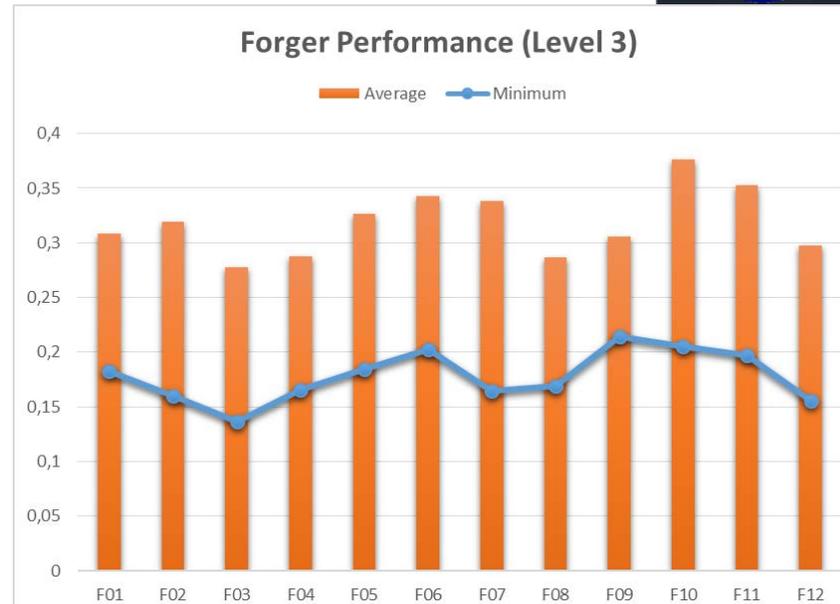
- Minimum: F03, F12, F02
- Average: F03, F08, F04

## Level 7:

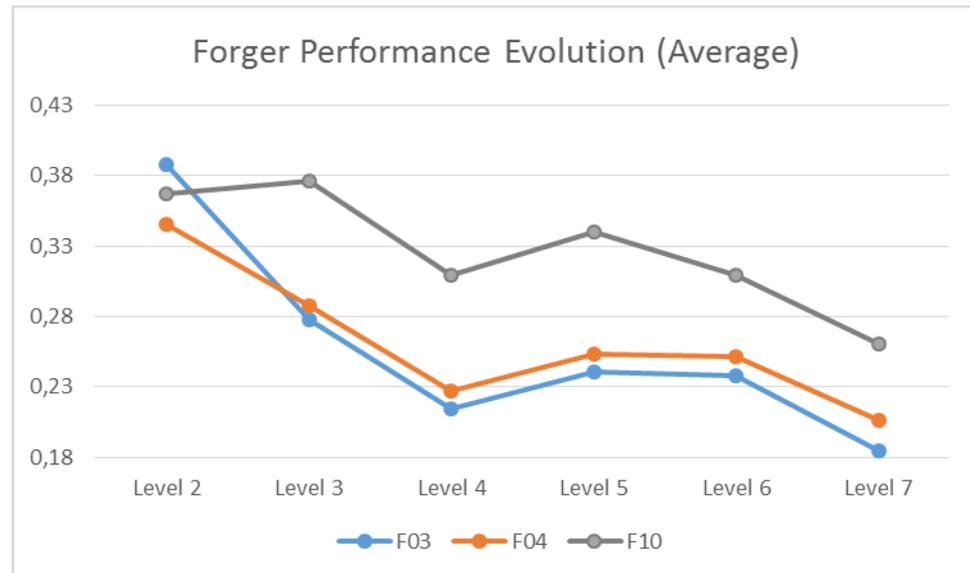
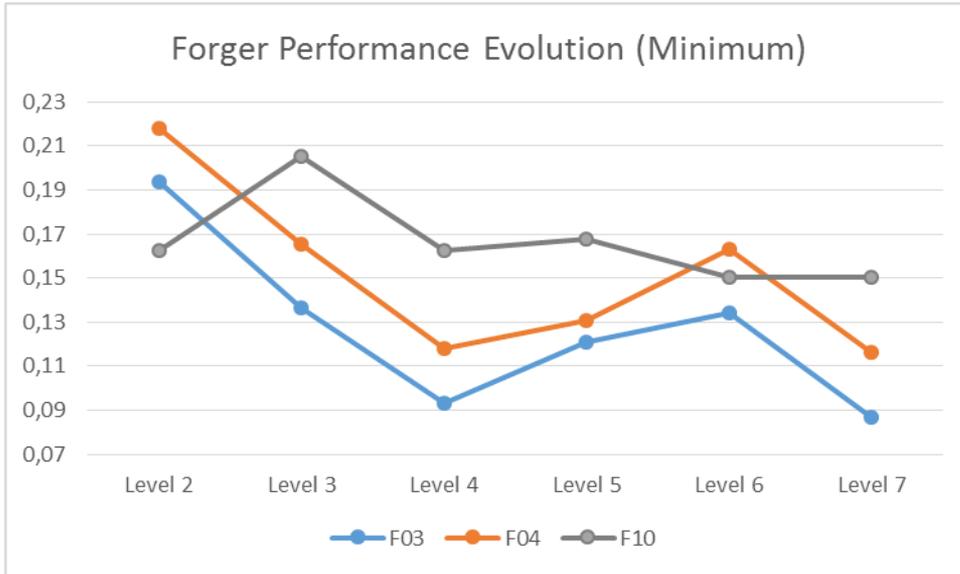
- Minimum: F03, F07, F01
- Average: F03, F05, F04

## Overall:

- Average: F03, F04, F09



# FORGER PERFORMANCE

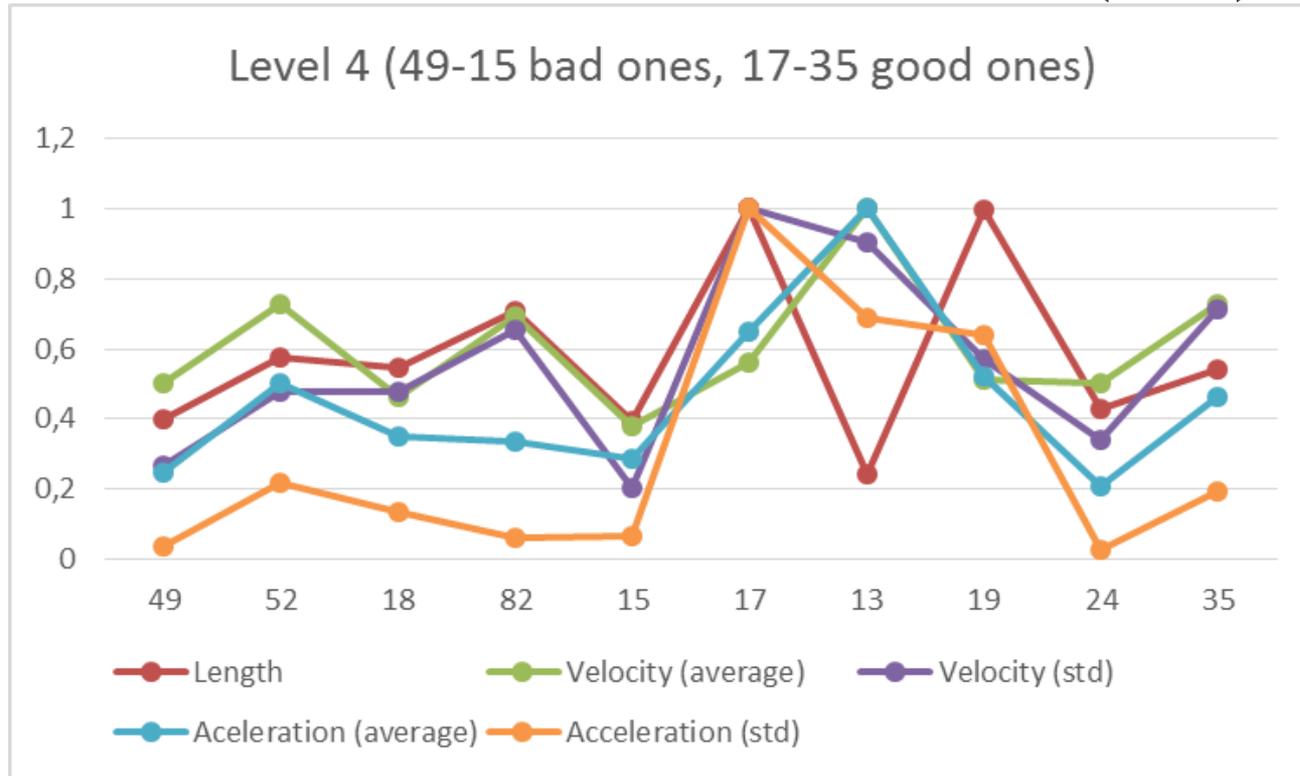


# SIGNATURE ROBUSTNESS

- ◉ With all this information, is it possible to conclude some tendency for the “robustness” (or quality) of the signatures?
- ◉ It has been taken the users within the 30 best and worst distances
  - Level 4 (only providing static information to the forger)
  - Level 7 (after providing dynamic information to the forger)
- ◉ Parameters analysed:
  - Length
  - Velocity (average and std)
  - Acceleration (average and std)



# SIGNATURE ROBUSTNESS (L4)

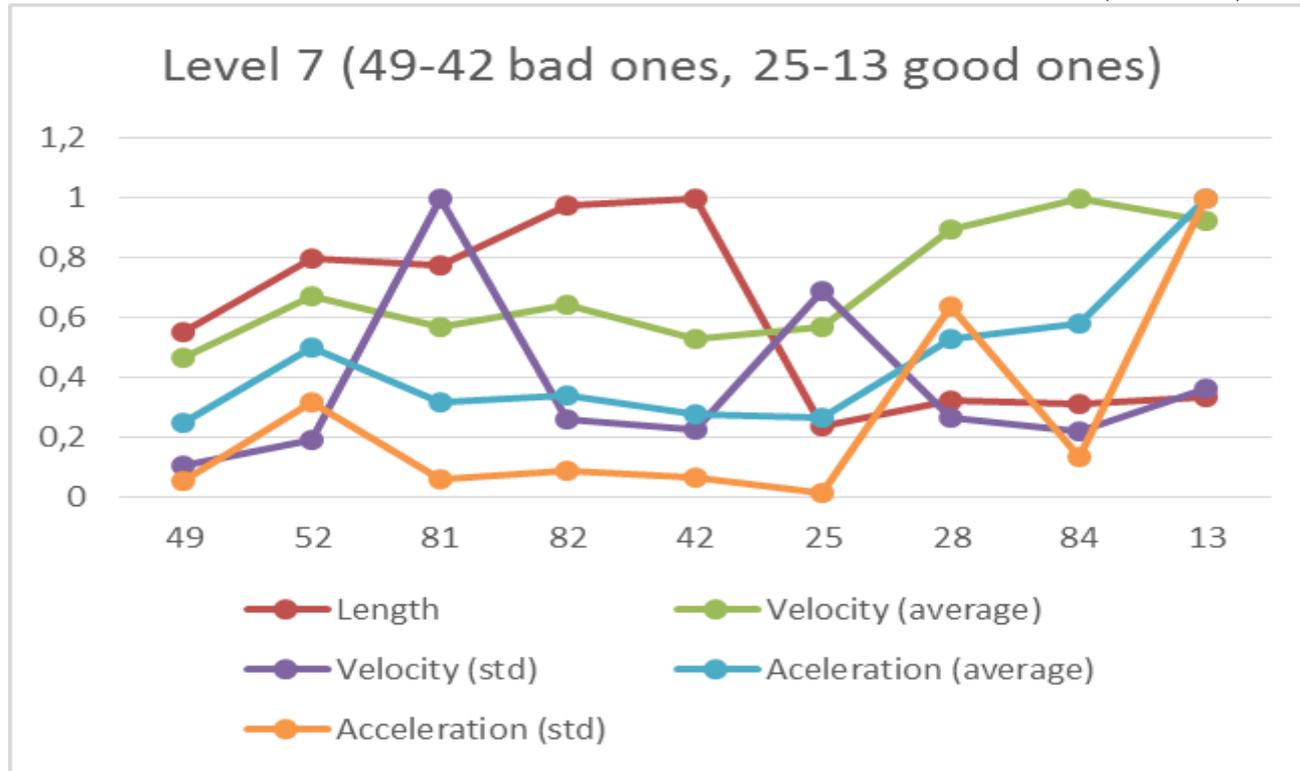


⦿ Not solid conclusion as good ones may have the same values as bad ones!

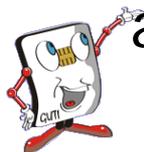
- Further analysis to be done



# SIGNATURE ROBUSTNESS (L7)



- Tendency for improvement with shorter signatures (??)
- Slight improvement with average acceleration
- Questionable tendency when increasing acceleration std



# SIGNATURE ROBUSTNESS

- ◉ Not having objective metrics working, how about analysing the signatures subjectively?
- ◉ Level 4 (only static information):
  - The worst ones seem to have:
    - ◉ Easy to understand drawing (e.g. names clearly written)
    - ◉ Conventional writing flow
    - ◉ Conventional aspect ratio as of regular writing
  - The best ones are:
    - ◉ Complex in strokes and superposition of strokes
    - ◉ Not understandable (i.e. only abstract strokes)
    - ◉ Not conventional writing flow
- ◉ Level 7 (dynamics added):
  - The worst ones present the same characteristics of those at Level 4, but now without the “protection” of non-conventional writing flow
  - The best ones are:
    - ◉ Not showing understandable letters
    - ◉ Variable and non conventional proportions
    - ◉ Some of them even look very simple in drawing

Are these results dependent on the forger and/or algorithm?



# ANTI-SPOOFING INFLUENCE

- ◉ Just with the results on the different levels (just the graphics and numbers, not the forgeries), the manufacturer provided a new version of the algorithm with some anti-spoofing mechanisms implemented.
- ◉ If the signature was detected as a potential forgery, the system responded with an “artificial score” of 1 (i.e. maximum distance)
  - Request made by the laboratory
- ◉ The evaluation was carried out with the same databases:
  - Genuines / Impostors
  - Forgeries (i.e. attacks)



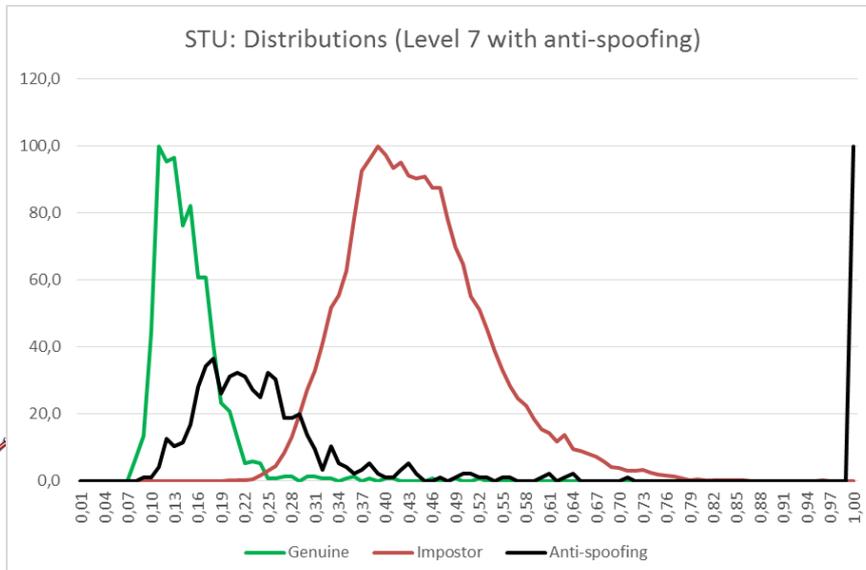
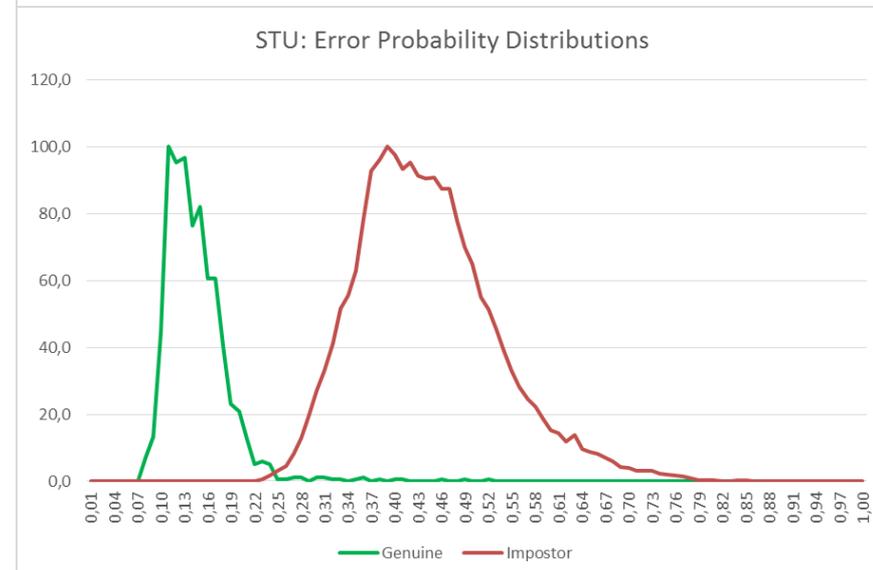
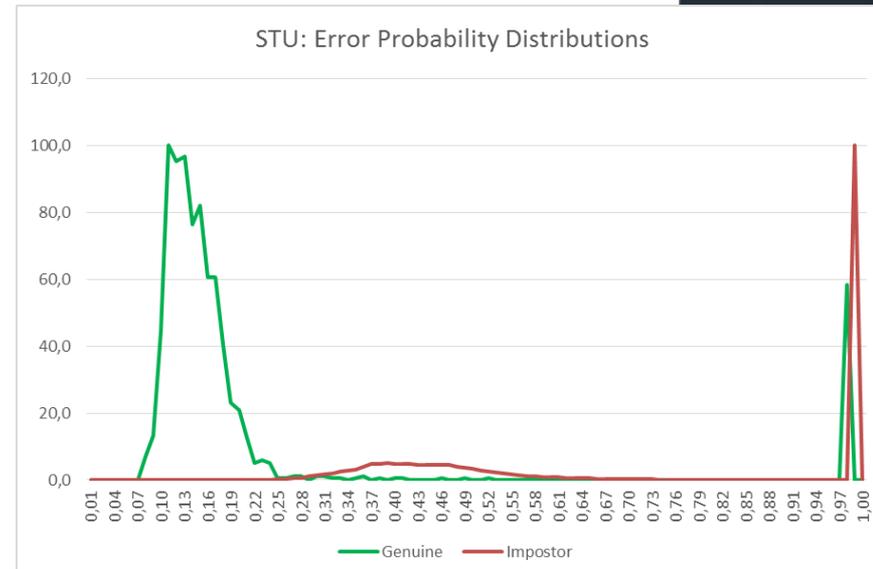
# ANTI-SPOOFING INFLUENCE

## Changes in Algorithm Performance:

- 7.1% of False PAD
- 48.8% of True Zero-Effort PAD
- EER with PAD rejections increased to 7.8%
- EER without PAD rejections (e.g. taken as FTA) = 1.2% (<1.4%)

## Real forgeries detection:

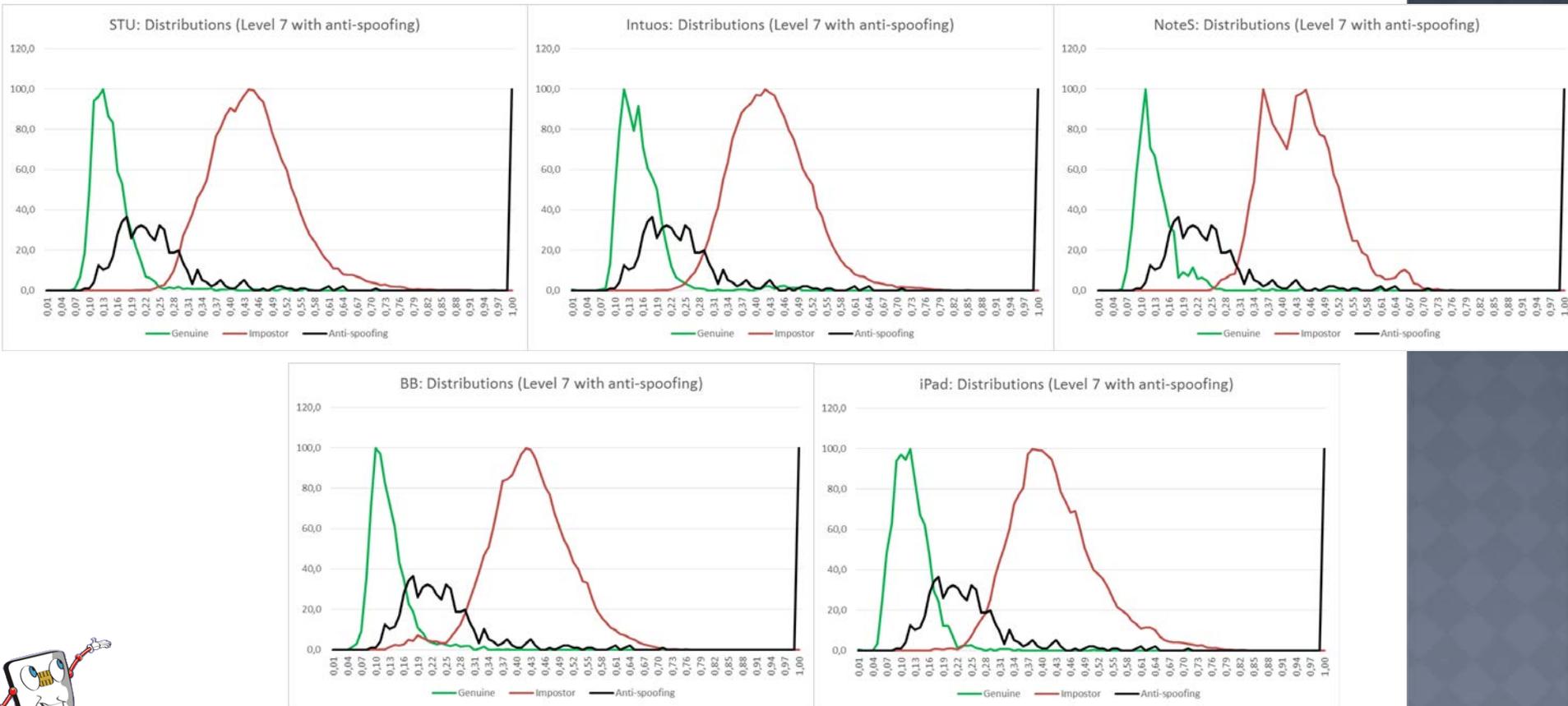
- 15.7% True PAD



# ANTI-SPOOFING INFLUENCE

## FPADER:

- STU (67.3%) Intuos (67.3%), Note-S (64.4%), iPad (56.7%), BB (47.7%)



# CONCLUSIONS

- ◉ A tool to evaluate forgeries in handwritten signature has been created
  - Exploiting the different knowledge of the forger
- ◉ For the algorithm evaluated:
  - Behaviour is independent of the capture device
  - Major success in achieving forgeries with carbon-copy (is it really a threat?) and with the single static information
  - Dynamic knowledge improves forgery, but not as much as expected
    - Some signatures get benefit of this being protected by non-conventional writing
- ◉ Robustness of the signature seems to increase with the lack of use of recognizable letters and non-conventional aspect ratio
- ◉ Anti-spoofing mechanisms, impact seriously on the behaviour of the algorithm
  - At least it increases the FTA (or equivalent rate)
  - They reduce FPADER, but its impact may be questionable
- ◉ The work done is dependent on the algorithm tested and the forgers used
  - Future work in analysing that dependency



# THANKS! QUESTIONS?



THIS WORK HAS BEEN SUPPORTED BY THE  
SPANISH MINISTRY OF ECONOMY AND  
COMPETITIVENESS BY THE PROJECT TEC2012-  
38329: “URBE-UNIVERSAL ACCESS THROUGH  
BIOMETRICS IN MOBILE SCENARIOS”

R. Sanchez-Reillo, J. A. Amores-Duran, J. Liu-  
Jimenez, B. Fernandez-Saavedra  
University Group for Identification Technologies  
(GUTI)

Carlos III University of Madrid

<http://guti.uc3m.es>  
[rsreillo@ing.uc3m.es](mailto:rsreillo@ing.uc3m.es)

