Biometric Presentation Attack Detection

Spoofing and Anti-Spoofing

Sébastien Marcel and presented by Vedrana Krivokuca
Biometrics Security and Privacy group
Idiap research institute
Switzerland
www.idiap.ch/~marcel

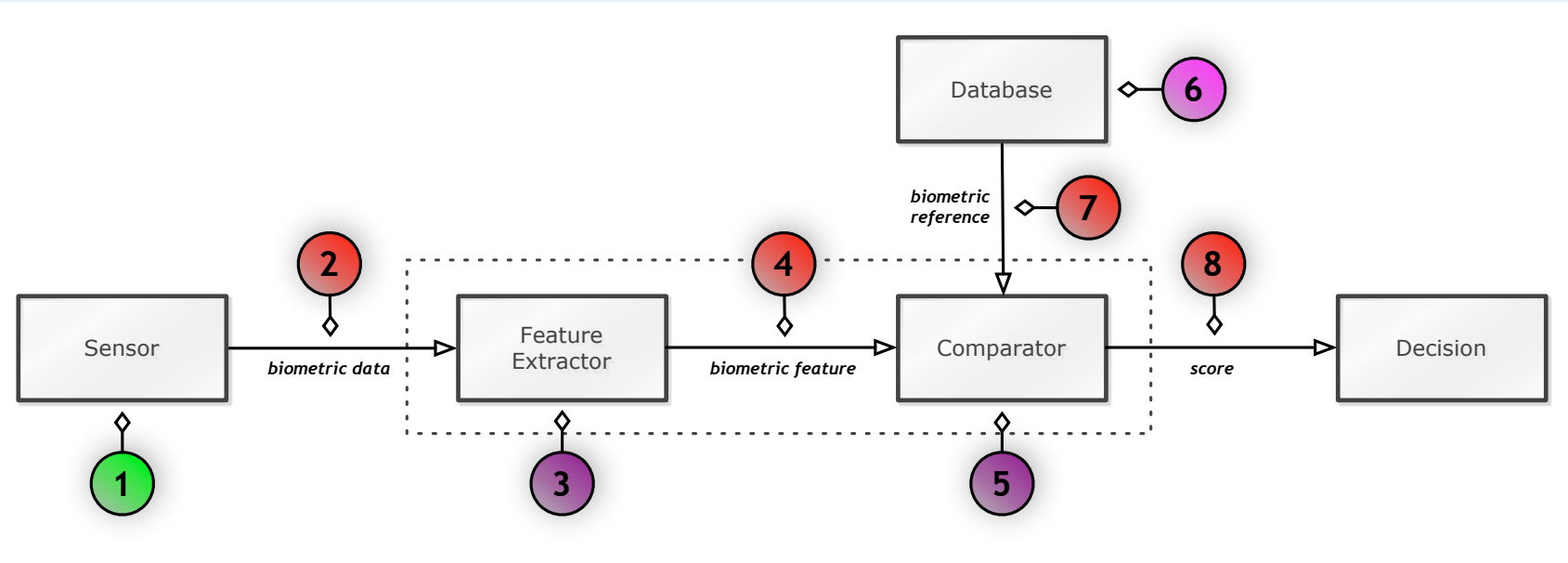
Outline

- Introduction
  - Biometrics Security
  - Presentation attacks in movies
  - Presentation attacks in reality
  - Definition
  - Importance
- Presentation attacks
- Presentation attack detection
- Performance evaluation

Introduction

Biometrics Security

A biometric system is vulnerable to attacks [1]

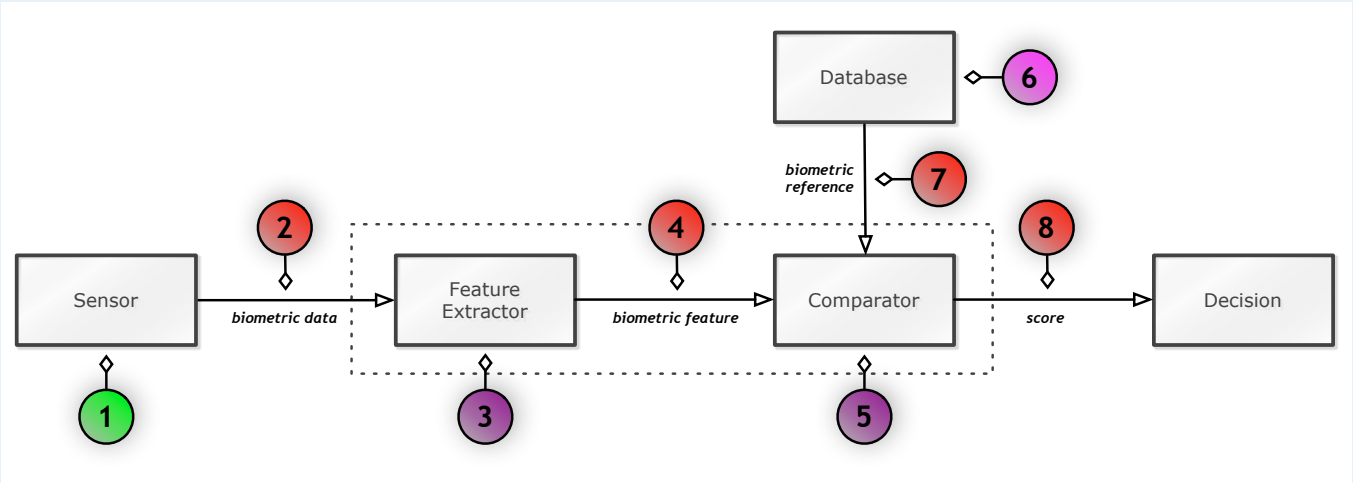


- Indirect attacks (**2-8**)
- Direct attacks (**1**)

[1] *Enhancing security and privacy in biometrics-based authentication systems*, NK. Ratha et al., IBM Systems Journal, 40(3):614–634, 2001.

Biometrics Security

Indirect Attacks

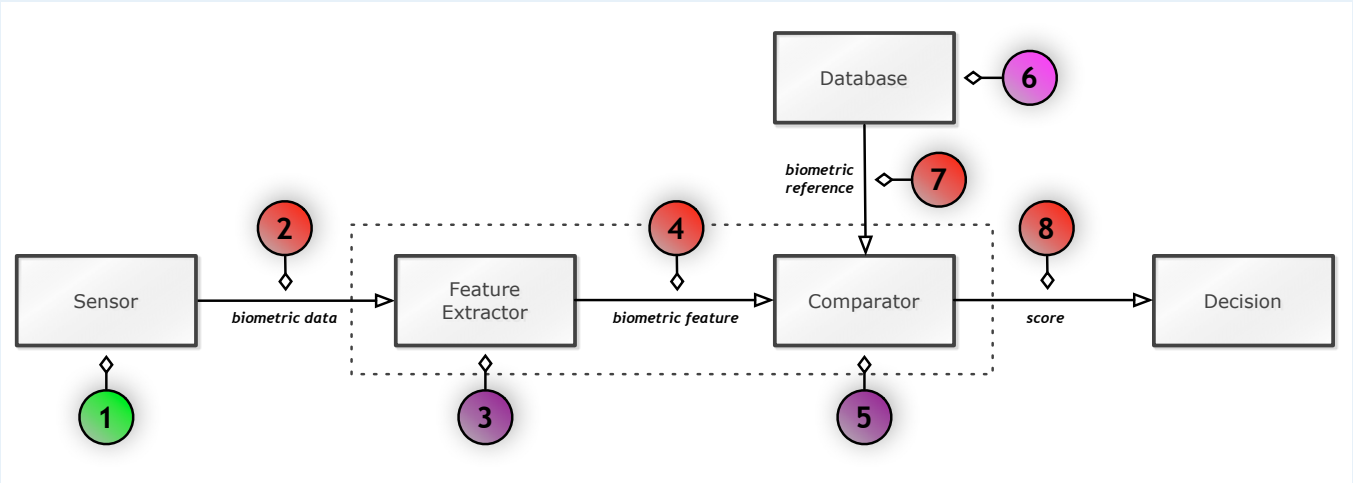


Indirect attacks are performed inside the system by:

- bypassing the feature extractor or the comparator (**3**, **5**),
- manipulating the biometric references in the biometric reference database (**6**),
- exploiting possible weak points in communication channels (**2**, **4**, **7**, **8**).

Biometrics Security

Direct Attacks



Direct attacks (**spoofing or presentation attacks – PAs**) are performed at the sensor level: the sensor is fooled and not replaced nor tampered.

In this lecture we are concerned with **presentation attacks**

PAs in Movies

MacGyver - The Human Factor (S02E01 1986)

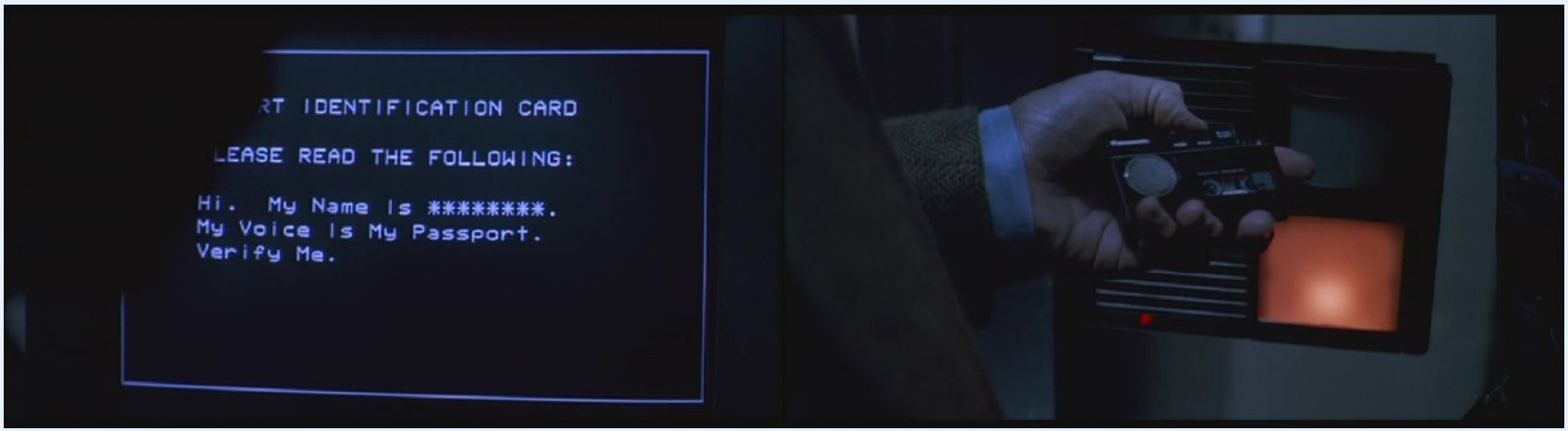
1. scraped some plaster off the walls,
2. sprinkled the plaster dust over the palm print reader revealing the Colonels hand print,
3. laid a jacket down over the plaster hand print impression and lightly pressed down on the reader.

PAs in Movies

Sneakers (1992)

PAs in Movies

Sneakers (1992)



Replay a voice recording in front of a speaker recognition system !

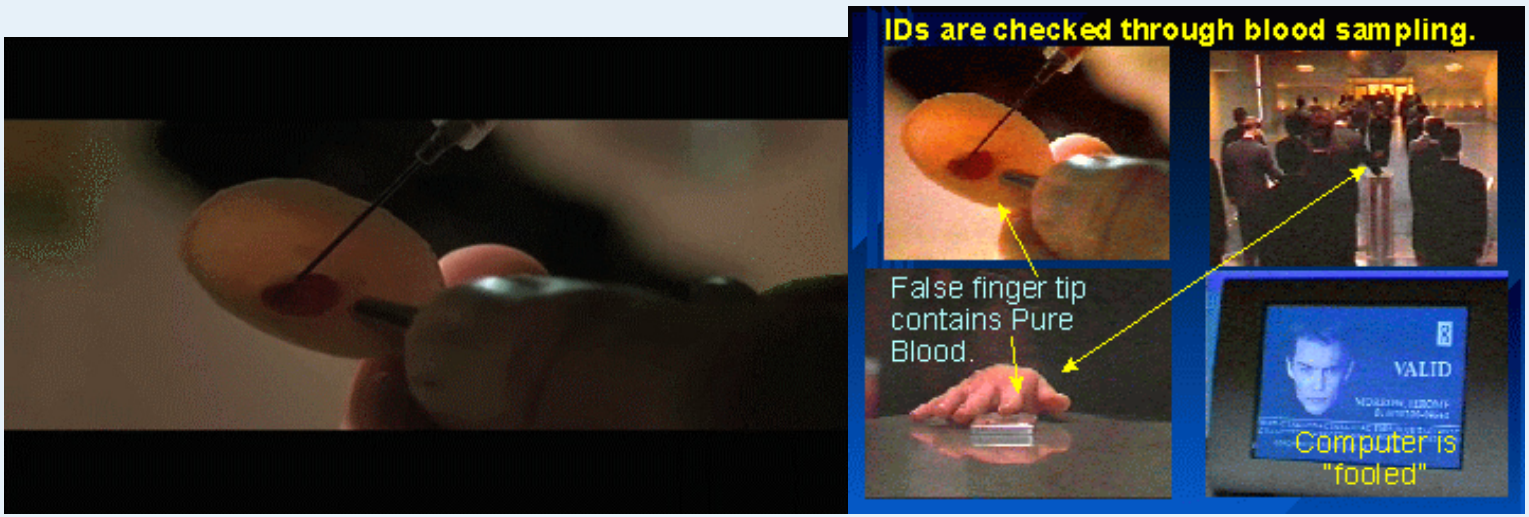
PAs in Movies

Demolition Man (1993)

Present an eyeball in front of a iris scanner !

PAs in Movies

GATTACA (1997)



Injecting blood samples in a false finger tip to fool DNA identification !

PAs in Movies

Minority Report (2002)

Using eyeball-swapping surgery to avoid iris identification !

PAs in Movies

RED 2 (2013)

PAs in Movies

RED 2 (2013)

Iris spoofing (not retina) with a fake contact lens !

PAs in reality

Bank robbery (2010) [2]

Conrad Zdzierak used a silicon masks to pass himself off as a black character “SPFX The Player” during robberies !

[2] http://www.telegraph.co.uk/news/worldnews/northamerica/usa/8193185/US-criminals-using-film-quality-masks-during-bank-robberies.html

PAs in reality

Hong Kong - Vancouver (Jan 2011) [3] [4]

A passenger boarded a plane in Hong Kong with an old man mask and arrived in Canada !

[3] http://www.dailymail.co.uk/news/article-2153346/Black-armed-robber-disguised-white-man-using-latex-mask.html

[4] http://www.dailymail.co.uk/news/article-1326885/Man-boards-plane-disguised-old-man-arrested-arrival-Canada.html

PAs in reality

Android 4.0 (Nov 2011) [5]

Android 4.0 Face UnLock feature spoofed by photograph [6]

[5] https://www.youtube.com/watch?v=BwfYSR7HttA

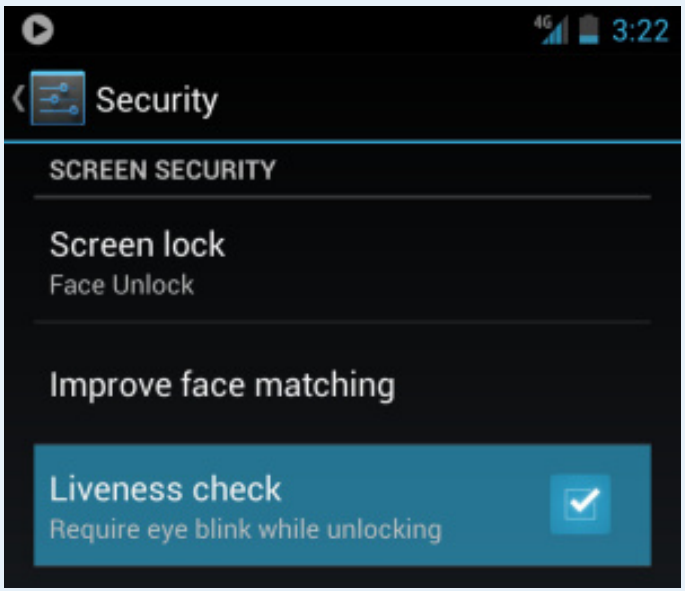
[6] http://www.geek.com/android/android-face-lock-feature-spoofed-by-photograph-1440953

PAs in reality

Android 4.0 (Nov 2011)

PAs in reality

Android 4.1 (Jun 2012)



Liveness check (eye blink) introduced in Android 4.1

PAs in reality

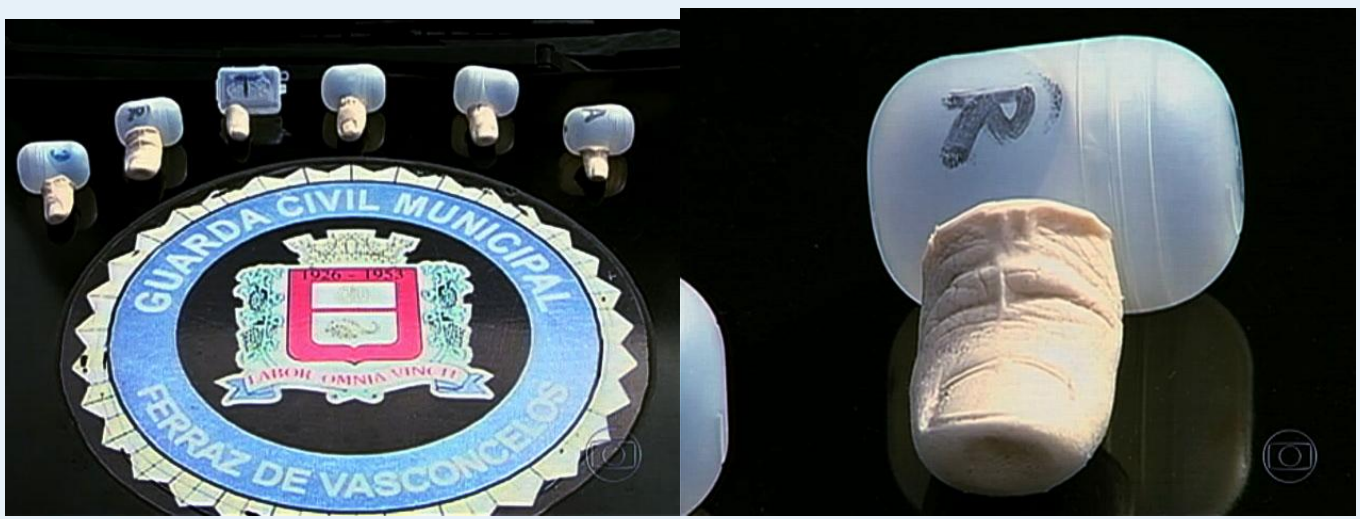
Bank robbery again (2012)

Burglars who robbed a cash-checking store in Queens disguised as cops [7]

[7] http://www.dailymail.co.uk/news/article-2108276/Bank-robbers-stump-NYPD-life-like-masks-look-white-black-Hispanic.html

PAs in reality

Brazil (March 2013) [8]

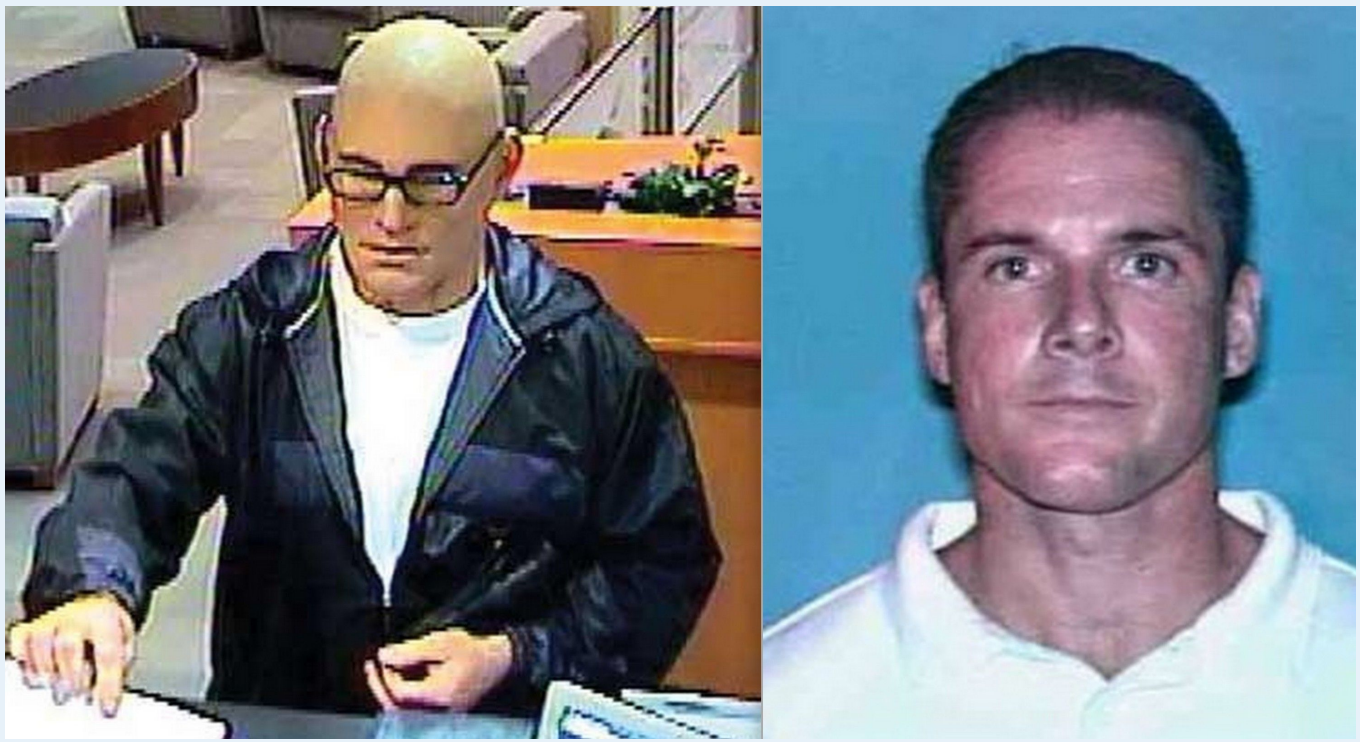


Fake fingers used to fool Hospital clock-in scanner

[8] http://news.sky.com/story/1063956/fake-fingers-fool-hospital-clock-in-scanner

PAs in reality

More bank robbery (2013) [9]

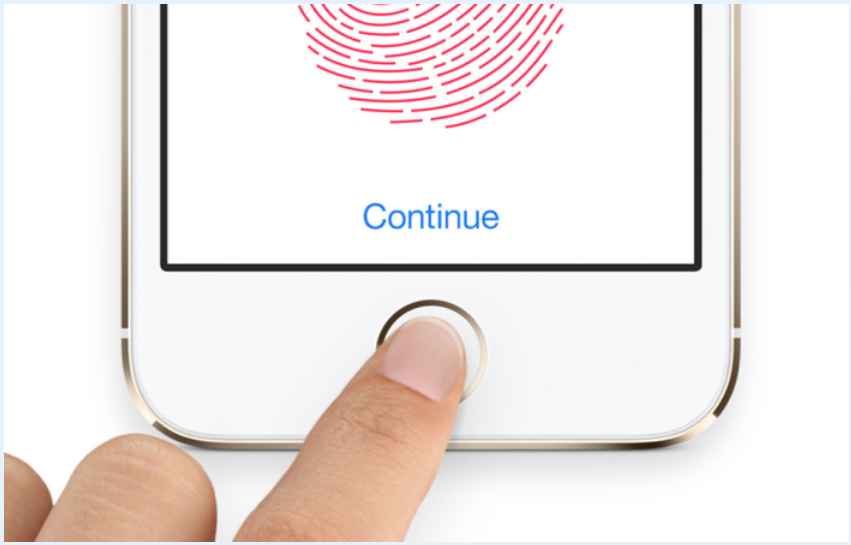


Steven Ray Milam robbed 11 banks in Texas with "SPFY The Handsome Guy" silicon mask

[9] http://dfw.cbslocal.com/2012/05/22/handsome-guy-bandit-pleads-guilty-in-federal-court

PAs in reality

iPhone 5s spoofed by CCC (Sep 21 2013) [10]

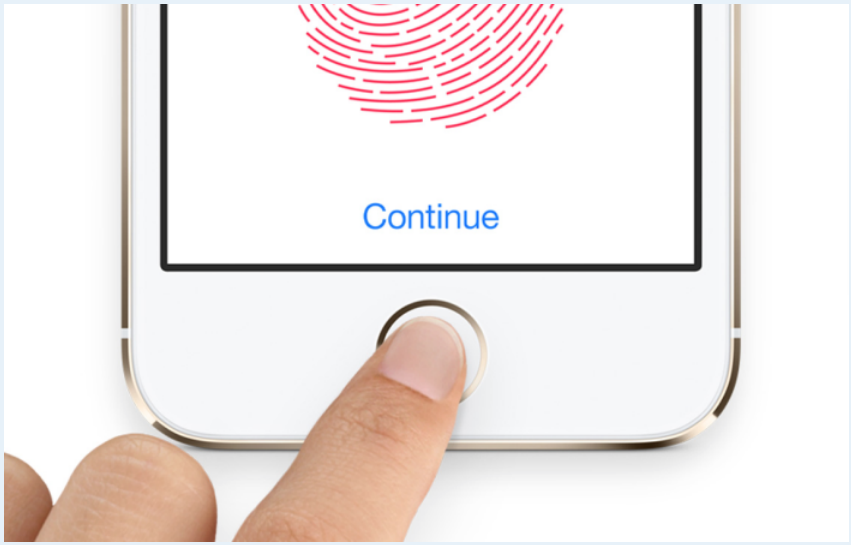


1. How many days will it take to spoof it ? 2 days !

[10] http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid

PAs in reality

iPhone 5s spoofed by CCC (Sep 21 2013) [10]



1. How many days will it take to spoof it ? 2 days !
2. iPhone 5s spoofed by the Chaos Computer Club (1st public ...)

[10] http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid

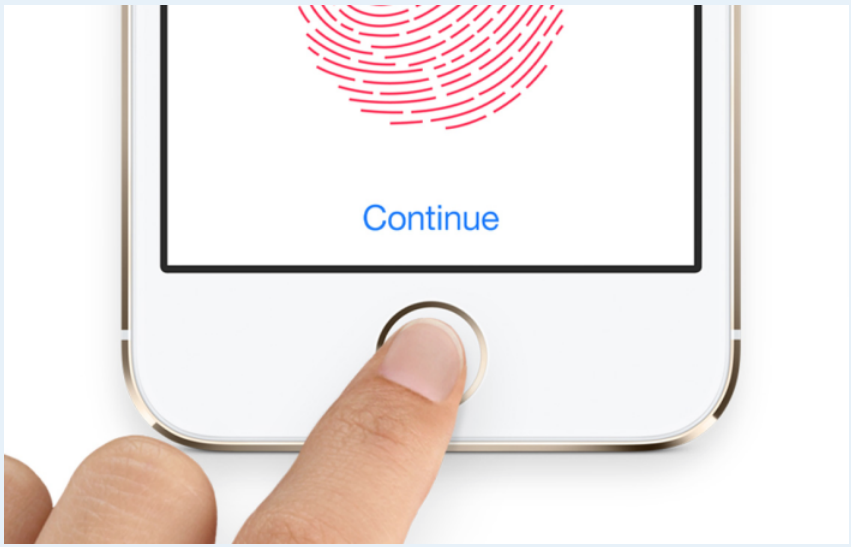
PAs in reality

iPhone 5s spoofed by CCC (Sep 21 2013) [11]

[11] https://www.youtube.com/watch?v=HM8b8d8kSNQ

PAs in reality

Apple and fingerprints the full story [12]



[12] http://fingerchip.pagesperso-orange.fr/biometrics/types/fingerprint_apple.htm

PAs in reality

Finger-vein (Oct 2014) [13]

- Finger-vein commercial system spoofed by a piece of paper
- Full recipe (https://www.youtube.com/watch?v=zxb9xwaoeTU)

[13] https://www.youtube.com/watch?v=8HuL6cHJTK0

PAs in reality

Samsung Galaxy S8 Iris spoofed by CCC (May 23 2017) [14]

[14] https://media.ccc.de/v/biometrie-s8-iris-en

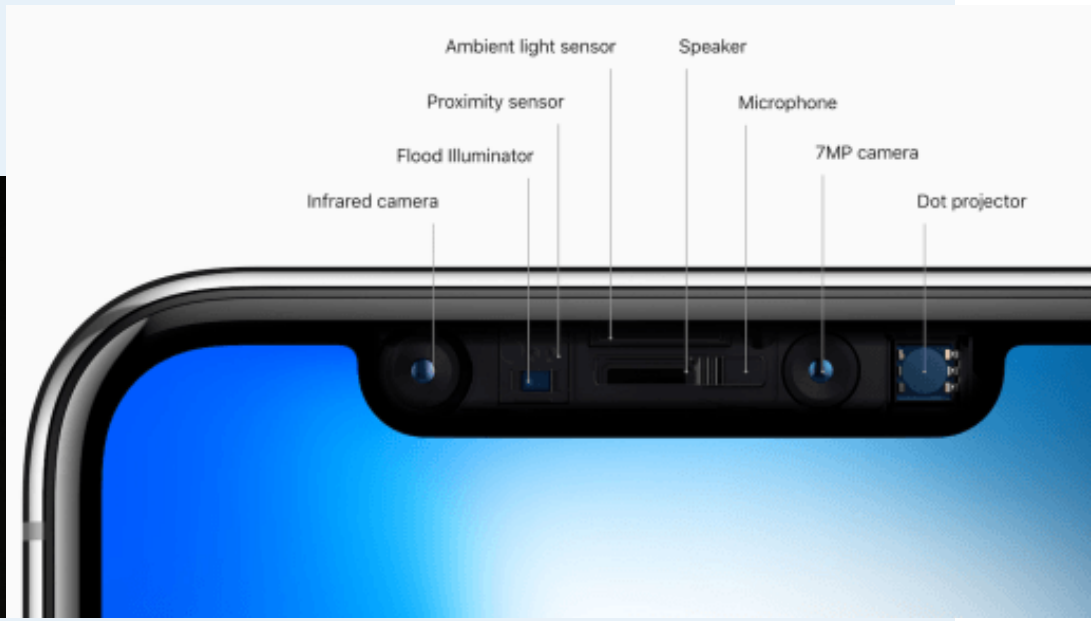
PAs in reality

Samsung Galaxy S8 Iris spoofed by CCC (May 23 2017) [15]

[15] https://www.youtube.com/watch?v=gtQ4yzbsi-c

PAs in reality

iPhone X FaceID (Sep 2017)

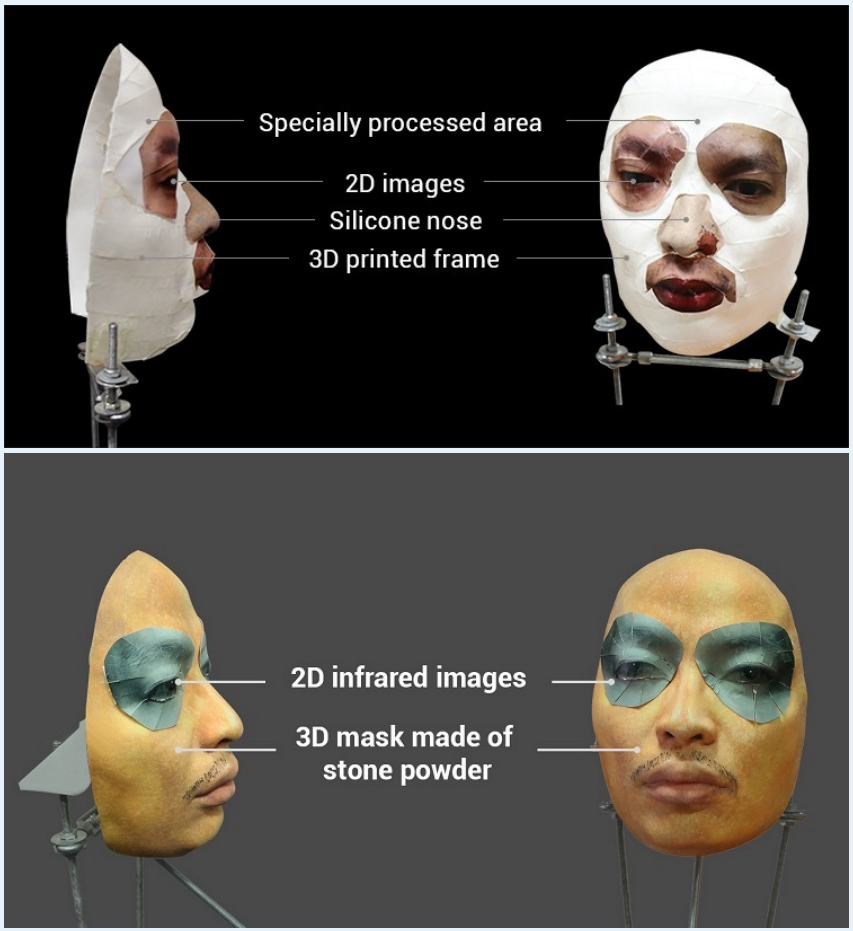


PAs in reality

iPhone X FaceID robust to masks (Sep 2017)

PAs in reality

iPhone X spoofed by Bkav (Nov 27 2017) [16] [17]



[16] http://www.bkav.com

[17] https://www.youtube.com/watch?v=i4YQRLQVixM

Definition [18]

Spoofing Attack

Outwitting a biometric sensor by presenting a counterfeit biometric evidence of a valid user

Anti-Spoofing

Countermeasure to spoofing attack

No common terminology so far

spoofing, **evasion/concealment**, anti-spoofing, liveness detection, presentation attack, presentation attack detection, ...

[18] *Spoof Detection Schemes*, K. Nixon et al., Handbook of Biometrics, 2008.

Definition by ISO [19]

Presentation Attack – PA

presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system

- methods: artefact, mutilations, replay, ...
- goals: impersonation or not being recognized (concealment)

Presentation Attack Instrument – PAI

biometric characteristic or object used in a presentation attack
eg. artefacts, dead bodies, altered fingerprints, ...

[19] *Biometric presentation attack detection – part 1*, ISO/IEC 30107-1:2016, 2016.

Definition by ISO

Normal (Bona Fide) Presentation

interaction of the biometric capture subject and the biometric data capture subsystem in the fashion intended by the policy of the biometric system in short anything which is not a PA !

Presentation Attack Detection – PAD

automated determination of a presentation attack

Importance

Presentation Attack is a major threat

because it can be created and performed by anyone with no specific skills in computer science

Importance

Funding programs/projects

- EU TABULA RASA "Trusted Biometrics under Spoofing Attacks" (2010-2014)

  www.tabularasa-euproject.org

- EU BEAT "Biometrics Evaluation and Testing" (2012-2016)

  www.beat-eu.org

- NO: SWAN "Secure Access Control Over Wide Area Network" (2016-2019)

  www.ntnu.edu/iik/swan

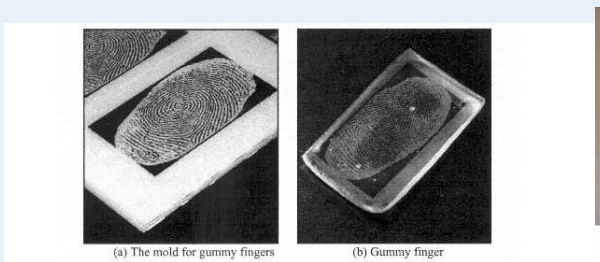
- US: IARPA Odin Thor/Loki red team approach (2017-2020)

  www.iarpa.gov/index.php/research-programs/odin

Presentation attacks

Seminal work

"Gummy Fingers" [20]



(a) The mold for gummy fingers (b) Gummy finger

Figure 4.5 Photographs of the outside appearance of the mold and a *gummy* finger. The *gummy* finger was produced from a residual fingerprint on a glass plate, enhancing it with a cyanoacrylate adhesive

Figure 4.6 The Fingerprint image of the *gummy* finger, which was displayed by the system with Device H (equipped with a capacitive sensor).

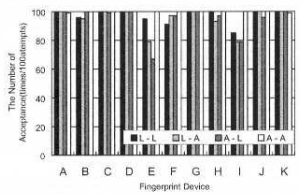
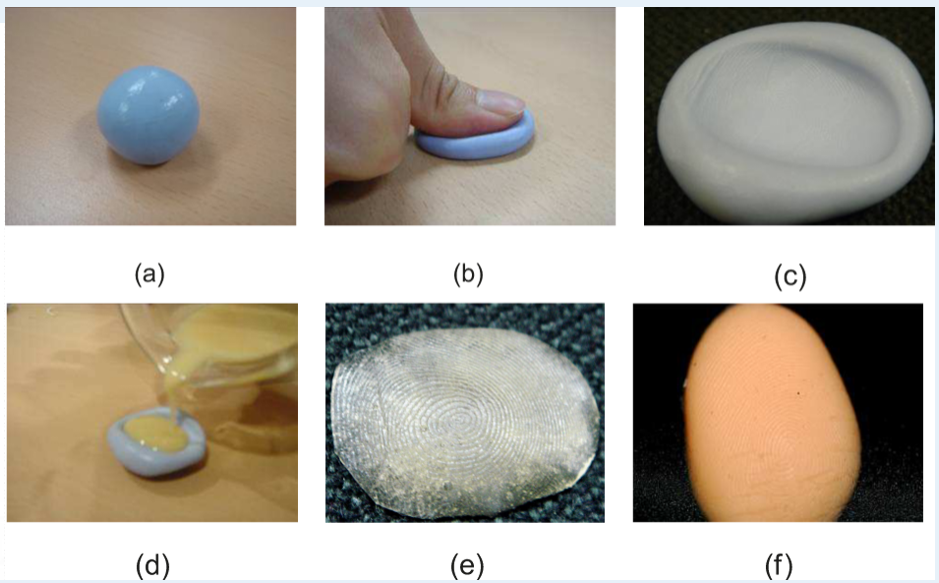


Figure 4.7 Average number of acceptance for each device, in terms of *gummy* fingers which were cloned from residual fingerprints. Here, the subject is one person.



Gelatin fake fingers to spoof 11 fingerprint biometric systems

[20] *Impact of Artificial Gummy Fingers on Fingerprint Systems*, T. Matsumoto et al., SPIE 4677, Optical Security and Counterfeit Deterrence Techniques IV, 275, 2002, (http://cryptome.org/gummy.htm).

Seminal work

Prior work with Fake Fingerprints

T. van der Putte and J. Keuning *Biometrical Fingerprint Recognition Don't Get Your Fingers Burned*, Conference on smart card research and advanced applications, 289-303, 2001 (`http://cryptome.org/fake-prints.htm`)

M. Kàkona *Biometrics: yes or no?*, 2001 (`http://home.i.cz/kakl/biometrics/Biometricsyesorno.htm`)

L. Thalheim et al. *Body Check: Biometric Access Protection Devices and their Programs Put to the Test*, 2002

Seminal work

Black Hat 2009 [21]

Printed photo to spoof face recognition systems on 3 laptops

[21] *Your Face Is NOT Your Password*, D. Nguyen et al., Black Hat, 2009.

Seminal work

Black Hat 2009

Printed photo to spoof face recognition systems on 3 laptops:

- Asus (F6S Series, X80 Series): Asus SmartLogin ver 1.0.0005
- Toshiba (L310, M300): Toshiba Face Recognition ver 2.0.2.32
- Lenovo (Y410, Y430): Lenovo Veriface III

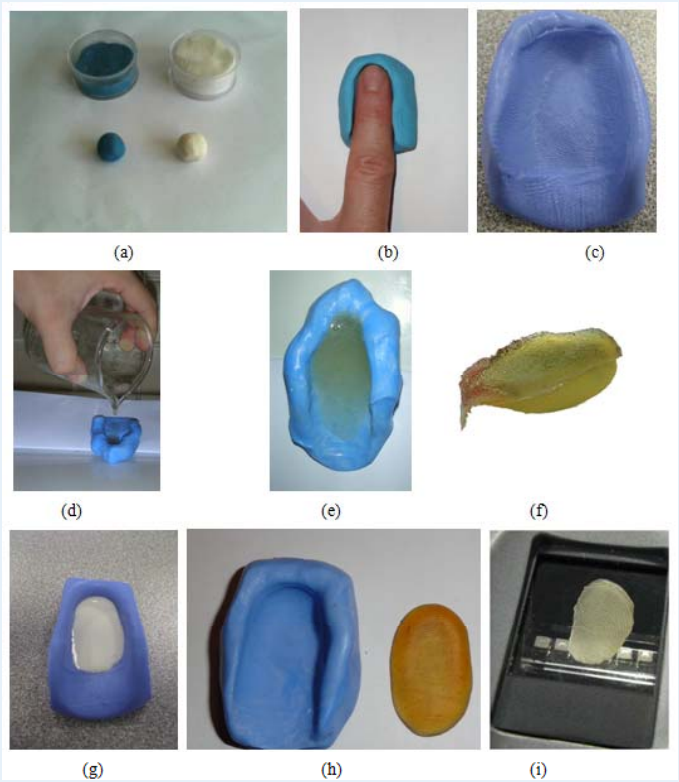
Presentation Attacks

Fingerprint PA

Presenting a fake fingerprint to a capture device

Presentation Attacks

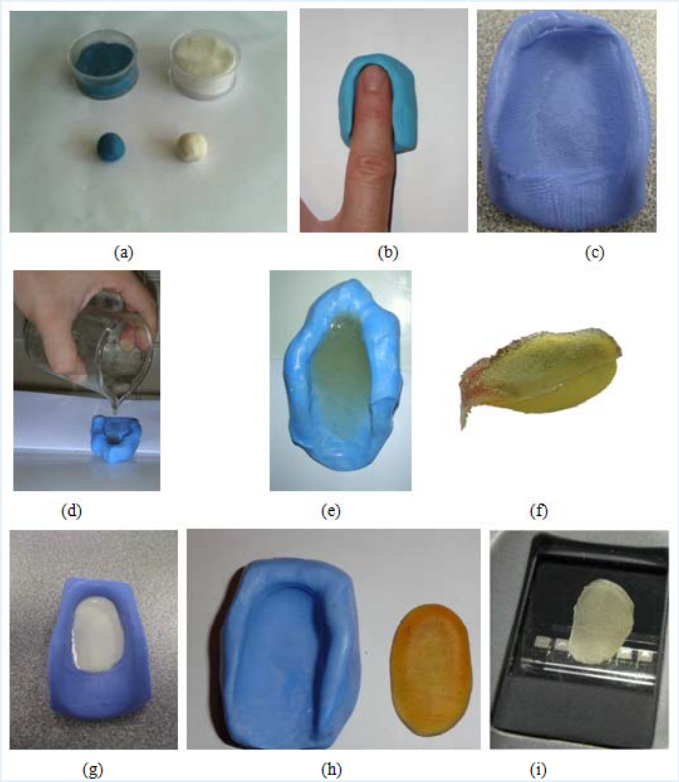
Fingerprint PA: latex/silicone PAI (with cooperation)



Prepare a silicone mold (a, b and c)

Presentation Attacks

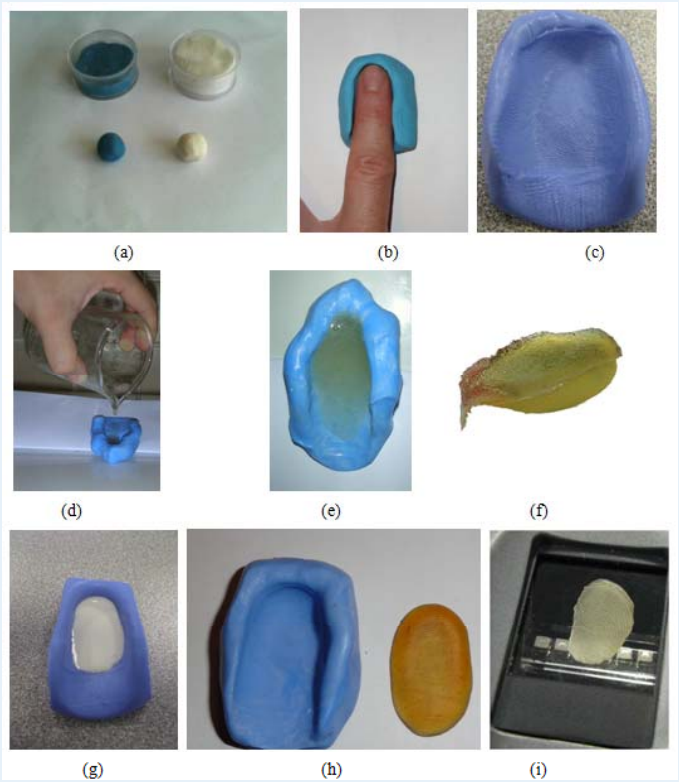
Fingerprint PA: latex/silicone PAI (with cooperation)



Prepare fake with liquid latex (d, e and f)

Presentation Attacks

Fingerprint PA: latex/silicone PAI (with cooperation)



Use fake (g, i and j)

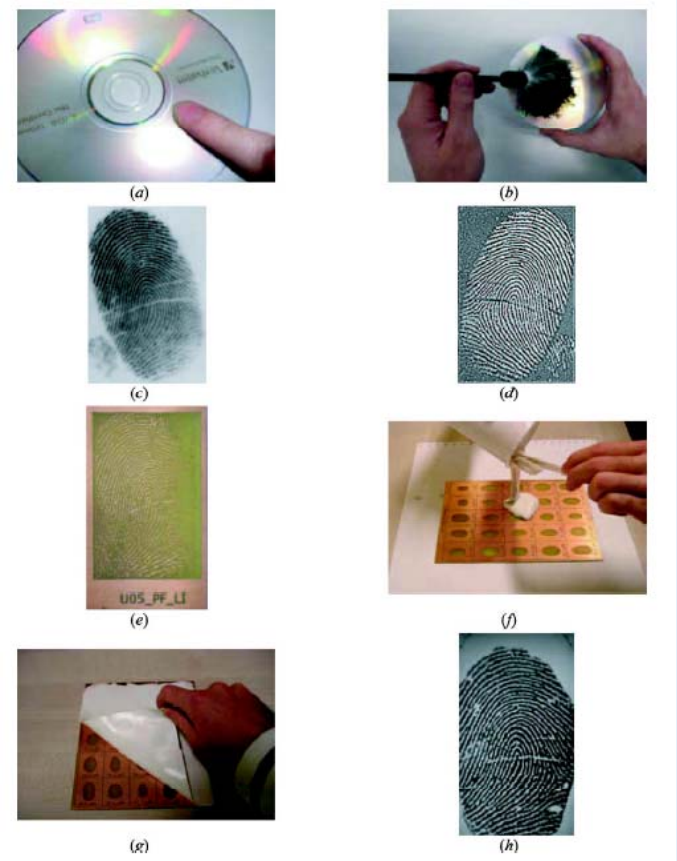
Presentation Attacks

Fingerprint PA: wood glue PAI (with cooperation)

Same recipe but with hot glue and wood glue !

Presentation Attacks

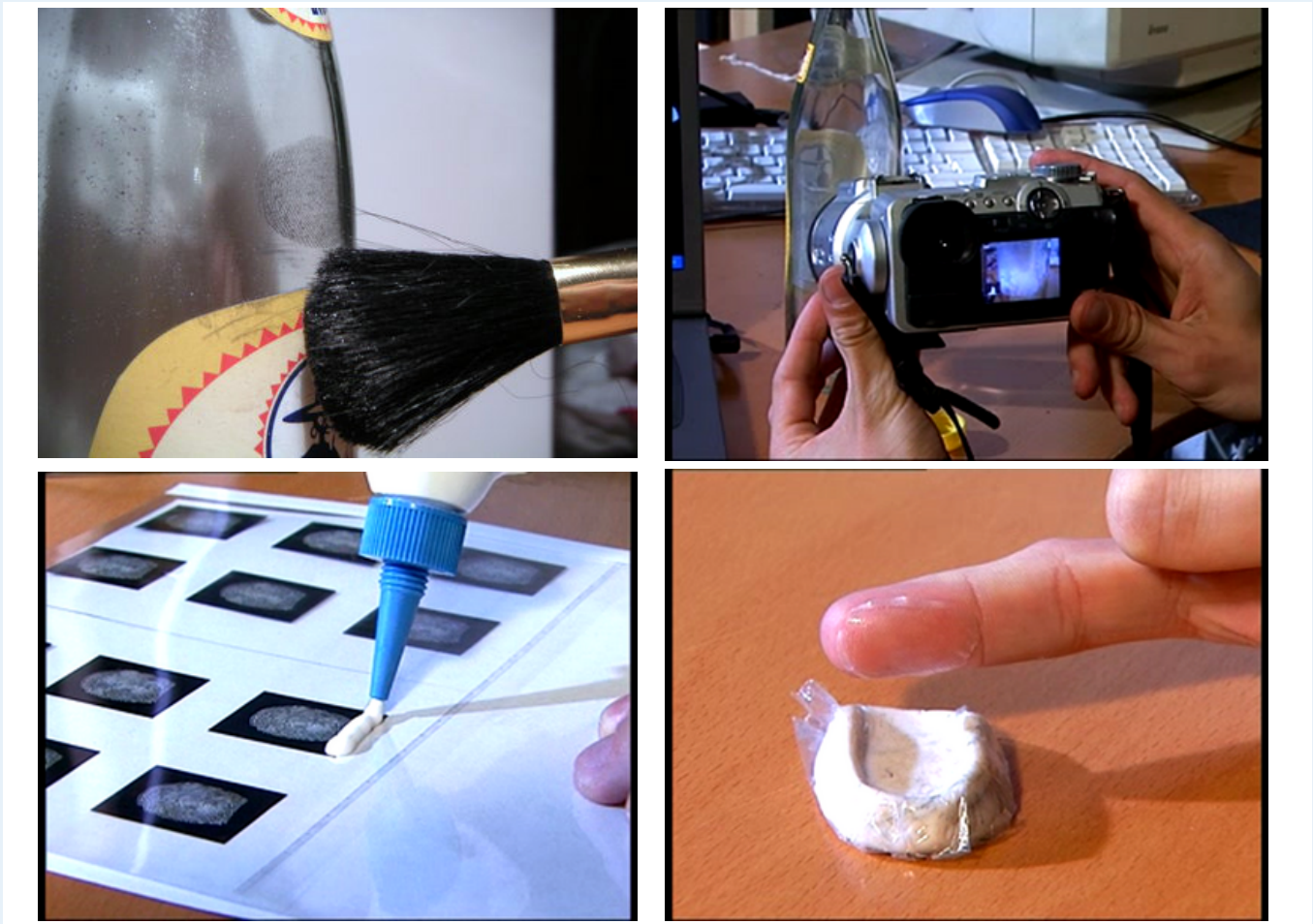
Fingerprint PA: latex/silicone PAI (without cooperation)



The lifted latent fingerprint is printed on a PCB (Printed Circuit Board) to serve as a mold

Presentation Attacks

Fingerprint PA: wood glue PAI (without cooperation)

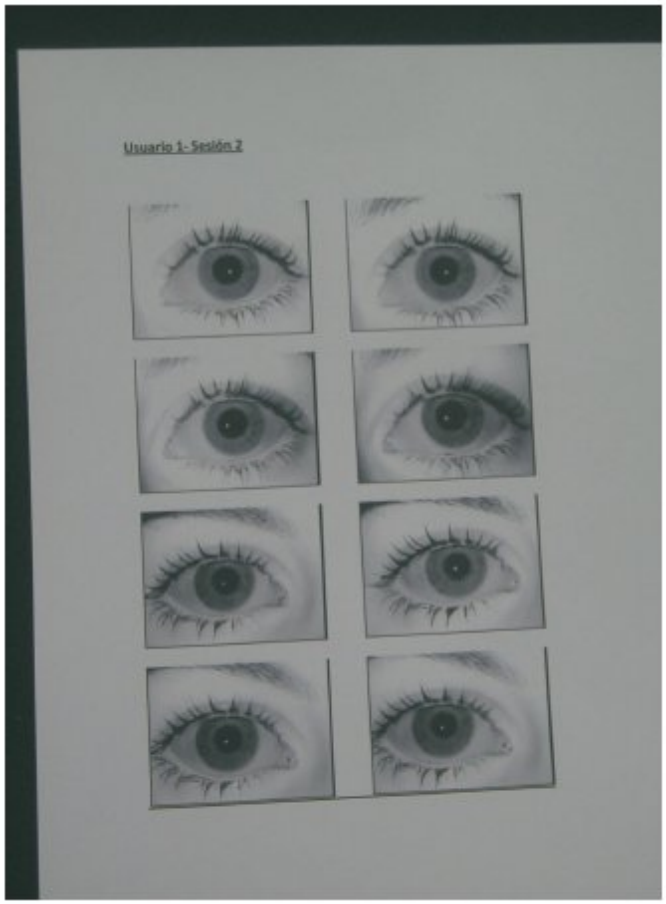


CCC vs iPhone5s [22]

[22] http://dasalte.ccc.de/biometrie/fingerabdruck_kopieren?language=en

Presentation Attacks

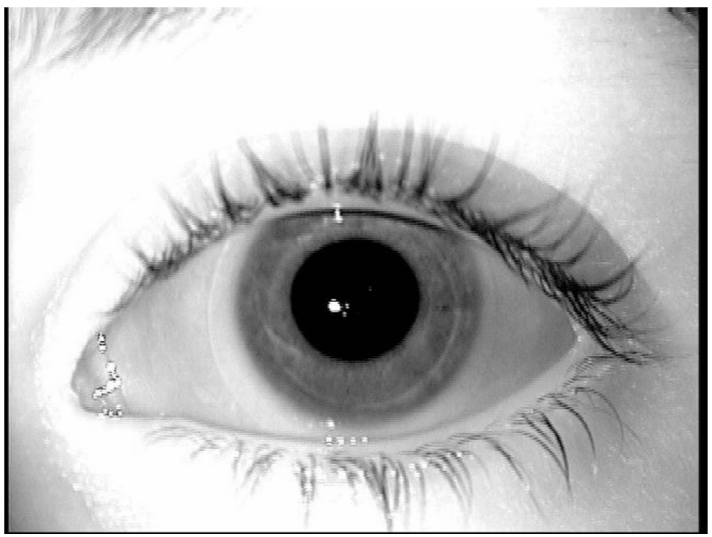
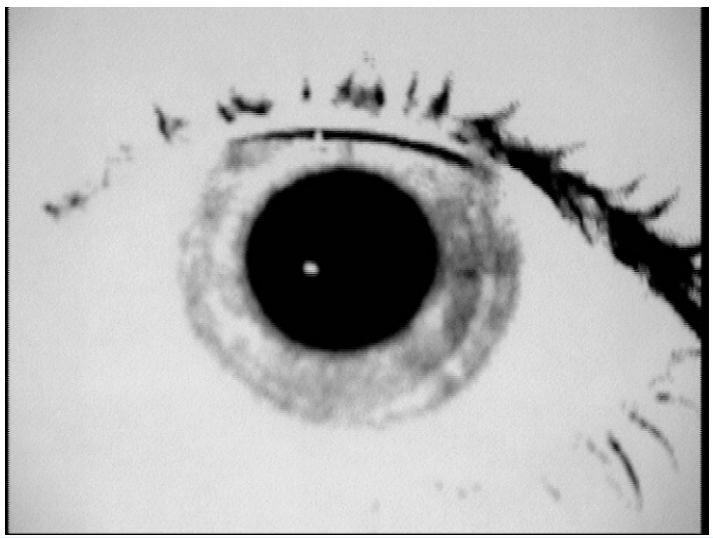
Iris PA: printed paper PAI



High quality paper and inkjet printer

Presentation Attacks

Iris PA: printed paper PAI

Real Iris (left) vs Fake Iris (right)

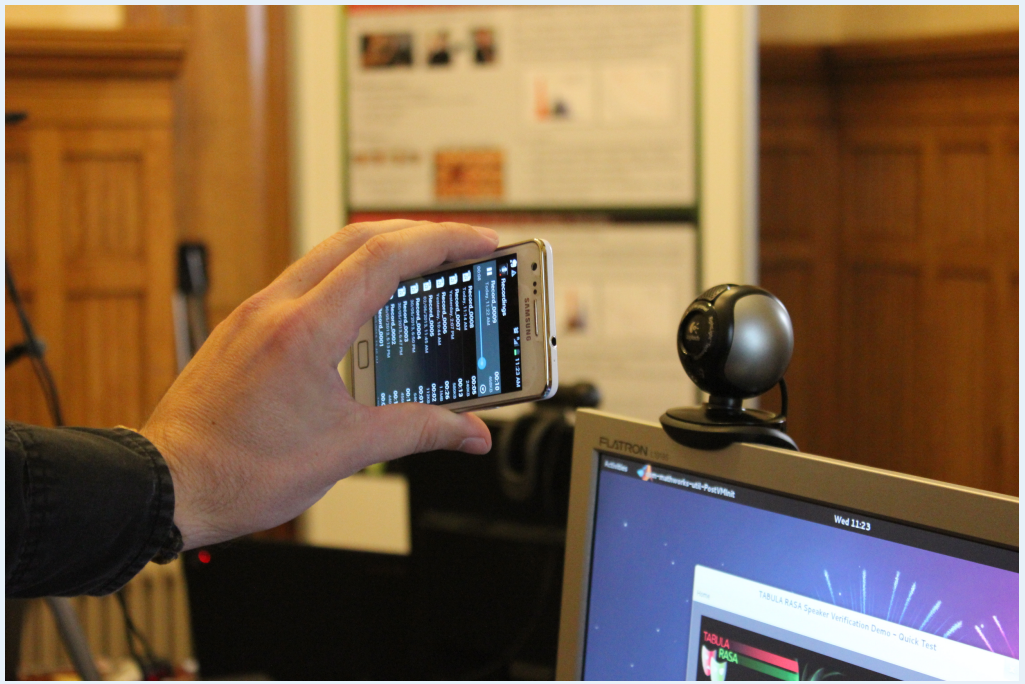
Presentation Attacks

2D face PA: printed paper PAI

Same recipe for photo and video attacks with a mobile phone or a tablet

Presentation Attacks

Voice PA – replay PAI [23]



Playback of a voice recording, a synthesised speech or a converted voice in front of a microphone

[23] *On the vulnerability of speaker verification to realistic voice spoofing*, S. Ergunay, E. Khoury, A. Lazaridis, and S. Marcel, IEEE BTAS, 2015.

Presentation Attacks

Voice PA: replay PAI

Original voice of target speaker (rec on HQ mic)
Playback with laptop (rec on laptop)
Playback with iPhone (rec on laptop)
Playback with Samsung (rec on laptop)

Voice PA: voice synthesis PAI

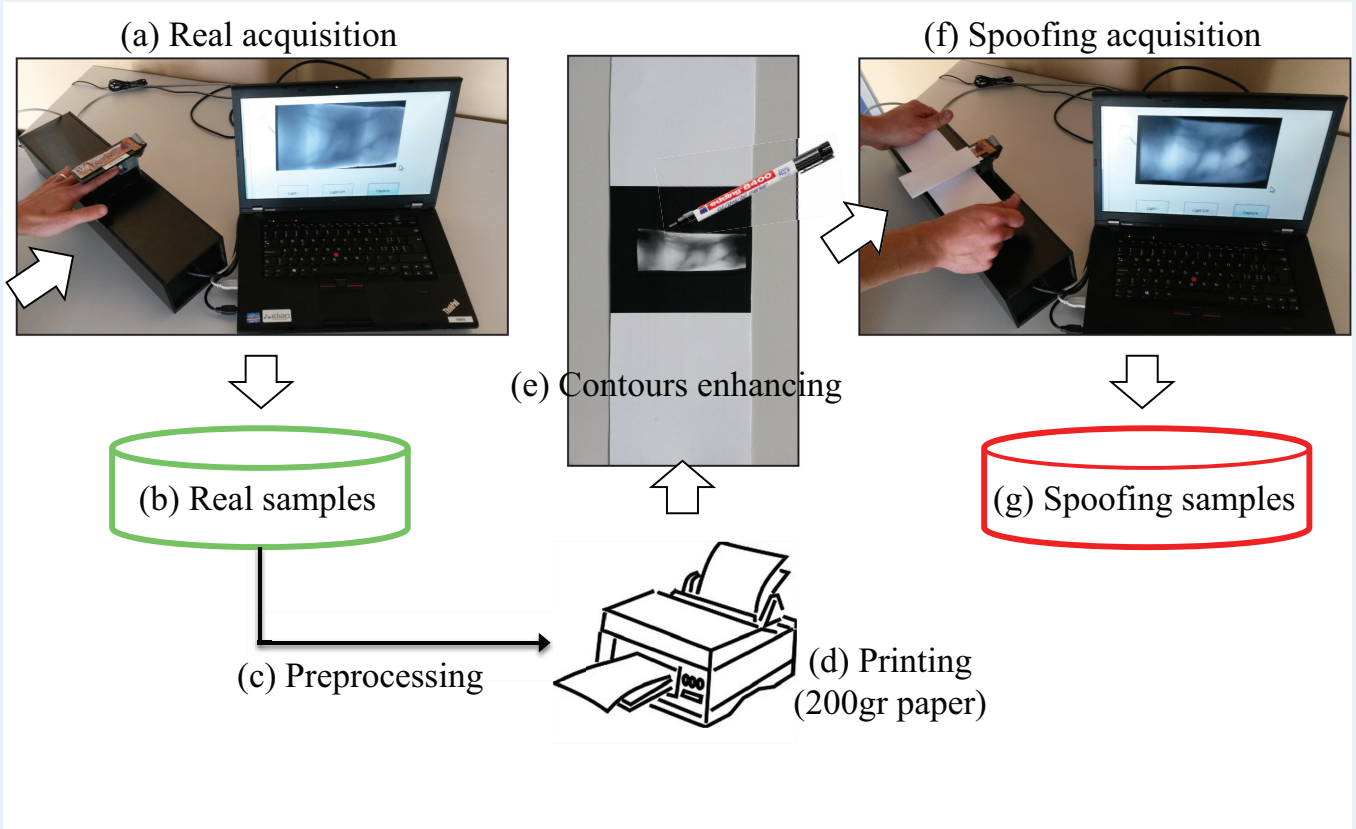
Voice of target speaker synthesized
Playback with laptop (rec on laptop)

Voice PA: voice conversion PAI

Original voice of source speaker (rec on laptop)
Voice of target speaker converted from source speaker
Playback with laptop (rec on laptop)

Presentation Attacks

Fingervein PA: printer paper PAI [24]

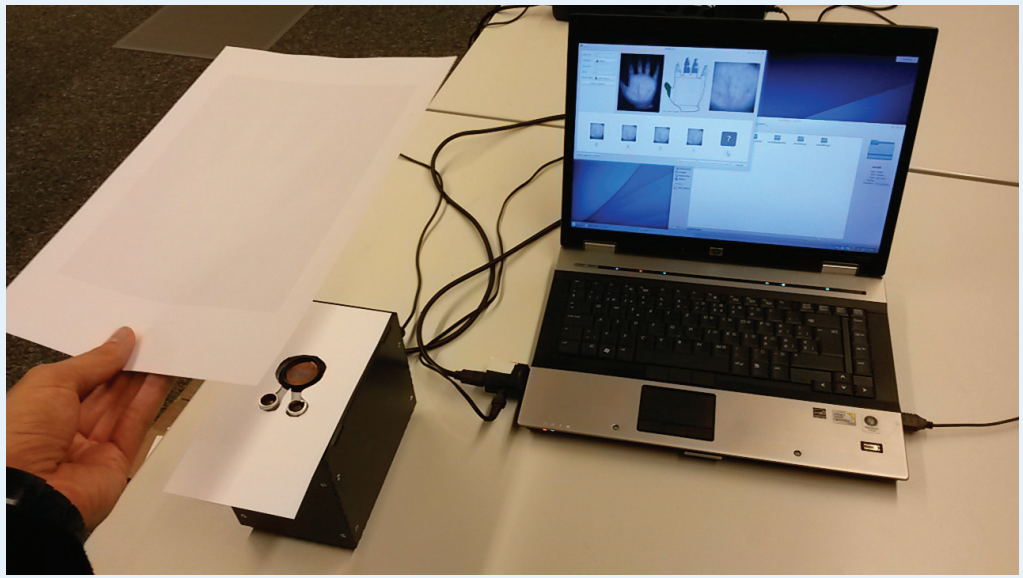


with paper

[24] *On the vulnerability of finger vein recognition to spoofing*, P. Tome, M. Vanoni and S. Marcel, IEEE BIOSIG, 2014.

Presentation Attacks

Palmvein PA: printed paper PAI [25]



with paper

[25] *On the vulnerability to palm vein recognition to spoofing attacks*, P. Tome and S. Marcel, IAPR ICB, 2015.

Face presentation attacks

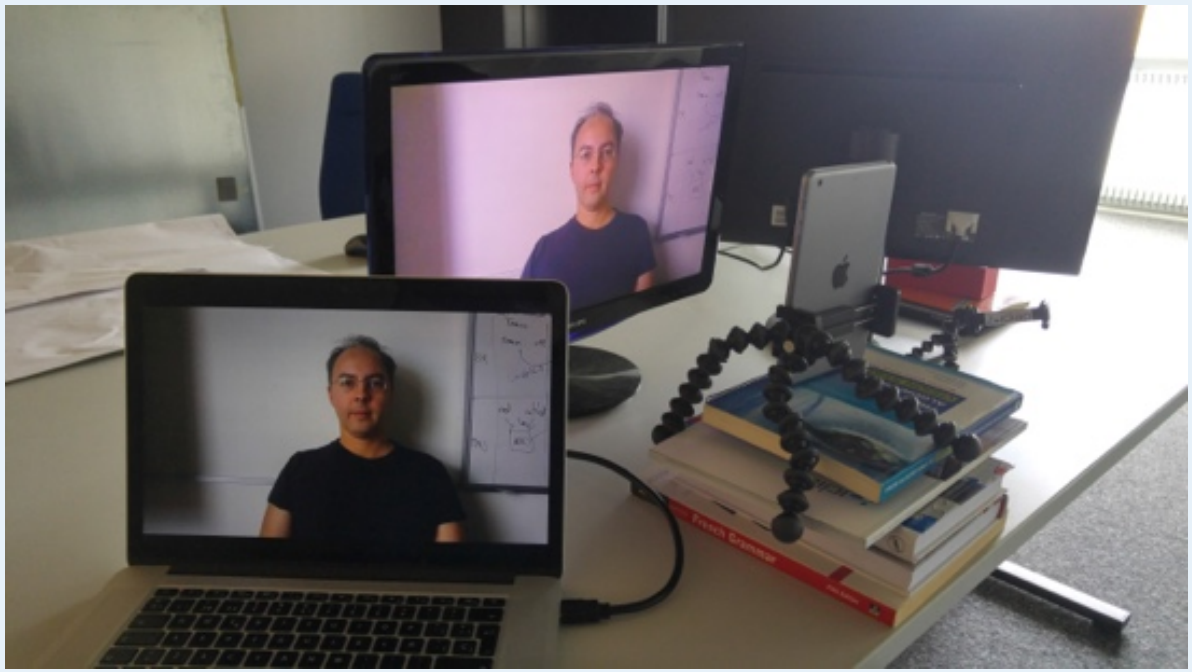
Face PA

2D face PA: printed paper PAI [26]

[26] *Counter-Measures to Photo Attacks in Face Recognition: a public database and a baseline*, A. Anjos and S. Marcel, IEEE/IAPR IJCB, 2001,
(http://www.idiap.ch/~marcel/professional/publications/anjos-ijcb-2011.pdf)

Face PA

2D face PA: photo/video screen PAI [27]



[27] *The REPLAY-MOBILE Face Presentation-Attack Database*, A. Costa-Pazo and al., IEEE BIOSIG, 2016, (http://publications.idiap.ch/downloads/papers/2016/Costa-Pazo_BIOSIG2016_2016.pdf).

Face PA

2D face PA: biometric data (print/photo/video PAI)

1. Which one is real (Bona Fide) or fake (PA) ?

Face PA

2D face PA: biometric data (print/photo/video PAI)

1. Which one is real (Bona Fide) or fake (PA) ?
2. All are fakes: print (left), iPhone (middle) and iPad (right) !

Face PA

2D face PA: printed paper PAI

PA with printed paper exhibits:

- Reduced image texture
- Printer halftoning artifacts
- Mechanical artifacts (horizontal lines)
- No local motion (e.g., eye blinks)
- Borders of image may be visible

Face PA

2D face PA: biometric data (print/photo/video PAI)

Bona Fide samples !

Face PA

2D face PA: biometric data (print/photo/video PAI)

PA samples !

Face PA

2D face PA: photo/video replay PAI

PA with an electronic screen exhibits:

- Blurred image texture
- Reduced color diversity
- Moire pattern

Face PA

2D face PA: 3D (rigid) mask PAI [28]

Hard resin composite in full 24-bit color !

[28] *Spoofing Face Recognition with 3D Masks*, N. Erdogmus and S. Marcel, IEEE TIFS, 9(7):1084–1097, 2014.

Face PA

2D face PA: 3D (rigid) mask PAI

Cost: $\sim$ USD 300

Face PA

2D face PA: 3D (rigid) mask PAI [29]

1 frontal and 2 profile pictures

[29] http://www.thatsmyface.com

Face PA

2D face PA: 3D (paper) mask PAI

Cost: $\sim$ USD 25 – but not effective

Face PA

2D face PA: 3D (ridid) mask PAI

PA with 3D (rigid) mask exhibits:

- vivid colors
- no facial motion (no lips or eye movement)

Face PA

2D face PA: 3D (rigid) mask with holes PAI

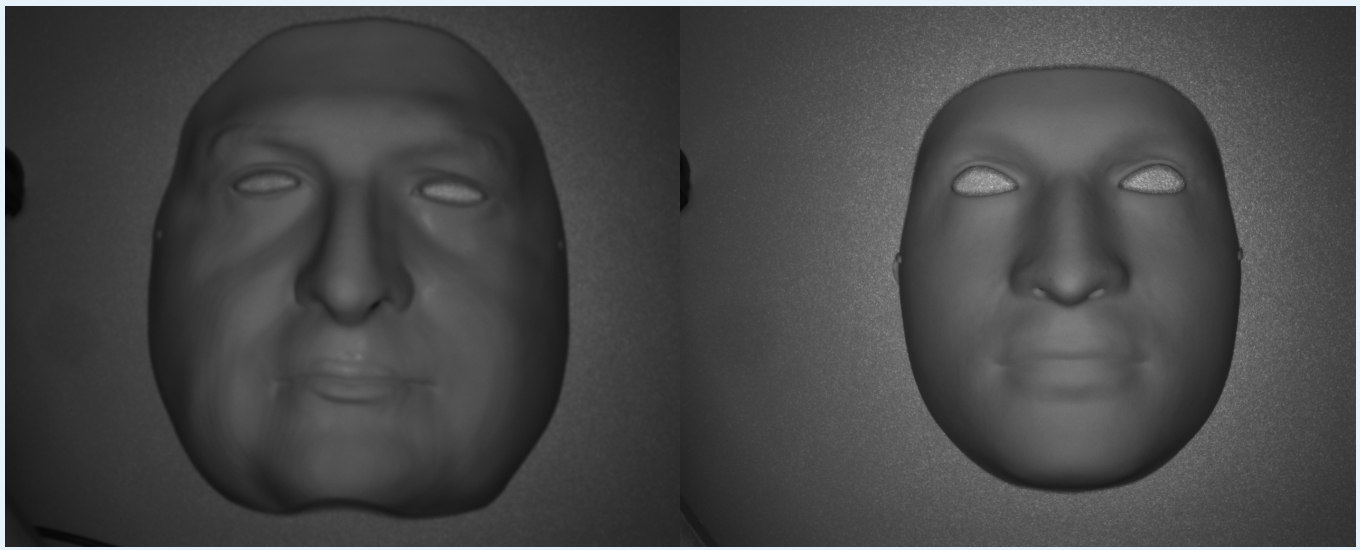
Cost: $\sim$ USD 400

Face PA

2D face PA: 3D (ridid) mask with holes PAI

PA with 3D (rigid) mask with holes exhibits:

- vivid colors
- no facial motion
- no texture in NIR



Face PA

2D face PA: 3D (ridid) mask with holes PAI

PA with 3D (rigid) mask don't absorb heat (much):

thermal imaging

Face PA

2D/3D face PA: 3D silicone masks PAI

Cost: $\sim$ USD 800

Face PA

2D/3D face PA: 3D silicone custom masks PAI

Cost for full head: starting USD 6'000

Face PA

2D/3D face PA: 3D silicone custom masks PAI

Cost for half-face: starting USD 3'000

Face PA

2D/3D face PA: 3D silicone custom masks PAI

Face PA

2D/3D face PA: 3D silicone custom masks PAI [30]

PA with 3D silicone mask exhibits:

- skin-like appearance and reflexion
- facial motion

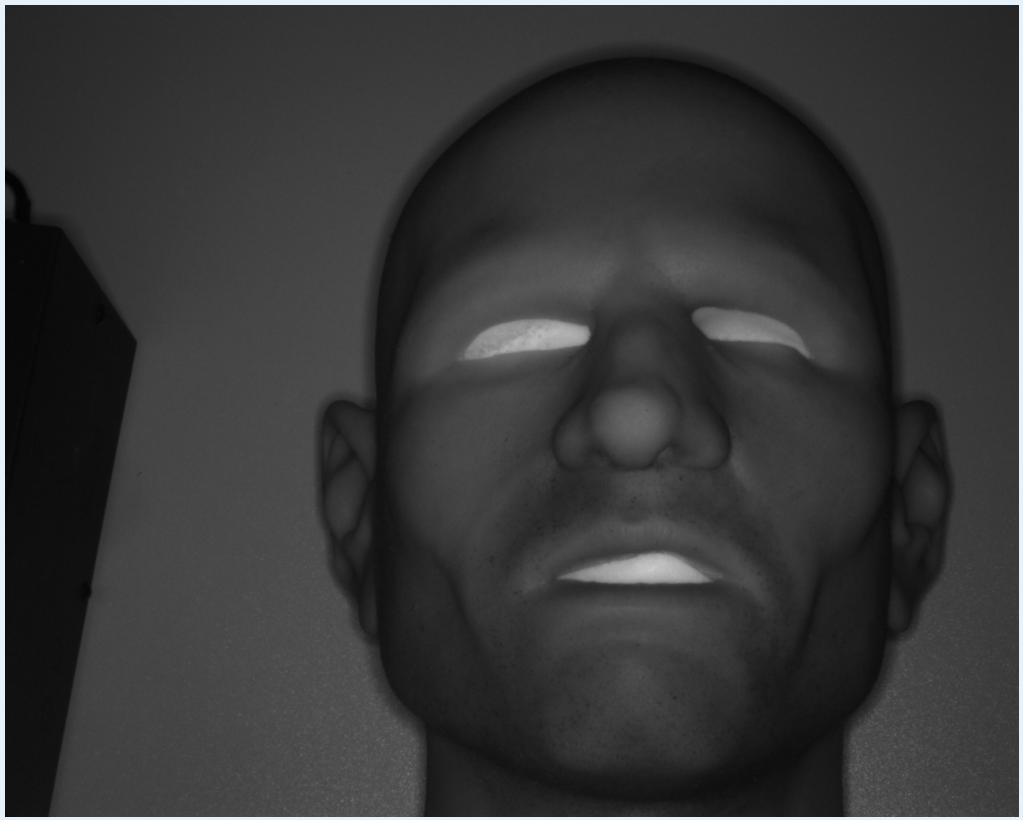
[30] *What you can't see can help you – extended-range imaging for 3D-mask presentation attack detection*, S. Battacharjee and al., IEEE BIOSIG, 2017.

Face PA

2D/3D face PA: 3D silicone custom masks PAI

PA with 3D silicone mask exhibits:

- texture in NIR



Face PA

2D/3D face PA: 3D silicone custom masks PAI

PA with 3D silicone mask exhibits:

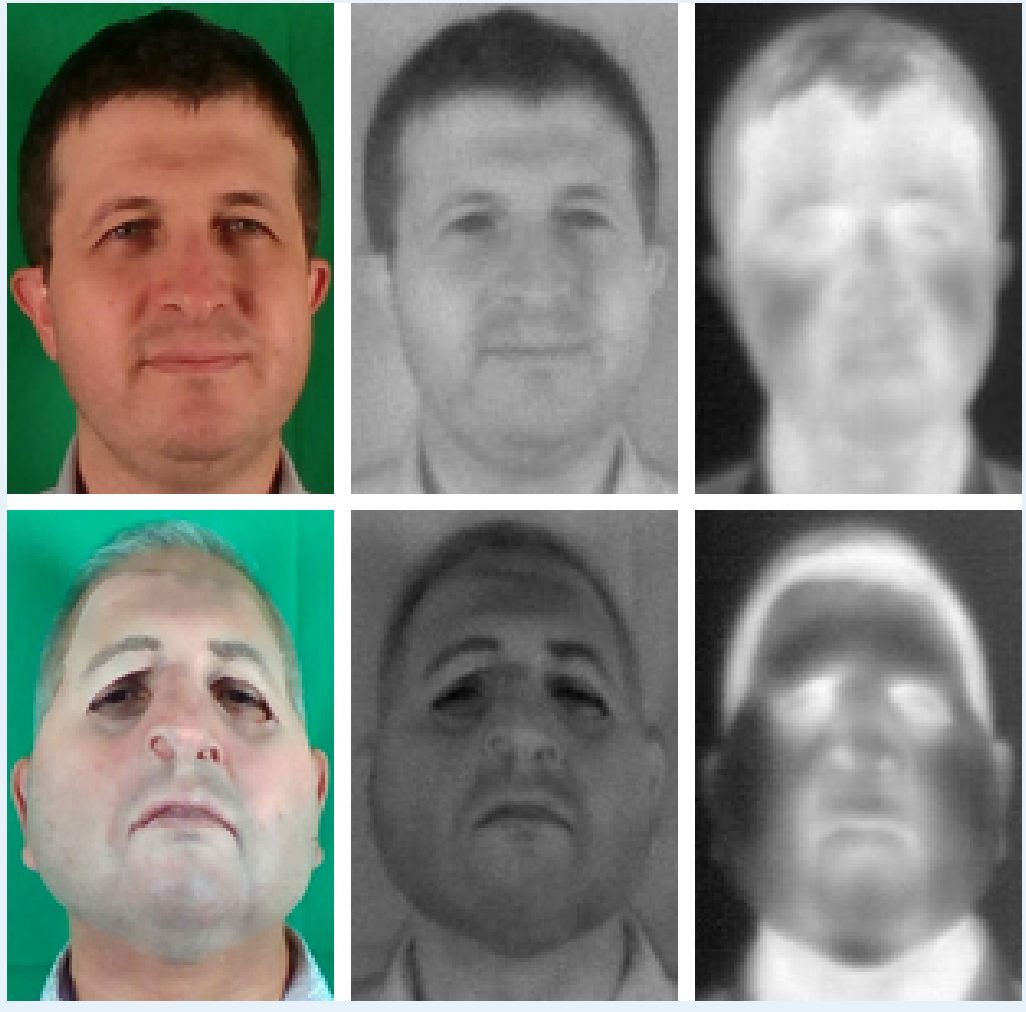
- thermal imaging ?

Silicone absorbs heat !

Face PA

2D/3D face PA: 3D silicone custom masks PAI

PA with 3D silicone mask exhibits thermal imaging:



Face PA

2D/3D face PA: make-up PAI

Face PA

2D/3D face PA: make-up PAI

PA with make-up exhibits:

- skin-like appearance and reflexion in VIS and NIR
- facial motion
- thermal imaging ?

Face PA

The Magic Passport [31]

Once upon a time there was a criminal; he was reading his e-mail when a banner caught his attention: low cost flights for the destination of his dreams! He had already started to book the trip when suddenly realized that, being wanted by the police, he could not use his passport without being arrested. What to do? He could not miss that opportunity, so he called a good friend and they started to think for a possible solution. Do you want to know if they succeeded? Read the rest of the paper and find it out.

[31] *The magic passport*, M. Ferrara, A. Franco, D. Maltoni, IEEE/IAPR IJCB, 2014.

Face PA

The Magic Passport: a morphed face image as template !

Face PA

2D Face PA: a morphed face PAI

It was shown that:

- 2 COTS face recognition system are matching correctly identities A and B against the morphed face (A+B),
- giving to the citizens the possibility of providing a printed face photo poses serious concerns in terms of security.

A test organized by FRONTEX demonstrated that a human expert can be easily fooled

Face PA

2D Face PA: a morphed face PAI

PA with morphing exhibits:

- symmetric features
- smooth texture
- morphing artefacts

Face PA

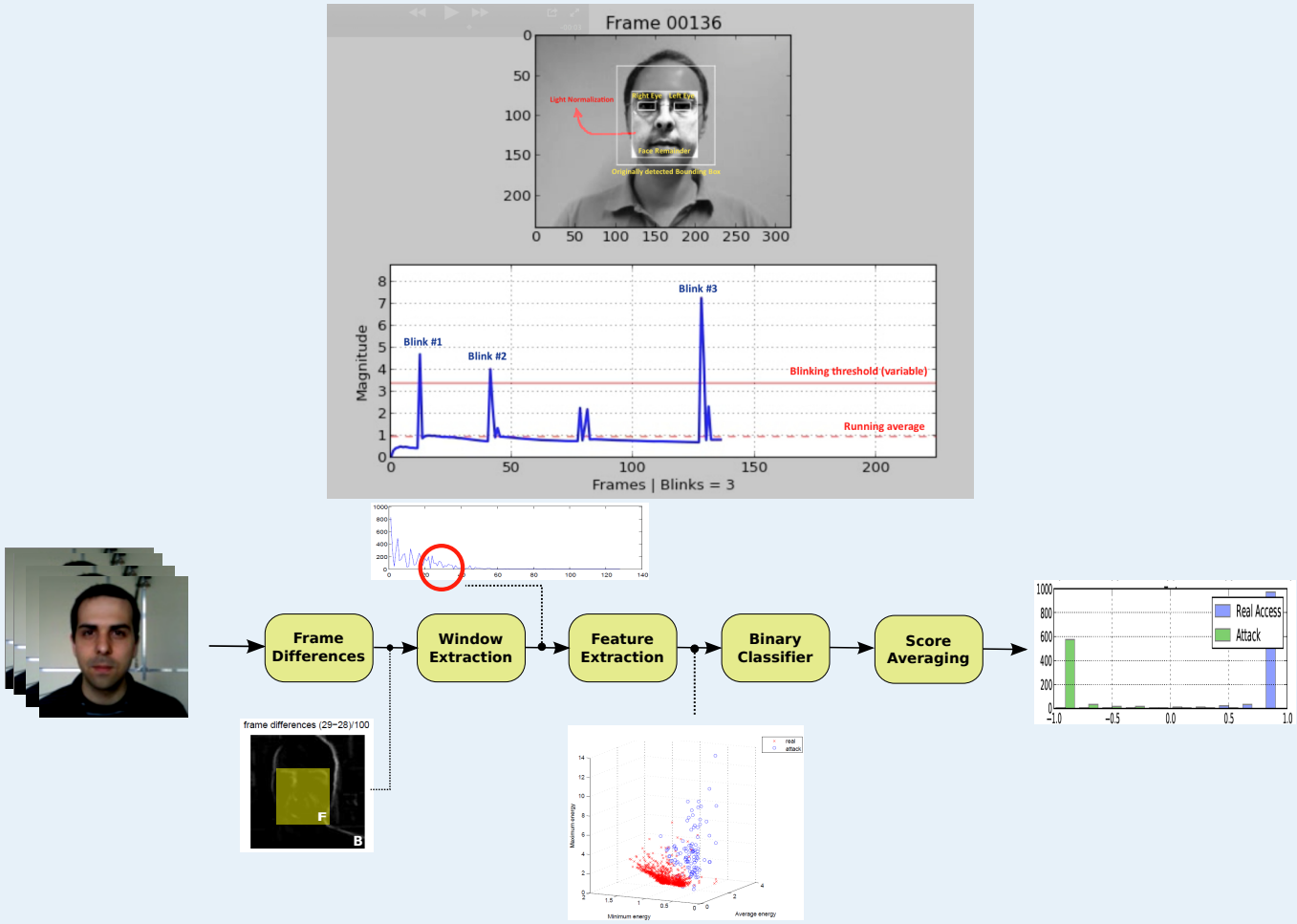
2D Face PA: DeepFakes

Realistic face swap of two people in videos using a pre-trained Generative Adversarial Network (GAN)

- Can DeepFake videos fool face recognition?
- How to detect DeepFakes?

Presentation Attack Detection (PAD)

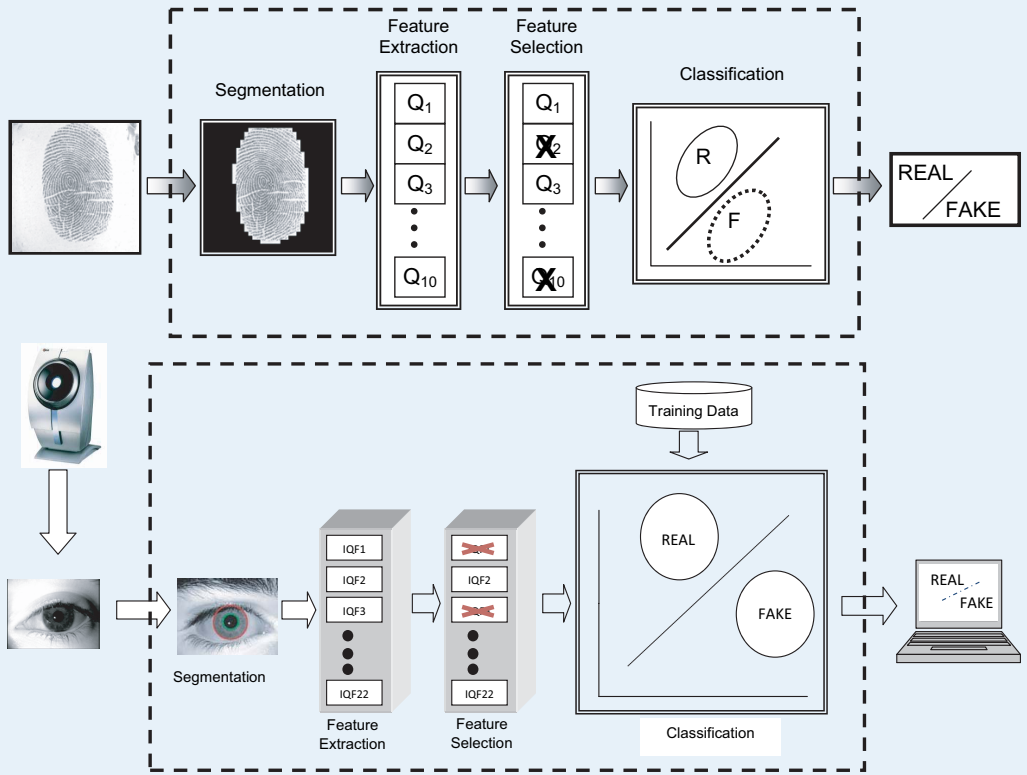
Face PAD [32]



using eye blinking or motion

[32] *Motion-Based Counter-Measures to Photo Attacks in Face Recognition*, A. Anjos and S. Marcel, IET

Fingerprint/Iris PAD [33]

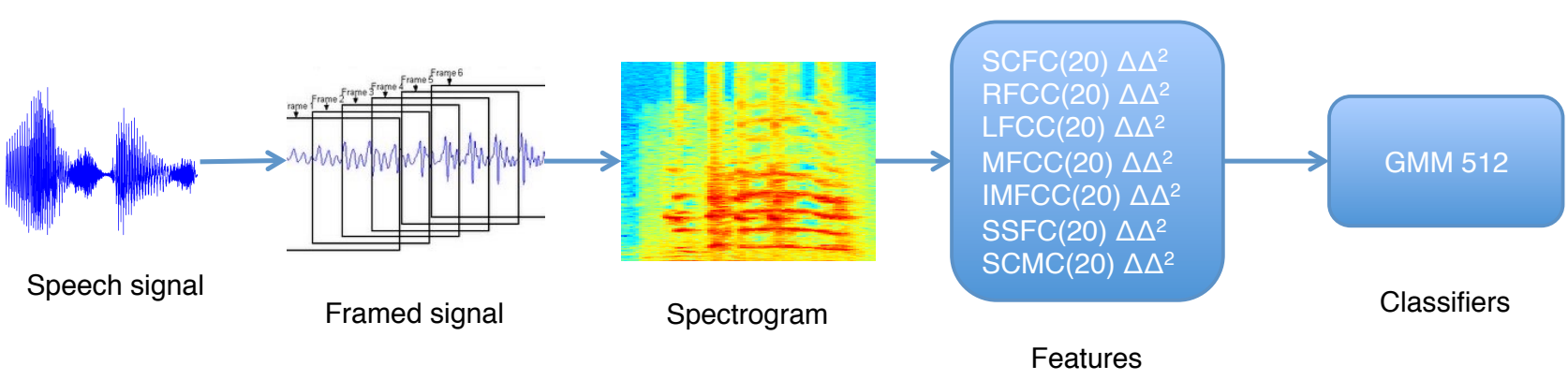


using generic image quality measures

[33] *Image quality assessment for fake biometric detection: Application to iris, fingerprint and face recognition*, J. Galbally, S. Marcel, and J. Fierrez, IEEE TIP, 23(2):710–724, 2014.

PAD

Voice PAD [34]



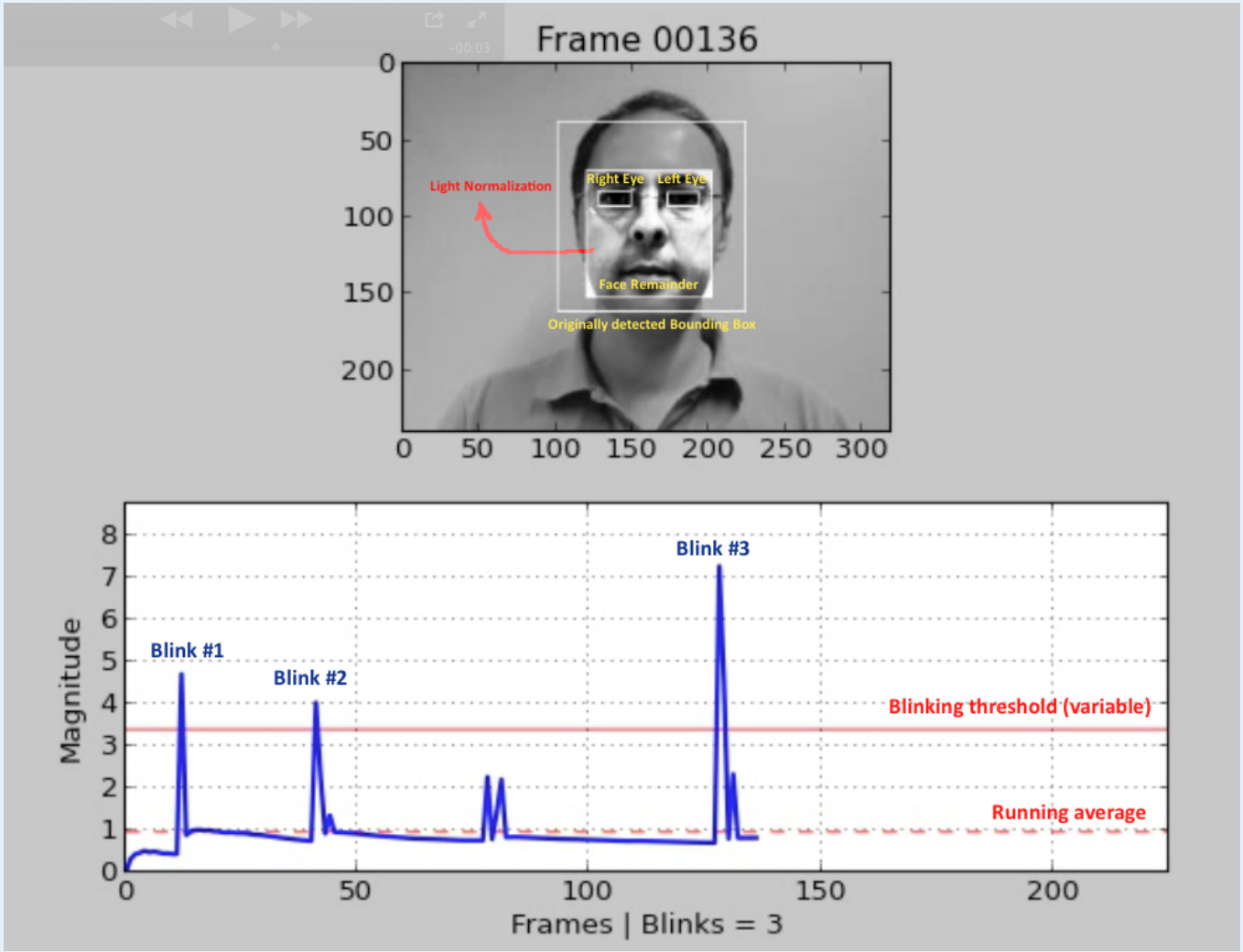
using cepstral-based features

[34] *Joint operation of voice biometrics and presentation attack detection*, P. Korshunov and S. Marcel, IEEE BTAS, 2016.

Face Presentation Attack Detection

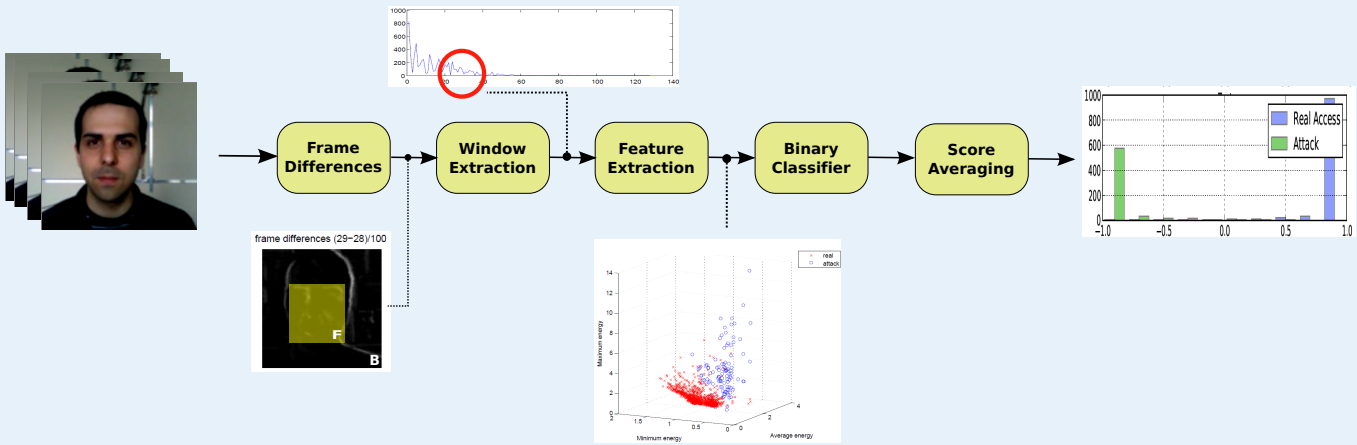
Face PAD

Eye-blinking



Face PAD

Motion [35]

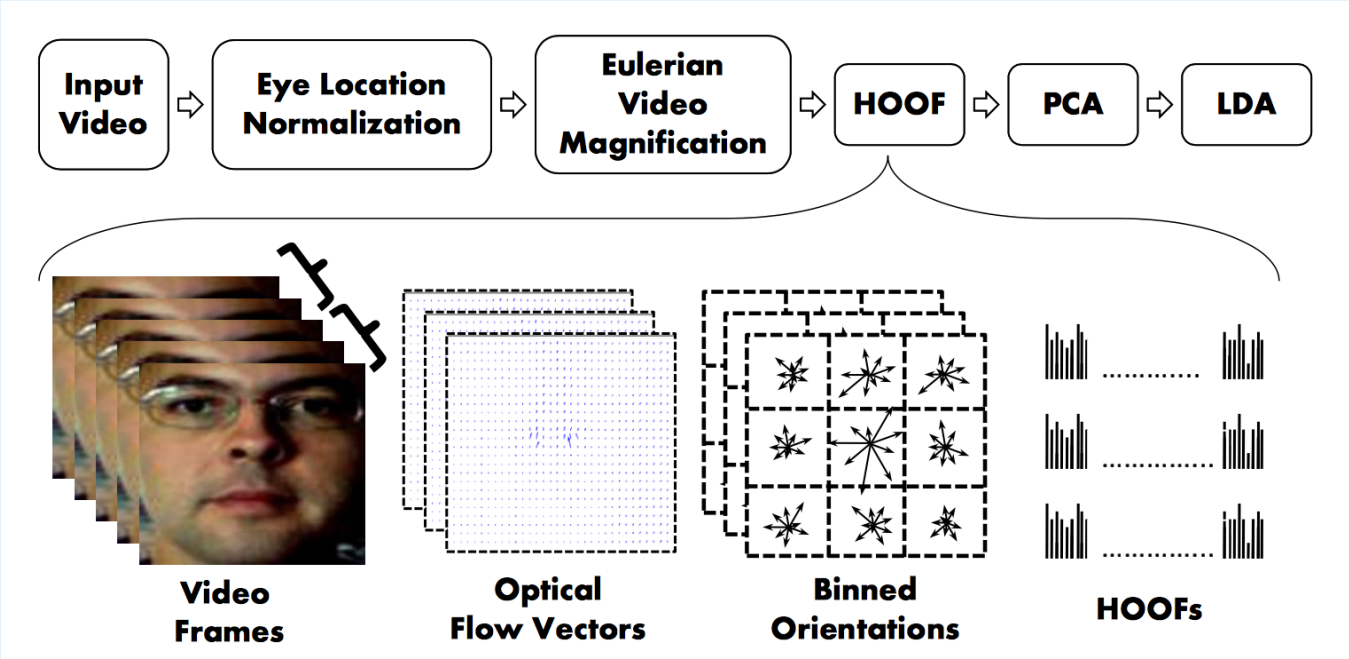


- use statistics of optical-flow between consecutive frames to detect print-attacks
- HTER (Half-Total Error Rate) on test data: 1.52%

[35] *Motion-Based Counter-Measures to Photo Attacks in Face Recognition*, A. Anjos and S. Marcel, IET Biometrics, 2013.

Face PAD

Motion [36]

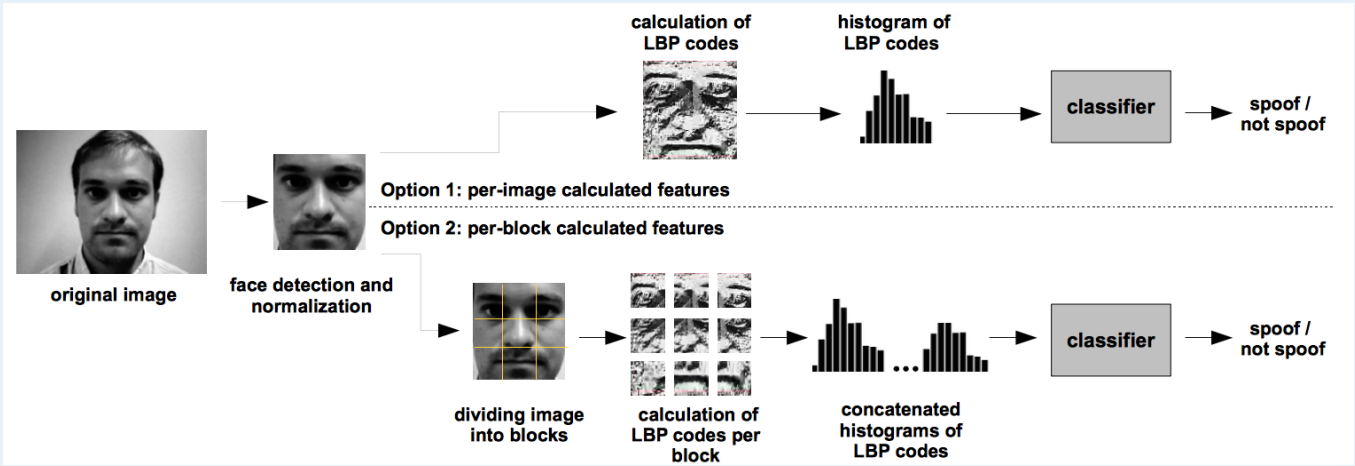


- use LBP and optical-flow to detect print-attacks and replay-attacks
- HTER: Print-attacks: 0% ∼ ∼ Replay-attacks: 1.25%

[36] *Computationally efficient face spoofing detection with motion magnification*, Bharadwaj et al., CVPR, 2013.

Face PAD

Texture analysis [37]



- use LBP in 3 dimensions (LBP-TOP) to differentiate between real and spoof face presentations
- HTER (Print and Replay attacks): 15%

[37] *On the effectiveness of local binary patterns (LBP) in face anti-spoofing*, Chingovska et al., BIOSIG, 2012.

Face PAD

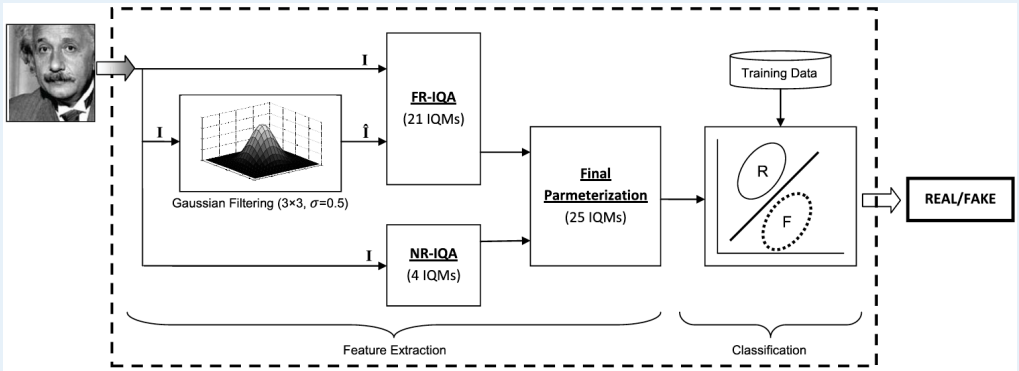
Frequency analysis [38]

- use LBP to detect the presence of moir'{e} patterns
- HTER on Replay-attack: 6%

[38] *Live face video vs. spoof face video: use of moiré patterns to detect replay video attacks*, Patel et al., ICB, 2015.

Face PAD

Image Quality Analysis [39]



- use 25 well known image quality measures for gray-level images to train a 2-class classifier

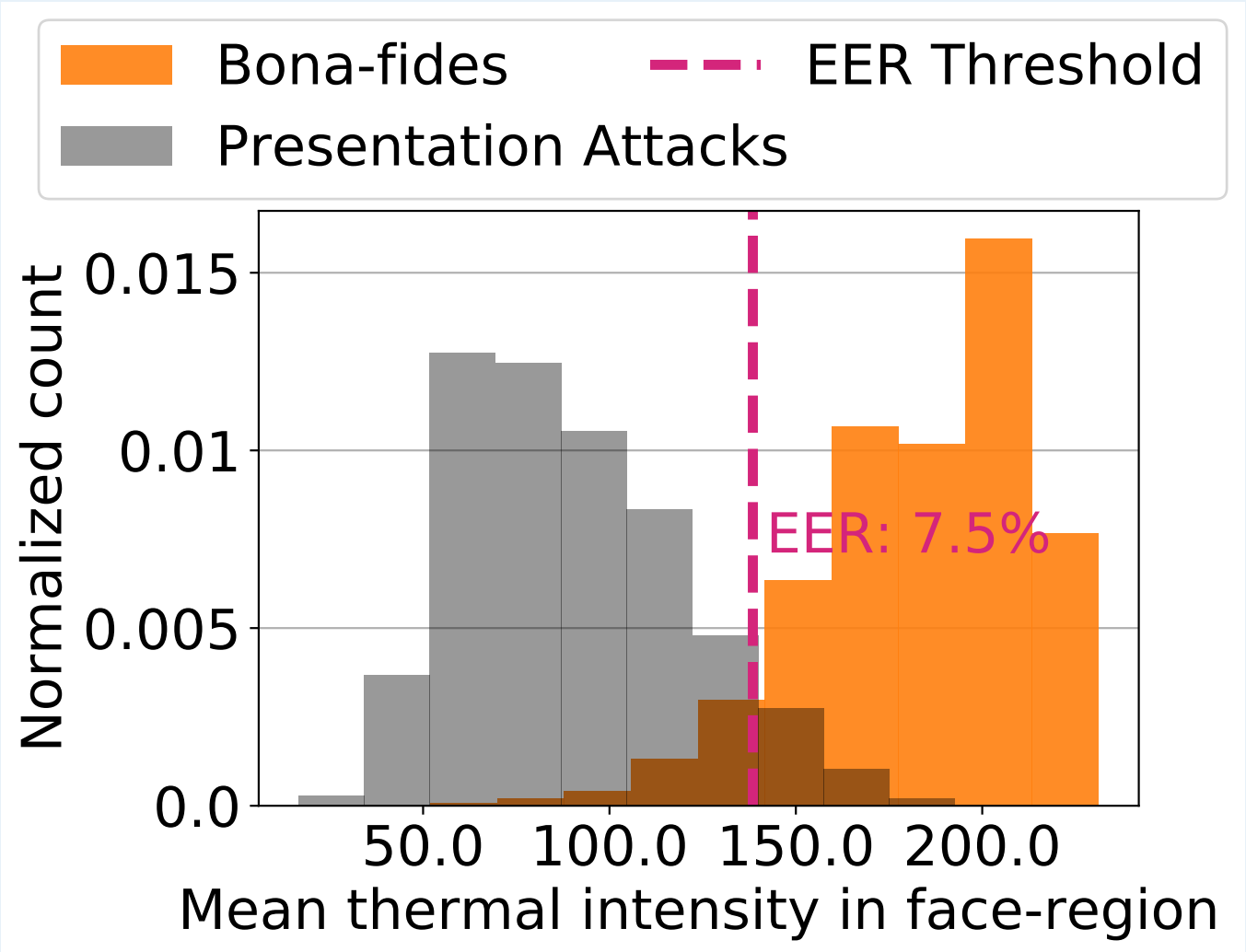
1	FR	MSE	Mean Squared Error	[29]	$MSE(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j})^2$
2	FR	PSNR	Peak Signal to Noise Ratio	[30]	$PSNR(\mathbf{I},\hat{\mathbf{I}}) = 10\log(\frac{\max(\mathbf{I}^2)}{MSE(\mathbf{I},\hat{\mathbf{I}})})$
3	FR	SNR	Signal to Noise Ratio	[31]	$SNR(\mathbf{I},\hat{\mathbf{I}}) = 10\log(\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}{N\cdot M\cdot MSE(\mathbf{I},\hat{\mathbf{I}})})$
4	FR	SC	Structural Content	[32]	$SC(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\hat{\mathbf{I}}_{i,j})^2}$
5	FR	MD	Maximum Difference	[32]	$MD(\mathbf{I},\hat{\mathbf{I}}) = \max\lvert\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\rvert$
6	FR	AD	Average Difference	[32]	$AD(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j})$
7	FR	NAE	Normalized Absolute Error	[32]	$NAE(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\rvert}{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{I}_{i,j}\rvert}$

- HTER: Replay-attack: 15.4%

[39] *Image quality assessment for fake biometric detection: application to iris, fingerprint, and face recognition*, Galbally et al. , IEEE TIP, 2014.

Face PAD

Thermal [40]



[40] *Spoofing Deep Face Recognition with Custom Silicone Masks*, S. Battacharjee and al., BTAS, 2018.

Face PAD

Using rPPG [41]

- Surpassed state-of-the-art in rPPG-based PAD on 4 datasets (HTER)
- Reliable detection of various attacks
- Main challenge: accurate pulse signal for real accesses

[41] *Pulse-based Features for Face Presentation Attack Detection*, G. Heusch and al., BTAS, 2018.

Face PAD

DeepFakes detection

- DeepFakes can be detected with basic Image Quality metrics
- Good accuracy in LQ videos (5% HTER) but it is more difficult in HD (15% HTER)

Face PAD

Open source (face) PAD framework

Open source tools to run comparable and reproducible generic PAD experiments

http://pythonhosted.org/bob.pad.base

eg. face PAD with native support for Replay Attack, Replay Mobile and MSU MFSD

source code: https://gitlab.idiap.ch/bob/bob.pad.face
doc: https://www.idiap.ch/software/bob/docs/bob/bob.pad.face/master/index.html

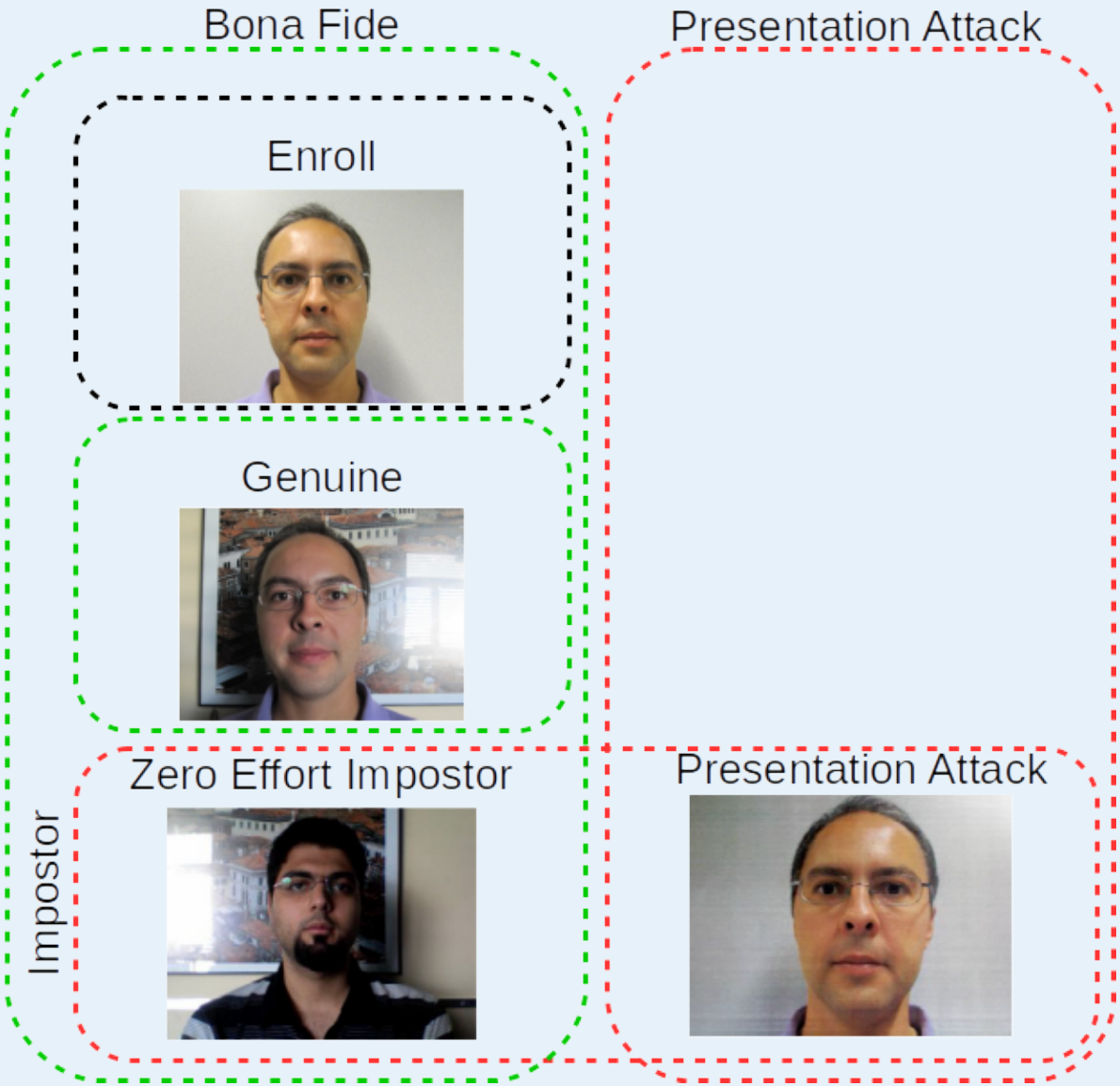
based on the Bob signal-processing and machine learning toolbox

https://www.idiap.ch/software/bob/

Biometrics and PAD

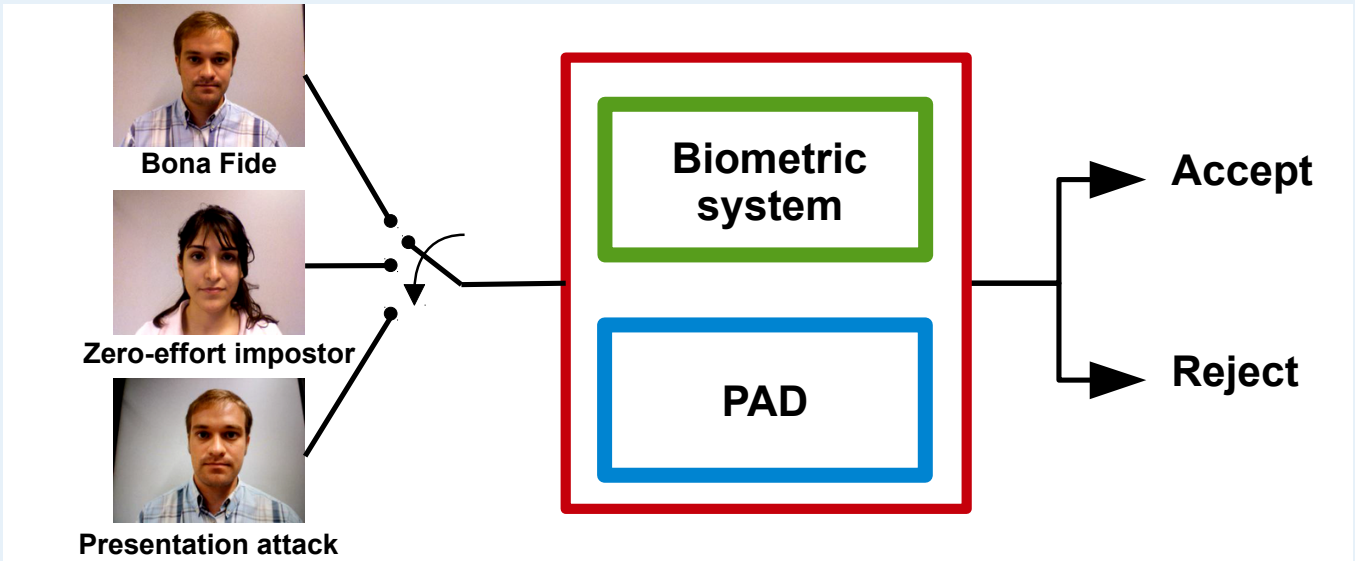
Biometrics and PAD

Bona Fide, Zero Effort Impostor and PA



Biometrics and PAD

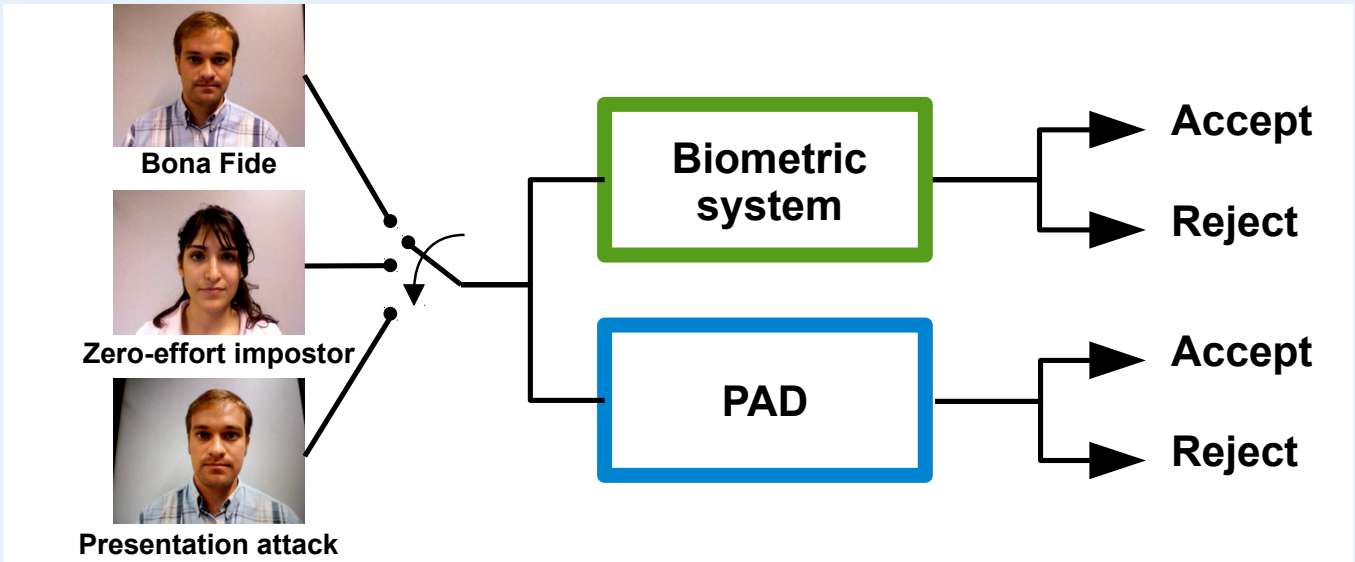
Two separate components



- A biometric sub-system
- A PAD sub-system

Biometrics and PAD

Two separate components

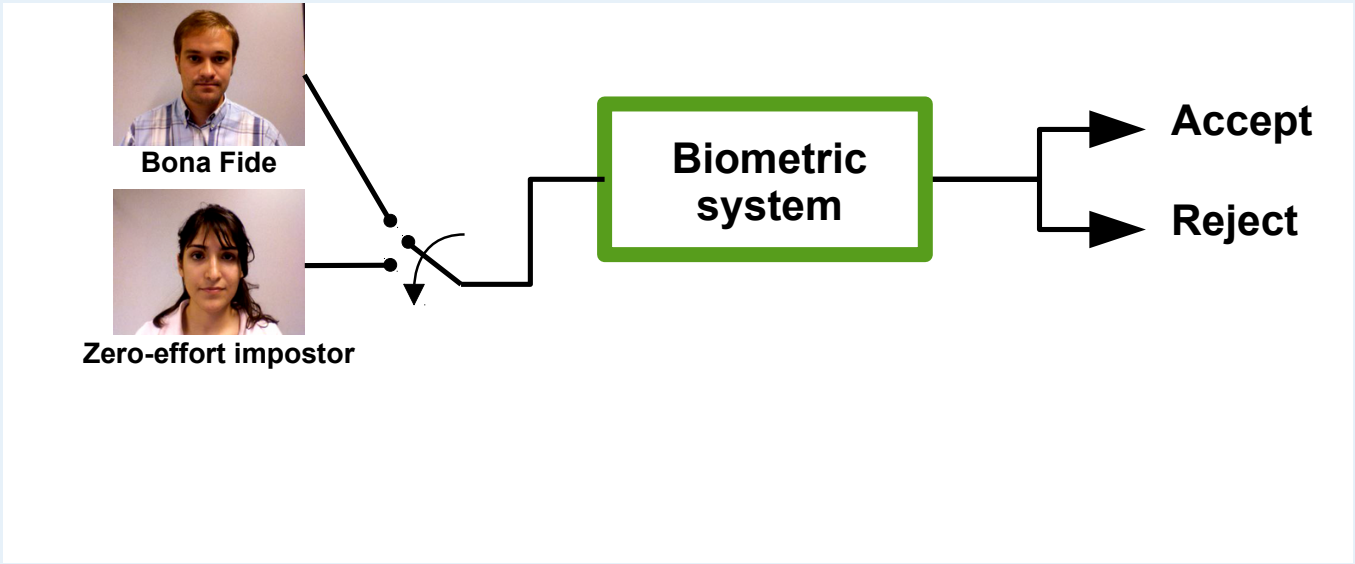


Overall

- Accept: genuine and bona fide
- Reject: zero-effort impostor and presentation attack

Biometrics and PAD

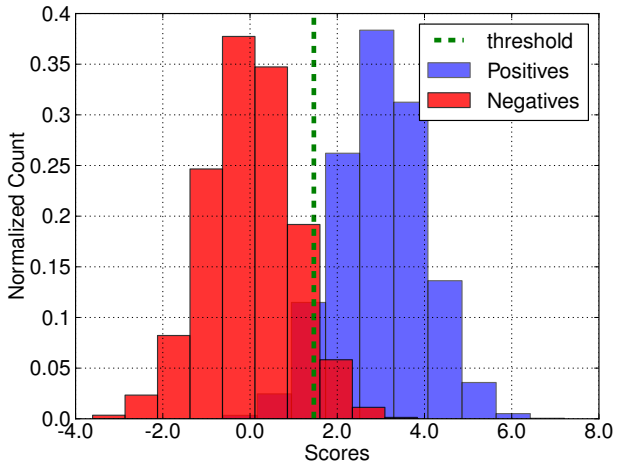
Biometric sub-system: a binary classifier

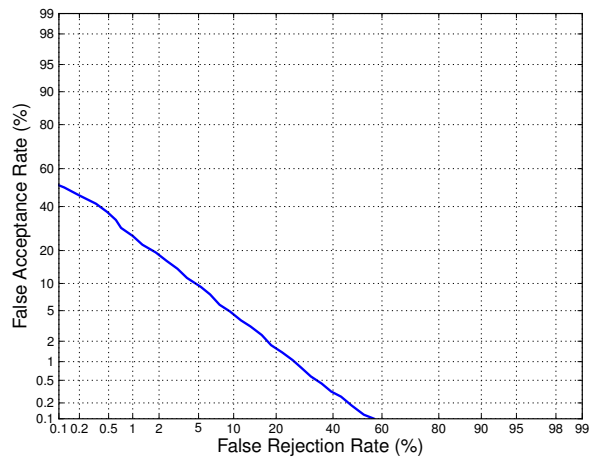


We measure 2 errors:

- False Match Rate (FMR): zero-effort impostors incorrectly matched as genuines – also referred to as False Acceptance Rate (FAR)
- False Non-Match Rate (FNMR): genuines not matched – also referred to as False Rejection Rate (FRR)

Biometric sub-system: a binary classifier



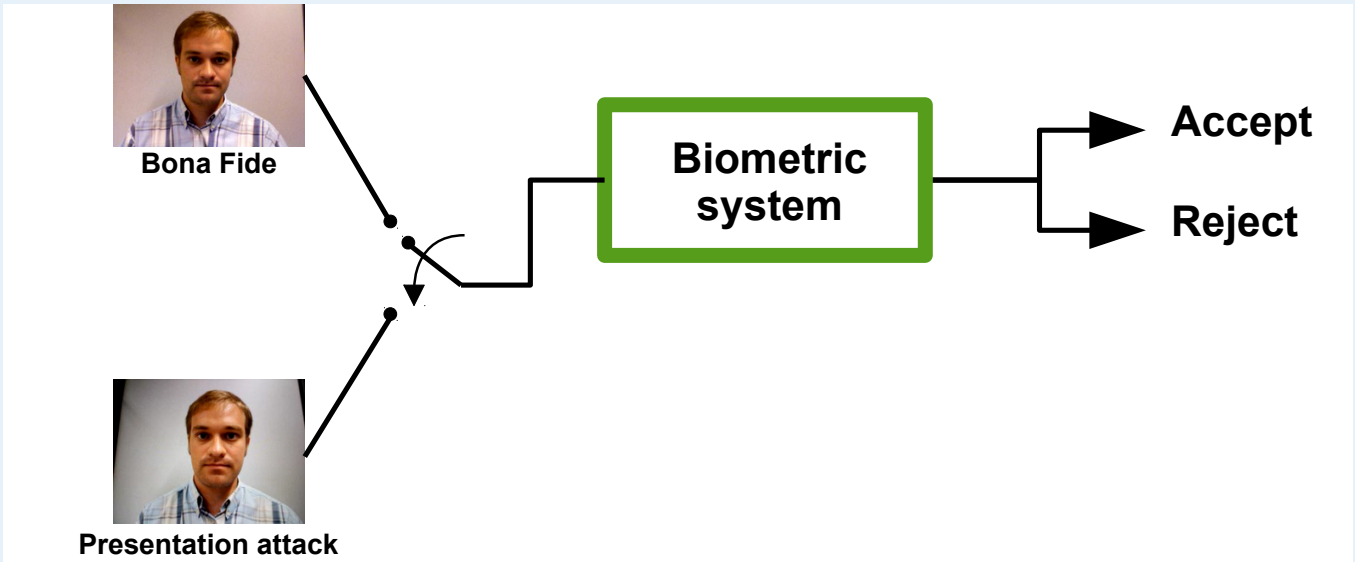


We measure 2 errors:

- False Match Rate (FMR): zero-effort impostors incorrectly matched as genuines – also referred to as False Acceptance Rate (FAR)
- False Non-Match Rate (FNMR): genuines not matched – also referred to as False Rejection Rate (FRR)

Biometrics and PAD

Biometric sub-system: a binary classifier

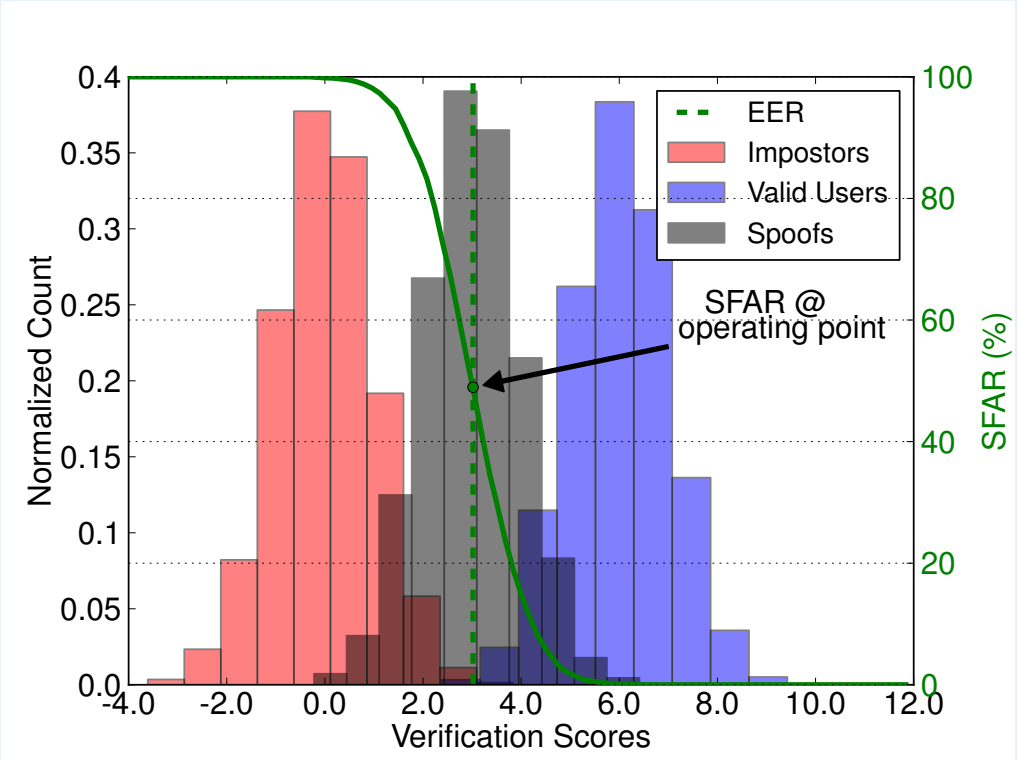


We measure the vulnerability as:

- Impostor Attack Presentation Match Rate (IAPMR): PAs which are accepted as genuine samples – also referred to as Spoofing False Accept Rate (SFAR)

Biometrics and PAD

Biometric sub-system: a binary classifier

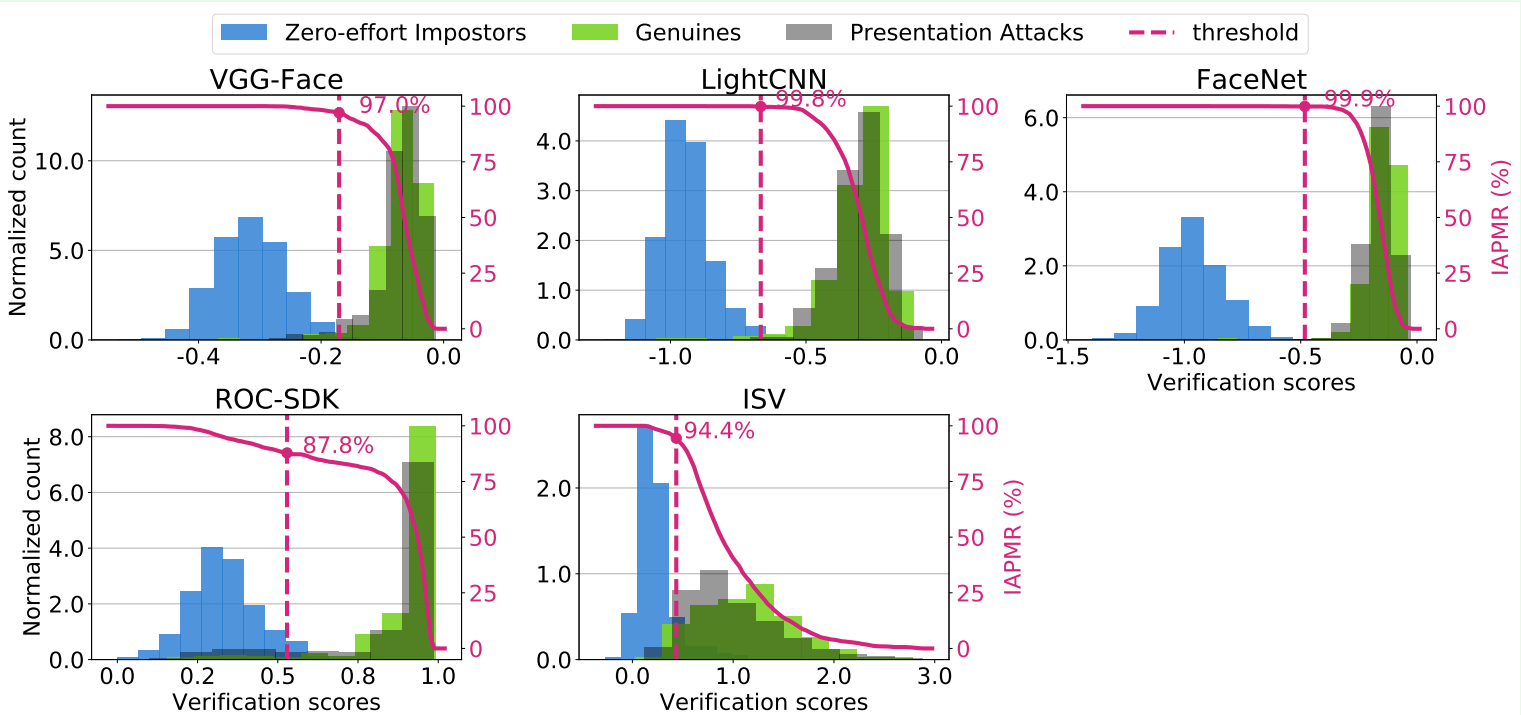


We measure the vulnerability as:

- Impostor Attack Presentation Match Rate (IAPMR): PAs which are accepted as genuine samples – also referred to as Spoofing False Accept Rate (SFAR)

Biometrics and PAD

IAPMR Deep Face Recognition (print and replay PA) [42]

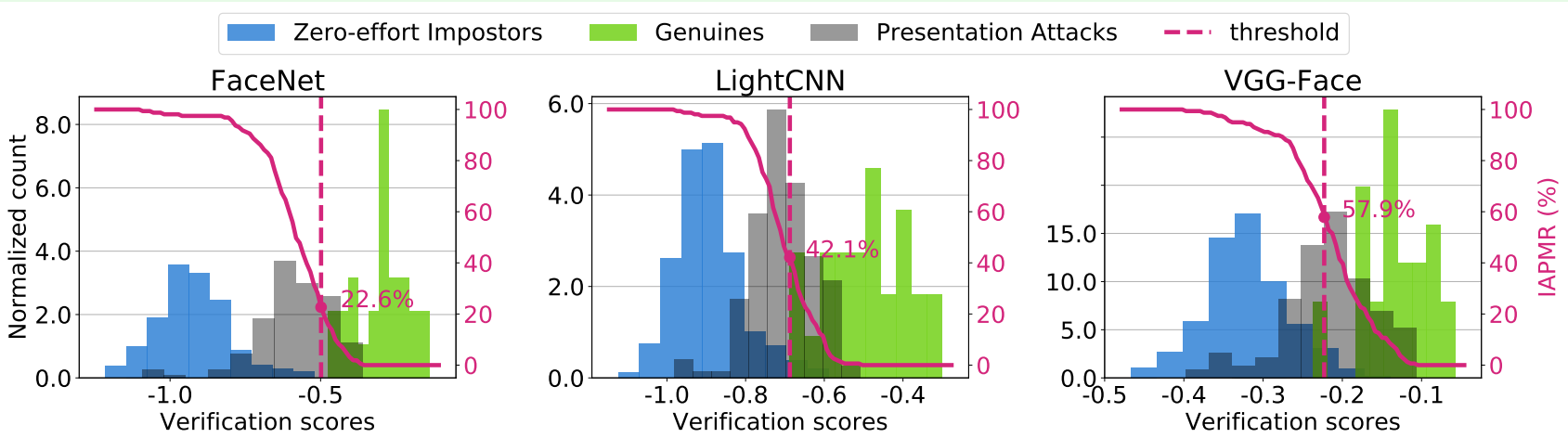


- FR systems using CNN are very vulnerable (up to 99% IAPMR)
- Improved FR accuracy translates into improved vulnerability

[42] *Deeply vulnerable: a study of the robustness of face recognition to presentation attacks*, A. Mohammadi and al., IET Biometrics, 2017.

Biometrics and PAD

IAPMR Deep Face Recognition (silicone masks PA) [43]

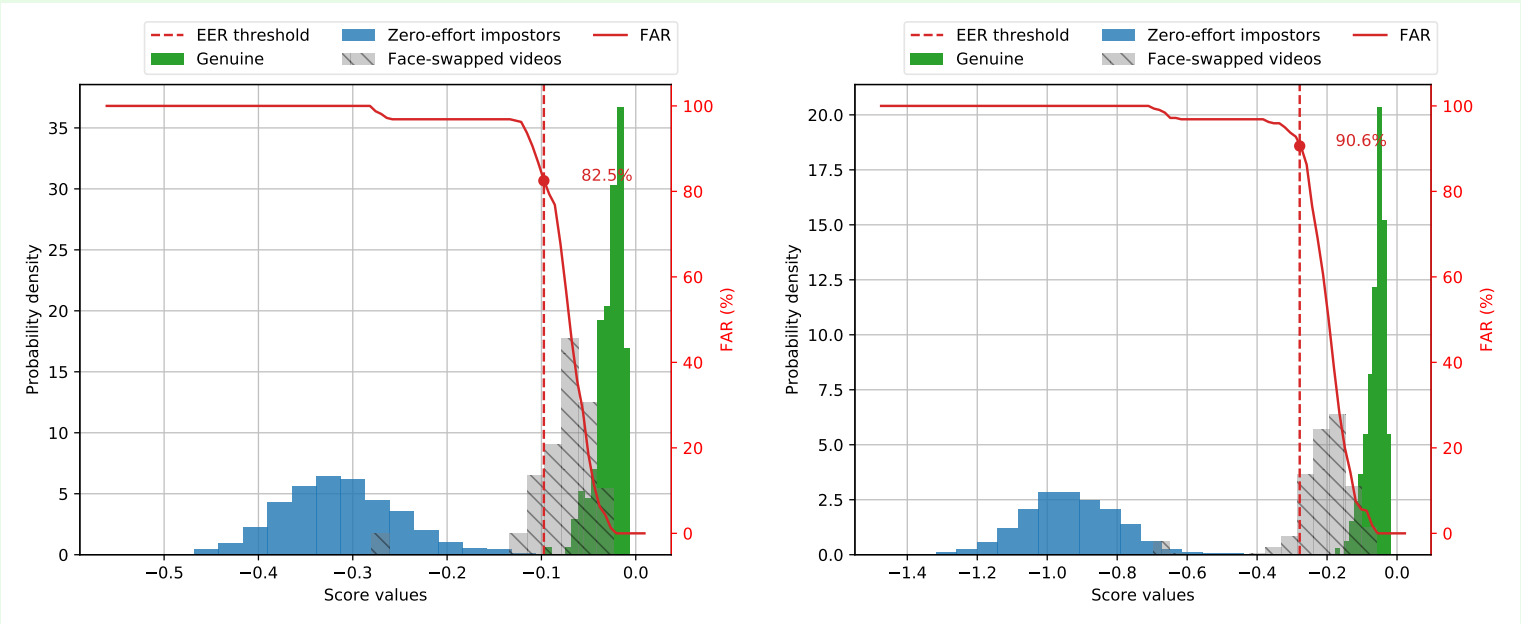


- FR systems using CNN are vulnerable as well (up to 45% IAPMR)
- IAPMR is 10 times greater than FMR

[43] *Spoofing Deep Face Recognition with Custom Silicone Masks*, S. Battacharjee and al., BTAS, 2018.

Biometrics and PAD

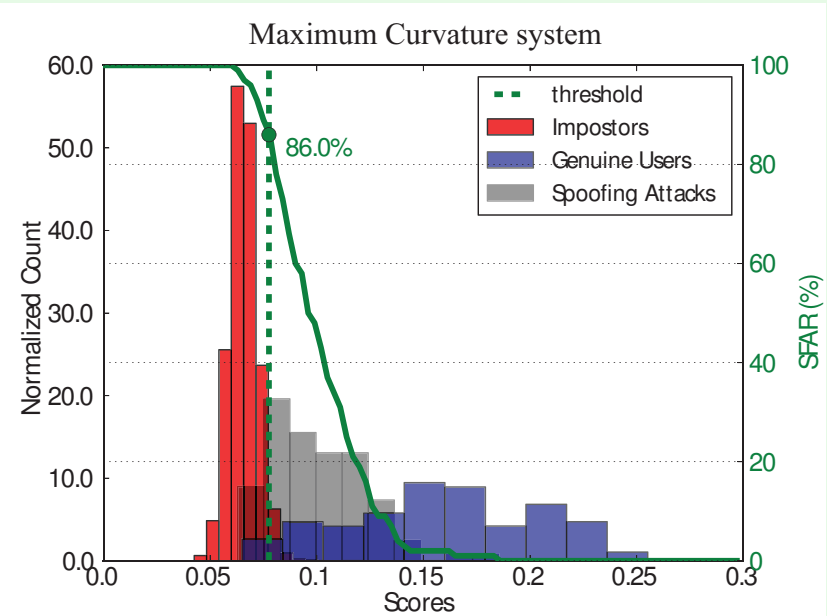
IAPMR DeepFakes (unpublished)

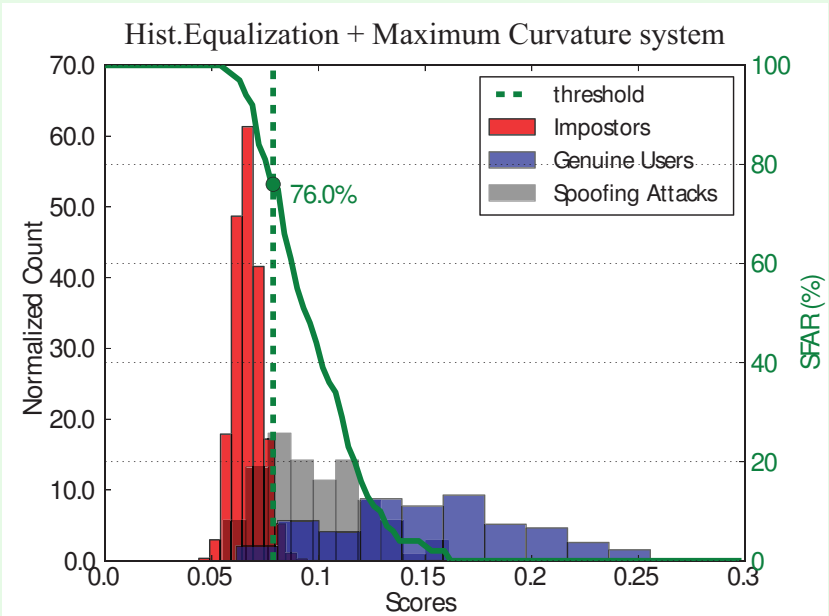


CNN-based FR systems (VGG, Facenet) are vulnerable to DeepFakes (up to 90%)

Biometrics and PAD

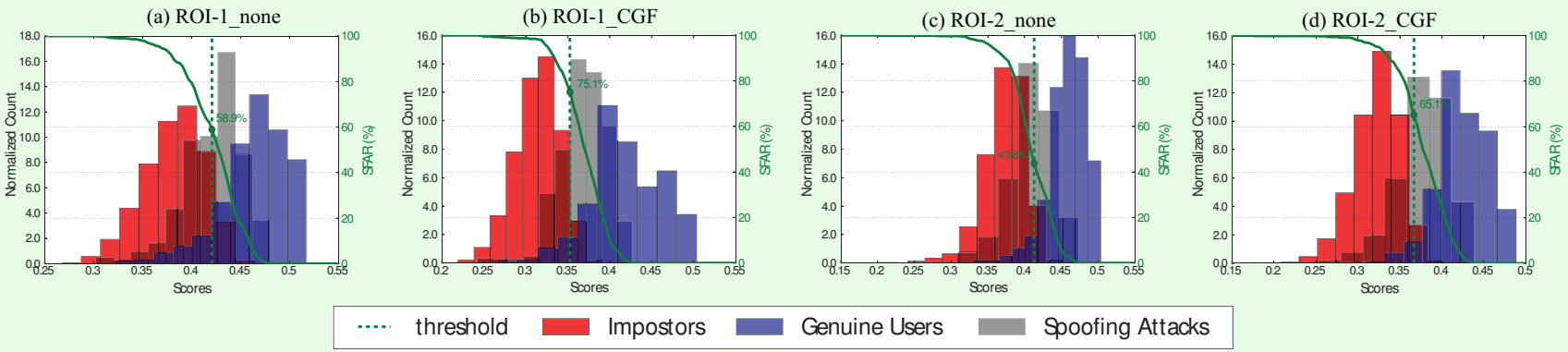
IAPMR Fingervein





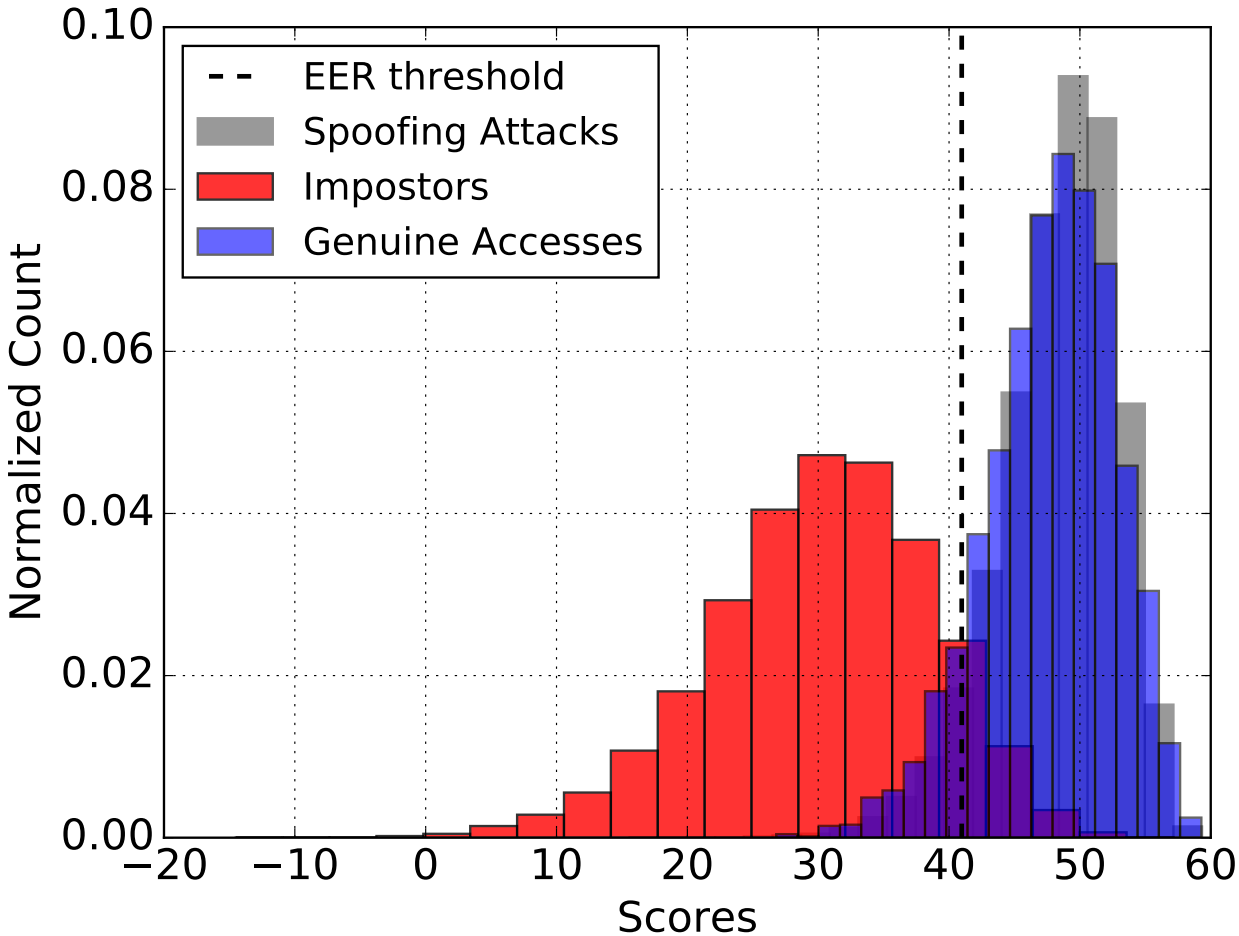
Biometrics and PAD

IAPMR Palmvein



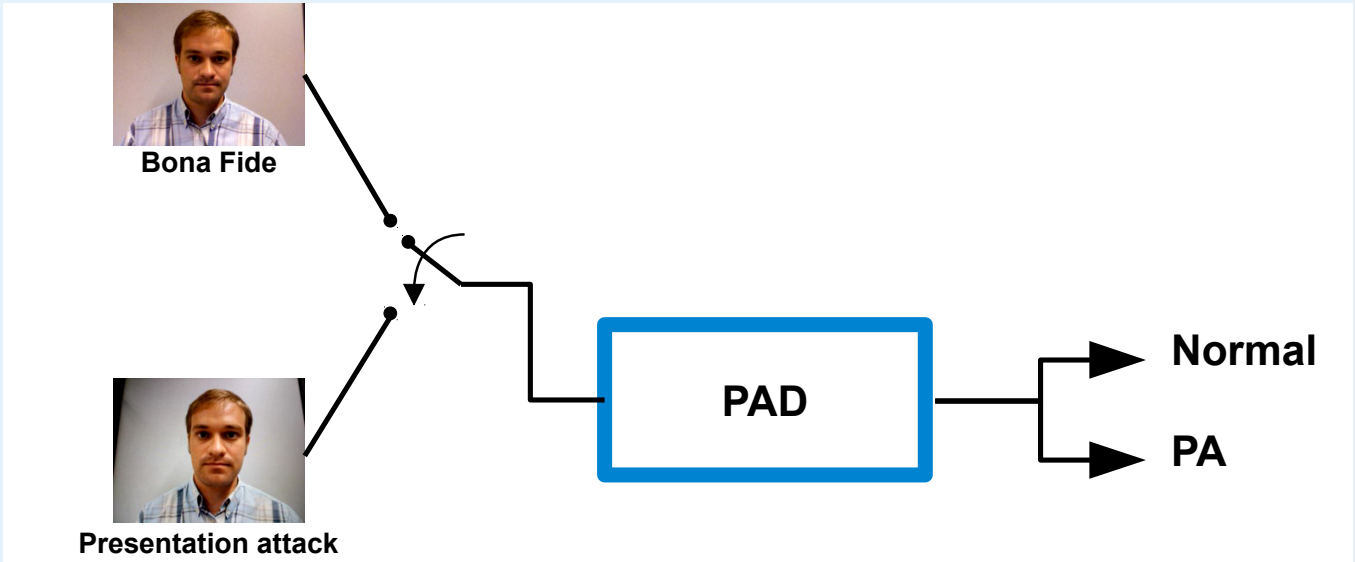
Biometrics and PAD

IAPMR Voice



Biometrics and PAD

PAD sub-system: a binary classifier



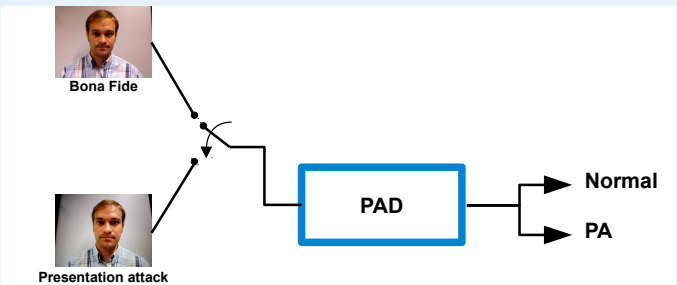
We measure 2 errors:

- Attack Presentation Classification Error Rate (APCER): PAs incorrectly classified as normal presentations
- Normal Presentation Classification Error Rate (NPCER): normal presentations incorrectly classified as PAs

Biometrics and PAD

PAD methods

- software-based: biometric data from the sensor is analysed to discriminate bona fide vs PA (eg. motion, texture)
- hardware-based: an additional sensor is used and its data analysed to discriminate bona fide vs PA (eg. temperature, pulse)
- challenge-response: the user interacts with the system (eg. prompted text in face/speaker recognition)



References

Books

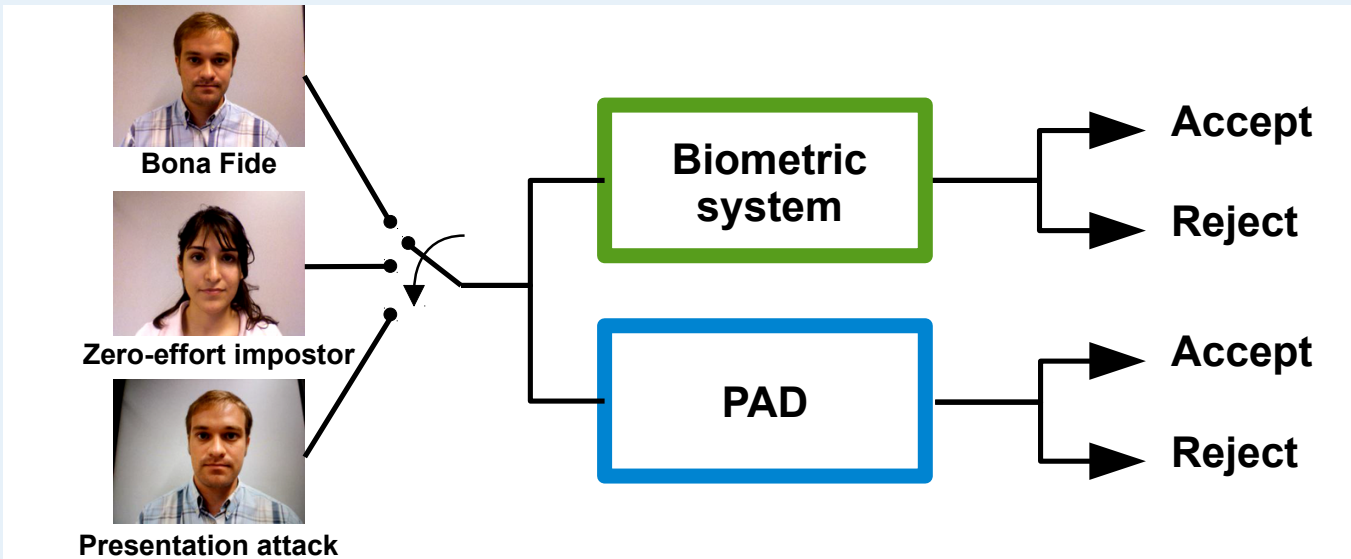
- Handbook of Biometric Anti-Spoofing (Ed1), S. Marcel and al. (2014)
- Handbook of Biometric Anti-Spoofing (Ed2), S. Marcel and al. (2019)

Papers

- Special Issue on Biometric Spoofing and Countermeasures, N. Evans and al. IEEE TIFS (2015).
- Special Issue on Biometric Security and Privacy, N. Evans and al., IEEE SPM (2015).
- Biometrics Evaluation under Spoofing Attacks, I. Chingovska and al., IEEE TIFS (2014).

Expected Performance and Spoofability Curve (EPSC)

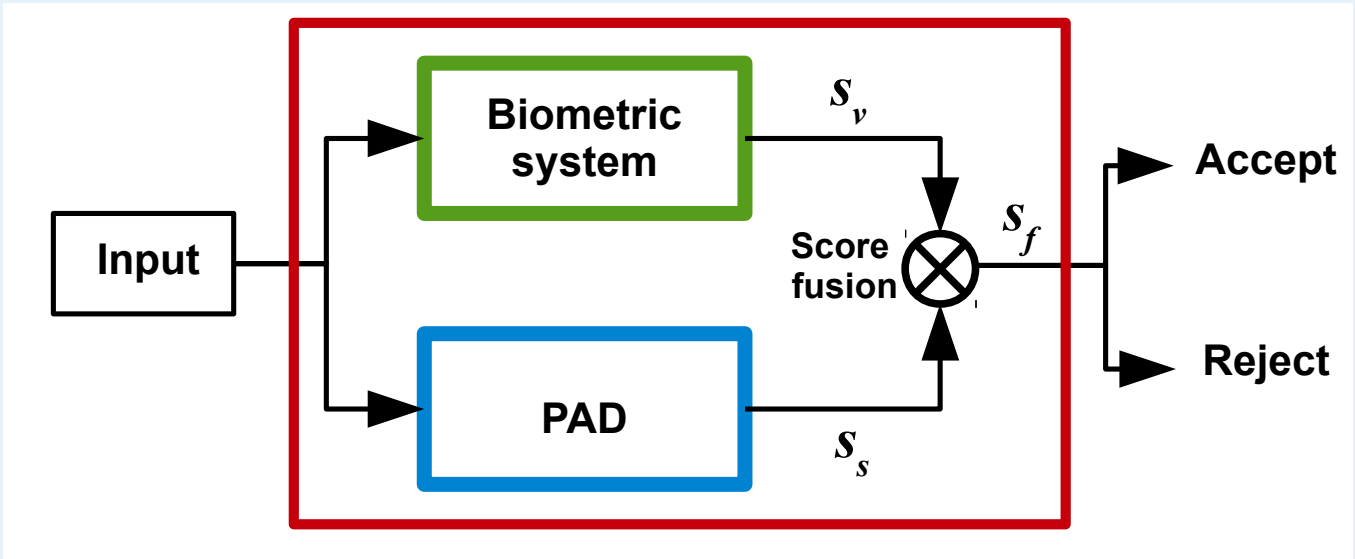
Two separate components



How to combine these two components ?

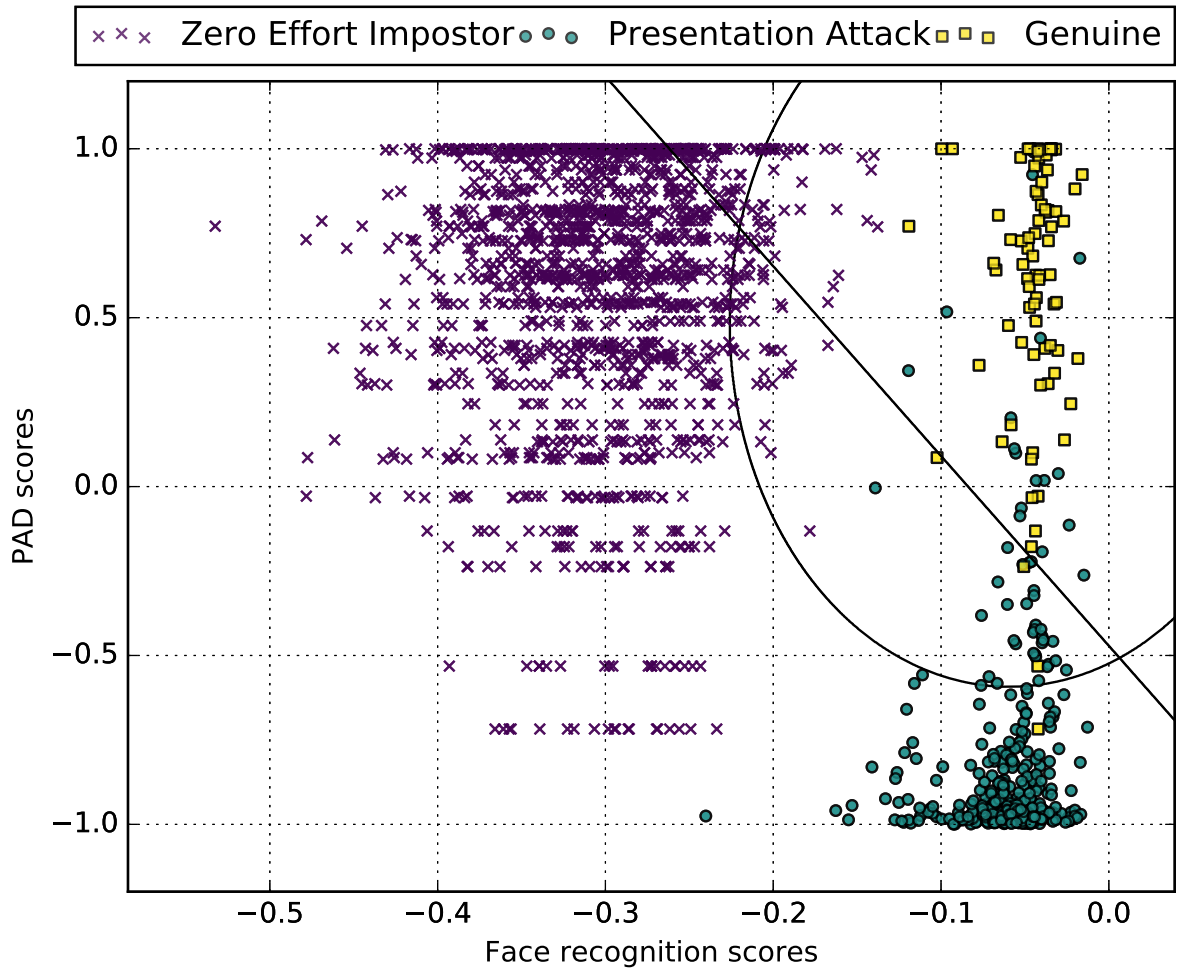
[44] *Biometrics Evaluation under Spoofing Attacks*, I. Chingovska and al., IEEE TIFS, 2014.

Fusion scheme

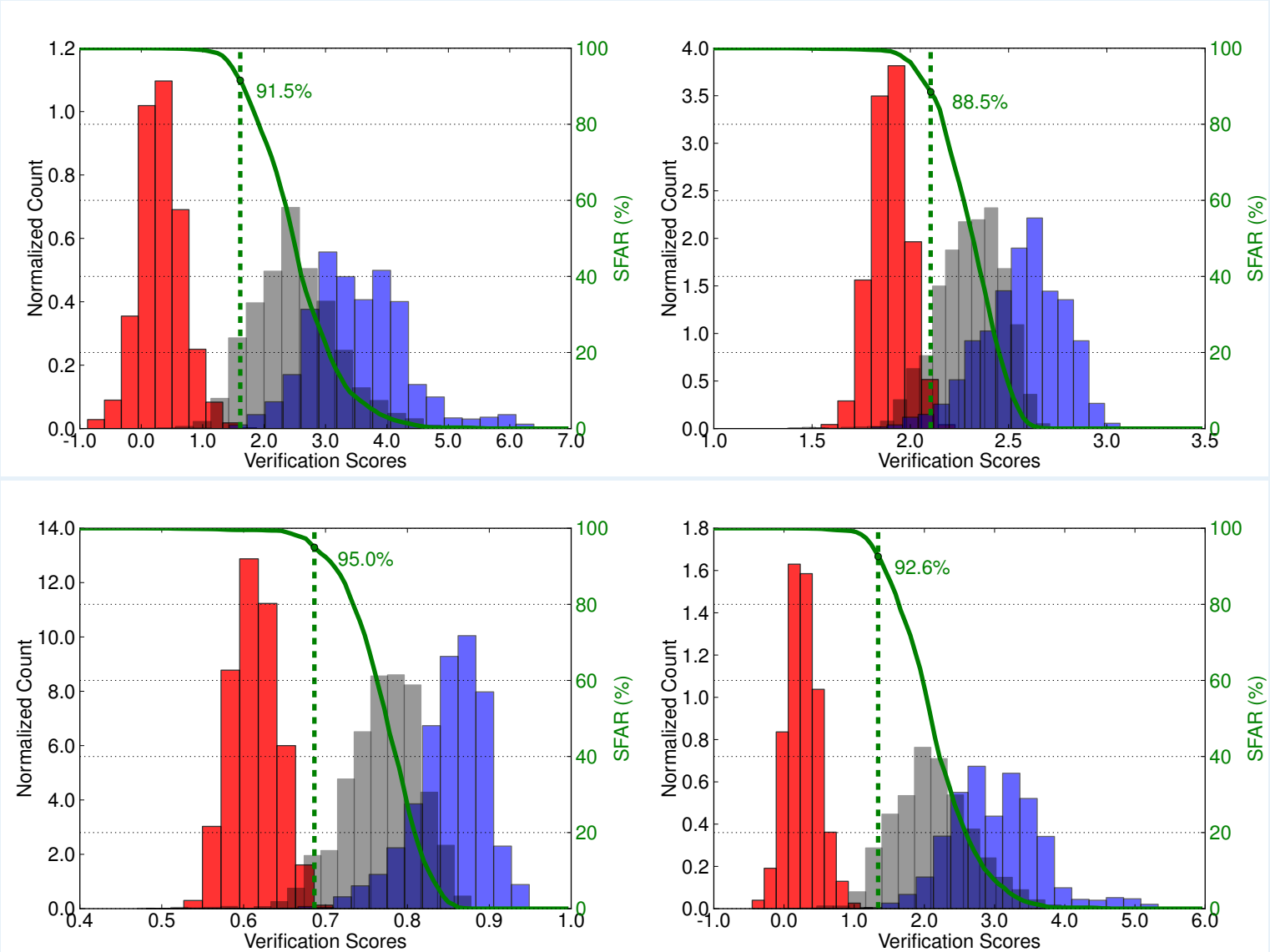


One unique threshold to be determined

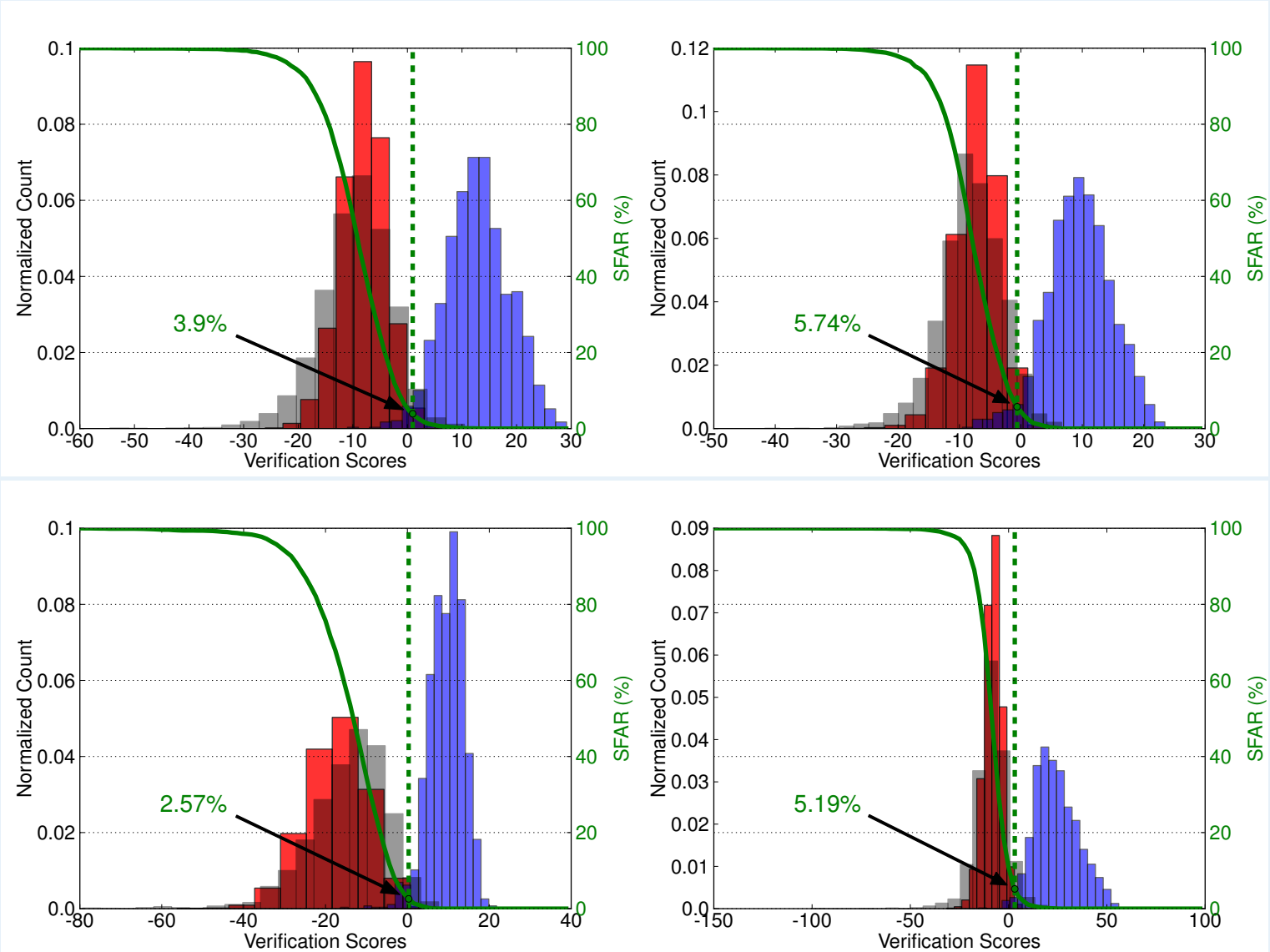
Fusion scheme



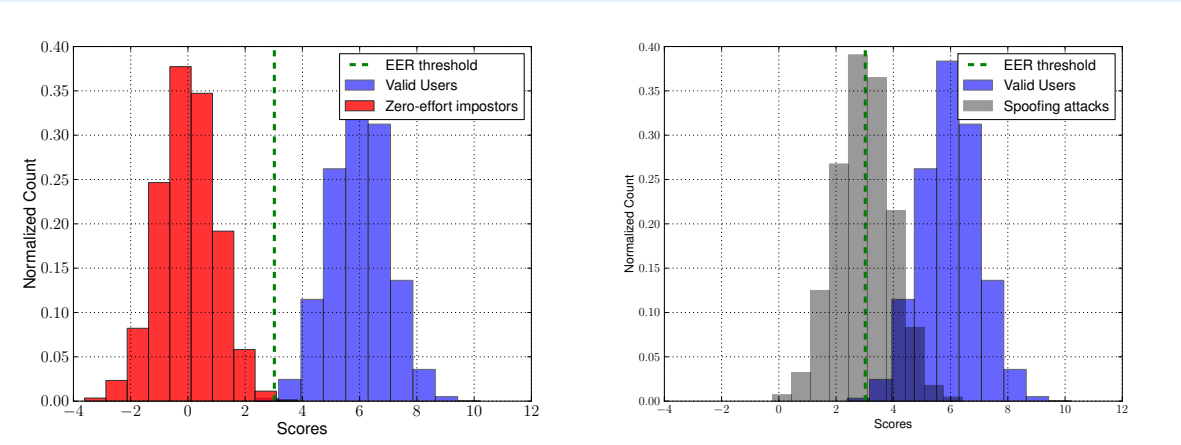
Biometric systems without PAD (no fusion)



Biometric systems + PAD (fusion)



Measuring the performance



We still measure 3 errors:

- False Rejection Rate (FRR): % of genuine users falsely rejected
- False Acceptance Rate (FRR): % of zero-effort impostors falsely accepted
- Spoof False Acceptance Rate (SFAR): % of presentation attacks falsely accepted

EPSC

FAR_ω (development set)

Weighted error rate for the two negative classes (zero-effort impostors and presentation attacks):

$$\text{FAR}_\omega = (1-\omega) \cdot \text{FAR} + \omega \cdot \text{SFAR}$$

Determine τ_ω^* to minimize the difference between FAR_ω and FRR on the development set:

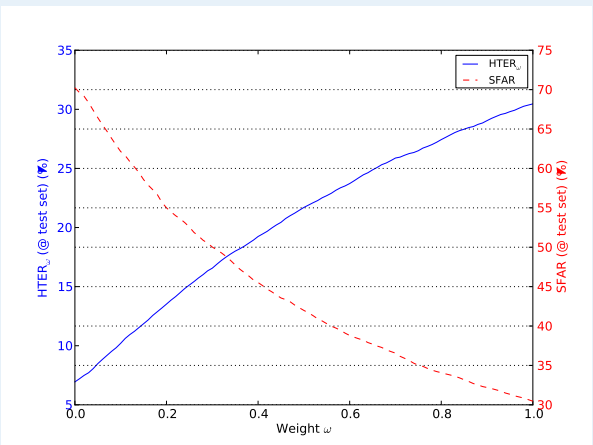
$$\tau_\omega^* = \arg \min_\tau |\text{FAR}_\omega(\tau, \mathcal{D}_{dev}) - \text{FRR}(\tau, \mathcal{D}_{dev})|$$

HTER_ω (test set)

Measuring both the verification performance and the spoofability of the system

$$\text{HTER}_\omega(\tau_\omega^*, \mathcal{D}_{test}) = \frac{\text{FAR}_\omega(\tau_\omega^*, \mathcal{D}_{test}) + \text{FRR}(\tau_\omega^*, \mathcal{D}_{test})}{2}$$

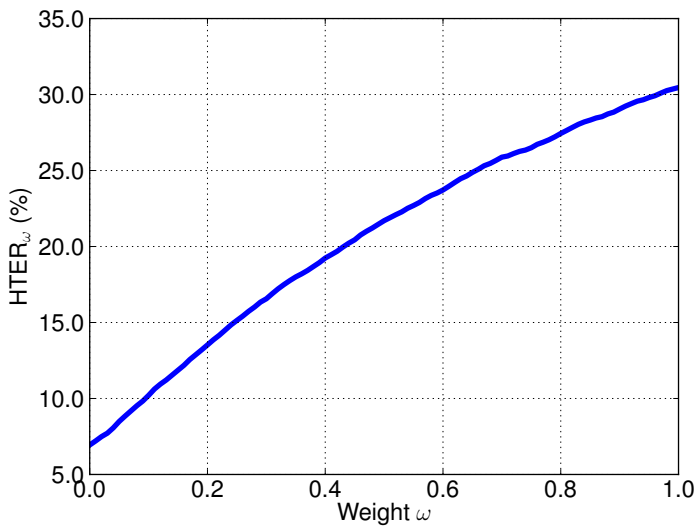
Ploting HTER_ω or SFAR

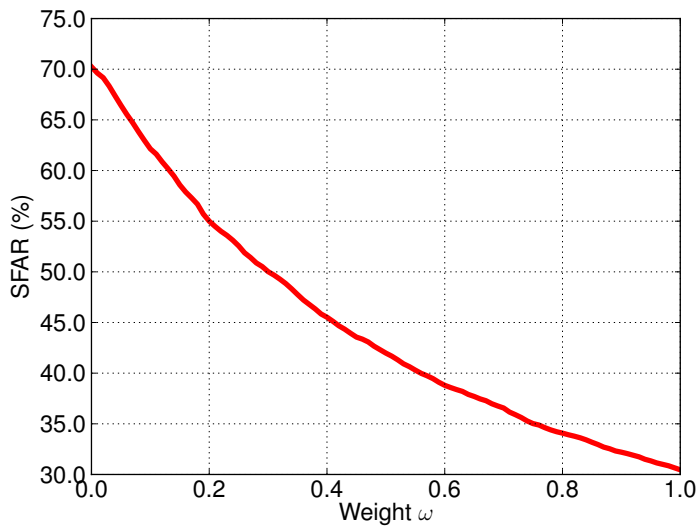


EPSC

EPSC in action

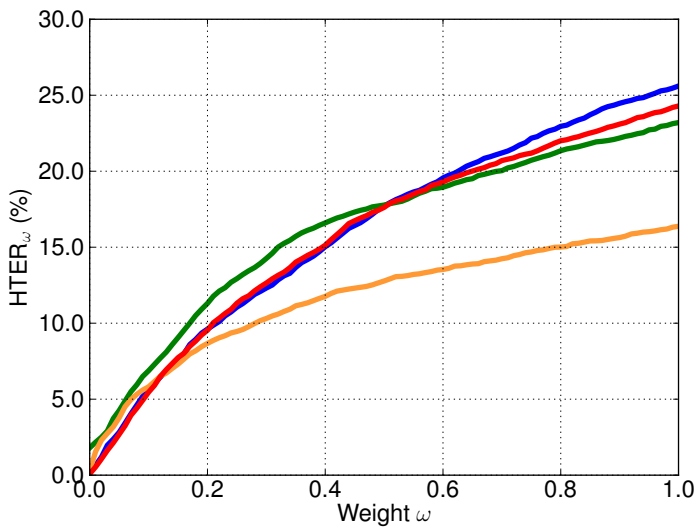
EPSC: HTER$_\omega$ and SFAR

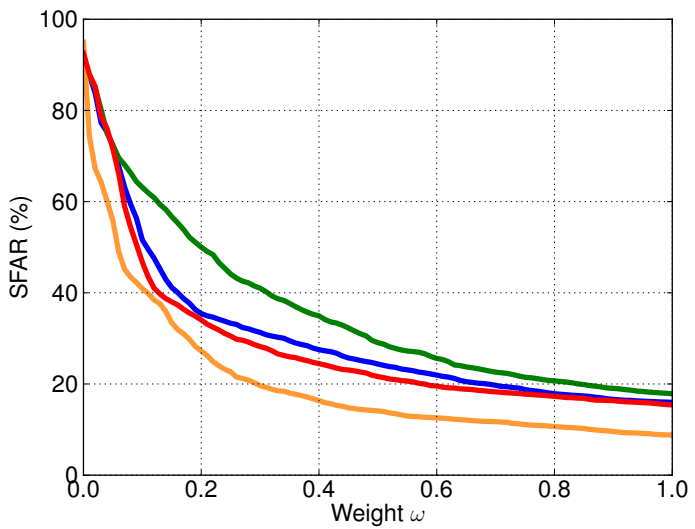




EPSC Examples

EPSC to compare biometric systems only

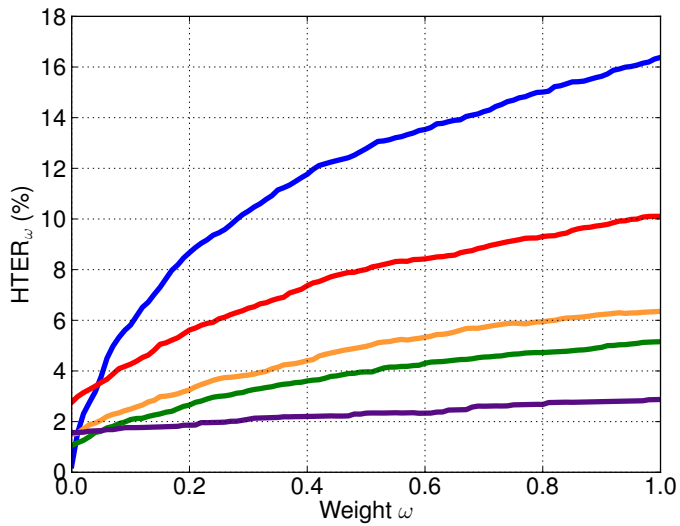


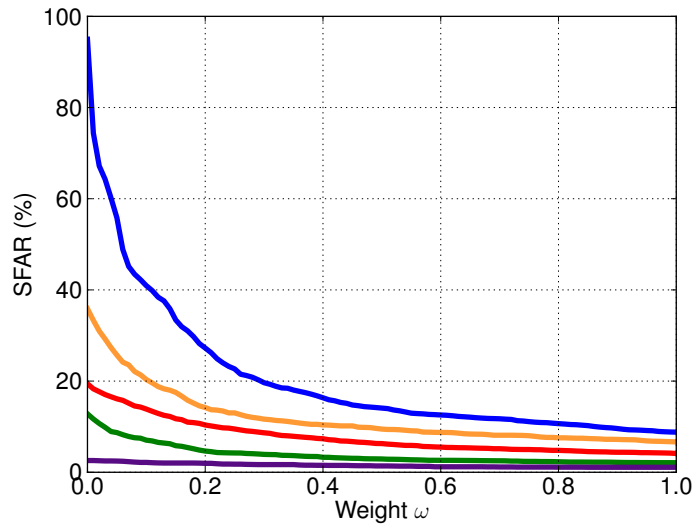


4 biometric systems (no PAD): using the orange subsequently

EPSC Examples

EPSC to compare PAD

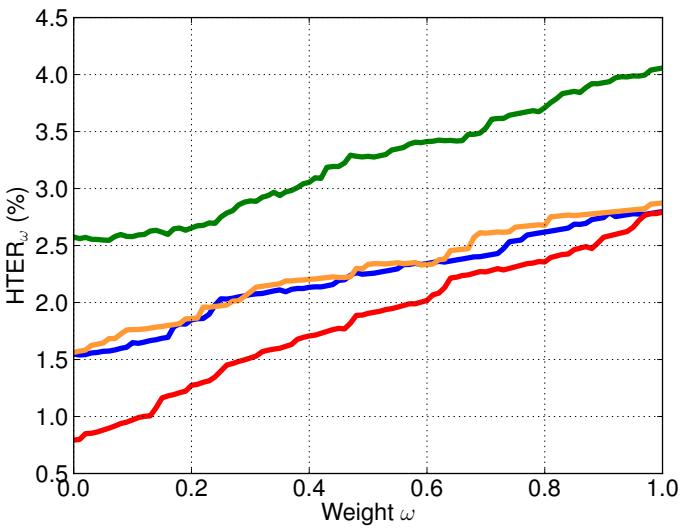


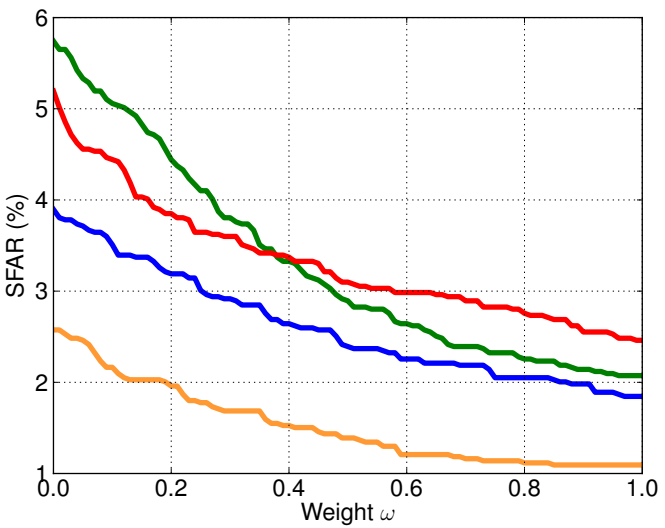


1 biometric system (blue), same system + 3 PADs (red, orange,green), same system + all PADs (purple)

EPSC Examples

EPSC to compare biometric systems fused with ALL PADs





4 biometric system + all PADs