

# Biometric Presentation Attack Detection

A tutorial

Dr Sébastien Marcel

January 12, 2020



# Outline

Introduction

Presentation Attacks in movies

Presentation Attacks in reality

Definitions

Presentation Attacks (PAs)

Understanding the Vulnerability to PAs

Face PAs

Presentation Attack Detection (PAD)



# Outline

## Introduction

Presentation Attacks in movies

Presentation Attacks in reality

Definitions

Presentation Attacks (PAs)

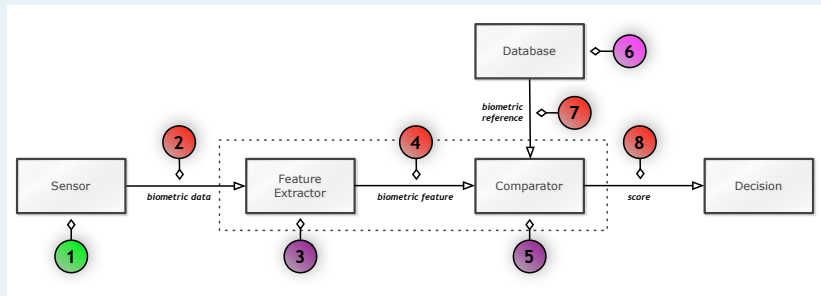
Understanding the Vulnerability to PAs

Face PAs

Presentation Attack Detection (PAD)

# Introduction

## A biometric system is vulnerable to attacks

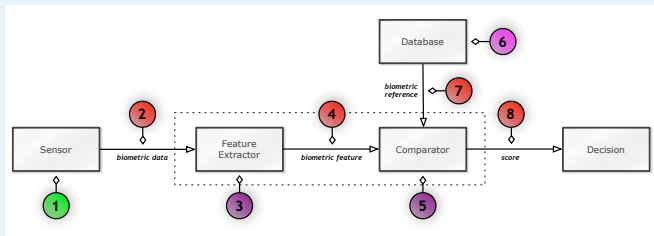


- Indirect attacks (2-8)
- Direct attacks (1)

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

# Introduction

## Indirect Attacks

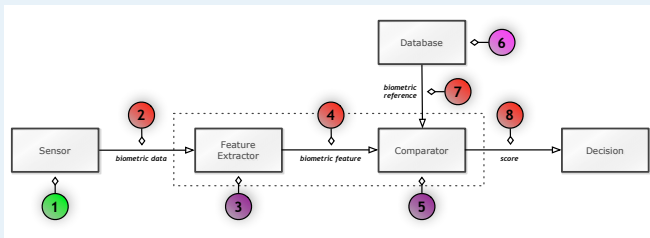


Indirect attacks are performed inside the system by:

- 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).

# Introduction

## 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**

# Outline

Introduction

**Presentation Attacks in movies**

Presentation Attacks in reality

Definitions

Presentation Attacks (PAs)

Understanding the Vulnerability to PAs

Face PAs

Presentation Attack Detection (PAD)

# PAs in movies

## MacGyver - The Human Factor (S02E01 1986)



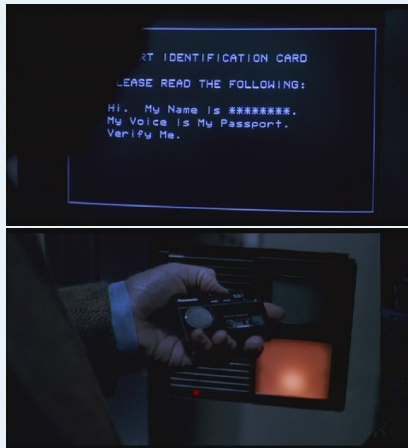
1. scraped some plaster off the walls,
2. sprinkled the plaster dust over the palm print reader revealing the Colonels hand print,
3. laid a jacket down over the plaster hand print impression and lightly pressed down on the reader.

# PAs in movies

Sneakers (1992)

# PAs in movies

## Sneakers (1992)



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

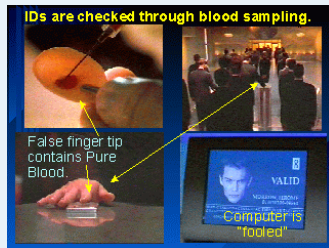
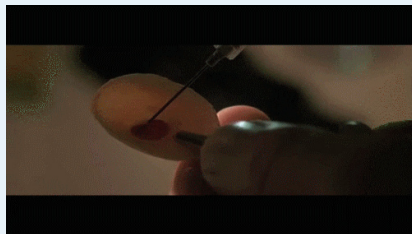


## Demolition Man (1993)



Present an eyeball in front of a iris scanner !

## 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

X-Men 2 (2003)

## X-Men 2 (2003)



High-tech iris spoofing !

# PAs in movies

RED 2 (2013)

## RED 2 (2013)



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

# Outline

Introduction

Presentation Attacks in movies

**Presentation Attacks in reality**

Definitions

Presentation Attacks (PAs)

Understanding the Vulnerability to PAs

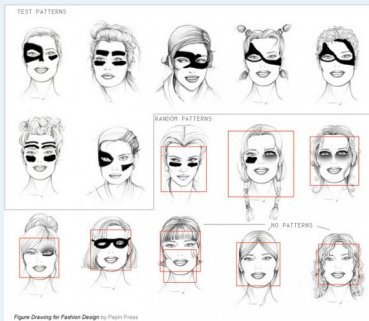
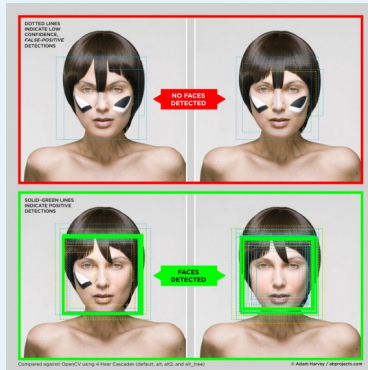
Face PAs

Presentation Attack Detection (PAD)



# PAs in reality

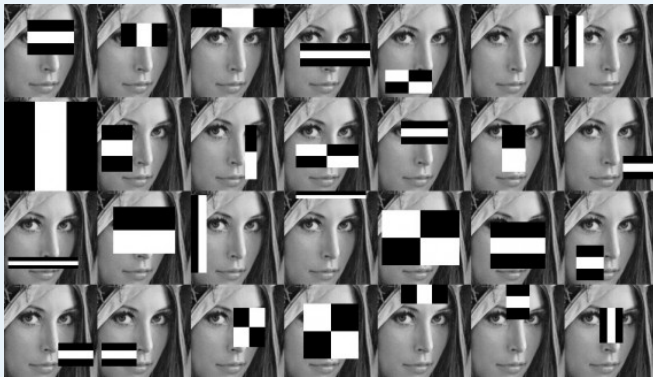
## CVDazzle (Apr 2010)



Camouflage from face detection (Adam Harvey)

<http://ahprojects.com/projects/cv-dazzle>

## CVDazzle (Apr 2010)



Designed to confuse boosted weak-learners based on Haar-like features (OpenCV implementation of Viola-Jones)

## Bank robbery (2010)



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

---

<sup>2</sup><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)



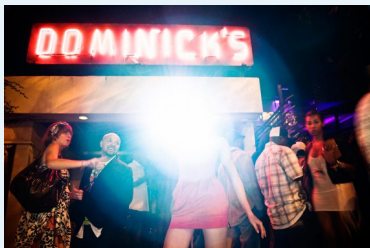
A passenger boarded a plane in Hong Kong with an old man mask and arrived in Canada !

---

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

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

## Camoflash (Nov 2011)



Anti-paparazzi fashion accessory using high brightness LEDs (Adam Harvey <http://ahprojects.com/projects/camoflash>)

## Android 4.0 (Nov 2011)



Android 4.0 Face UnLock feature spoofed by photograph <sup>6</sup>

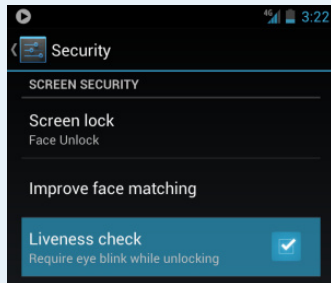
---

<sup>5</sup> <https://www.youtube.com/watch?v=BwfYSR7HttA>

<sup>6</sup> <http://www.geek.com/android/android-face-lock-feature-spoofed-by-photograph-1440953>

Android 4.0 (Nov 2011)

## 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<sup>7</sup>

---

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

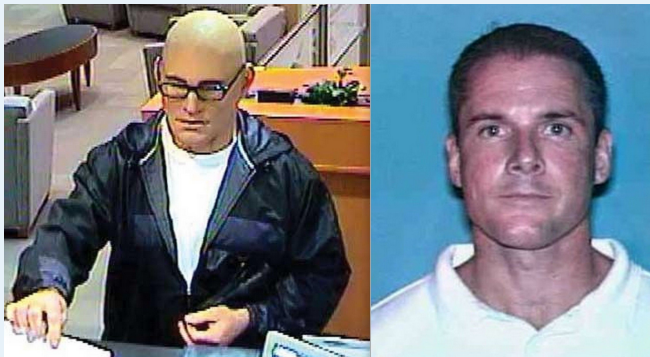
## Brazil (March 2013)



Fake fingers used to fool Hospital clock-in scanner

<sup>8</sup><http://news.sky.com/story/1063956/fake-fingers-fool-hospital-clock-in-scanner>

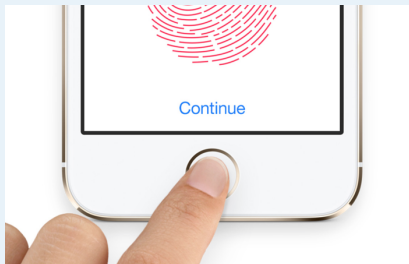
## More bank robbery (2013)



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

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

## iPhone 5s spoofed by CCC (Sep 21 2013)

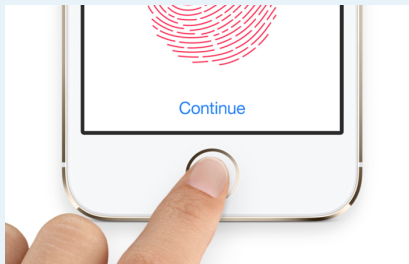


1. How many days will it take to spoof it ? 2 days !

---

<sup>10</sup> <http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid>

## iPhone 5s spoofed by CCC (Sep 21 2013)



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

---

<sup>10</sup> <http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid>

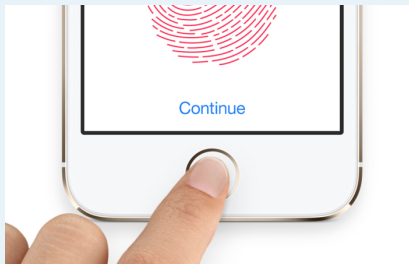
# PAs in reality

iPhone 5s spoofed by CCC (Sep 21 2013)

---

<sup>11</sup><https://www.youtube.com/watch?v=HM8b8d8kSNQ>

## Apple and fingerprints the full story



---

<sup>12</sup>[http://fingerchip.pagesperso-orange.fr/biometrics/types/fingerprint\\_apple.htm](http://fingerchip.pagesperso-orange.fr/biometrics/types/fingerprint_apple.htm)

## Finger-vein (Oct 2014)



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

<sup>13</sup> <https://www.youtube.com/watch?v=8HuL6cHJTK0>



# PAs in reality

## Samsung Galaxy S8 Iris spoofed by CCC (May 23 2017)



<sup>14</sup><https://media.ccc.de/v/biometrie-s8-iris-en>

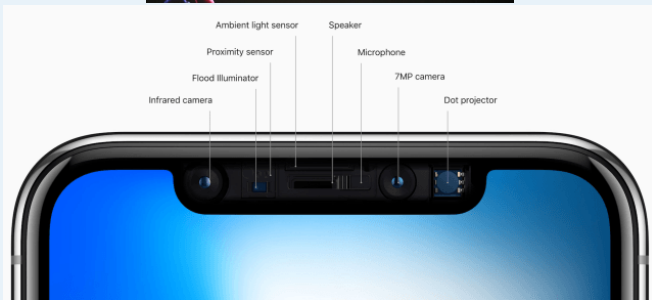
# PAs in reality

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

---

<sup>15</sup> <https://www.youtube.com/watch?v=gtQ4yzbsi-c>

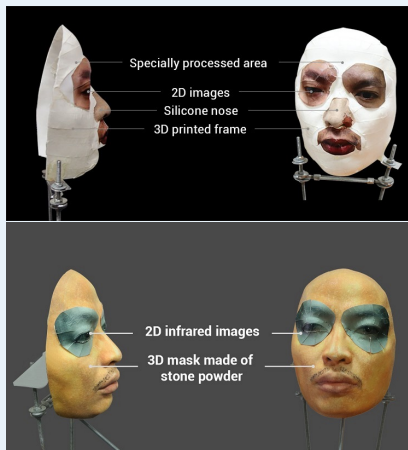
## iPhone X FaceID (Sep 2017)



## iPhone X FaceID robust to masks (Sep 2017)



## iPhone X spoofed by Bkav (Nov 27 2017)



<sup>16</sup> <http://www.bkav.com>

<sup>17</sup> <https://www.youtube.com/watch?v=i4YQRLQVixM>

# PAs in reality

## Jailbreak in Brazil (Aug 2019)



<sup>18</sup> <https://www.theguardian.com/world/2019/aug/05/brazil-gang-leader-dresses-up-as-teenage-daughter-in-jail-break-attempt>

<sup>19</sup> <https://www.youtube.com/watch?v=XxgANx1IAHg>

## Robbery in Brazil (Aug 2019)



<sup>20</sup> <https://g1.globo.com/sc/santa-catarina/noticia/2019/08/12/ex-funcionario-usa-mascara-de-idoso-e-e-preso-em-tentativa-de-assalto-a-banco-em-jaragua-do-sul-foto-ghtml>

## Facial Recognition Smart Lockers Hacked by Fourth-Graders in China

---

<sup>21</sup><http://www.sixthtone.com/news/1004698/facial-recognition-smart-lockers-hacked-by-fourth-graders>



# Outline

Introduction

Presentation Attacks in movies

Presentation Attacks in reality

**Definitions**

Presentation Attacks (PAs)

Understanding the Vulnerability to PAs

Face PAs

Presentation Attack Detection (PAD)

## 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, . . .

---

<sup>22</sup> *Spoof Detection Schemes*, K. Nixon et al., *Handbook of Biometrics*, 2008.

## 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, . . .

---

<sup>23</sup> *Biometric presentation attack detection – part 1, ISO/IEC 30107-1:2016, 2016.*

## 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*

# Outline

Introduction

Presentation Attacks in movies

Presentation Attacks in reality

Definitions

**Presentation Attacks (PAs)**

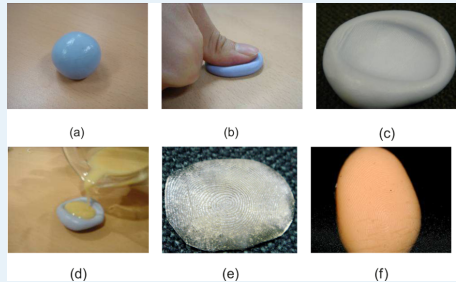
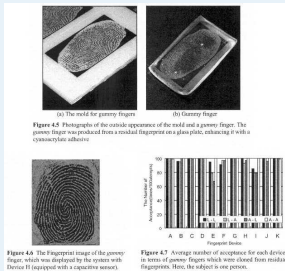
Understanding the Vulnerability to PAs

Face PAs

Presentation Attack Detection (PAD)

# Seminal work

## “Gummy Fingers”



Gelatin fake fingers to spoof 11 fingerprint biometric systems

<sup>24</sup> *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



Printed photo to spoof face recognition systems on 3 laptops

---

<sup>25</sup> *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

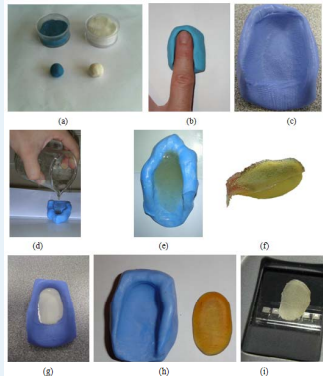
## Fingerprint PA



Presenting a fake fingerprint to a capture device

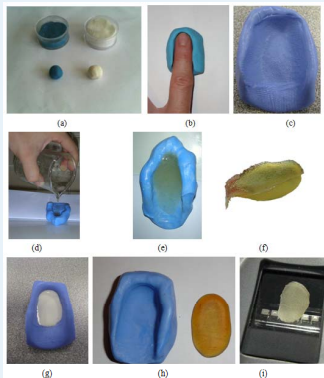
# Presentation Attacks

## Fingerprint PA: latex/silicone PAI (with cooperation)



Prepare a silicone mold (a, b and c)

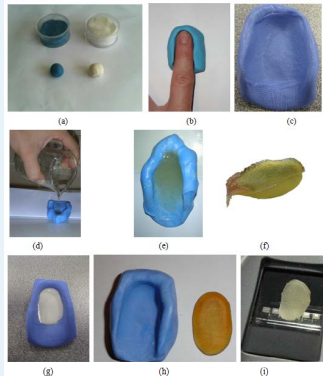
## Fingerprint PA: latex/silicone PAI (with cooperation)



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

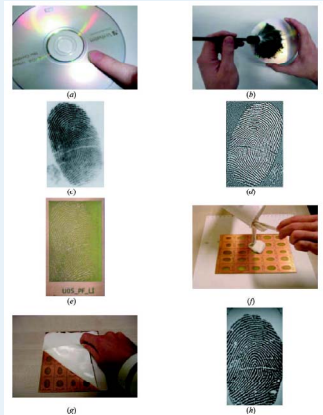
## Fingerprint PA: wood glue PAI (with cooperation)



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)



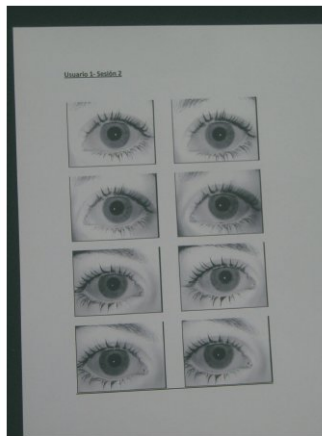
CCC vs iPhone5s <sup>26</sup>

<sup>26</sup> [http://dasalte.ccc.de/biometrie/fingerabdruck\\_kopieren?language=en](http://dasalte.ccc.de/biometrie/fingerabdruck_kopieren?language=en)



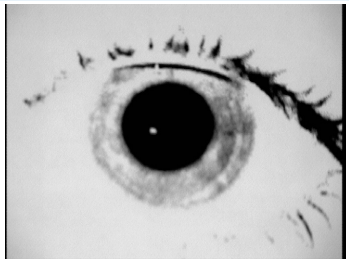
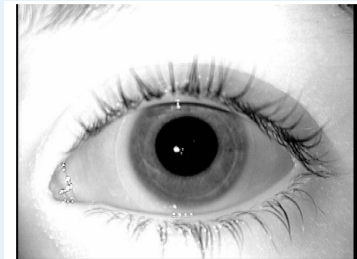
# Presentation Attacks

## Iris PA: printed paper PAI



High quality paper and inkjet printer

## 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



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

<sup>27</sup> *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)

# Presentation Attacks

## Voice PA: voice synthesis PAI

Voice of target speaker synthesized

Playback with laptop (rec on laptop)

# Presentation Attacks

## Voice PA: voice conversion PAI

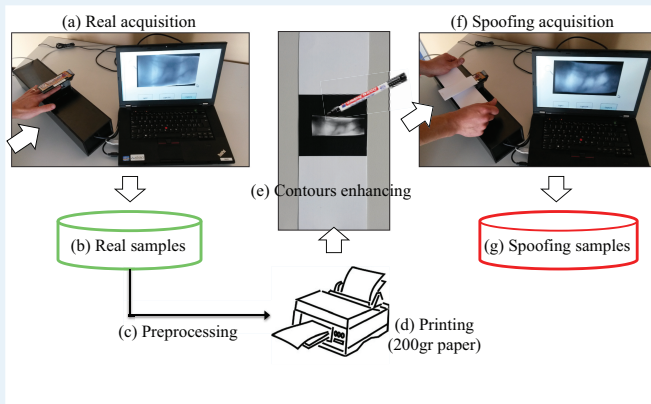
Original voice of source speaker (rec on laptop)

Voice of target speaker converted from source speaker

Playback with laptop (rec on laptop)

# Presentation Attacks

## Fingervein PA: printer paper PAI

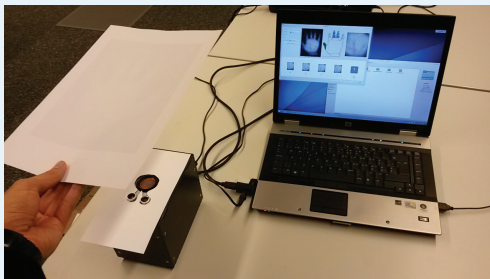


with paper



# Presentation Attacks

## Palmvein PA: printed paper PAI



with paper

---

<sup>29</sup> On the vulnerability to palm vein recognition to spoofing attacks, P. Tome and S. Marcel, IAPR ICB, 2015.

# Outline

Introduction

Presentation Attacks in movies

Presentation Attacks in reality

Definitions

Presentation Attacks (PAs)

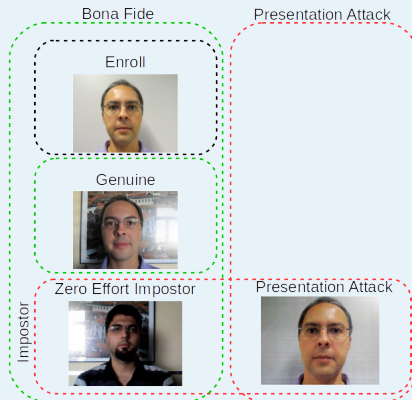
**Understanding the Vulnerability to PAs**

Face PAs

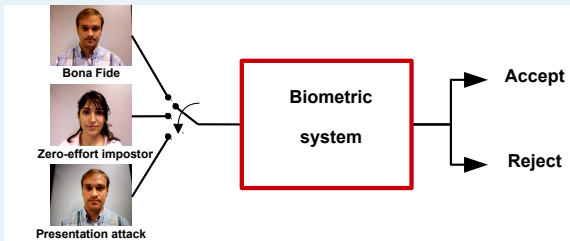
Presentation Attack Detection (PAD)

# Biometrics and PA

## Bona Fide, Zero Effort Impostor and PA

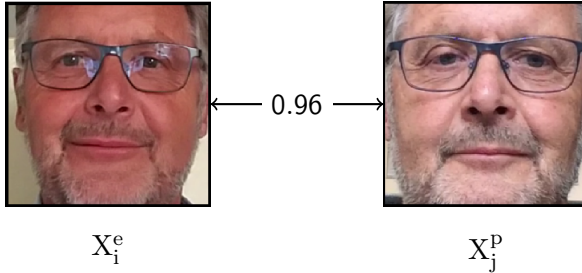


## Bona Fide, Zero Effort Impostor and PA



- Accept Bona Fide
- Reject Zero Effort Impostor and PA

# Biometrics and PA

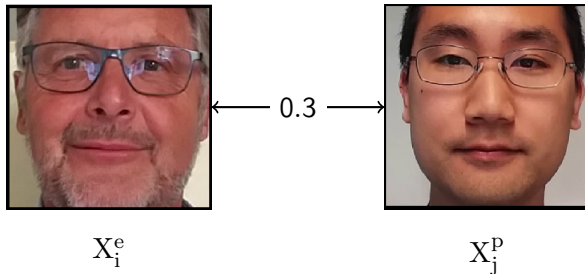


## Comparison function

with  $i = 01$ ,  $j = 01$  and  $X^p \neq X^e$  (2 different images of 01):

- **dissimilarity:**  $z$  as low (close to 0) as possible
- **probability:**  $z$  as high (close to 1) as possible

# Biometrics and PA

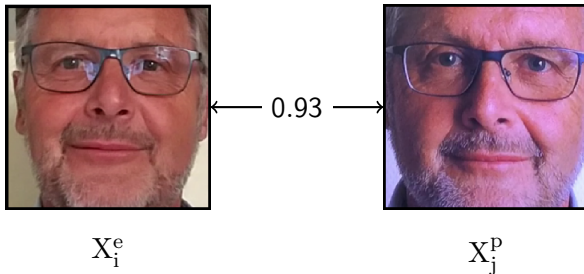


## Comparison function

with  $i = 01$ ,  $j = 02$  (**different identities**):

- **dissimilarity**:  $z > 0$  and as high as possible
- **probability**:  $z < 1$  and as low (close to 0) as possible

# Biometrics and PA



## Comparison function

with  $i = 01$ ,  $j = 01$  and  $X^p$  is a presentation attack:

- **dissimilarity**:  $z$  as low (close to 0) as possible
- **probability**:  $z$  as high (close to 1) as possible

# Outline

Introduction

Presentation Attacks in movies

Presentation Attacks in reality

Definitions

Presentation Attacks (PAs)

Understanding the Vulnerability to PAs

**Face PAs**

Presentation Attack Detection (PAD)



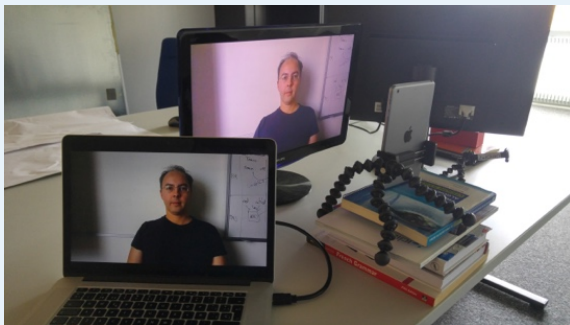
## 2D face PA: printed paper PAI



---

<sup>30</sup> *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>)

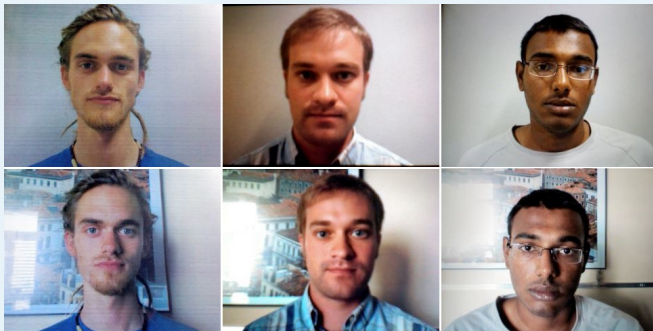
## 2D face PA: photo/video screen PAI



---

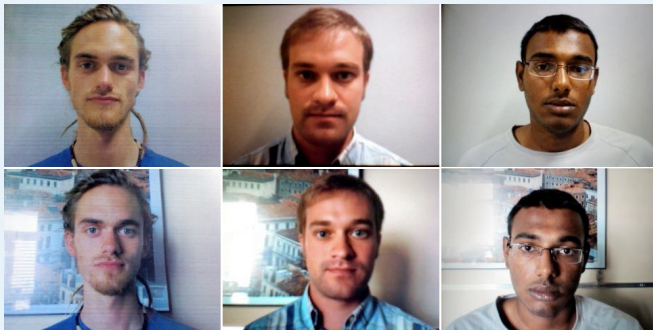
<sup>31</sup> *The REPLAY-MOBILE Face Presentation-Attack Database*, A. Costa-Pazo and al., IEEE BIOSIG, 2016, ([http://publications.idiap.ch/downloads/papers/2016/Costa-Pazo\\_BIOSIG2016\\_2016.pdf](http://publications.idiap.ch/downloads/papers/2016/Costa-Pazo_BIOSIG2016_2016.pdf)).

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



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

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



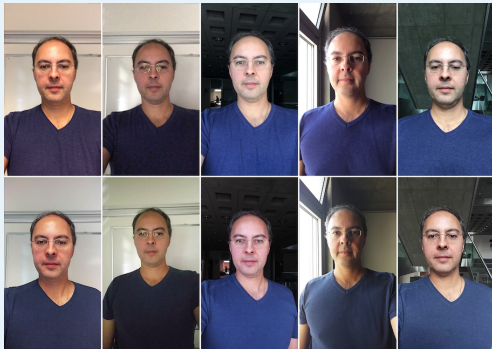
1. Which one is real (Bona Fide) or fake (PA) ?
2. All are fakes: print (left), iPhone (middle) and iPad (right) !

## 2D face PA: printed paper PAI

PA with printed paper exhibits:

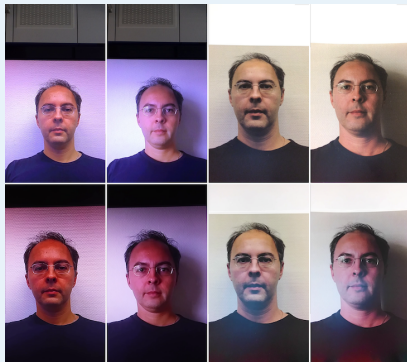
- Reduced image texture
- Printer halftoning artifacts
- Mechanical artifacts (horizontal lines)
- No local motion (e.g., eye blinks)
- Borders of image may be visible

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



Bona Fide samples !

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



PA samples !

## 2D face PA: photo/video replay PAI

PA with an electronic screen exhibits:

- Blurred image texture
- Reduced color diversity
- Moire pattern



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



Hard resin composite in full 24-bit color !

---

<sup>32</sup> *Spoofing Face Recognition with 3D Masks*, N. Erdogmus and S. Marcel, IEEE TIFS, 9(7):1084–1097, 2014.

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



Cost:  $\sim$  USD 300

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



1 frontal and 2 profile pictures

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



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

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

PA with 3D (rigid) mask exhibits:

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

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

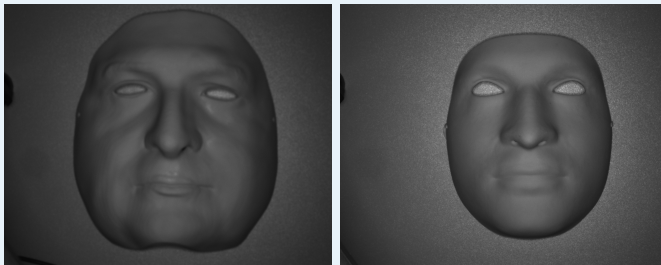


Cost: ~ USD 400

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

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

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



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

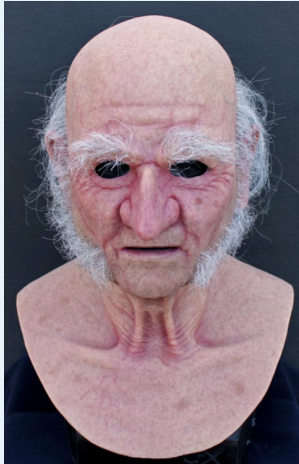
PA with 3D (rigid) mask don't absorb heat (much):



thermal imaging



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



Cost: ~ USD 800

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



Cost for full head: starting USD 6'000

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



Cost for half-face: starting USD 3'000

# Face PAs

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

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

PA with 3D silicone mask exhibits:

- skin-like appearance and reflexion
- facial motion

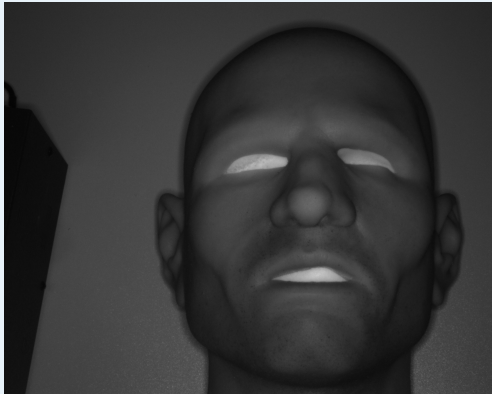


<sup>34</sup> *What you can't see can help you – extended-range imaging for 3D-mask presentation attack detection*, S. Battacharjee and al., IEEE BIOSIG, 2017.

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

PA with 3D silicone mask exhibits:

- texture in NIR



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

PA with 3D silicone mask exhibits:

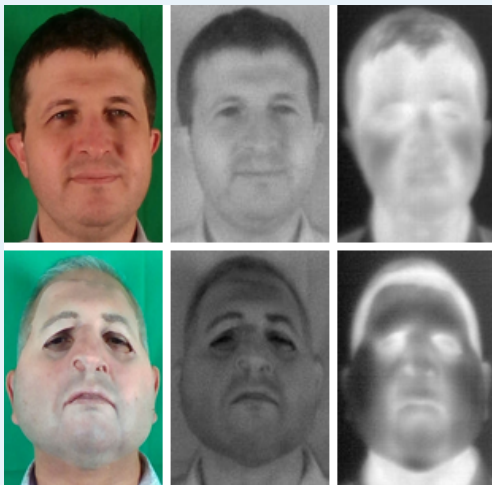
- thermal imaging ?



Silicone absorbs heat !

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

PA with 3D silicone mask exhibits thermal imaging:





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



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



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

PA with make-up exhibits:

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

## The Magic Passport

*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.*

---

<sup>35</sup> *The magic passport*, M. Ferrara, A. Franco, D. Maltoni, IEEE/IAPR IJCB, 2014.

## The Magic Passport: a morphed face image as template !



## 2D Face PA: a morphed face PAI



It was shown that:

- 2 COTS face recognition systems 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*

## 2D Face PA: a morphed face PAI

PA with morphing exhibits:

- symmetric features
- smooth texture
- morphing artefacts

## 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?



# Outline

Introduction

Presentation Attacks in movies

Presentation Attacks in reality

Definitions

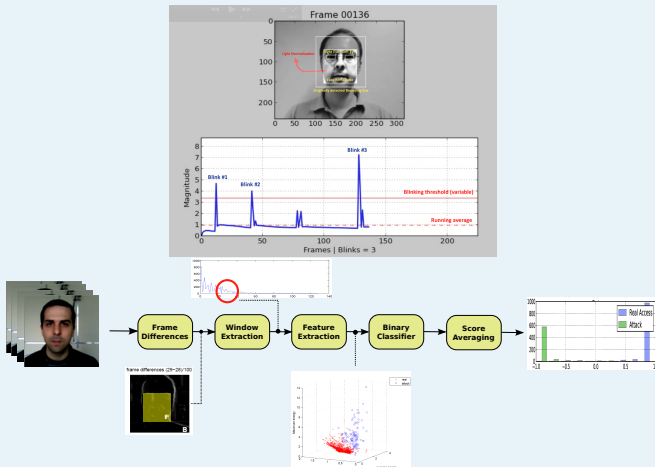
Presentation Attacks (PAs)

Understanding the Vulnerability to PAs

Face PAs

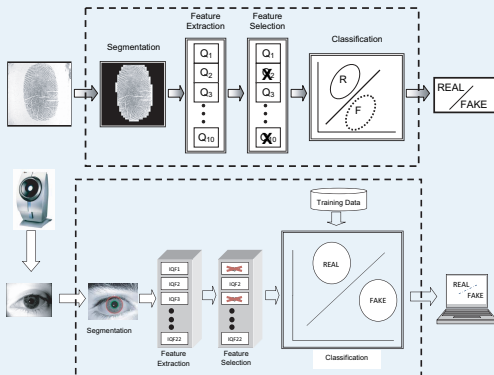
Presentation Attack Detection (PAD)

## Face PAD



using eye blinking or motion

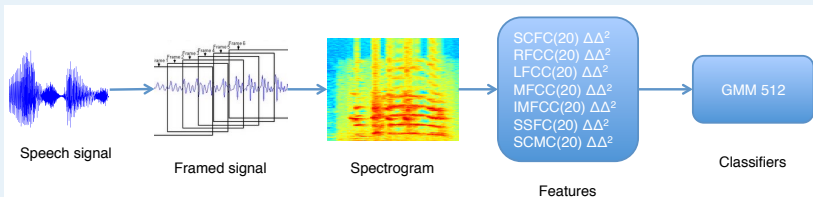
## Fingerprint/Iris PAD



using generic image quality measures

<sup>37</sup> *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.

## Voice PAD



using cepstral-based features

# Outline

Introduction

Presentation Attacks in movies

Presentation Attacks in reality

Definitions

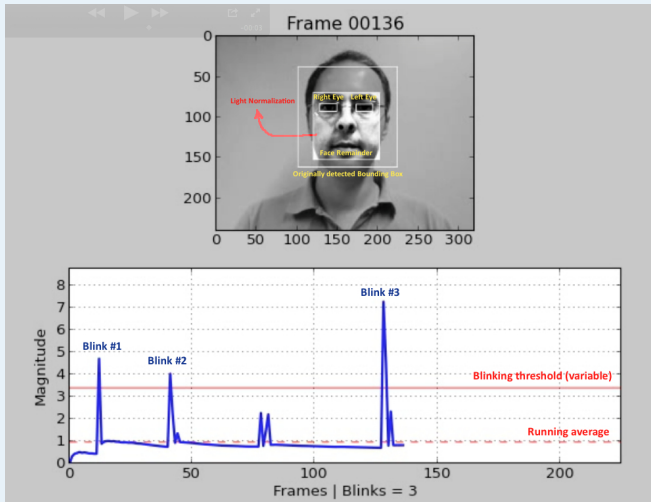
Presentation Attacks (PAs)

Understanding the Vulnerability to PAs

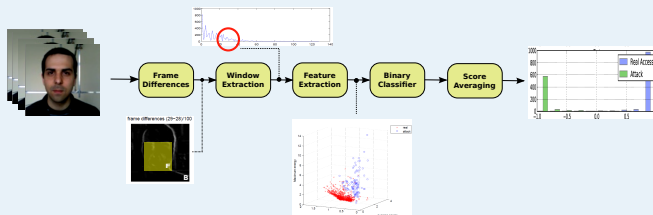
Face PAs

Presentation Attack Detection (PAD)

## Eye-blinking

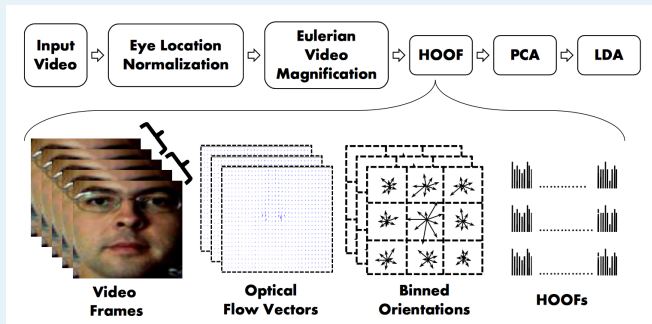


## Motion



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

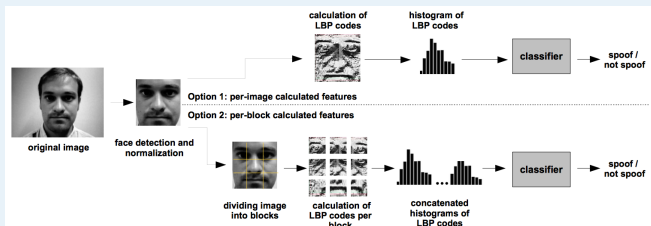
## Motion



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



## Texture analysis



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

<sup>41</sup> On the effectiveness of local binary patterns (LBP) in face anti-spoofing, Chingovska et al., BIOSIG, 2012.

## Frequency analysis

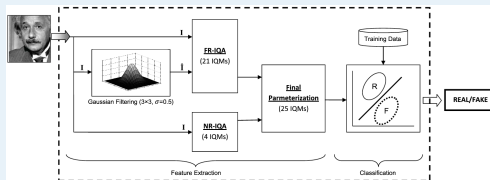


- use LBP to detect the presence of moiré patterns
- HTER on Replay-attack: 6%

---

<sup>42</sup> *Live face video vs. spoof face video: use of moiré patterns to detect replay video attacks*, Patel et al., ICB, 2015.

## Image Quality Analysis

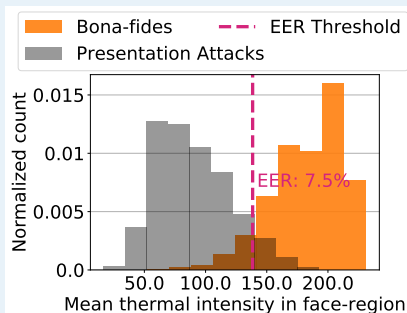


- use 25 well known image quality measures for gray-level images to train a 2-class classifier

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

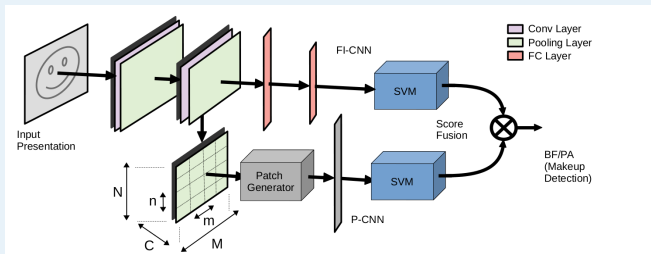
- HTER: Replay-attack: 15.4%

## PAD with thermal imaging



<sup>44</sup> *Spoofing Deep Face Recognition with Custom Silicone Masks*, S. Battacharjee and al., BTAS, 2018.

## Make-up PAD with fusion of holistic and local CNNs

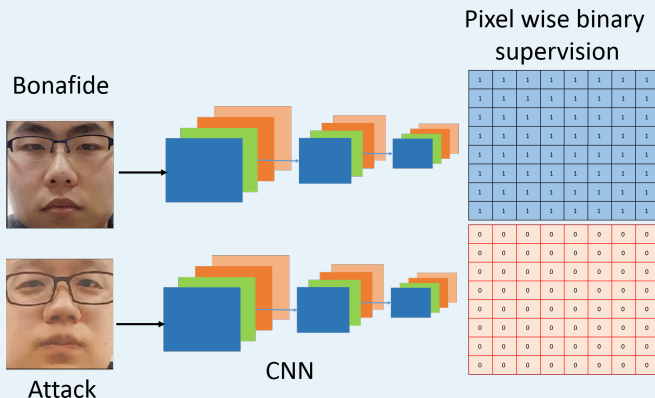


Prior work on make-up analysis by A. Ross and al. (MSU)

45

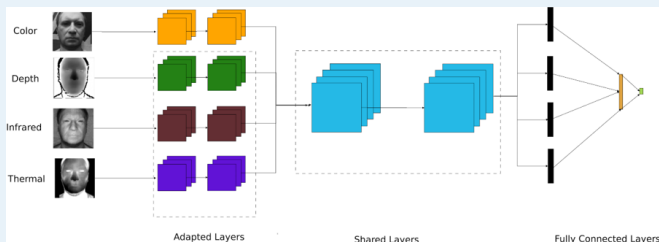
*Detection of Age-Induced Makeup Attacks on Face Recognition Systems Using Multi-Layer Deep Features*, K. Kotwal and al., TBIOM, 2019.

## Deep Pixel-wise



## Multi-Spectral PAD

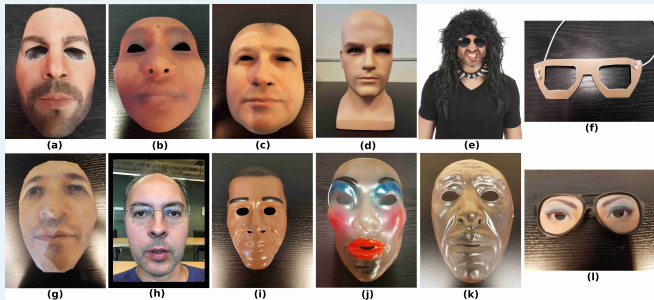
A multi-channel (VIS, NIR, Depth, TH) CNN-based approach for PAD (MC-CNN):



- Leverages a pre-trained CNN used for FR
- Adapting the low-level layers of the MC-CNN

## Multi-Spectral

Wide Multi Channel Presentation Attack (WMCA) dataset<sup>48</sup>:



- Large range of PAI (fakehead, masks, glasses, paper, print, replay, makeup)
- Robust to environmental conditions

<sup>48</sup><https://www.idiap.ch/dataset/wmca>



## Multi-Spectral

Wide Multi Channel Presentation Attack (WMCA) dataset:

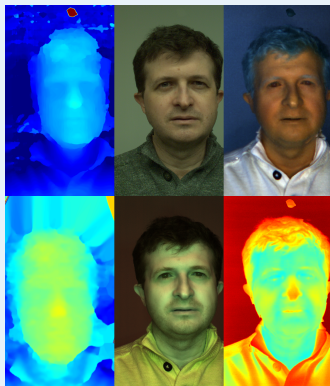


5TB of data:

- VIS, NIR and Depth from Intel SR300
- Thermal from SeekThermal camera

## Multi-Spectral

HQ Wide Multi Channel Presentation Attack (WMCA) dataset  
(available soon)



## Multi-Spectral

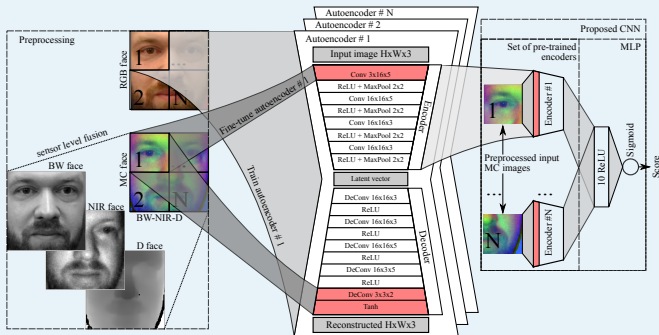
HQ Wide Multi Channel Presentation Attack (WMCA) dataset  
(available soon)

15TB of data:

- HQ VIS, HQ stereo NIR (stereo reconstruction)
- Depth from Intel SR435 (stereo) and HQ Thermal
- HQ SWIR
- illumination: 660nm, 735nm, 850nm, 940nm, 1050nm, 1200nm, 1300nm, 1450nm, 1550nm and 1650nm

# Face PAD

## Multi-Spectral Deep Autoencoder and Domain Adaptation



## Using rPPG

- 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

## 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)

## 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/>

# Outline

Introduction

Presentation Attacks in movies

Presentation Attacks in reality

Definitions

Presentation Attacks (PAs)

Understanding the Vulnerability to PAs

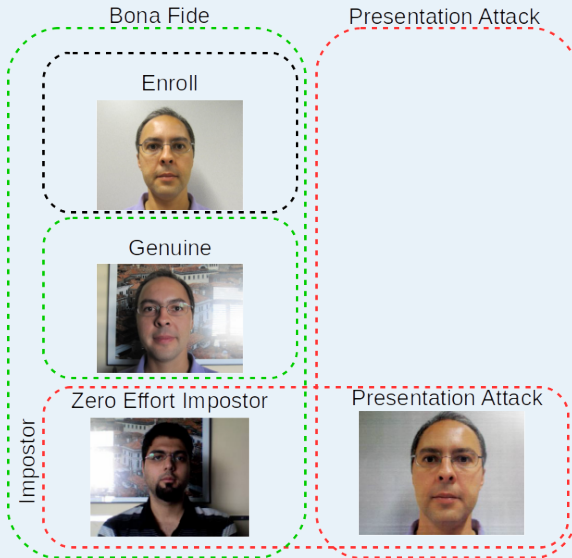
Face PAs

Presentation Attack Detection (PAD)

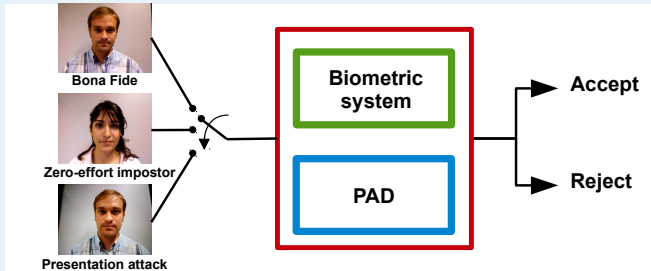


# Biometrics and PAD

## Bona Fide, Zero Effort Impostor and PA

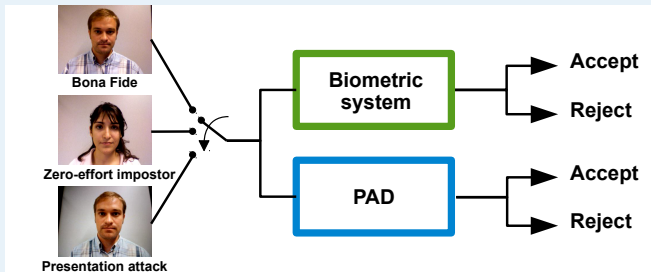


## Two separate components



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

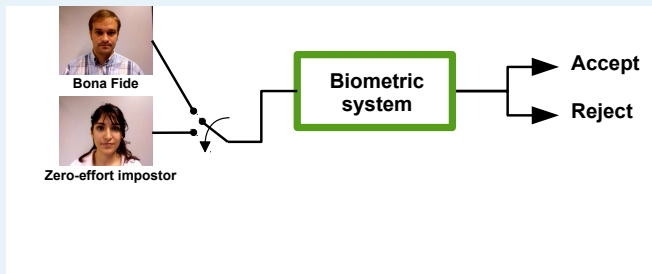
## Two separate components



## Overall

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

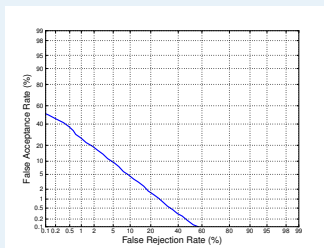
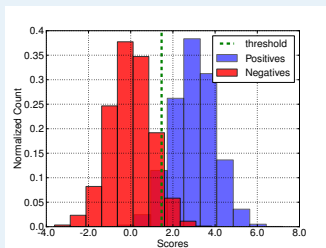
## Biometric sub-system: a binary classifier



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)

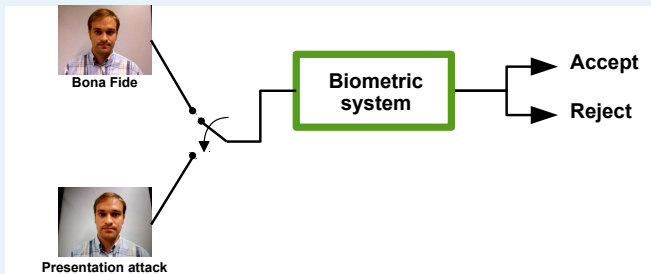
## Biometric sub-system: a binary classifier



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)

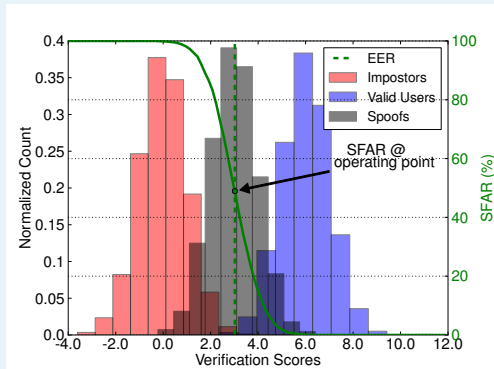
## Biometric sub-system: a binary classifier



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)

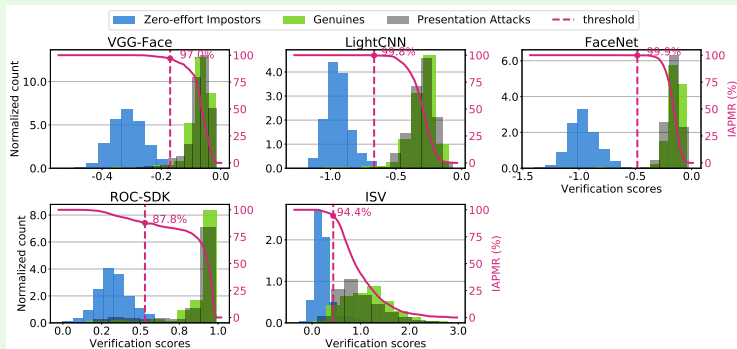
## Biometric sub-system: a binary classifier



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)

## IAPMR Deep Face Recognition (print and replay PA) <sup>51</sup>



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

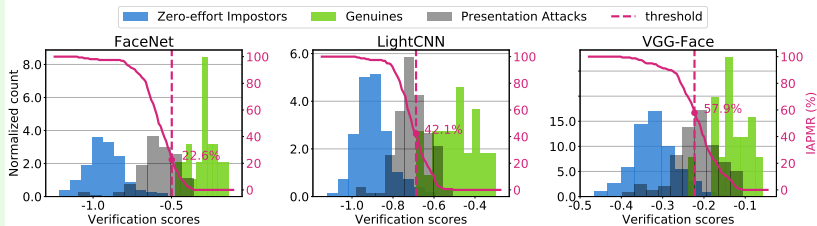
<sup>51</sup>

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



# Biometrics and PAD

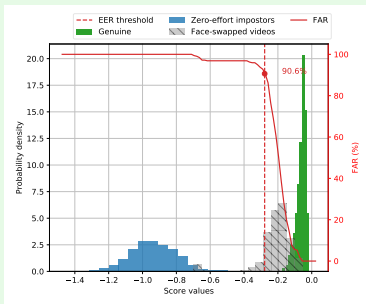
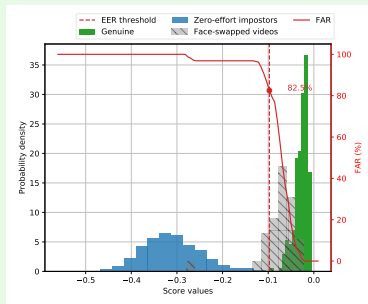
## IAPMR Deep Face Recognition (silicone masks PA) <sup>52</sup>



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

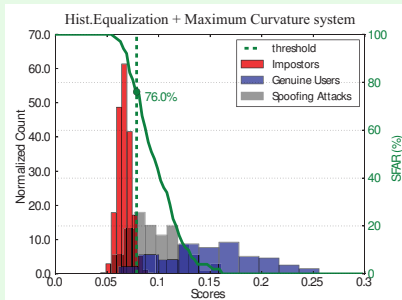
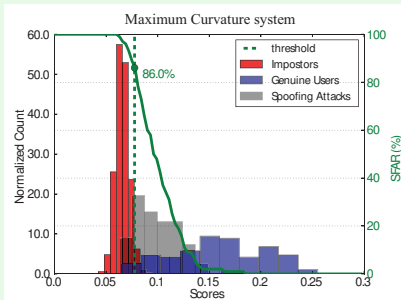
<sup>52</sup> *spoofing Deep Face Recognition with Custom Silicone Masks*, S. Battacharjee and al., BTAS, 2018.

## IAPMR DeepFakes (unpublished)

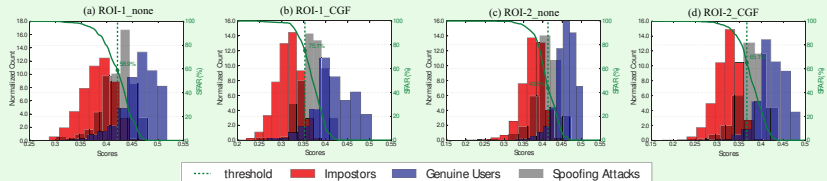


CNN-based FR systems (VGG, Facenet) are vulnerable to DeepFakes (up to 90%)

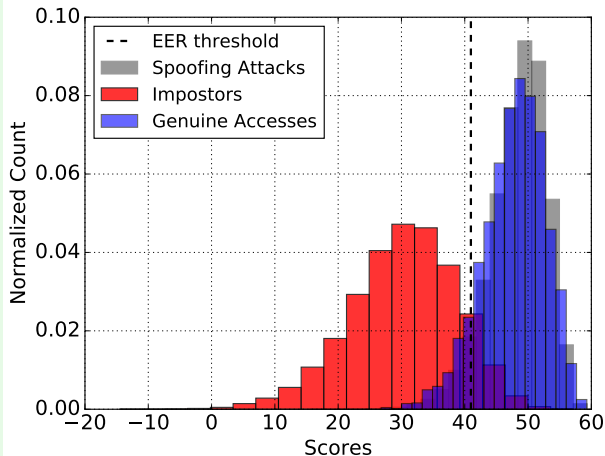
## IAPMR Fingervein



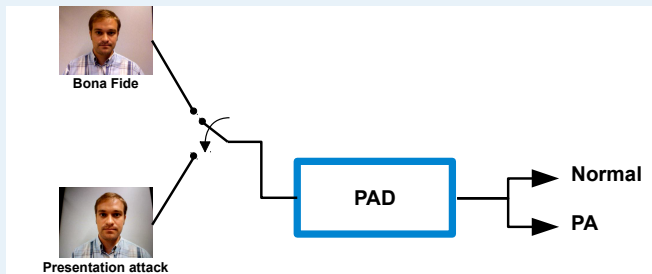
## IAPMR Palmvein



## IAPMR Voice



## PAD sub-system: a binary classifier

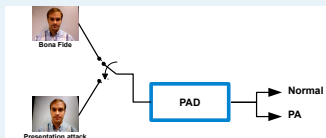


We measure 2 errors:

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

## 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)



# Outline

Introduction

Presentation Attacks in movies

Presentation Attacks in reality

Definitions

Presentation Attacks (PAs)

Understanding the Vulnerability to PAs

Face PAs

Presentation Attack Detection (PAD)



## Books

- [Handbook of Biometric Anti-Spoofing](#), S. Marcel and al. (2014)

## 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).

# Outline

Introduction

Presentation Attacks in movies

Presentation Attacks in reality

Definitions

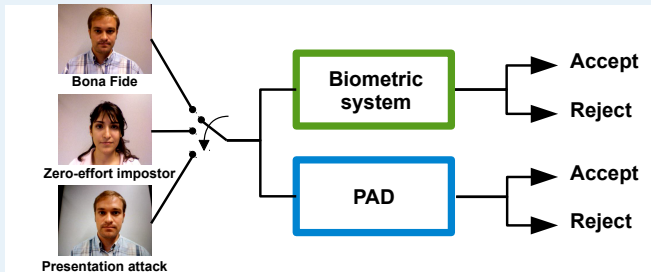
Presentation Attacks (PAs)

Understanding the Vulnerability to PAs

Face PAs

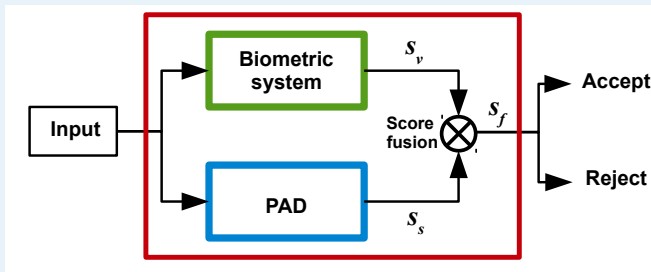
Presentation Attack Detection (PAD)

## Two separate components



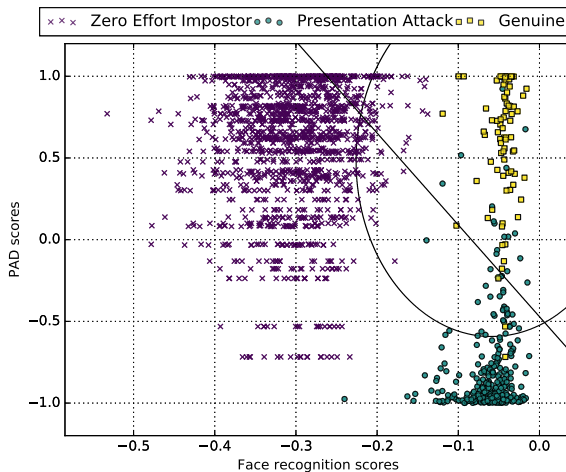
How to combine these two components ?

## Fusion scheme

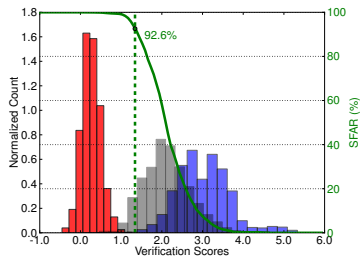
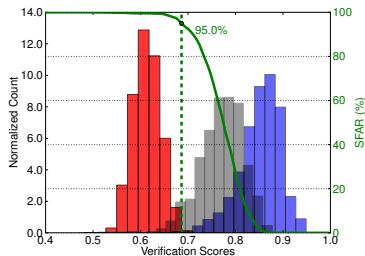
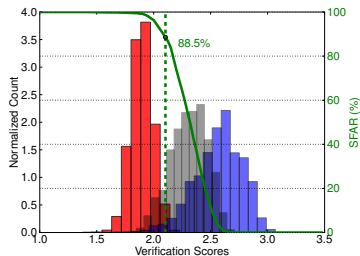
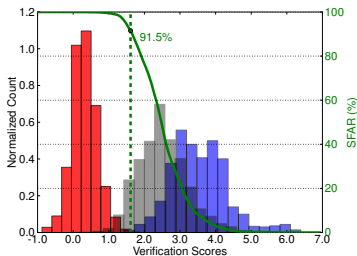


One unique threshold to be determined

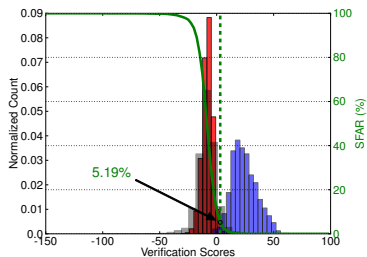
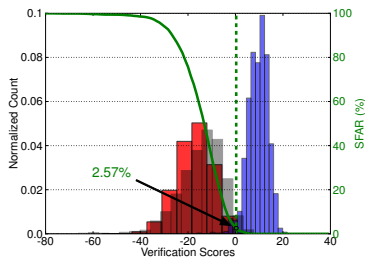
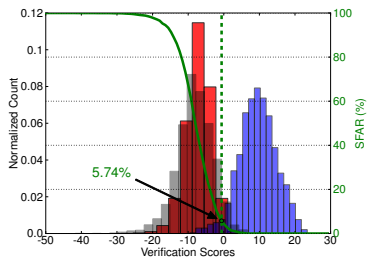
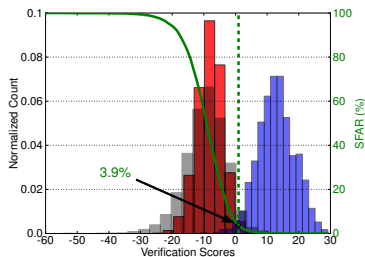
## Fusion scheme



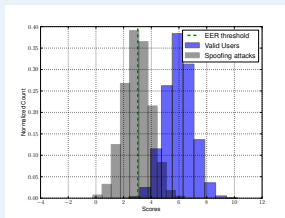
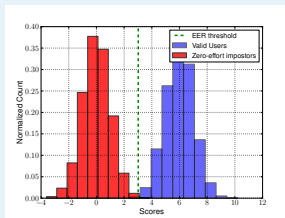
## Biometric systems without PAD (no fusion)



## Biometric systems + PAD (fusion)



## Measuring the performance



We still measure 3 errors:

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



## $\text{FAR}_\omega$ (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  $\tau_\omega^*$  to minimize the difference between  $\text{FAR}_\omega$  and  $\text{FRR}$  on the development set:

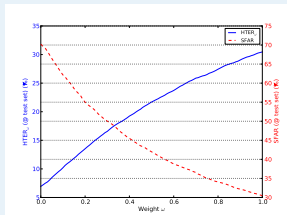
$$\tau_\omega^* = \arg \min_{\tau} |\text{FAR}_\omega(\tau, \mathcal{D}_{\text{dev}}) - \text{FRR}(\tau, \mathcal{D}_{\text{dev}})|$$

## $\text{HTER}_\omega$ (test set)

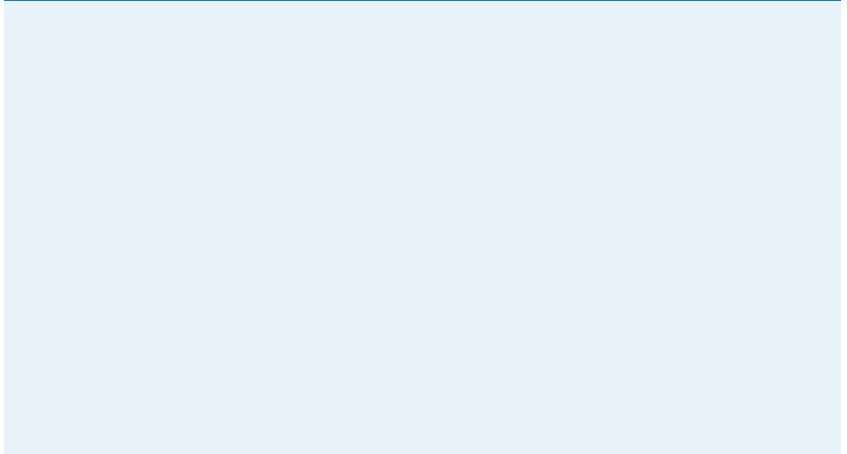
Measuring both the verification performance and the spoofability of the system

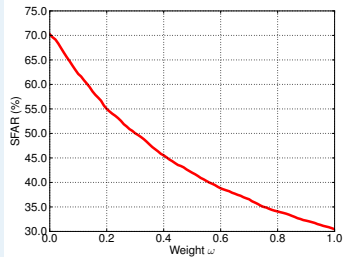
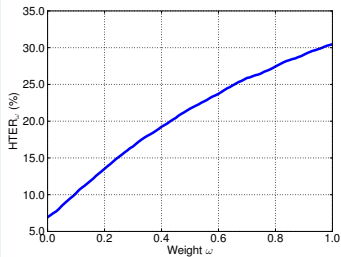
$$\text{HTER}_\omega(\tau_\omega^*, \mathcal{D}_{\text{test}}) = \frac{\text{FAR}_\omega(\tau_\omega^*, \mathcal{D}_{\text{test}}) + \text{FRR}(\tau_\omega^*, \mathcal{D}_{\text{test}})}{2}$$

## Plotting $\text{HTER}_\omega$ or SFAR

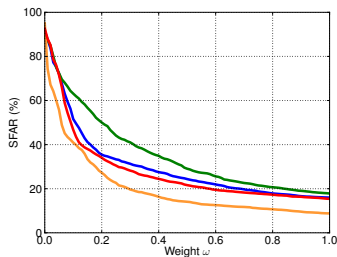
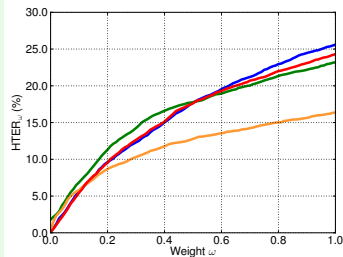


## EPSC in action



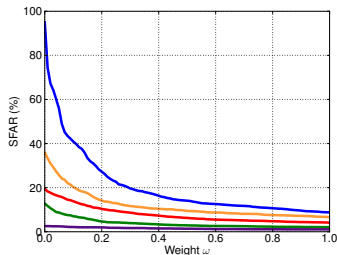
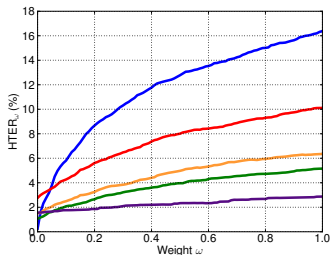
EPSC:  $\text{HTER}_\omega$  and SFAR

## EPSC to compare biometric systems only



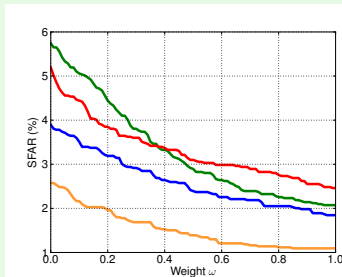
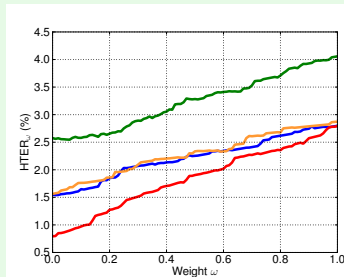
4 biometric systems (no PAD): using the orange subsequently

## EPSC to compare PAD



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

## EPSC to compare biometric systems fused with ALL PADs



4 biometric system + all PADs

# Thank you for your attention!

Dr Sébastien Marcel

Idiap Research Institute, Martigny, Switzerland

