Spoofing, Anti-Spoofing and Reproducible Research in Biometrics

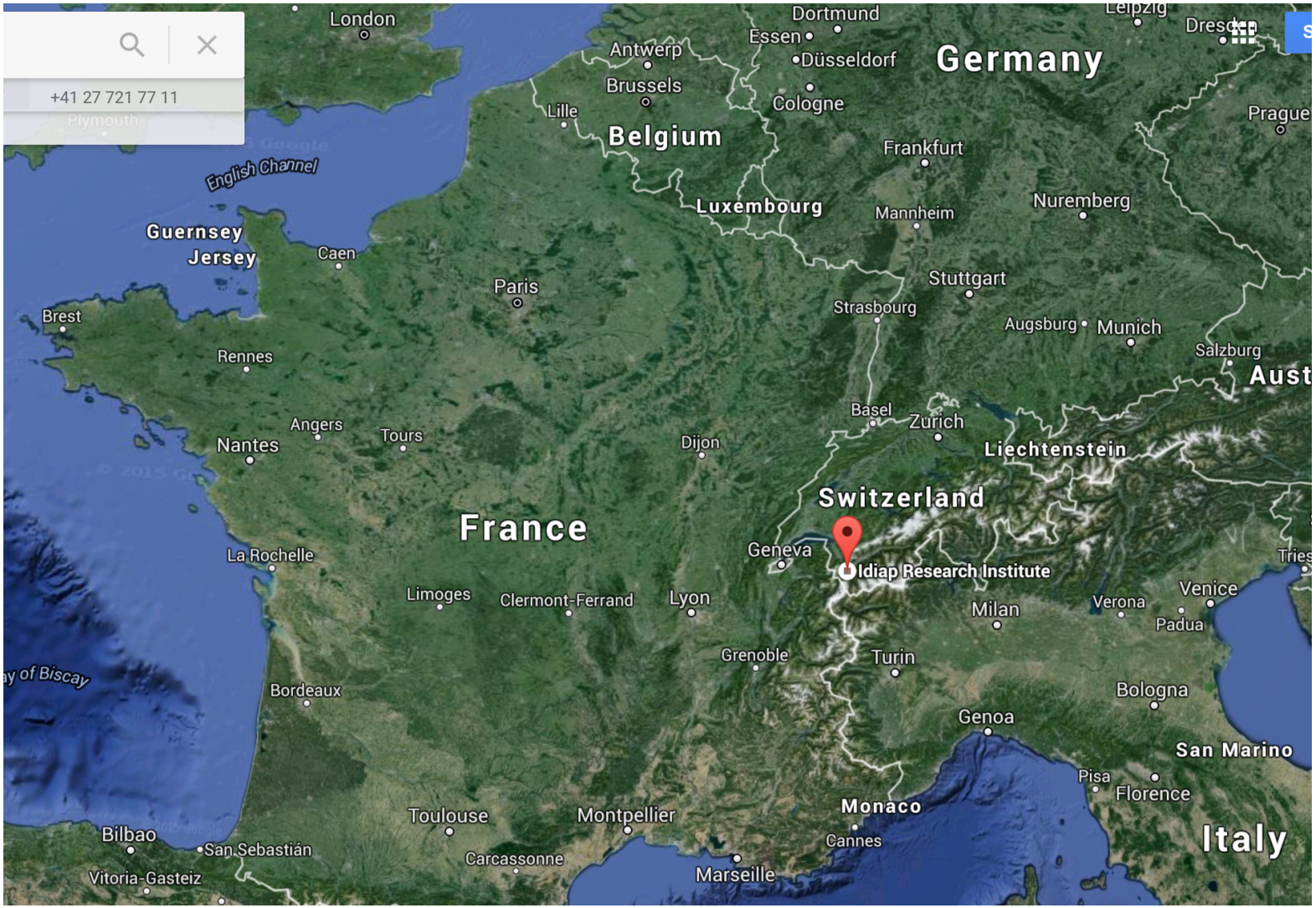
Moving to the BEAT ?

Sébastien Marcel
Head of Biometrics group
Idiap research institute
Switzerland
www.idiap.ch/~marcel

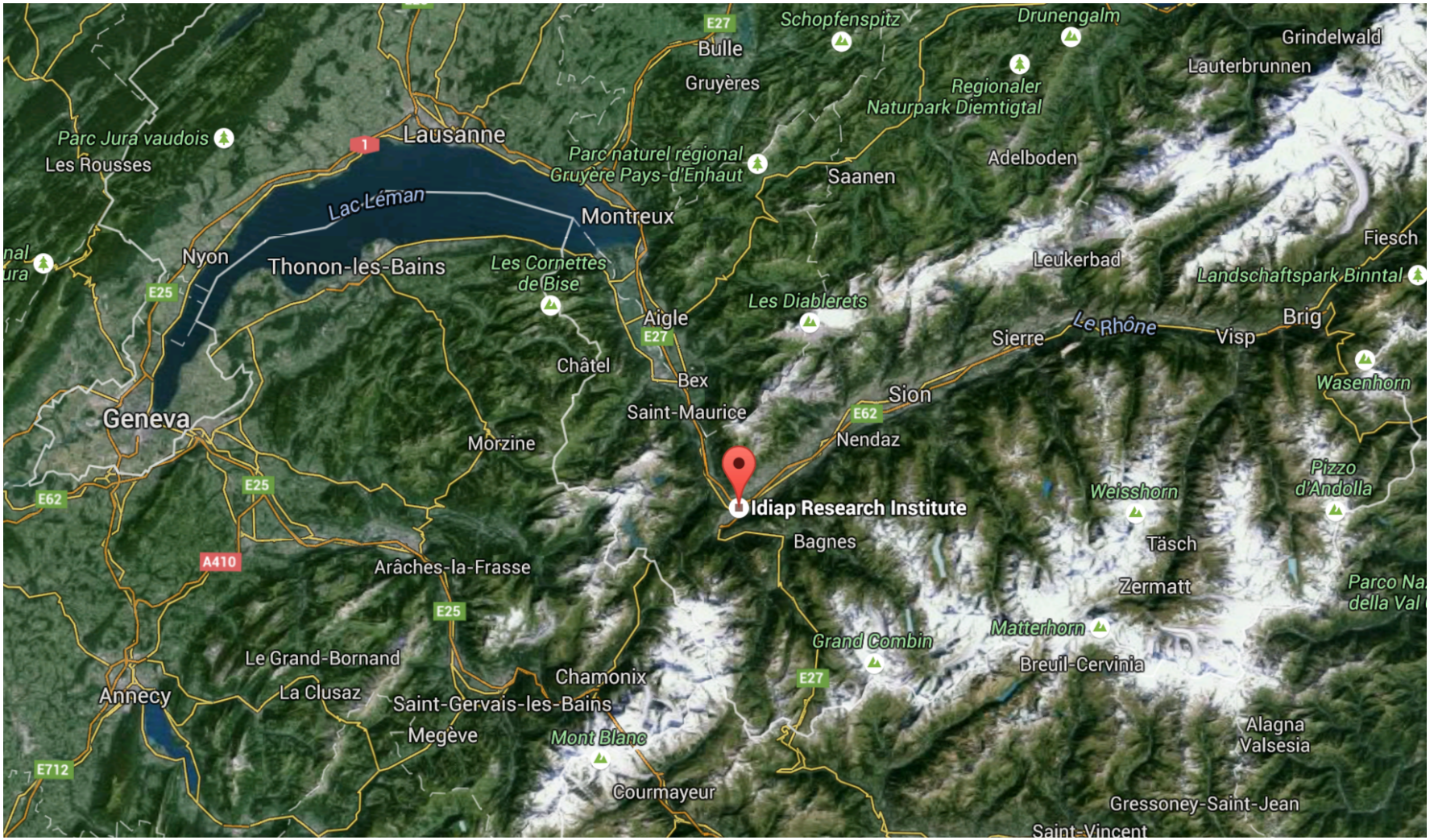
Michigan State University – Computer Science and Engineering
East Lansing – September 14, 2015

Go Spartans

Where is Idiap ?



Where is Idiap ?



Where is Idiap ?

Altitude to ski ranges from 1400m to 3000m

What is Idiap ?

- Non-for-profit research institute founded in 1991
- Affiliated with École polytechnique fédérale de Lausanne (EPFL)
- Research, Education and Technology transfer
- Budget: $\approx$ 10 CHF (50% public funding, 50% competitive/private funding)
- Staff
  - 17 permanent researchers and senior researchers,
  - 23 post-docs, 37 phds,
  - 20 systems and development engineers,
  - 10 admin.

What is Idiap ?

- Non-for-profit research institute founded in 1991
- Affiliated with École polytechnique fédérale de Lausanne (EPFL)
- Research, Education and Technology transfer
- Budget: $\approx$ 10 CHF (50% public funding, 50% competitive/private funding)
- Staff: $\approx$ 110
- 9 research groups
  - Speech & Audio Processing
  - Social Computing
  - Computer Vision and Learning
  - Perception and Activity Understanding
  - **Biometrics**
  - Natural Language Processing
  - Robot Learning & Interaction
  - Computational Bioimaging
  - Uncertainty Quantification and Optimal Design

The Biometrics group @ Idiap

Research themes

signal (image, audio) processing and machine learning (NN, GMM, ...) applied to Biometrics:

- Face and speaker recognition
- Vein recognition (fingervein and palmvein)
- "Soft-biometrics": gender recognition and age estimation
- **Spoofing and Anti-spoofing**

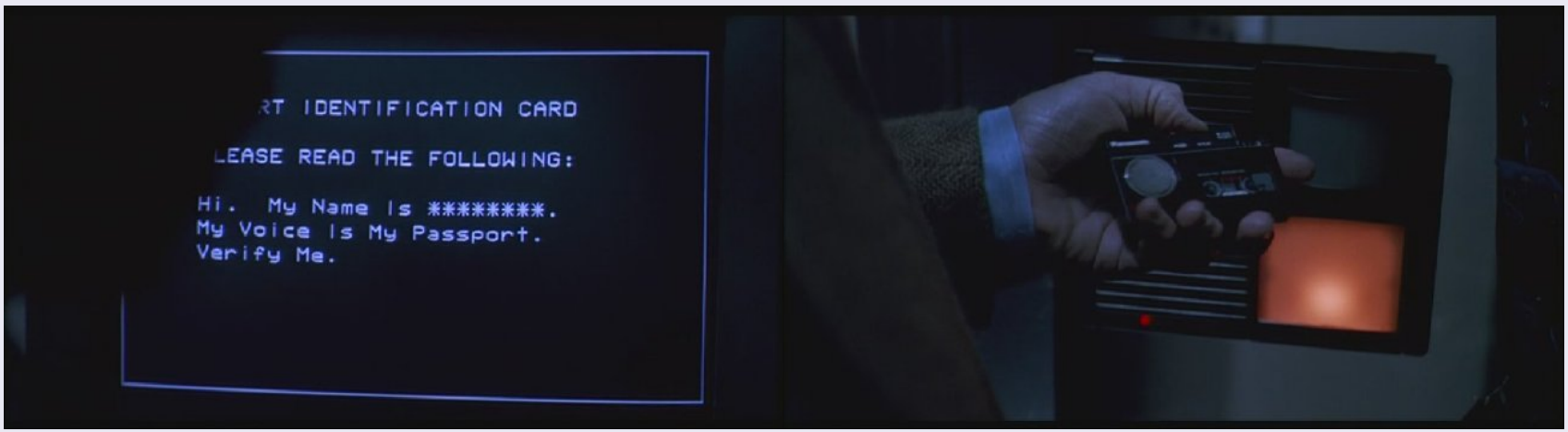
Keeping in mind the reproducible research principle whenever possible

More info on projects, team, publications, ...

`http://www.idiap.ch/~marcel`

Biometric Spoofing in Movies

Sneakers (1992)



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

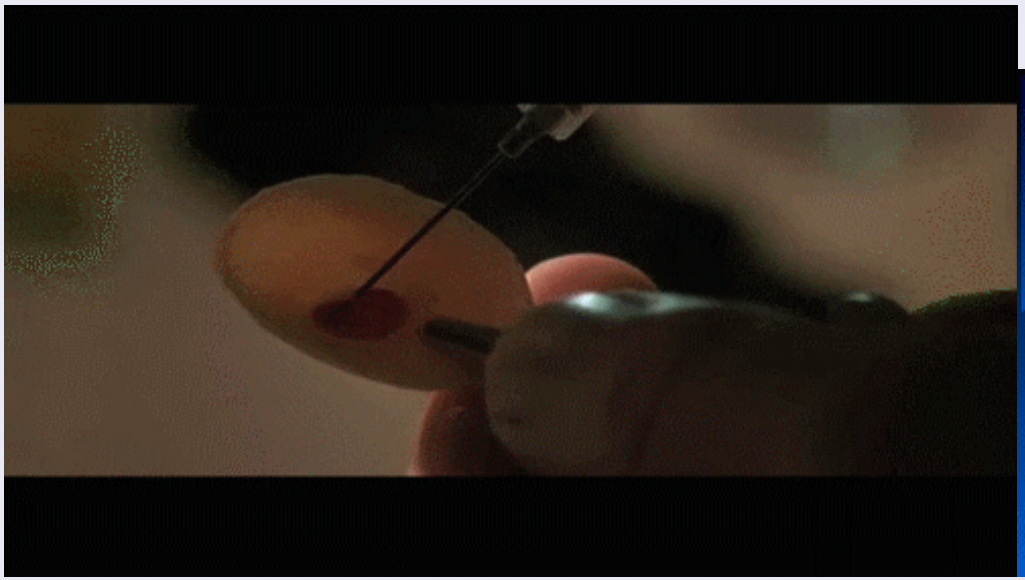
Biometric Spoofing in Movies

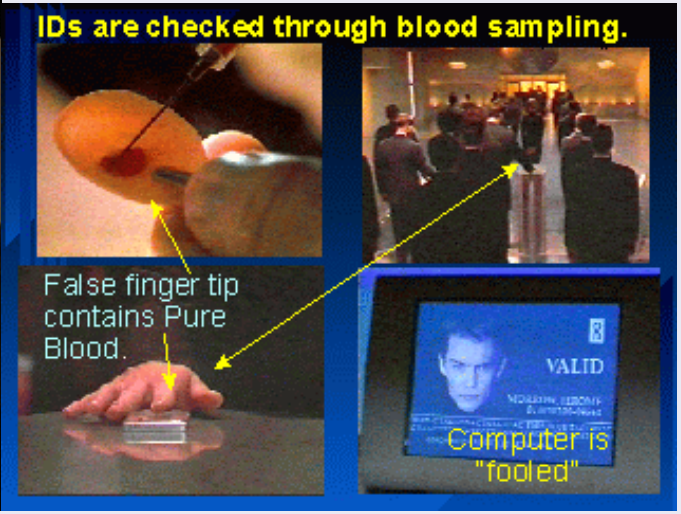
Demolition Man (1993)

Present an eyeball in front of a iris scanner !

Biometric Spoofing in Movies

GATTACA (1997)





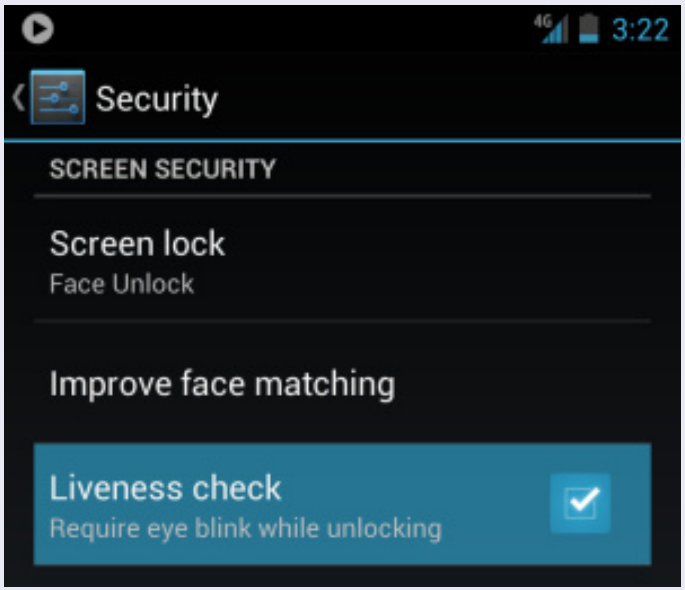
Injecting blood samples in a false finger tip to fool DNA identification !

Biometric Spoofing in reality

Android 4.0 (Nov 2011)

Android 4.0 Face UnLock feature spoofed by photograph

Android 4.1 (Jun 2012)



Liveness check (eye blink) introduced in Android 4.1

Biometric Spoofing in reality

Hong Kong - Vancouver (Jan 2011)

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

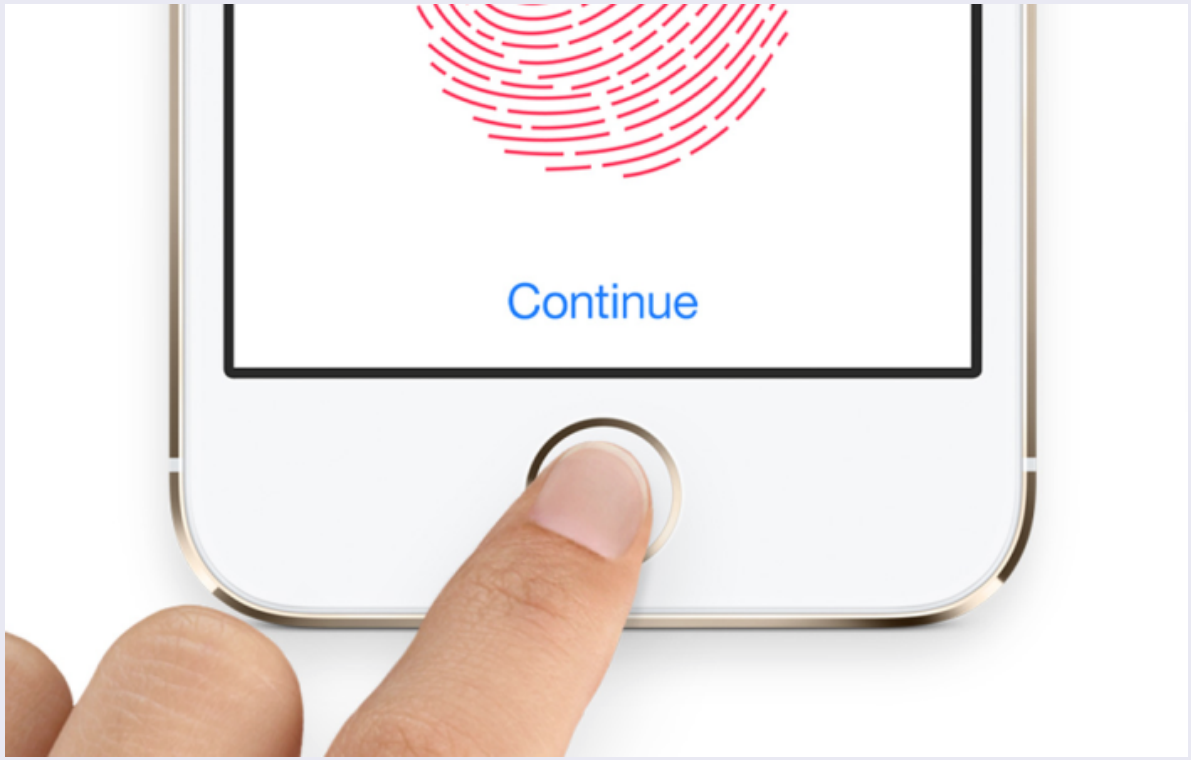
Biometric Spoofing in reality

Brazil (March 2013)

Fake fingers used to fool Hospital clock-in scanner

Biometric Spoofing in reality

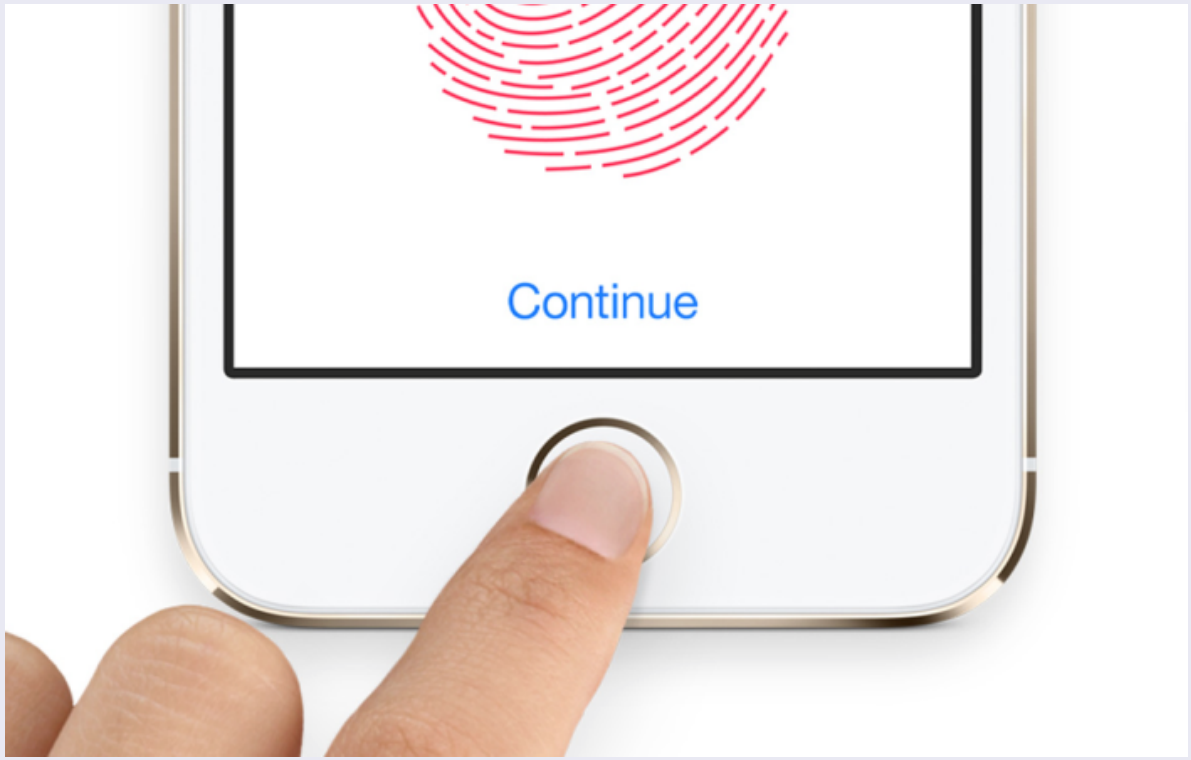
iPhone 5s - Touch ID (Sep 20 2013)



How many days will it take to spoof it ?

Biometric Spoofing in reality

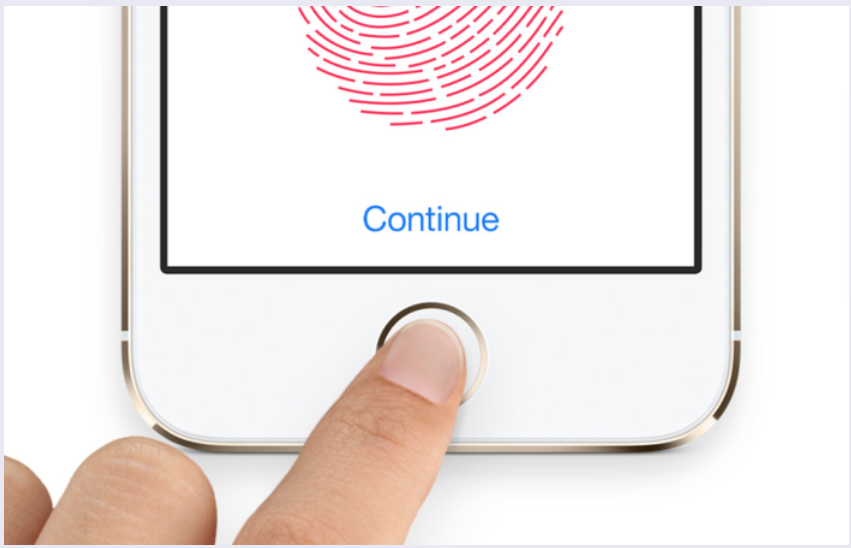
iPhone 5s - Touch ID (Sep 20 2013)



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

Biometric Spoofing in reality

Apple and fingerprints the full story



`http://fingerchip.pagesperso-orange.fr/biometrics/types/fingerprint_apple.htm`

Jean-François Mainguet (Sep 22 2013)

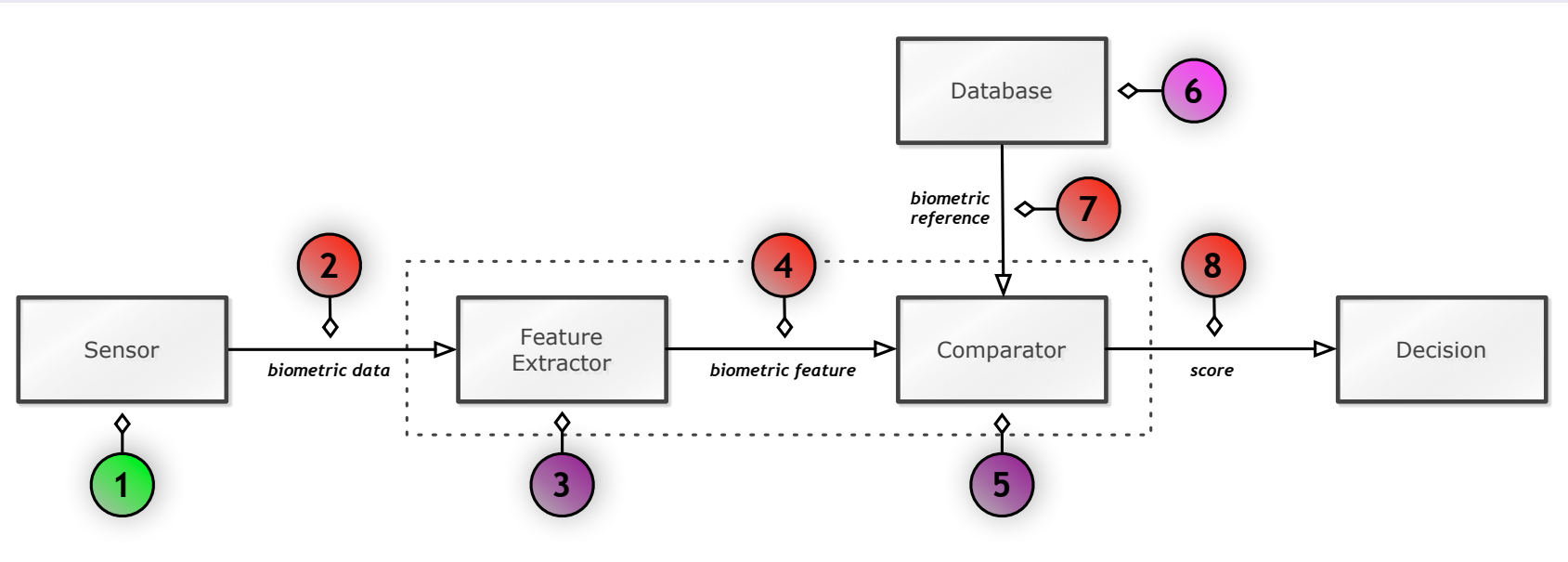
Biometric Spoofing in reality

More ?

How many cases that we don't know ?

Biometric Security Vulnerabilities

Attacks

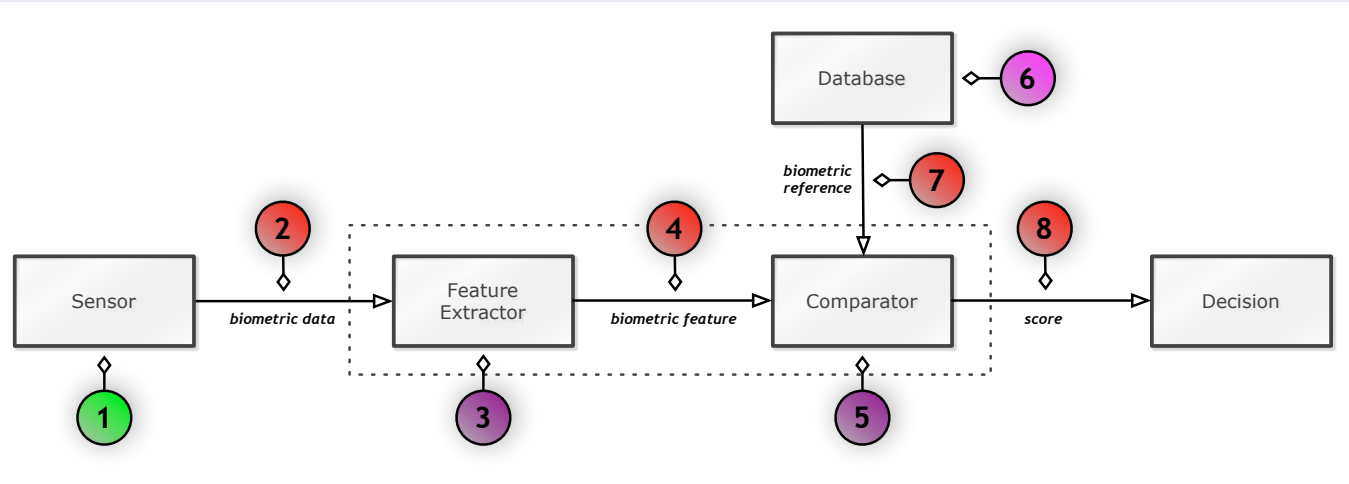


- Indirect attacks (**2-8**)
- Direct attacks (**1**)

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

Biometric Security Vulnerabilities

Indirect Attacks

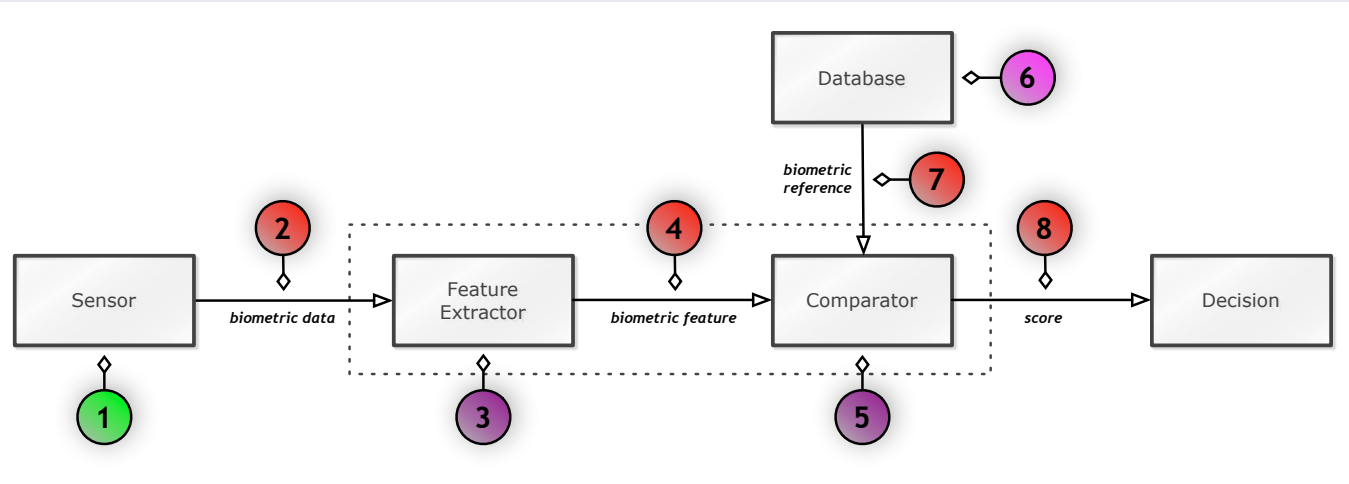


Indirect attacks are performed inside the system by:

- 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**).

Biometric Security Vulnerabilities

Direct Attacks

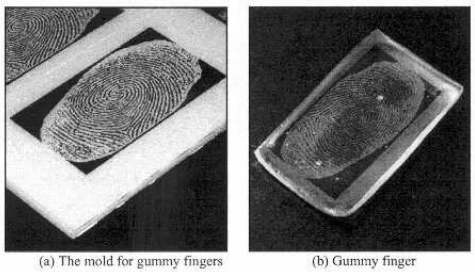


Direct attacks (**spoofing attacks**) are performed at the sensor level: the sensor is fooled (spoofed) and not replaced.

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

Literature

“Gummy Fingers”



(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).

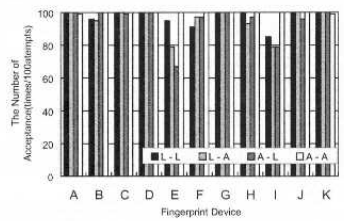
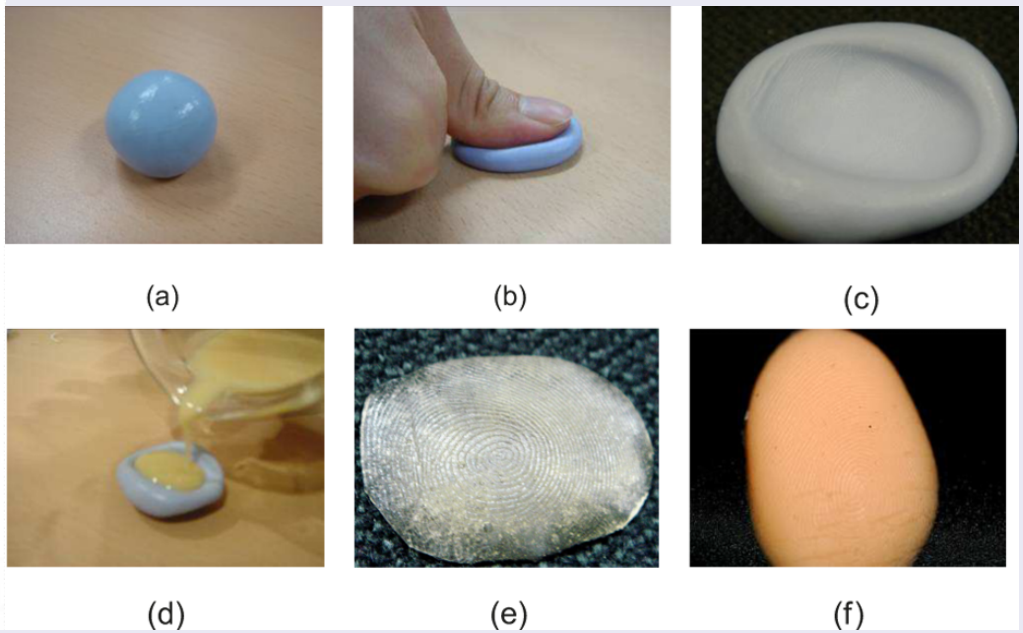


Figure 4.7 Average number of acceptance for each device, in terms of *gummy* fingers which were cloned from residual fingerprints. Here, the subject is one person.



Gelatin fake fingers to spoof 11 fingerprint biometric systems

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

Literature

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

Literature

Black Hat 2009

Printed photo to spoof face recognition systems on 3 laptops

D. Nguyen et al. *Your Face Is NOT Your Password*, 2009

Literature

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

Definition

Spoofing Attack

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

K. Nixon et al. *Spoof Detection Schemes; Handbook of Biometrics*, 2008

Also called *Presentation Attack*.

Anti-Spoofing

Countermeasure to spoofing attack

Also called *Presentation Attack Detection, Liveness Detection*.

Spoofing Attacks

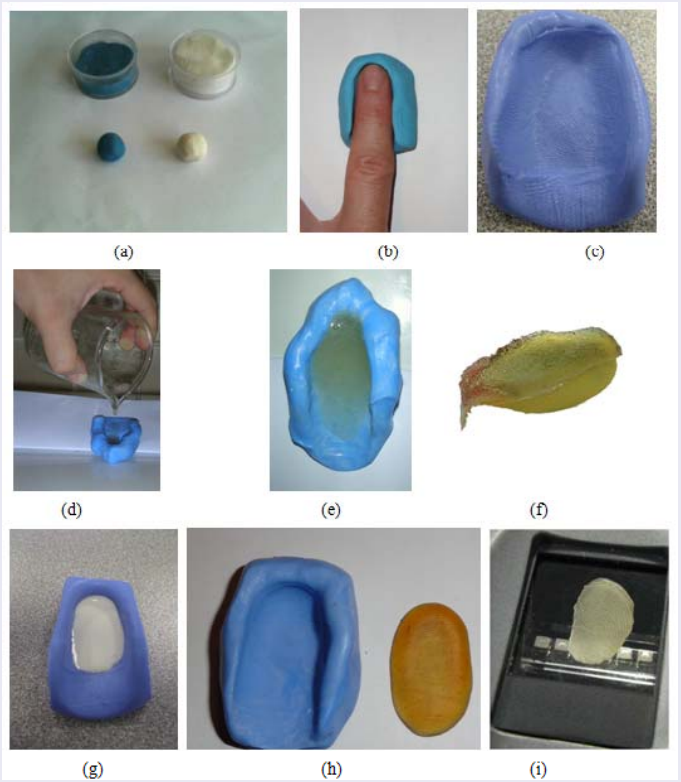
Fingerprint spoofing: fake fingerprint

Presenting a fake fingerprint to a capture device

Acknowledgement: Gian Luca Marcialis and Fabio Roli @ UNICA

Spoofing Attacks

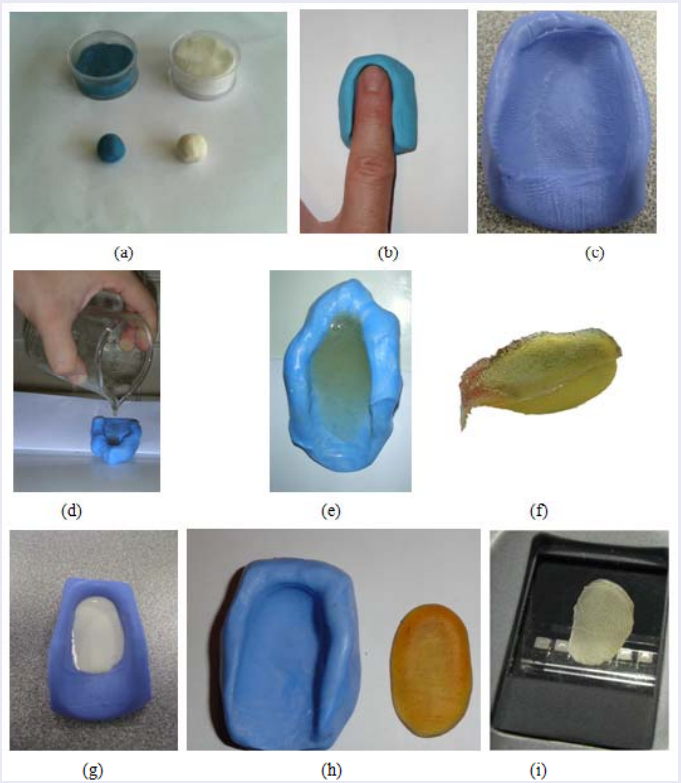
Fingerprint spoofing: fake fabrication (with cooperation)



Prepare a silicon mold (a, b and c)

Spoofing Attacks

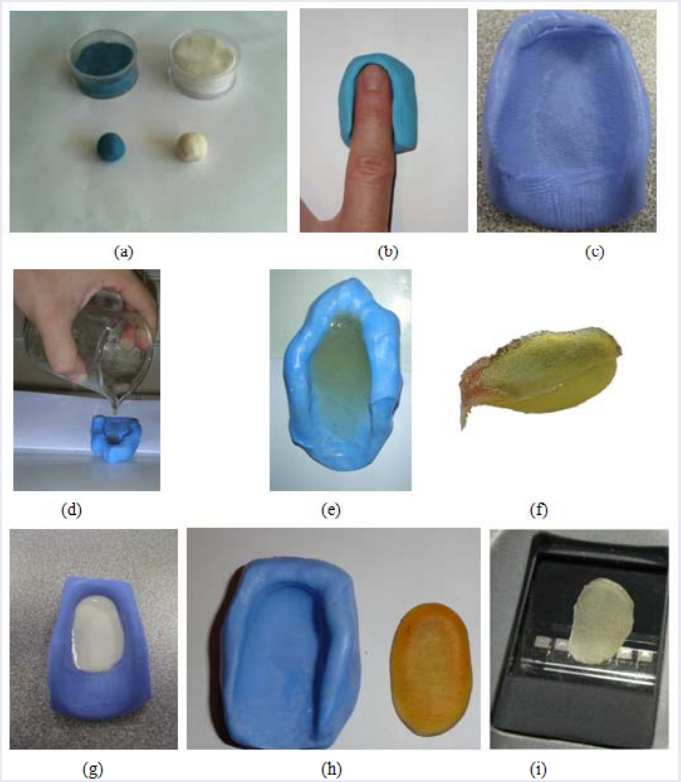
Fingerprint spoofing: fake fabrication (with cooperation)



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

Spoofing Attacks

Fingerprint spoofing: fake fabrication (with cooperation)



Use fake (g, i and j)

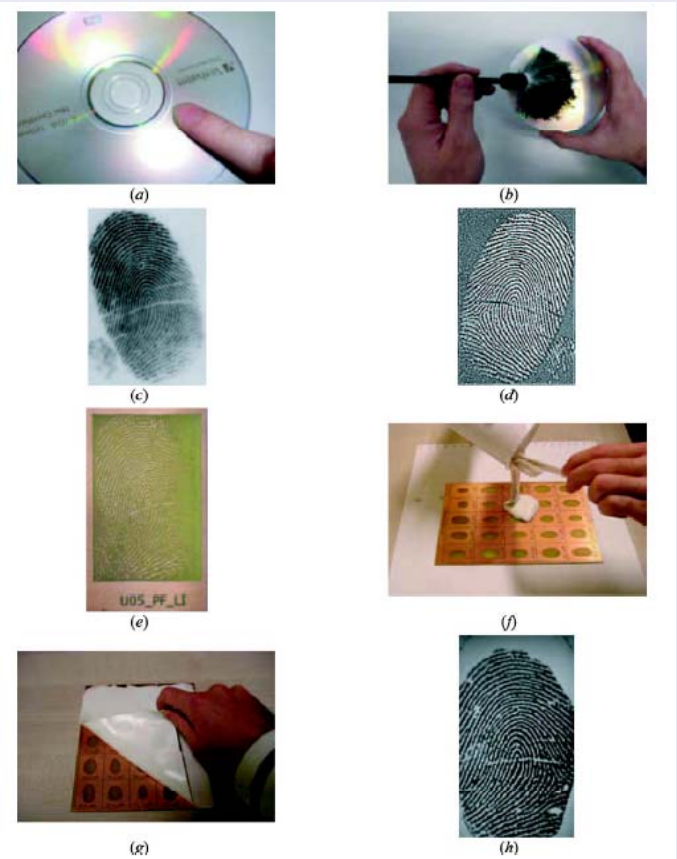
Spoofing Attacks

Fingerprint spoofing: fake fabrication (with cooperation)

Same recipe but with hot glue and wood glue !

Spoofing Attacks

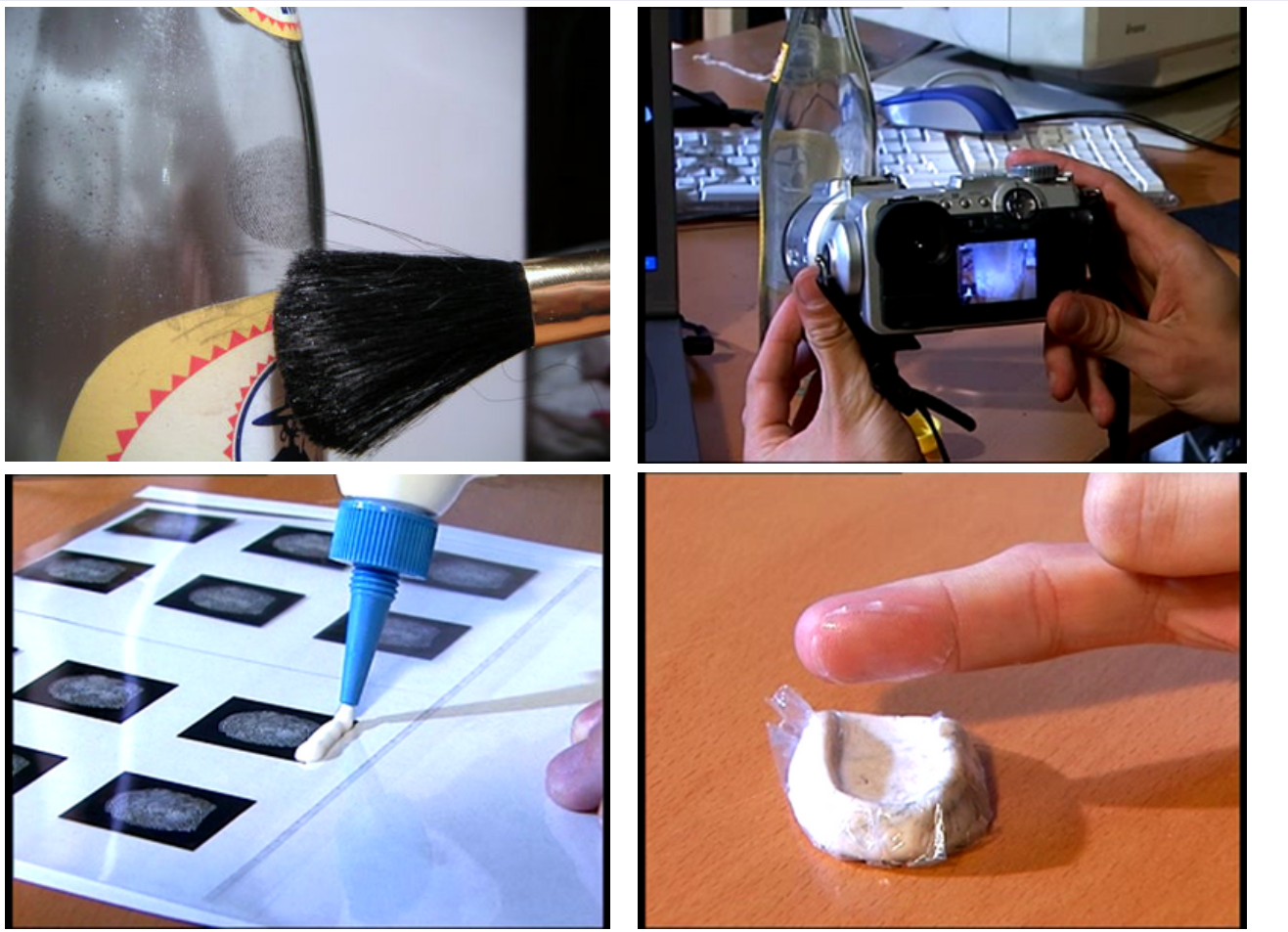
Fingerprint spoofing: fake fabrication (without cooperation)



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

Spoofing Attacks

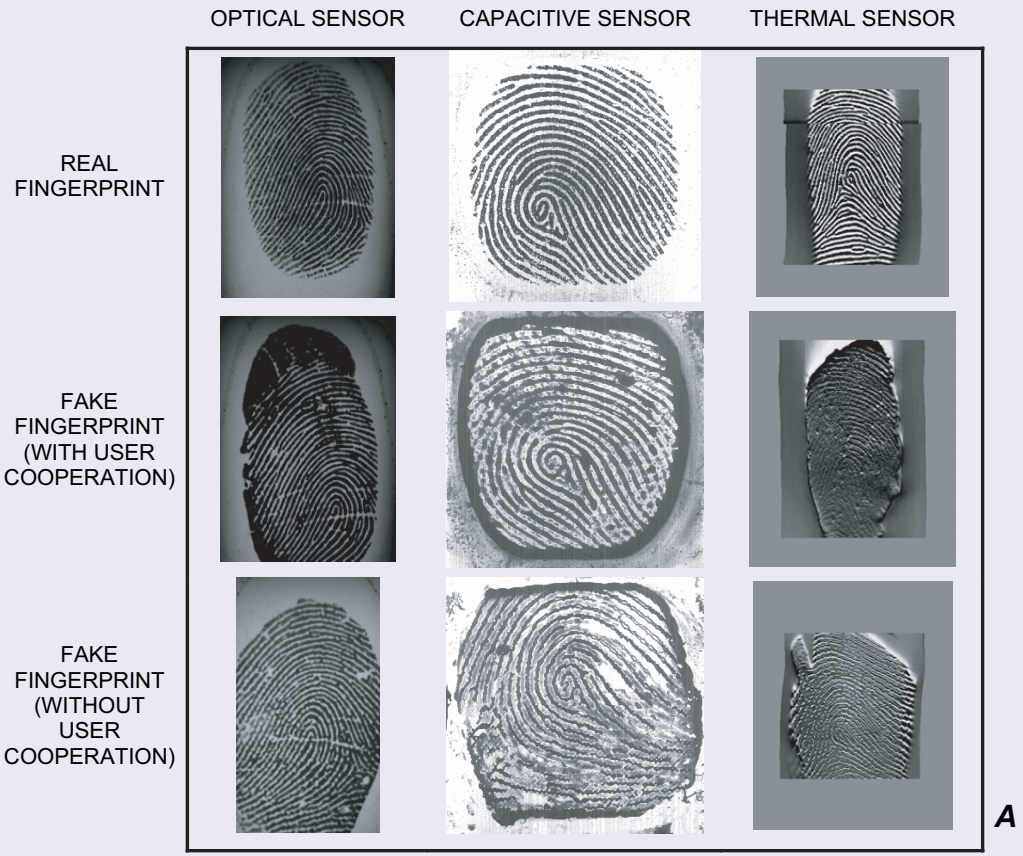
Fingerprint spoofing: fake fabrication (without cooperation)



CCC vs iPhone5s: `http://dasalte.ccc.de/biometrie/fingerabdruck_kopieren?language=en`

Spoofing Attacks

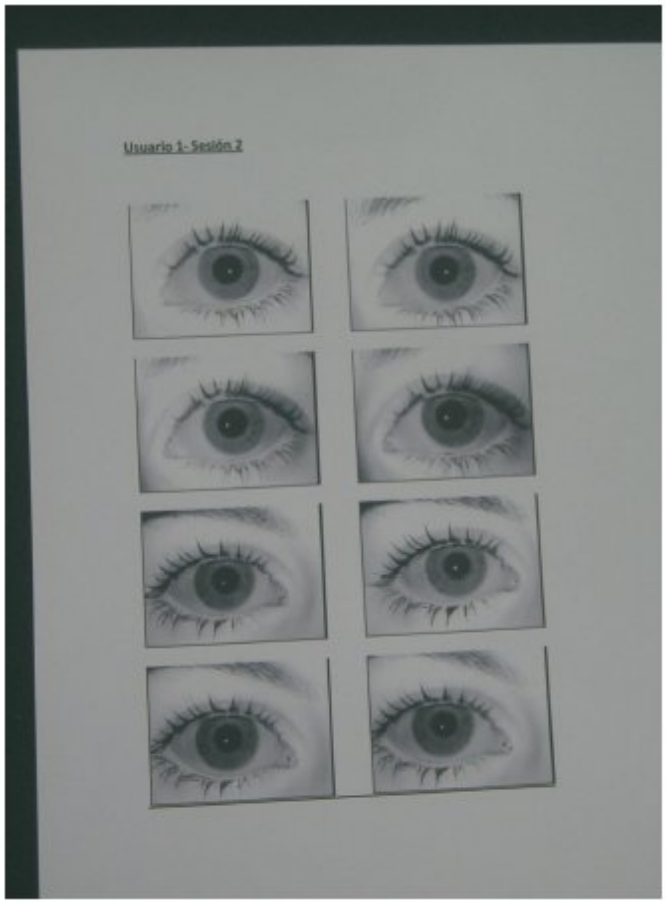
Fingerprint spoofing: biometric data



Acknowledgement: Julian Fierrez @ UAM

Spoofing Attacks

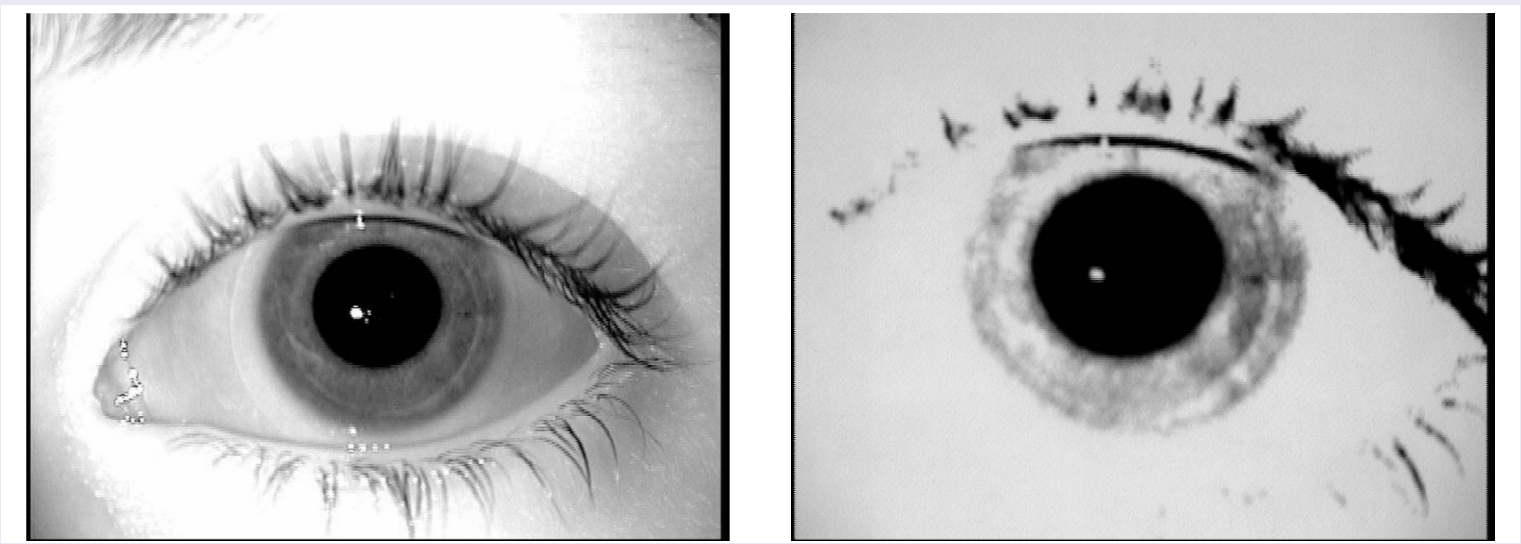
Iris spoofing: print attack



High quality paper and inkjet printer

Spoofing Attacks

Iris spoofing: biometric data (print)



Real Iris (left) vs Fake Iris (right)

Acknowledgement: Julian Fierrez @ UAM

Spoofing Attacks

2D face spoofing: print attack

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

Spoofing Attacks

2D face spoofing: biometric data (print/photo/video attack)

Why one is real or fake ?

Spoofing Attacks

2D face spoofing: biometric data (print/photo/video attack)

Why one is real or fake ?

All are fakes: print (left), iPhone (middle) and iPad (right) !

Acknowledgement: Andre Anjos @ IDIAP

Spoofing Attacks

2D face spoofing: 3D mask

Hard resin composite in full 24-bit color !

Acknowledgement: Nesli Erdogmus @ IDIAP

Spoofing Attacks

2D face spoofing: 3D mask

Cost: ∼USD300

Spoofing Attacks

2D face spoofing: 3D mask fabrication

1 frontal and 2 profile pictures

`http://www.thatsmyface.com`

Spoofing Attacks

2D face spoofing: 3D mask fabrication

Cost: ∼USD25

Spoofing Attacks

Voice spoofing: replay attack

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 spoofing: voice synthesis

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

Voice spoofing: voice conversion

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

Biometrics under Spoofing

Real and Attack accesses

- Licit scenario:
  - real accesses of users to enroll biometric references (gallery),
  - real accesses of users to perform biometric comparison (client and zero-effort impostor probes).

  to measure the baseline performance of a biometric system
- Spoof scenario: spoofing attack accesses to perform biometric comparison (impostor probes)
  to measure the vulnerability of a biometric system on the enrolled users

Biometrics under Spoofing

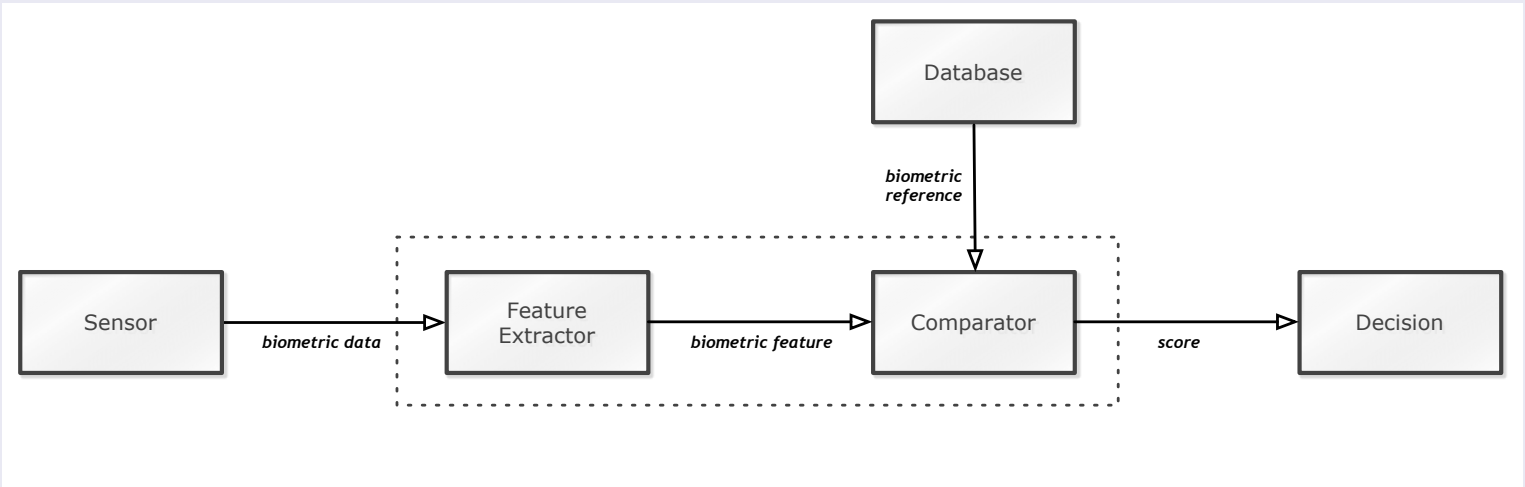
Unbiased Protocol (no identity overlap)

- Training set: biometric system (background models, eg. PCA/LDA) or countermeasure
- Development set:
  - enroll: enroll biometric references
  - probe: perform biometric comparison (client, zero-effort impostor, spoofing attacks)

  Determine the decision threshold and *a posteriori* performance at a given operation point
- Testing set:
  - enroll: enroll biometric references
  - probe: perform biometric comparison (client, zero-effort impostor, spoofing attacks)

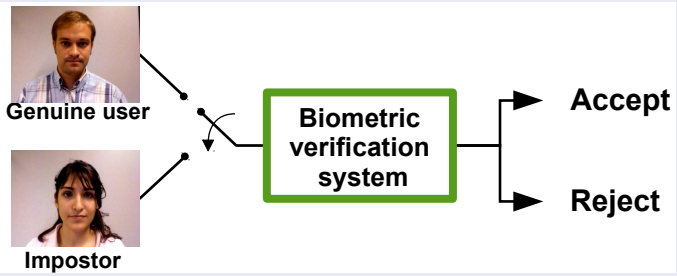
  Compute the *a priori* performance given the determined threshold

Biometric system: overview

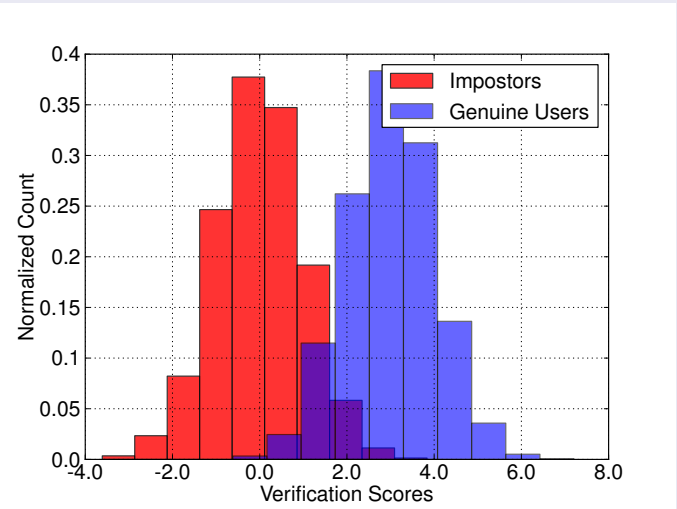


For a given input the biometric system produces a score !

Biometric system: score distribution



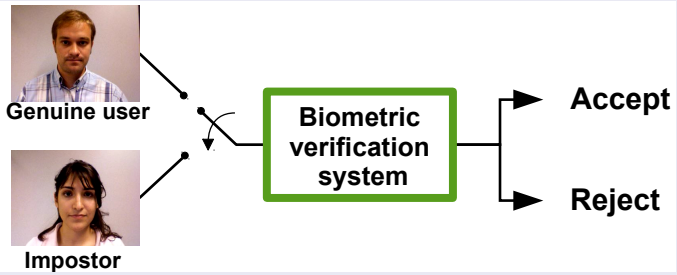
High score for genuine user and low score for zero-effort impostors



Spoofing attacks not considered here (**Licit scenario**)

Biometrics under Spoofing

Biometric system: measuring the performance

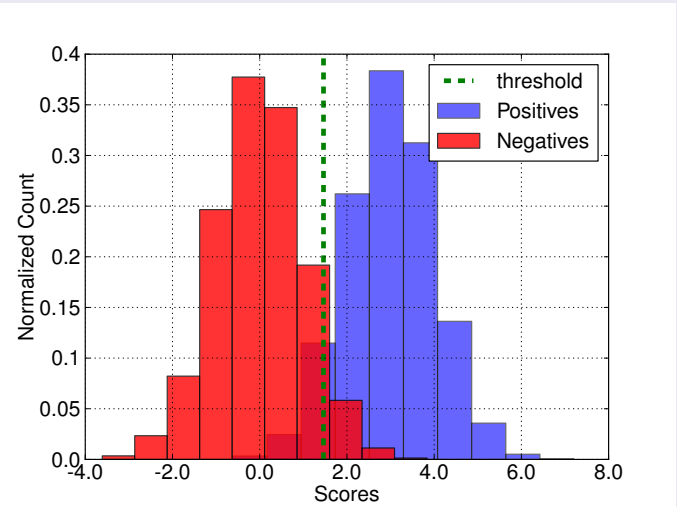


We measure 2 errors:

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

Spoofing attacks not considered here (**Licit scenario**)

Biometric system: measuring the performance

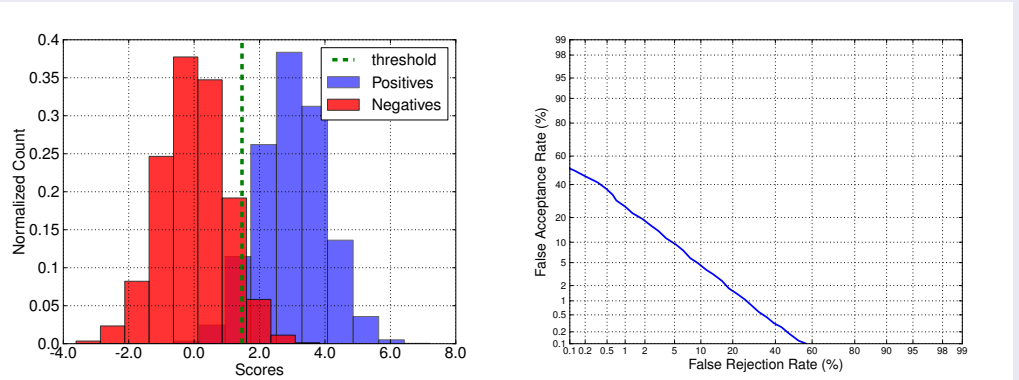


FAR and FRR for a given threshold τ and may report a single measure Half Total Error Rate (HTER):

$$\mathrm{HTER}(\tau, \mathcal{D}) = \frac{\mathrm{FAR}(\tau, \mathcal{D}) + \mathrm{FRR}(\tau, \mathcal{D})}{2}$$

Spoofing attacks not considered here (**Licit scenario**)

Biometric system: a posteriori performance



minimum Weighted Error Rate (WER) criteria on the development set $\mathcal{D}_{dev}$ to determine τ^*_{WER}:

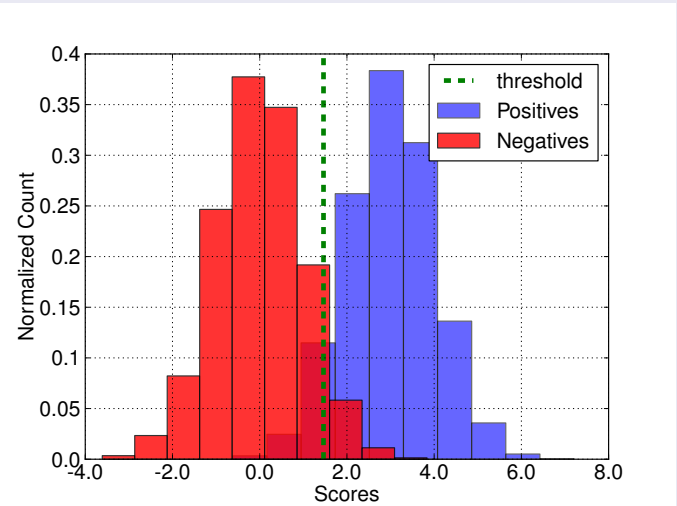
$$\tau^*_{\text{WER}} = \arg\min_{\tau} \left[\beta \cdot \text{FAR}(\tau, \mathcal{D}_{dev}) + (1-\beta) \cdot \text{FRR}(\tau, \mathcal{D}_{dev})\right]$$

with $\beta \in [0, 1]$ a predefined parameter which balances between the importance (cost) of FAR and FRR

$\beta = 0.5$ leads to minimum Half Total Error Rate (HTER) criteria !

Biometrics under Spoofing

Biometric system: a priori performance

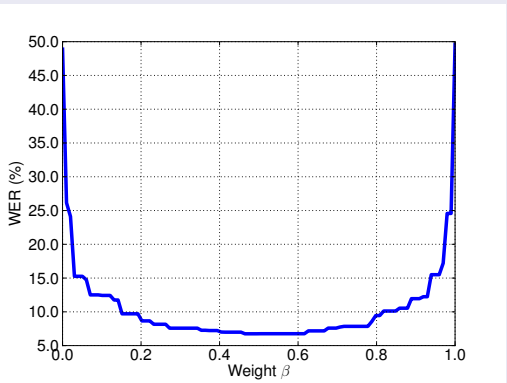


WER on the test set $\mathcal{D}_{test}$ using τ^*_{WER}:

$$\mathrm{WER}(\tau^*_{\mathrm{WER}}, \mathcal{D}_{test}) = \beta \cdot \mathrm{FAR}(\tau^*_{\mathrm{WER}}, \mathcal{D}_{test}) + (1-\beta) \cdot \mathrm{FRR}(\tau^*_{\mathrm{WER}}, \mathcal{D}_{test})$$

Biometric system: evaluation plot

Expected Performance Curve (EPC)[1]

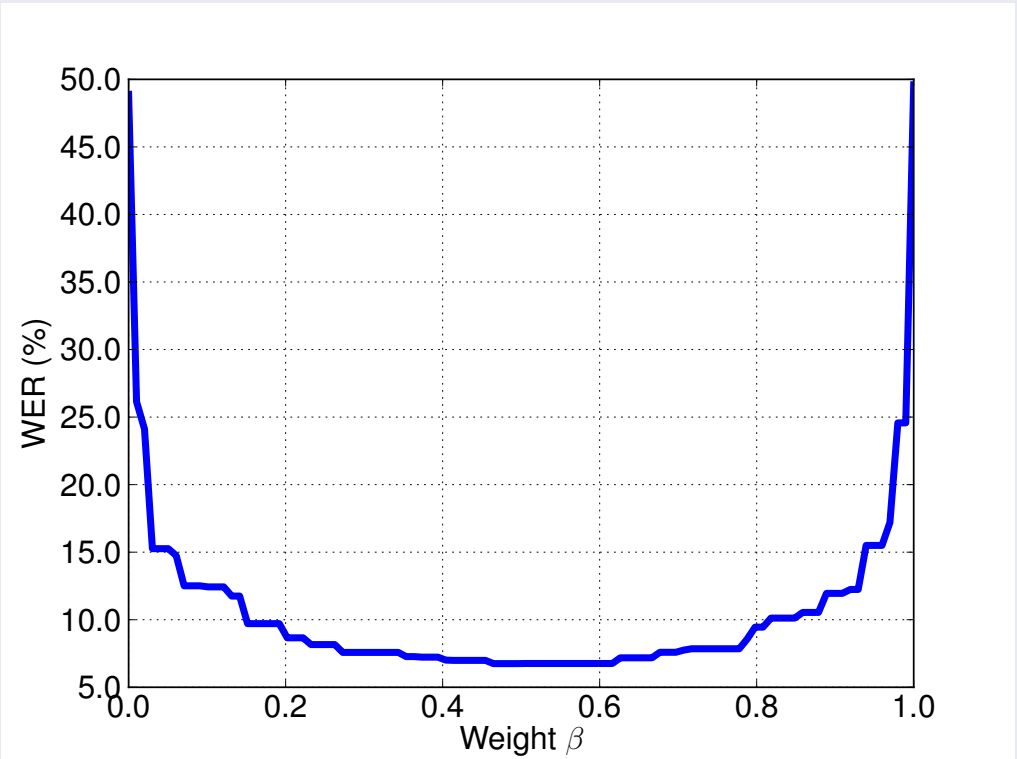


- plots the error rate on the test set depending on a threshold selected a priori on the development set;
- accounts for varying the cost $\beta \in [0, 1]$ of FAR and FRR when calculating the threshold.

[1] *The Expected Performance Curve*, Bengio, Mariéthoz and Keller, ICML 2005.

Biometric system: evaluation plot

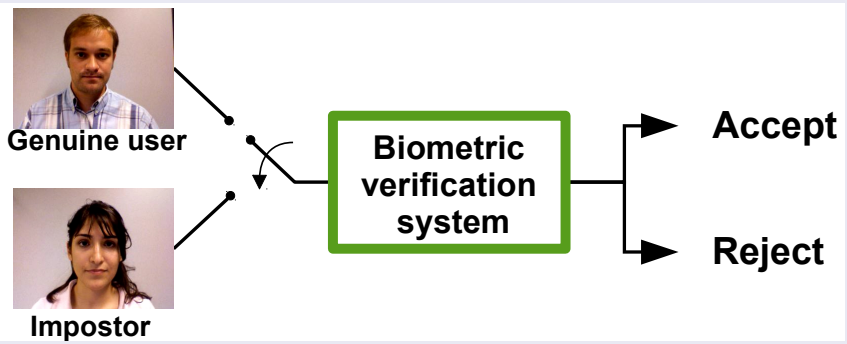
Expected Performance Curve (EPC)



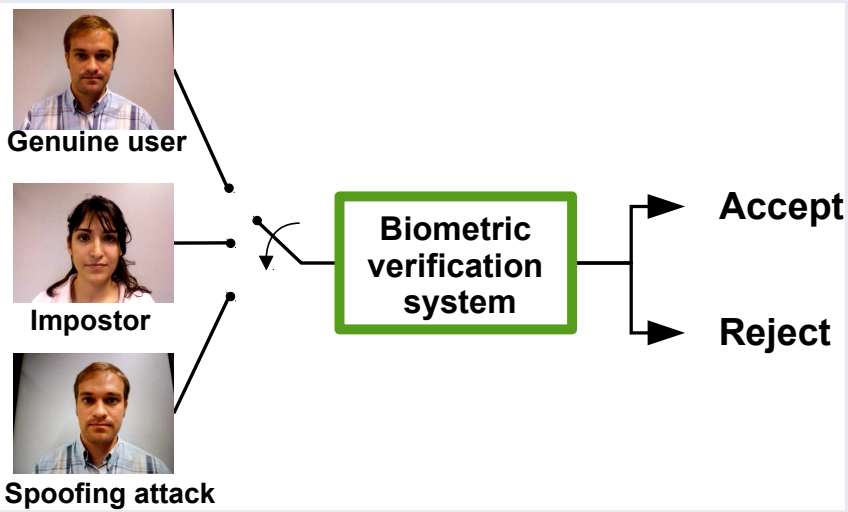
$$\mathrm{WER}(\tau^*_\beta, \mathcal{D}_{test}) = \beta \cdot \mathrm{FAR}(\tau^*_\beta, \mathcal{D}_{test}) + (1-\beta) \cdot \mathrm{FRR}(\tau^*_\beta, \mathcal{D}_{test})$$

Biometrics under Spoofing

Biometric system under spoofing attack: score distribution ?



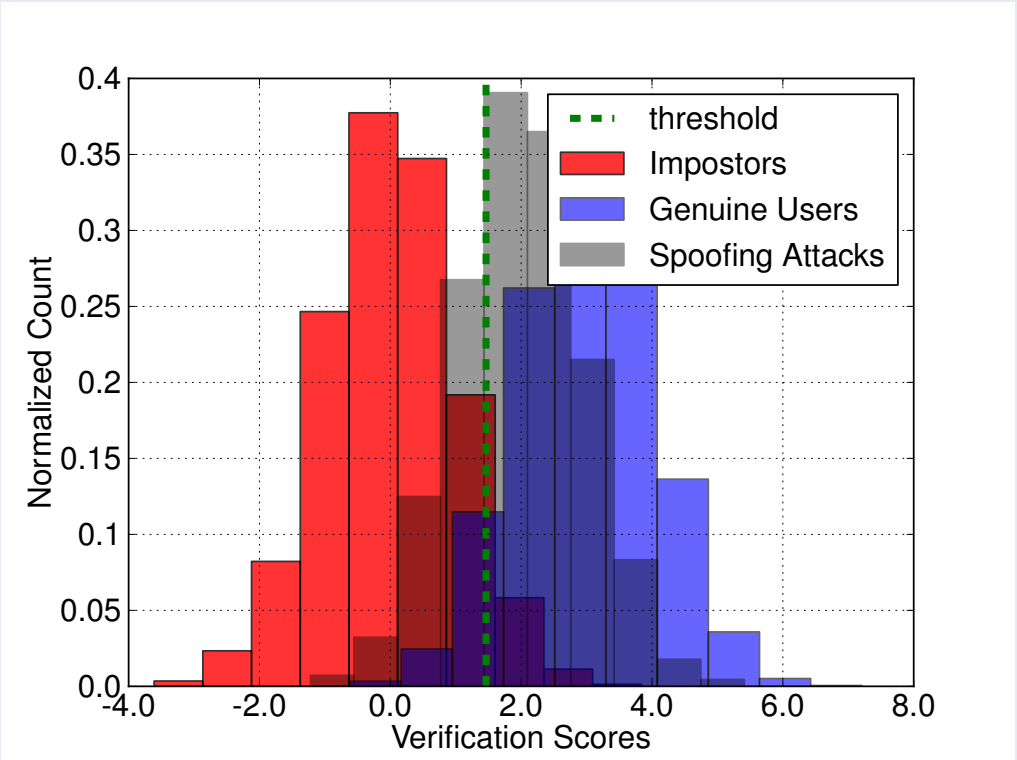
Spoofing attacks are now considered here (**Licit** + **Spoof scenario**)



Biometrics under Spoofing

Biometric system under spoofing attack: score distribution

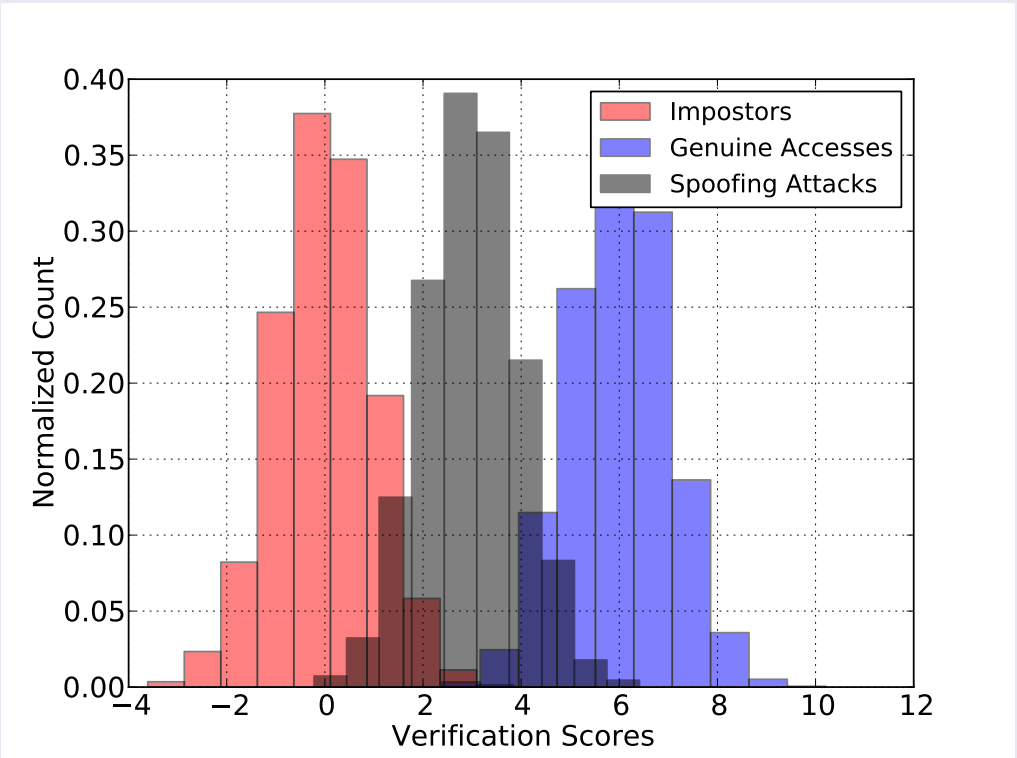
High score for genuine user, low score for zero-effort impostors but high score for spoofing attacks as well !



Scores produced by spoofing attacks overlap with the genuine scores

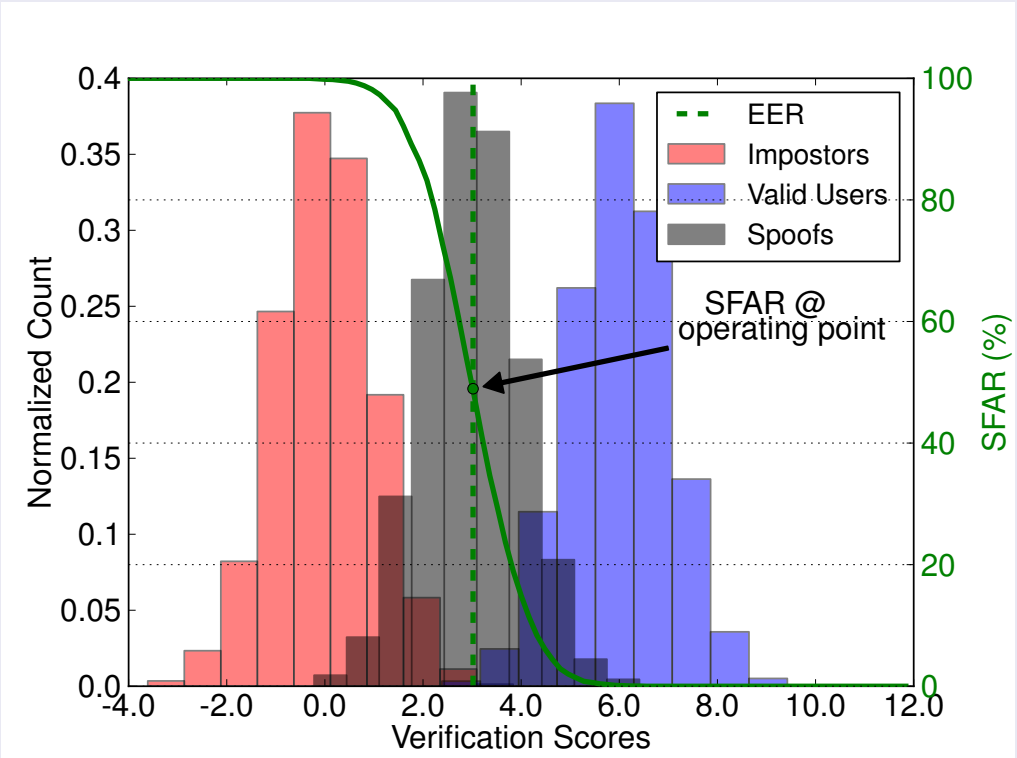
Biometrics under Spoofing

Biometric system under spoofing attack: measuring the vulnerability



Biometrics under Spoofing

Biometric system under spoofing attack: measuring the vulnerability

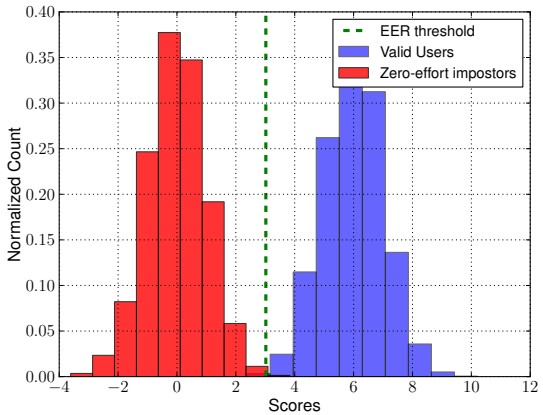


Spoof False Acceptance Rate (SFAR): % of spoofing attacks falsely accepted

Biometrics under Spoofing

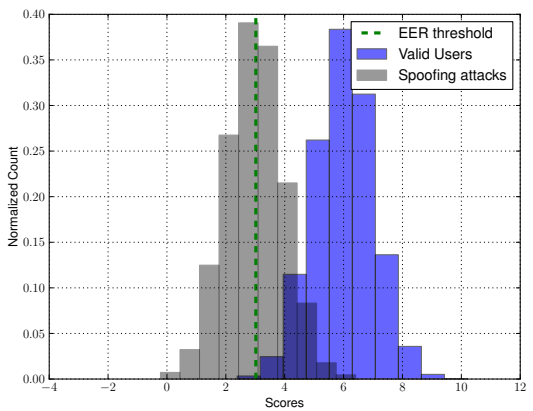
Licit scenario

- False Rejection Rate (FRR)
- False Acceptance Rate (FAR)
- Weighted Error Rate (WER)



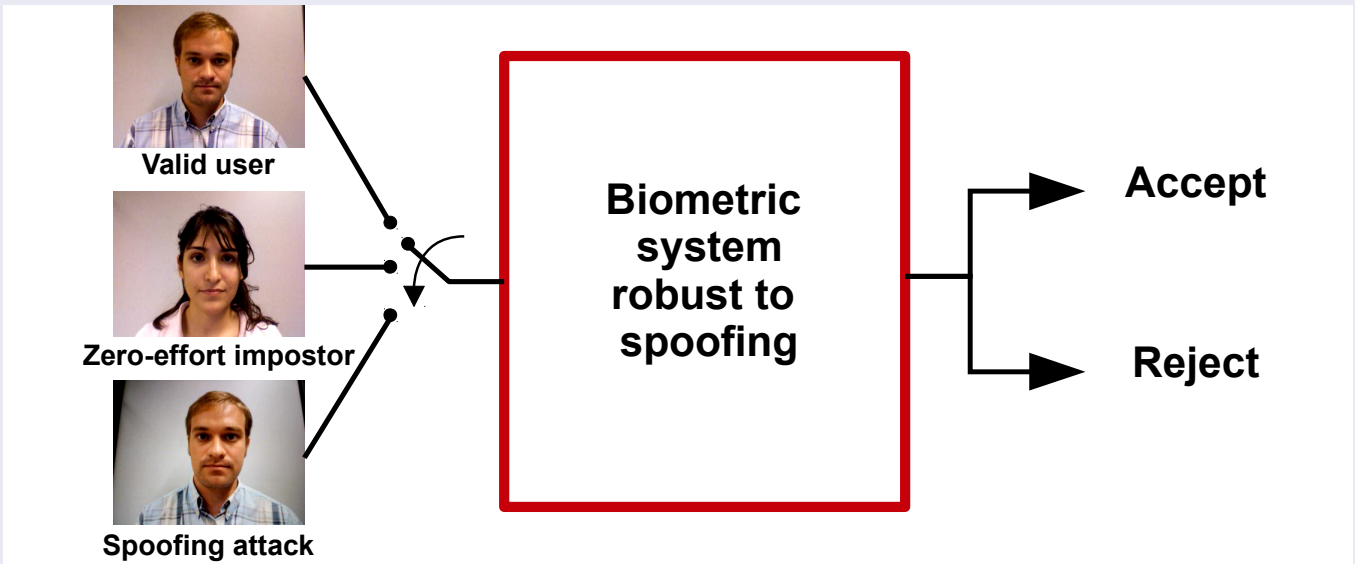
Spoof scenario

- Spoof False Acceptance Rate (SFAR)



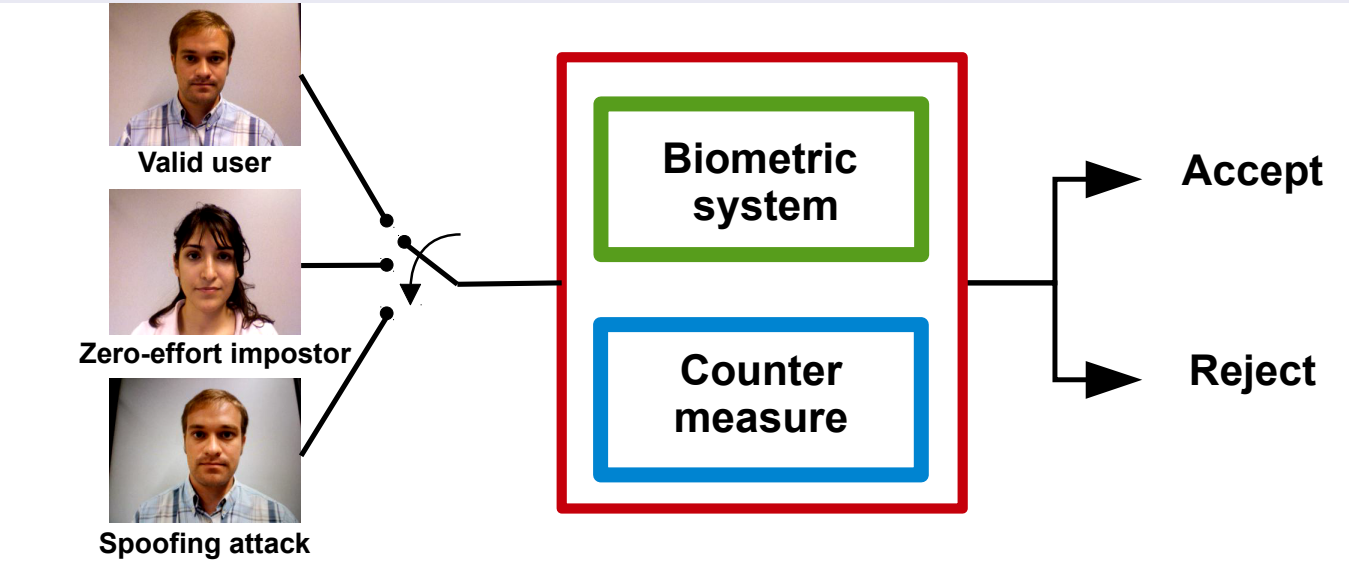
Anti-Spoofing

Single system robust to spoofing ?



Anti-Spoofing: adding a countermeasure

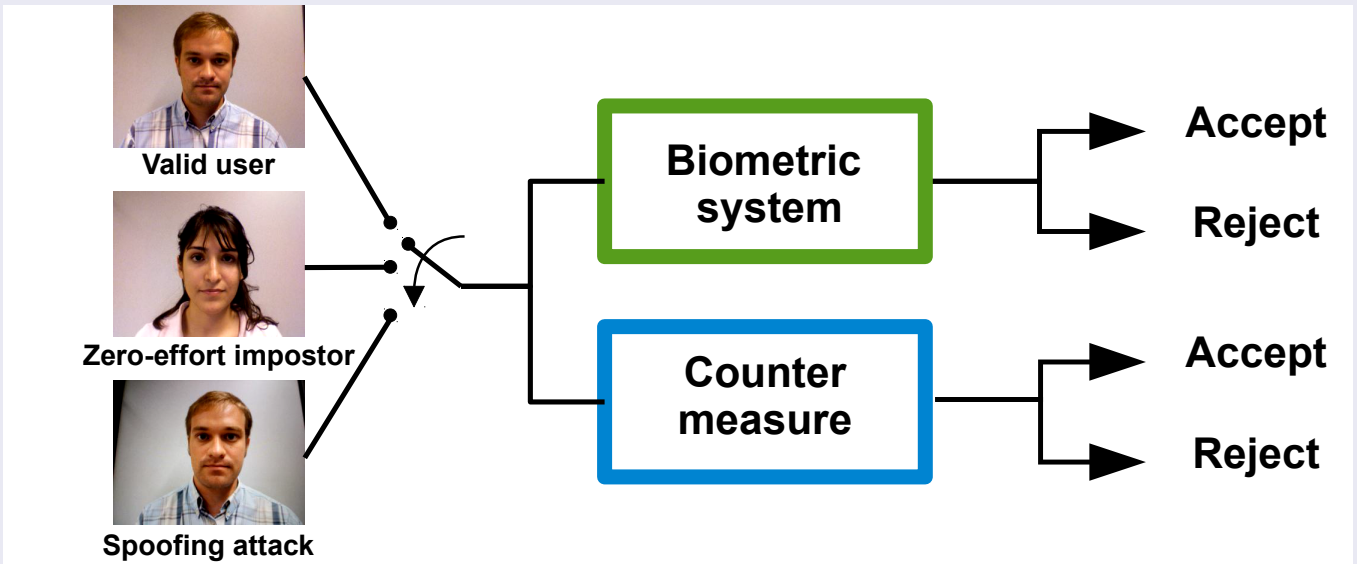
Two separate components



- A biometric system
- A countermeasure

Biometric System and Countermeasure

Two separate components

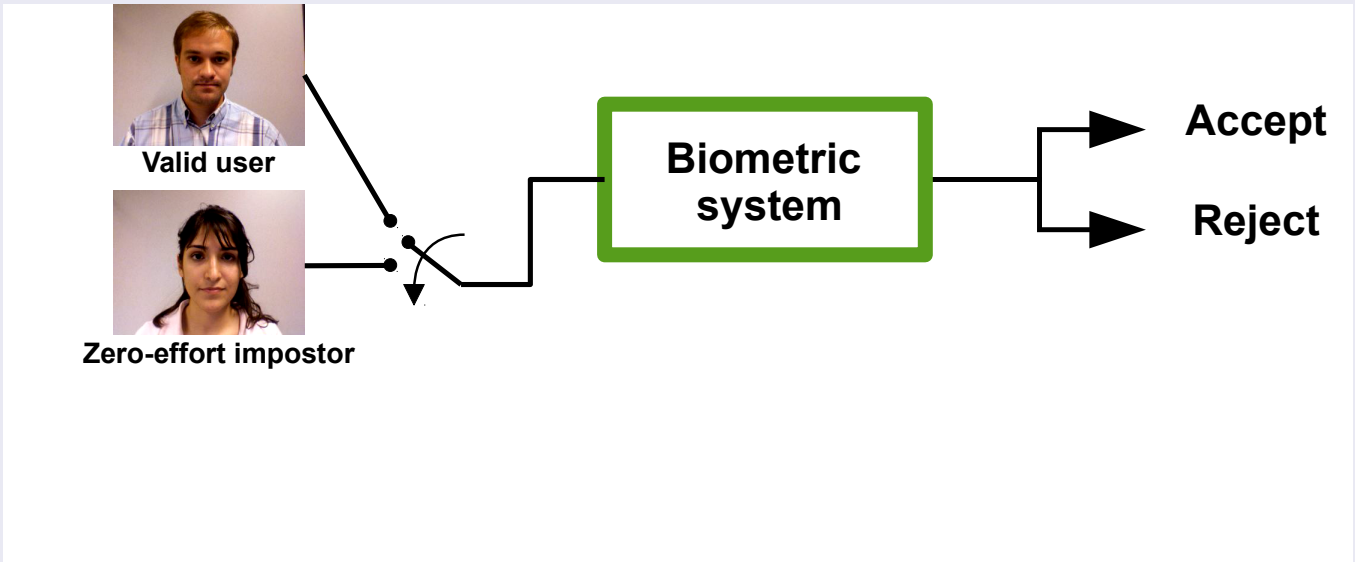


Overall

- Accept: genuine user and real access
- Reject: a zero-effort impostor and a spoofing attack

Biometric System and Countermeasure

Biometric System: a binary classifier

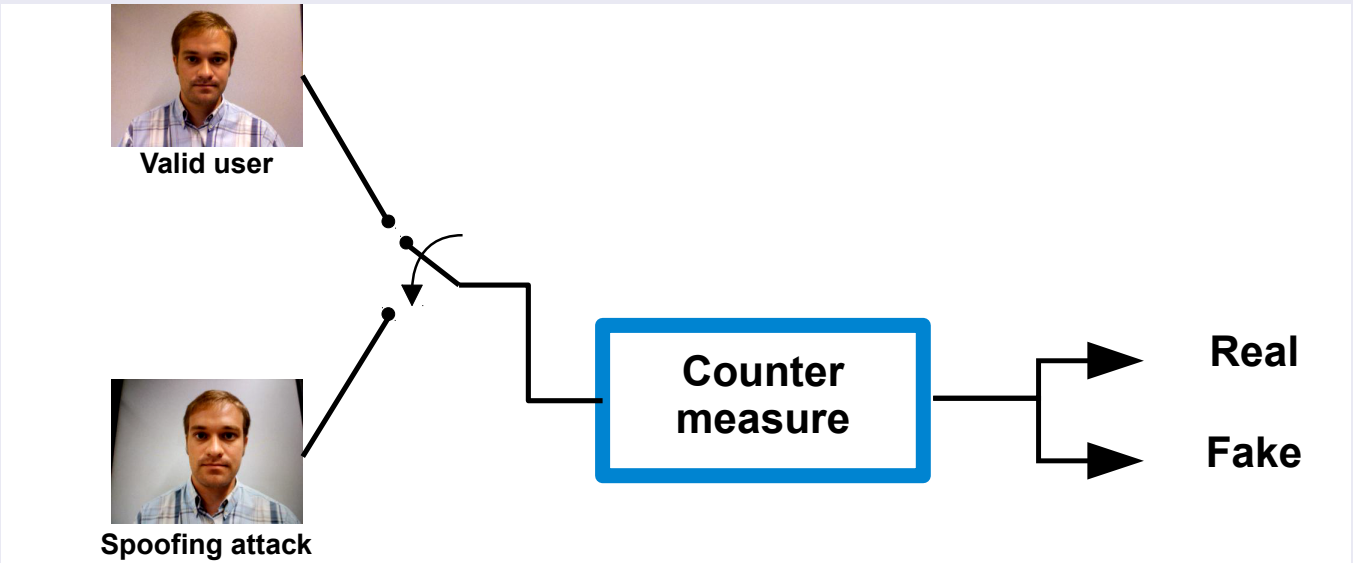


We measure 2 errors:

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

Biometric System and Countermeasure

Countermeasure: a binary classifier

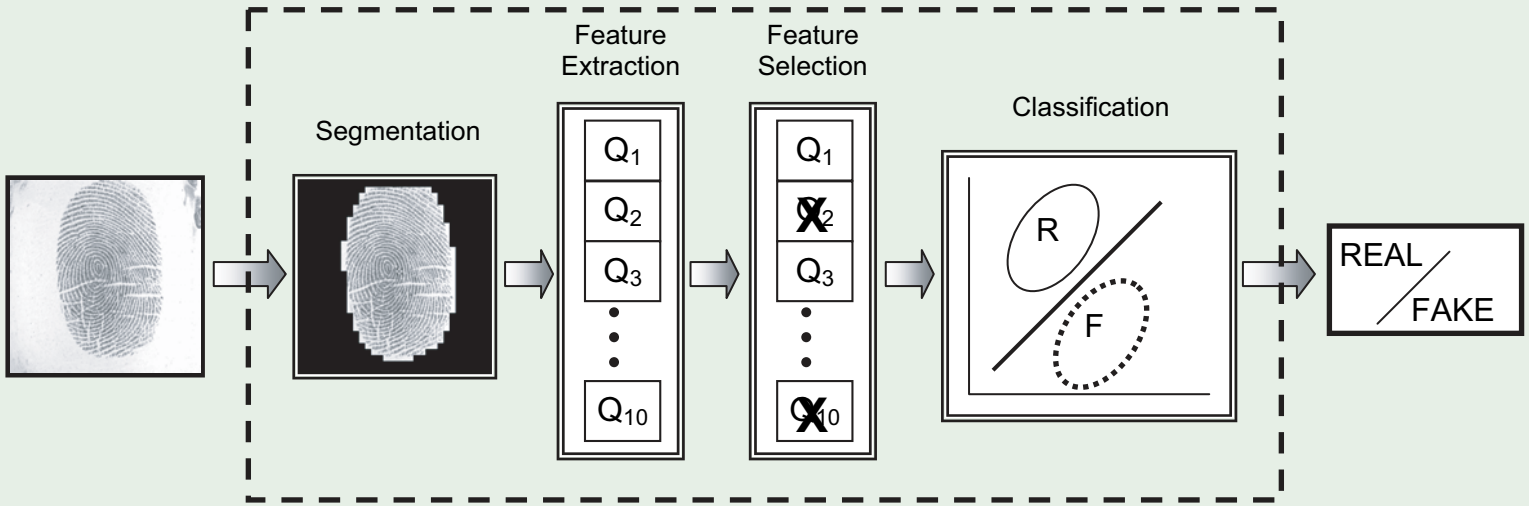


We measure 2 errors:

- False Living Rate (FLR): % of spoofing attacks misclassified as real
- False Fake Rate (FFR): % of real access misclassified as fake

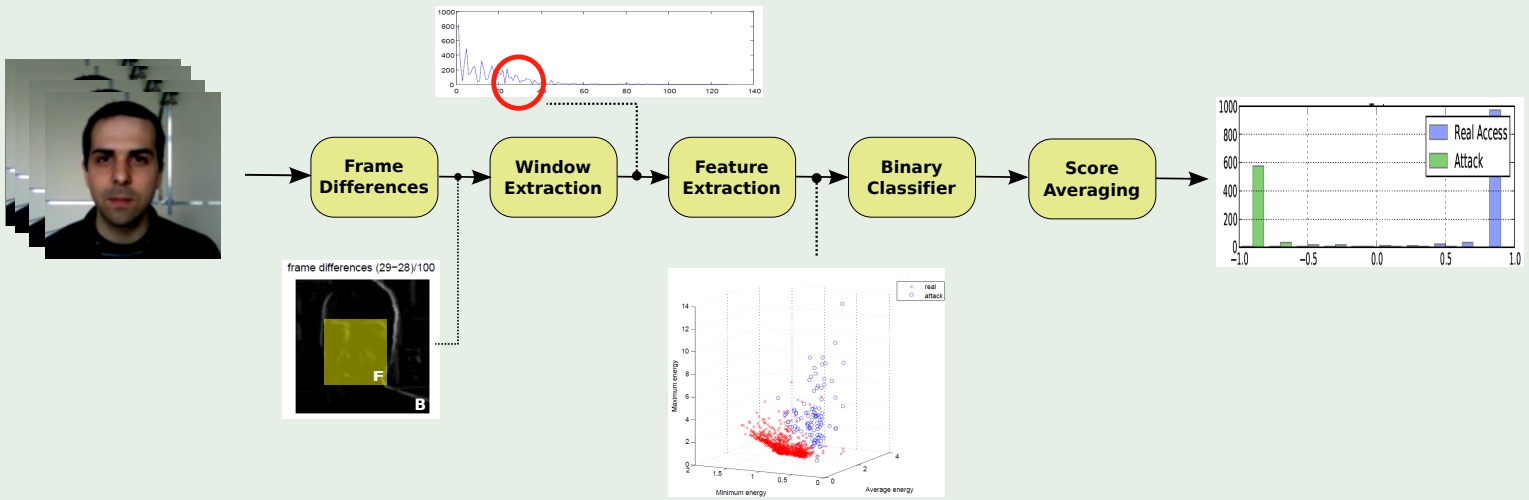
Biometric System and Countermeasure

Fingerprint: countermeasure



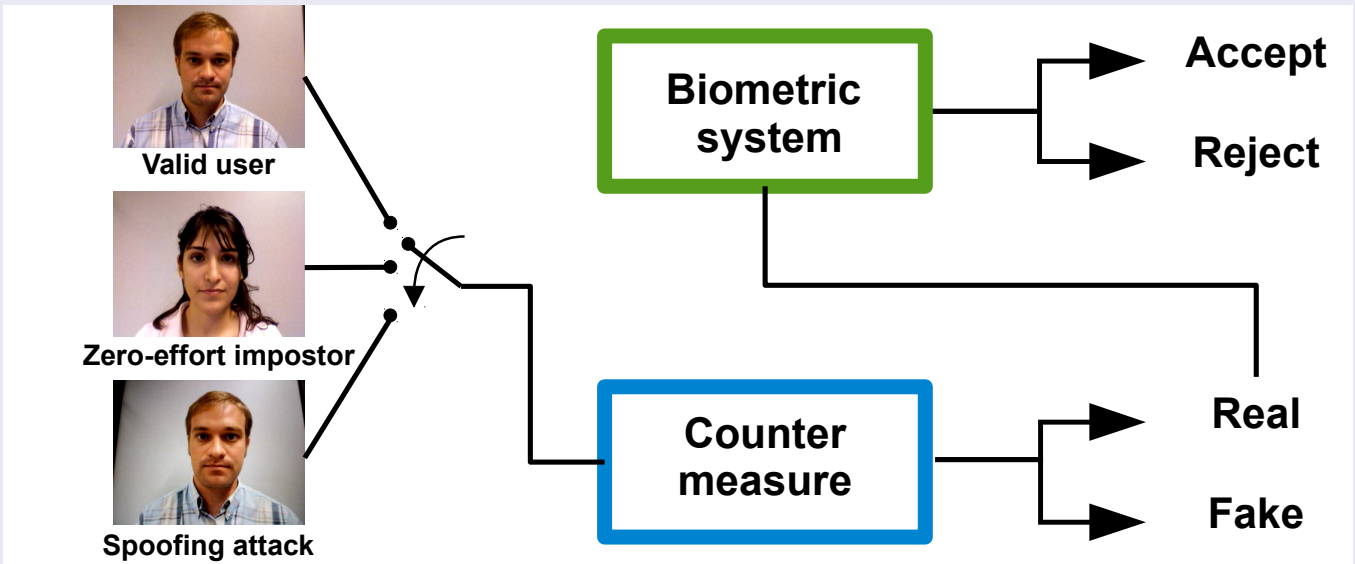
Biometric System and Countermeasure

2D face: countermeasure



Biometric System and Countermeasure

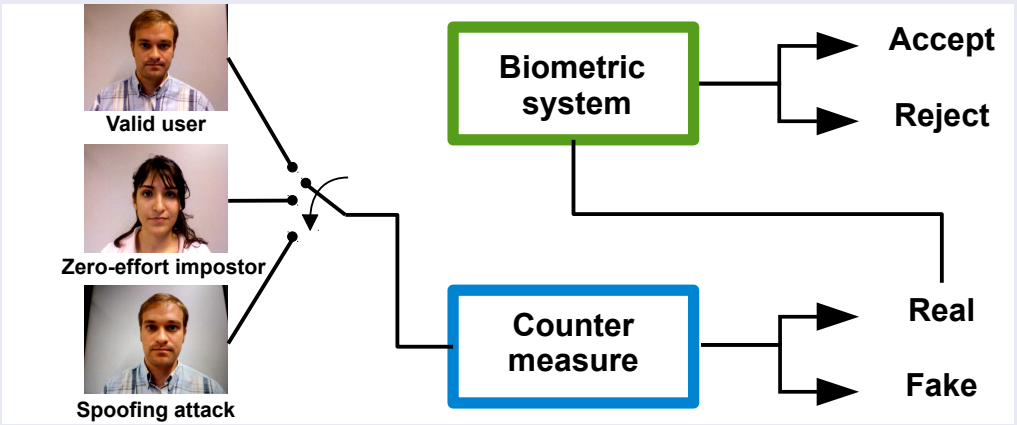
2-step process ?



Because the CM is a classifier a threshold need to be determined

Biometric System and Countermeasure

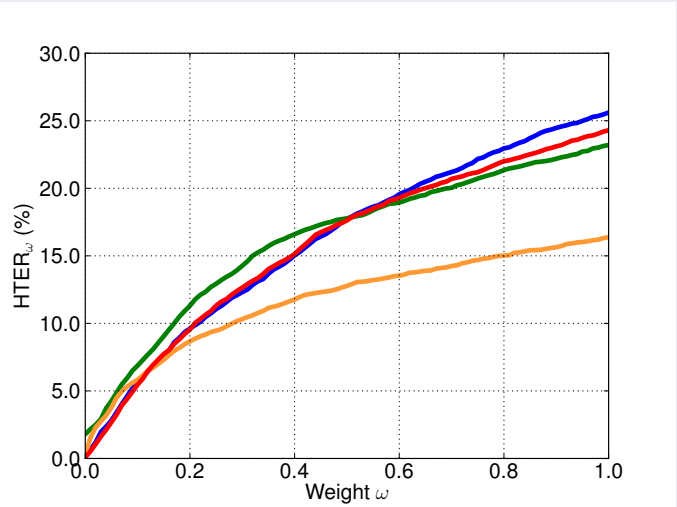
Drawback of the methodology



- 2 thresholds to determine
- the threshold for CM need to fixed beforehand
- a priori performance evaluation is tricky

Biometric System and Countermeasure

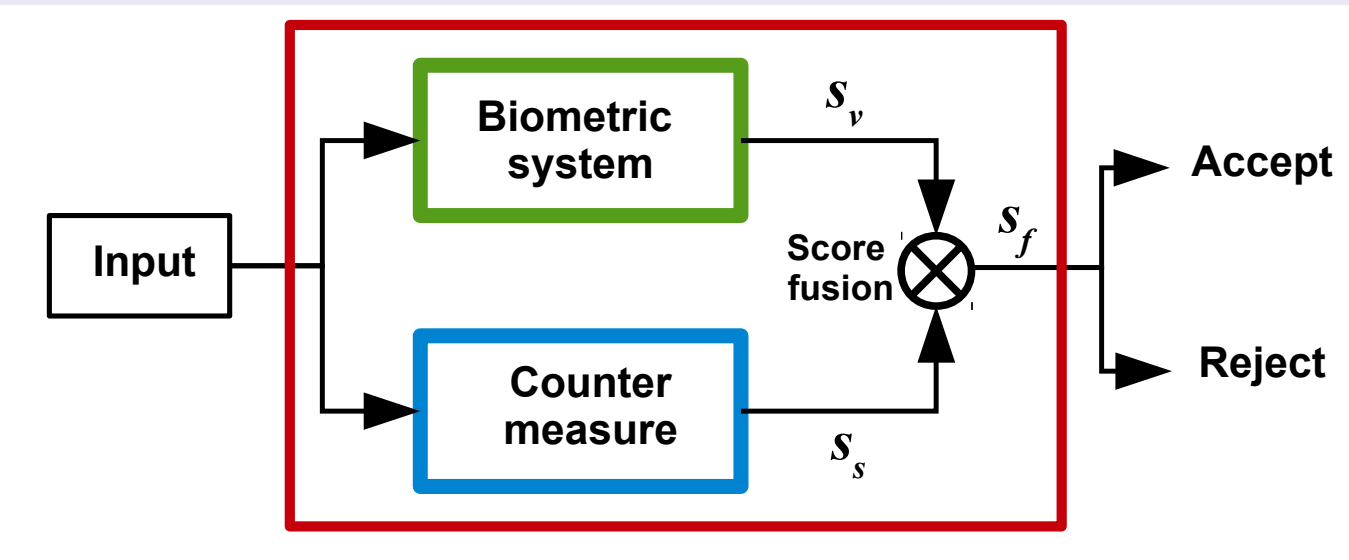
Ideally



- no threshold for CM to fixed
- 1 unique threshold to determine
- a priori performance evaluation considering spoofing

Expected Performance and Spoofability Curve

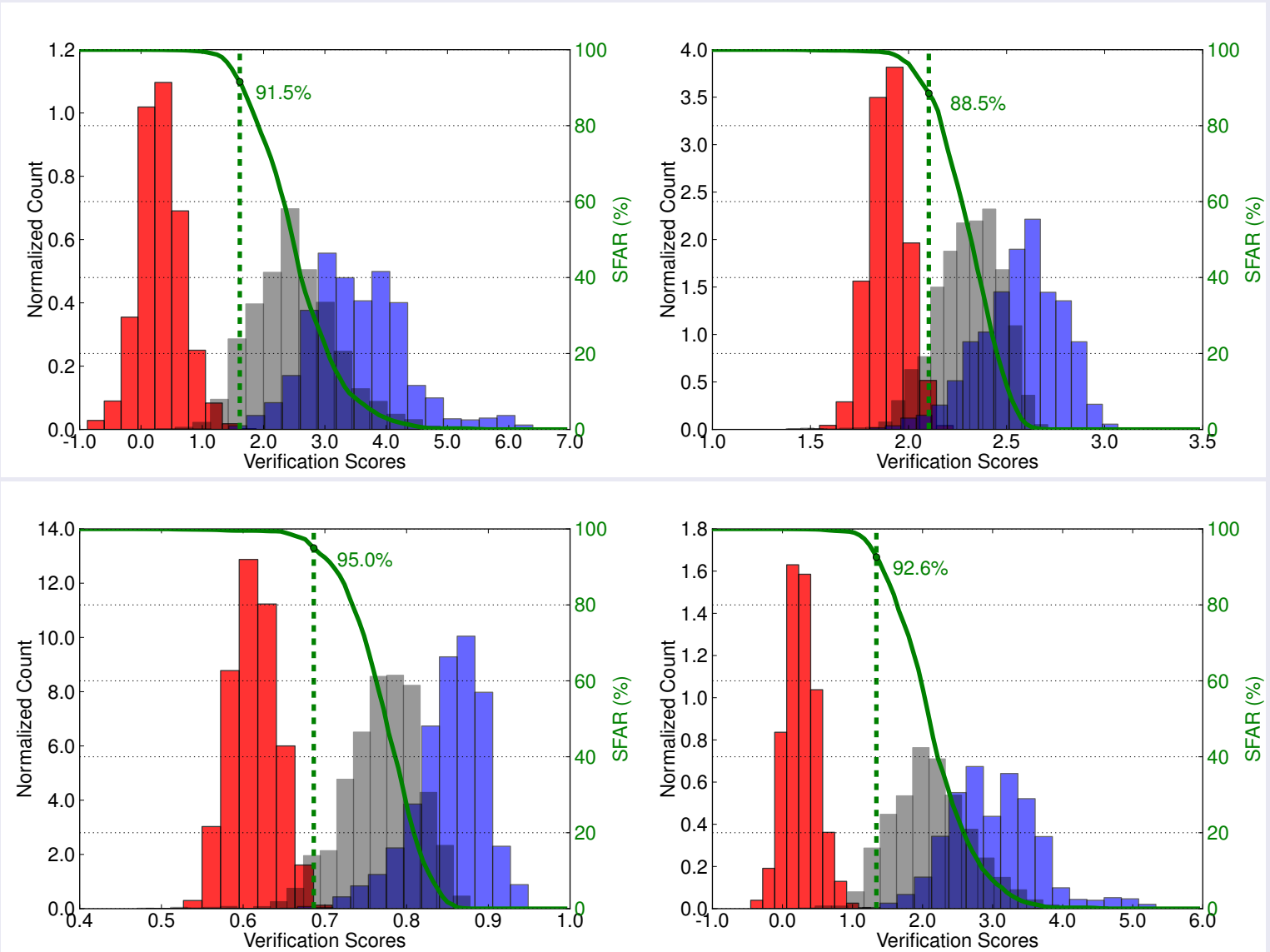
Fusion scheme



One unique threshold to be determined

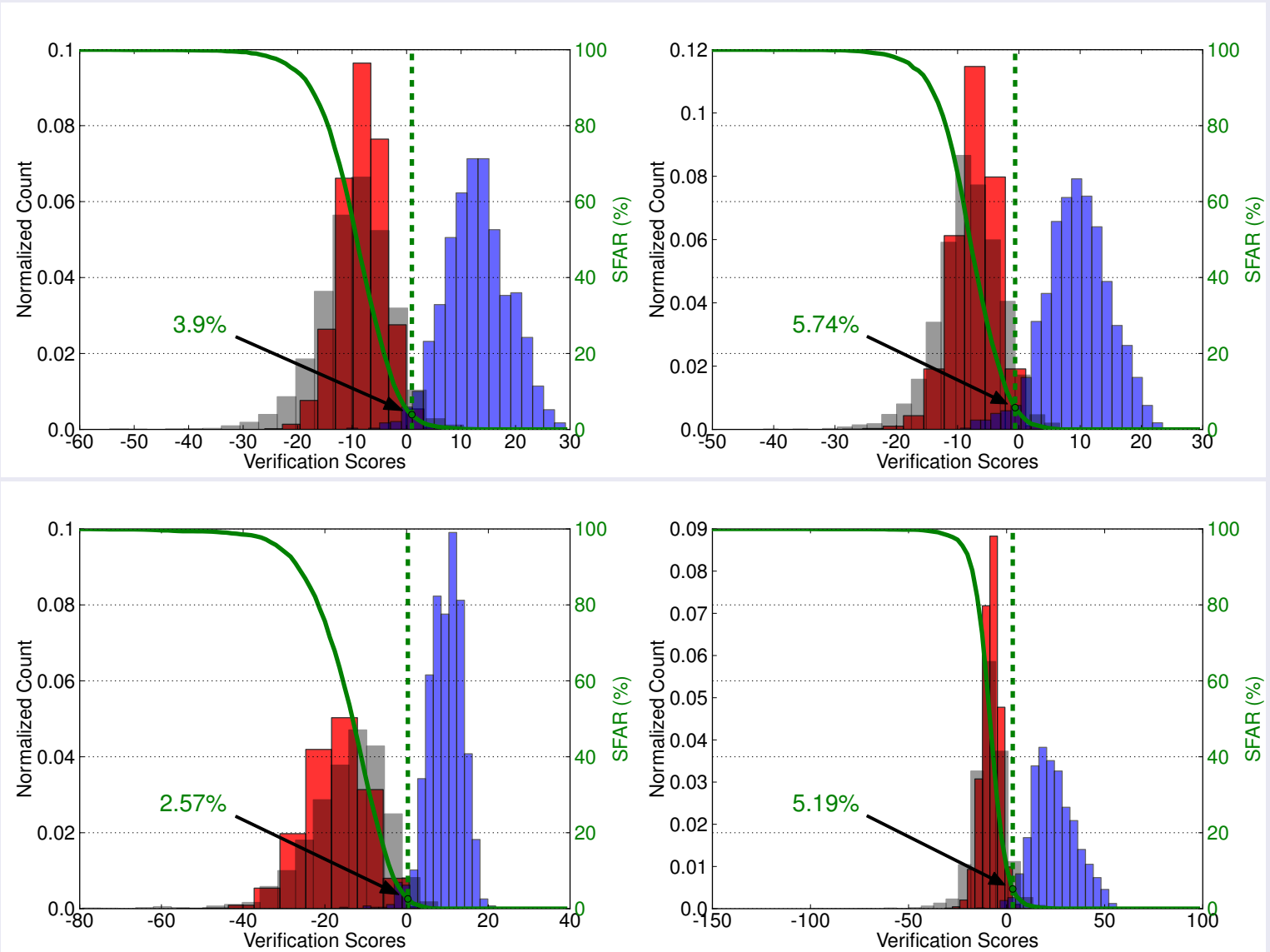
Expected Performance and Spoofability Curve

Biometric systems without countermeasure (no fusion)



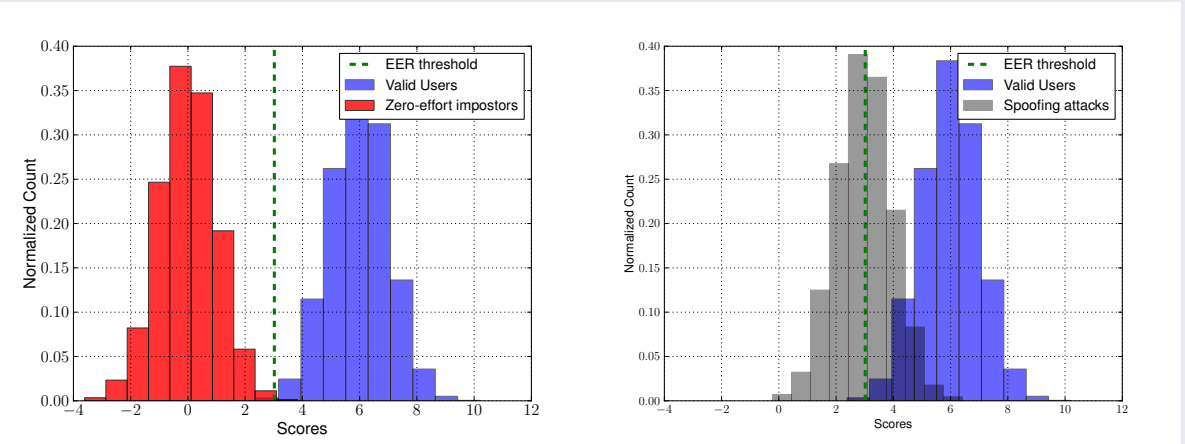
Expected Performance and Spoofability Curve

Biometric systems + countermeasure (fusion)



Expected Performance and Spoofability Curve

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 spoofing attacks falsely accepted

Expected Performance and Spoofability Curve

FAR_ω (development set)

Weighted error rate for the two negative classes (zero-effort impostors and spoofing 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:

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

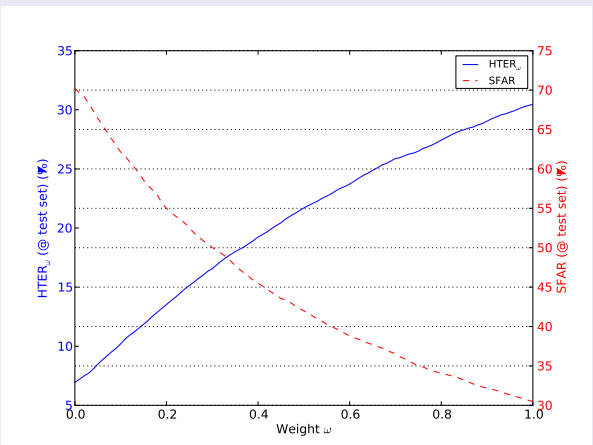
Expected Performance and Spoofability Curve

HTER_ω (test set)

Measuring both the verification performance and the spoofability of the system

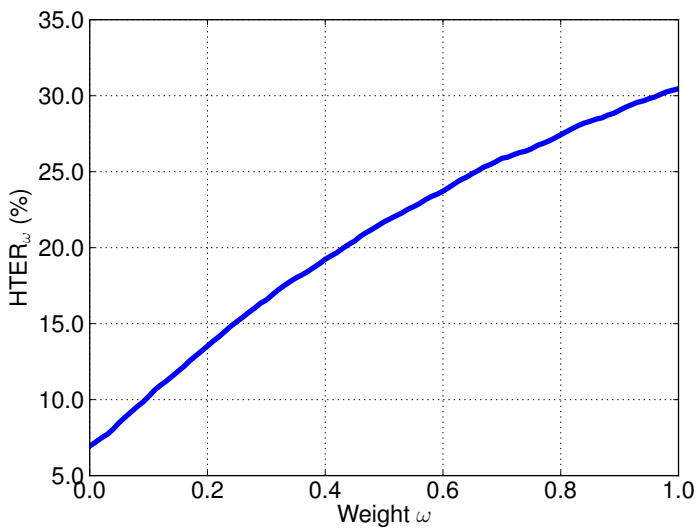
$$\mathrm{HTER}_\omega(\tau^*_\omega, \mathcal{D}_{test}) = \frac{\mathrm{FAR}_\omega(\tau^*_\omega, \mathcal{D}_{test}) + \mathrm{FRR}(\tau^*_\omega, \mathcal{D}_{test})}{2}$$

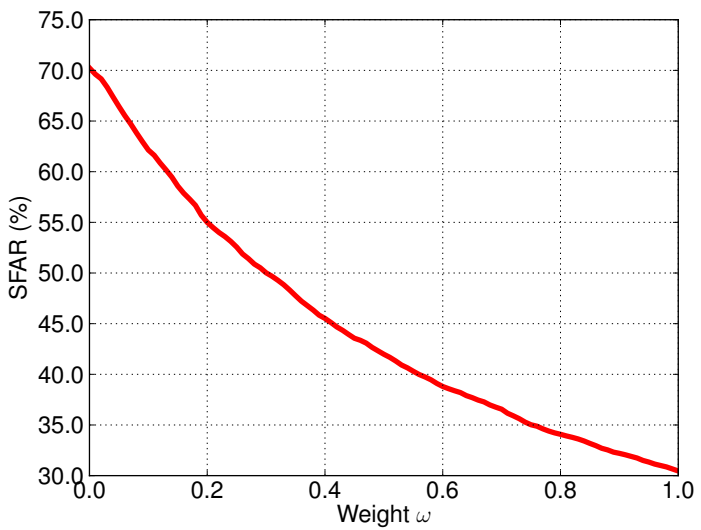
Ploting HTER_ω or SFAR



Expected Performance and Spoofability Curve

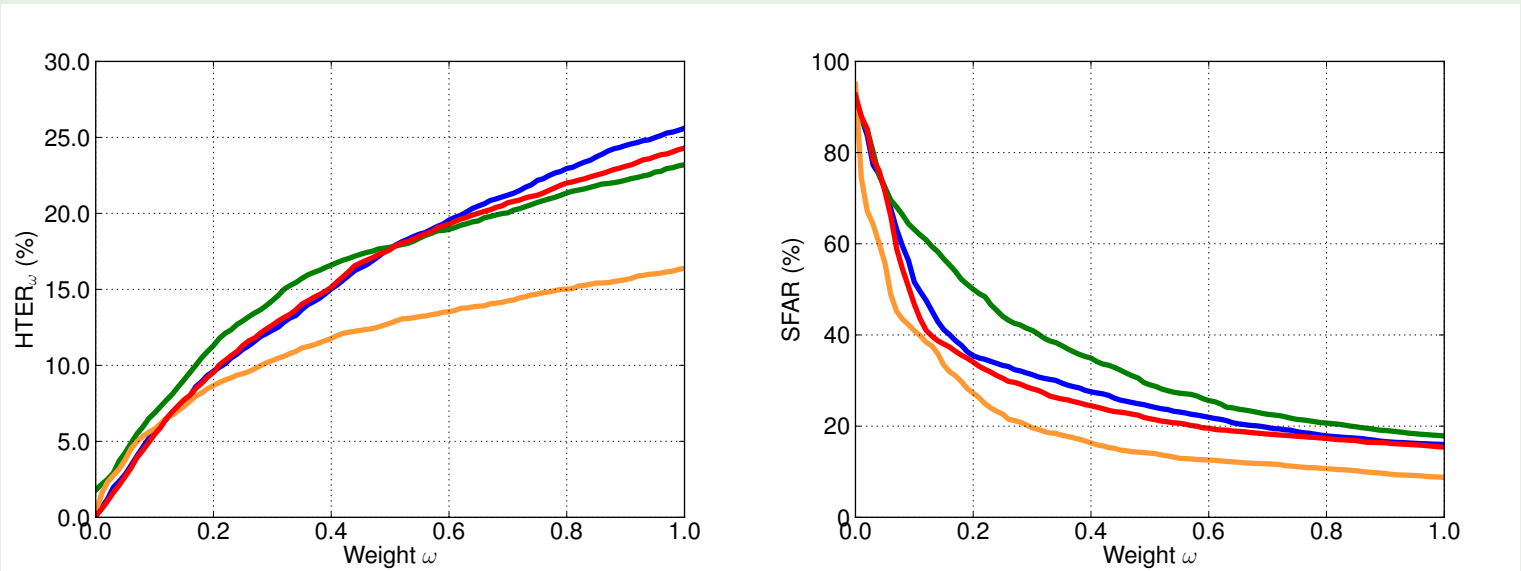
EPSC: HTER_ω and SFAR





EPSC examples

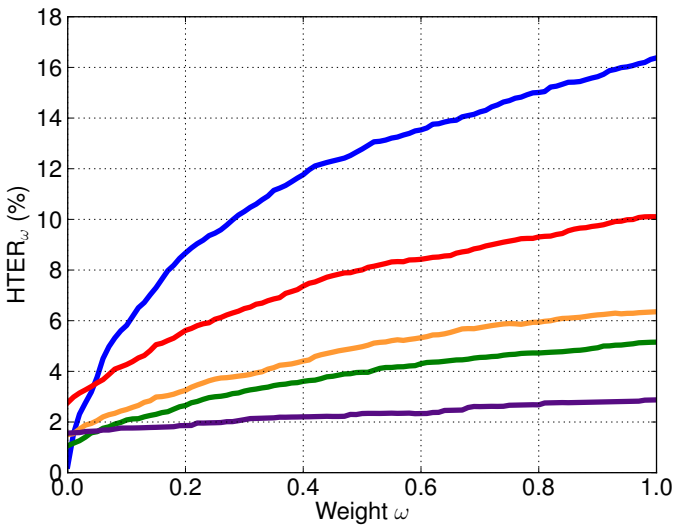
EPSC to compare biometric systems only

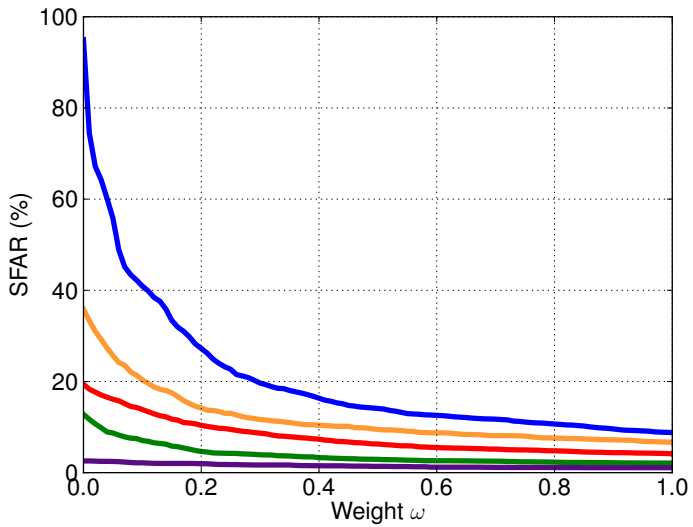


4 biometric systems (no CM)

EPSC examples

EPSC to compare countermeasures

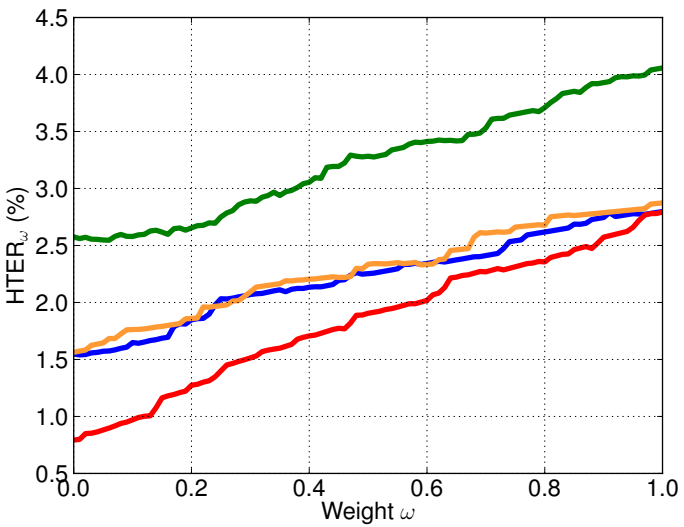


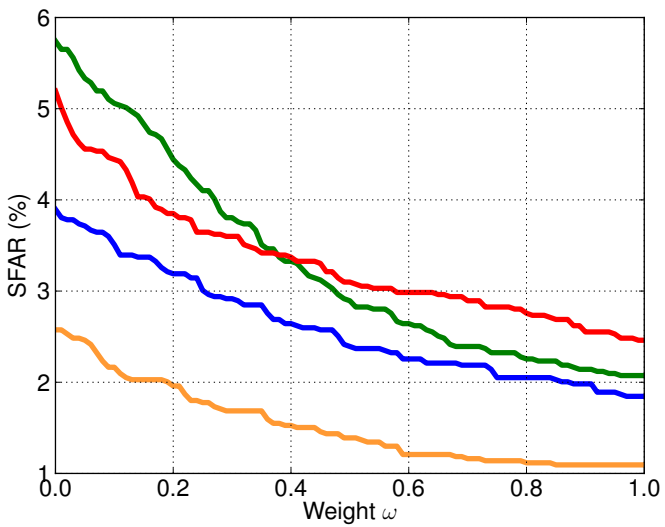


1 biometric system, same system + 3 CMs, same system + all CMs

EPSC examples

EPSC to compare biometric systems fused with ALL countermeasures





4 biometric system + all CMs

Don't trust me !

Public databases

- www.idiap.ch/dataset/mobio
- www.idiap.ch/dataset/replayattack
- www.idiap.ch/dataset/3dmad
- www.idiap.ch/dataset/avspoof
- www.idiap.ch/dataset/msspoof
- www.idiap.ch/dataset/vera-spoofingfingervein
- www.idiap.ch/dataset/vera-spoofingpalmvein

Don't trust me !

Replicable Research work

- pypi.python.org/pypi/antispoofing.crossdatabase
- pypi.python.org/pypi/antispoofing.lbptop
- pypi.python.org/pypi/antispoofing.fusion
- pypi.python.org/pypi/maskattack.lbp
- pypi.python.org/pypi/antispoofing.competition_icb2013
- pypi.python.org/pypi/antispoofing.fusion_faceverif
- pypi.python.org/pypi/antispoofing.lbp
- pypi.python.org/pypi/antispoofing.optflow
- pypi.python.org/pypi/antispoofing.motion

Don't trust me !

Bob: a free signal processing and machine learning toolbox

`www.idiap.ch/software/bob`

- Signal and image processing: filtering, LBP, SIFT, optical flow
- Machine learning: PCA, LDA, MLP, SVM, JFA, GMM, k-Means, PLDA
- Satellite packages: face recognition, speaker recognition, anti-spoofing
- DB interface: FRGC, LFW, GBU, CAS-PEAL, CMU-PIE, MOBIO, Replay, NIST SRE 2012

Some literature

Book

Handbook of Biometric Anti-Spoofing,
Sébastien Marcel, Mark S. Nixon and Stan Z. Li (Eds.)

- Fingerprint Anti-Spoofing
- Iris Anti-Spoofing
- Face Anti-Spoofing
- Voice Anti-Spoofing
- Gait Anti-Spoofing
- Multimodal Anti-Spoofing
- Evaluation Methodologies
- Standards
- Legal aspects

Some literature

Transactions on Information Forensics and Security (TIFS)

Special Issue on Biometric Spoofing and Countermeasures,
Guest Editors:
Nicholas Evans - EURECOM (France)
Sébastien Marcel – Idiap Research Institute (Switzerland)
Arun Ross – Michigan State University (USA)
Stan Z. Li – Chinese Academy of Sciences (China)

Some literature

IEEE Signal Processing Magazine

Special Issue on Biometric Security and Privacy,
Guest Editors:
Nicholas Evans – EURECOM (France)
Andrew Teoh Beng Jin – Yonsei University (South Korea)
Sébastien Marcel – Idiap Research Institute (Switzerland)
Arun Ross – Michigan State University (USA)

Acknowledgement

TABULA RASA (Nov 2010 - Apr 2014)

Trusted Biometrics under Spoofing Attacks (TABULA RASA)

`http://www.tabularasa-euproject.org`

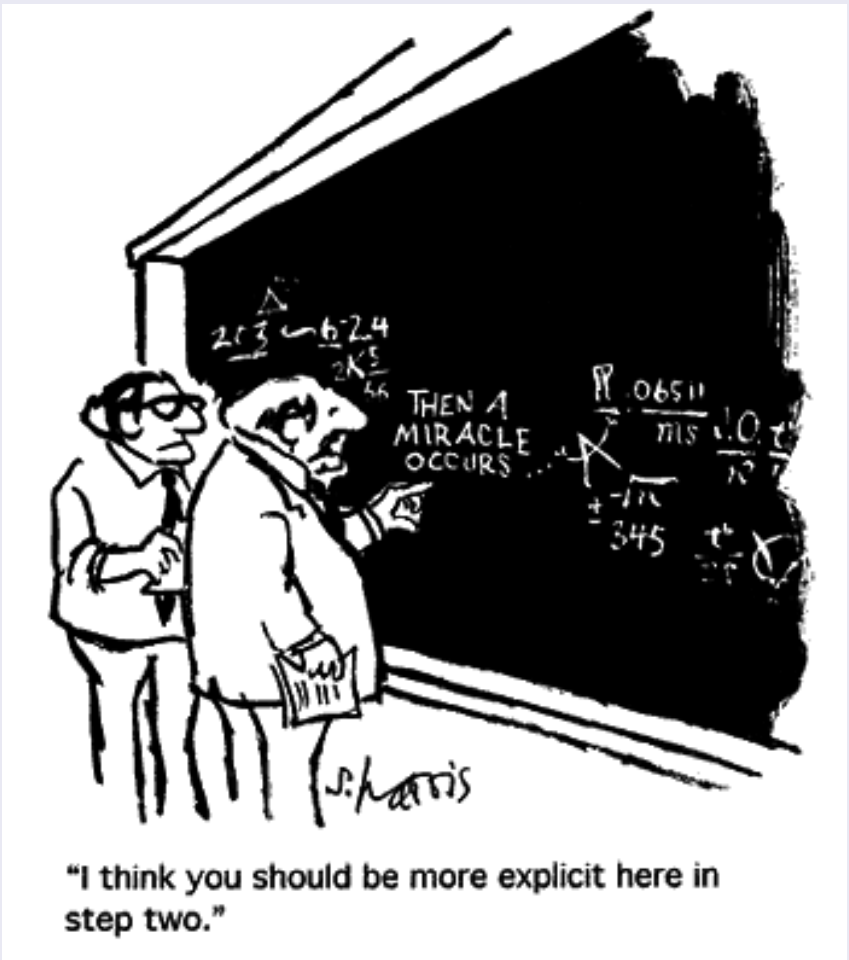
BEAT (Mar 2012 - Feb 2016)

Biometrics Evaluation and Testing (BEAT)

`http://www.beat-eu.org`

Motivation

Then a miracle occurs !



"I think you should be more explicit here in step two."

How many times?

Crossed a publication and openly decided to ***ignore it because it would be too hard to apply*** *it on your research?*

Appendix A
Mathematical Derivations

The goal of the following section is to provide more detailed proofs of the formulae given in the article for both training and computing the likelihood.

The following proofs make use of a formulation of the inverse of a block matrix that uses the Schur complement. The corresponding identity can be found in [1] (Equations 1.11 and 1.10),

$$\begin{bmatrix} L & M \\ N & O \end{bmatrix}^{-1} = \begin{bmatrix} R, & -RMO^{-1} \\ -O^{-1}NR, & O^{-1}+O^{-1}NRMO^{-1} \end{bmatrix}, \quad (51)$$

where we have substituted $R = \left(L - MO^{-1}N\right)^{-1}$.

Another related expression is the Woodbury matrix identity (Equation $C.7$ of [2]), which states that,

$$\left(L + MON\right)^{-1} = L^{-1} - L^{-1}M\left(O^{-1} + NL^{-1}M\right)^{-1}NL^{-1}. \quad (52)$$

of the number of training samples for the class. In addition, the inversion of $\mathcal{P}_0$ can be further optimised using the block matrix inversion identity introduced at the beginning of this section, leading to

$$\mathcal{P}_0^{-1} = \begin{bmatrix} \mathcal{F}_{J_i} & \sqrt{J_i}\mathcal{H}^T \\ \sqrt{J_i}\mathcal{H} & \left(I_{D_G} - J_i\mathcal{H}F^T\Sigma^{-1}G\right)\mathcal{G} \end{bmatrix}, \quad (54)$$

where $\mathcal{F}_{J_i}$ is defined by (33) and $\mathcal{H}$ by (37).

Then, the computation of $\mathring{\tilde{\mathcal{P}}}^{-1}\mathring{\tilde{A}}^T\tilde{\Sigma}^{-1}$ gives a block diagonal matrix, the first block being

$$\begin{bmatrix} \sqrt{J_i}\mathcal{F}_{J_i}F^T\mathcal{S} \\ \mathcal{G}G^T\Sigma^{-1}\left(I_{D_x} - J_iF\mathcal{F}_{J_i}F^T\mathcal{S}\right) \end{bmatrix},$$

and the other ones being equal to $\mathcal{G}G^T\Sigma^{-1}$.

As explained in section III.B.a of the article, h_i corresponds to the upper sub-vector of $\mathring{\tilde{y}}_i$ and is not affected by the change of variable, as depicted in (21). Therefore, the first order moment of h_i is directly obtained by multiplying the first block-rows of the matrix $\mathring{\tilde{\mathcal{P}}}^{-1}\mathring{\tilde{A}}^T\tilde{\Sigma}^{-1}$ with $\mathring{\tilde{x}}_i$, which gives (31).

Motivation

How many times?

*Worked day and night to **incorporate some results** on your own work but:*

- There were **untold parameters** that needed adjustment and you couldn't get hold of them?
- Realized the proposed algorithm **worked only on the specific data** shown at the original paper?
- Realized that something did **not quite add up** in the end?

Motivation

How many times?

*Had **to take over** the work from a student or another colleague that left and had to start from scratch - months into programming to make things work again?*

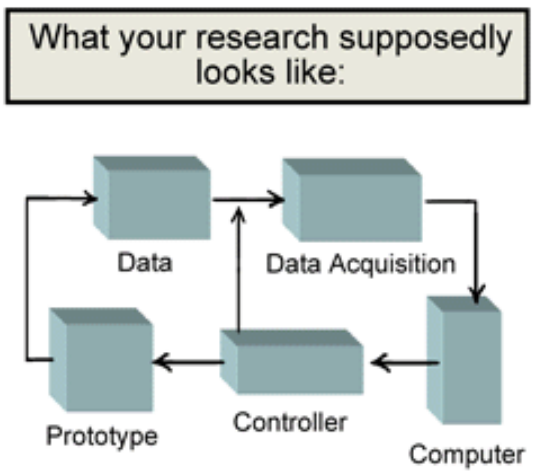


Figure 1. Experimental Diagram

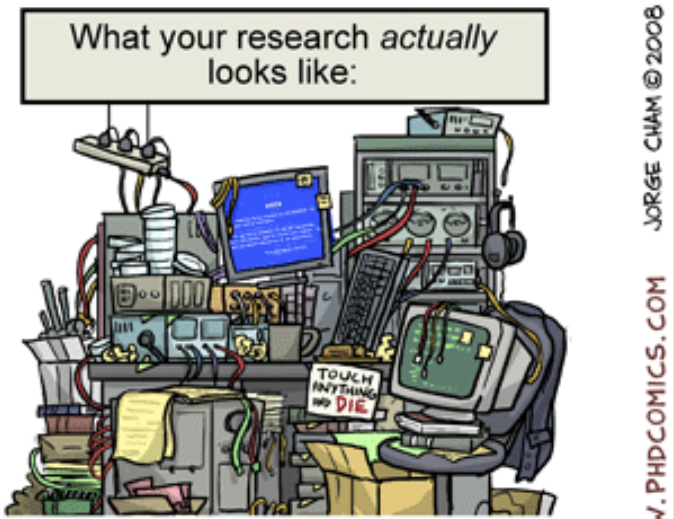


Figure 2. Experimental Mess

Motivation

How many times?

Would have liked to ***replay to someone about your work****, but you couldn't really remember all details when you first made it work? Or you* ***could not make it work*** *at all?*

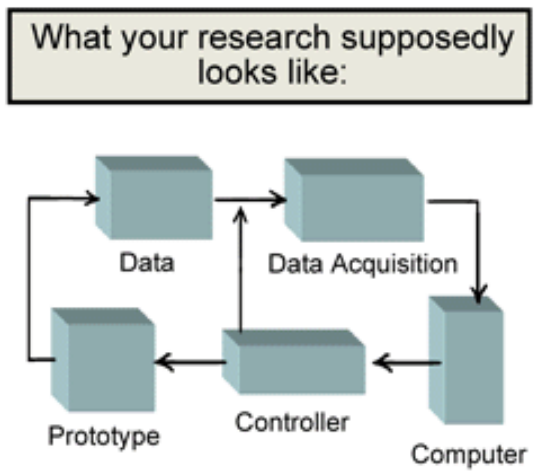


Figure 1. Experimental Diagram

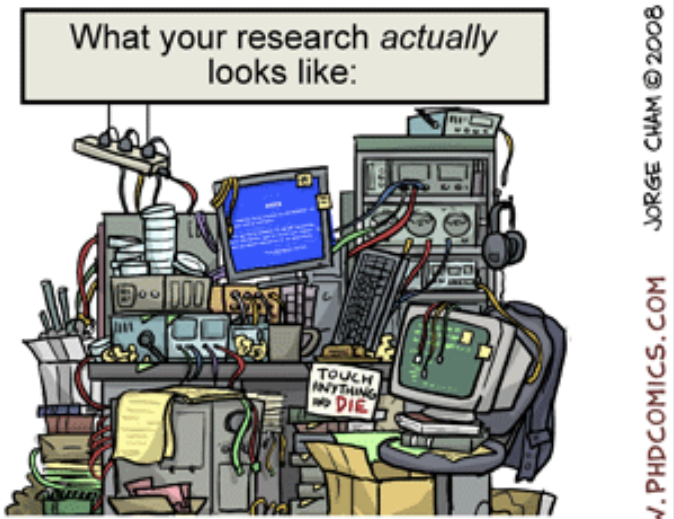


Figure 2. Experimental Mess

Scientific publications

for sharing ideas, knowledge, findings and results

A Scalable Formulation of Probabilistic Linear Discriminant Analysis: Applied to Face Recognition

Laurent El Shafey, Chris McCool, Roy Wallace, and Sébastien Marcel

APPENDIX A
MATHEMATICAL DERIVATIONS

The goal of the following section is to provide more detailed proofs of the formulae given in the article for both training and computing the likelihood.

The following proofs make use of a formulation of the inverse of a block matrix that uses the Schur complement. The corresponding identity can be found in [1] (Equations 1.11 and 1.10),

$$\begin{bmatrix} \boldsymbol{L} & \boldsymbol{M} \\ \boldsymbol{N} & \boldsymbol{O} \end{bmatrix}^{-1} = \begin{bmatrix} \boldsymbol{R}, & -\boldsymbol{R}\boldsymbol{M}\boldsymbol{O}^{-1} \\ -\boldsymbol{O}^{-1}\boldsymbol{N}\boldsymbol{R}, & \boldsymbol{O}^{-1} + \boldsymbol{O}^{-1}\boldsymbol{N}\boldsymbol{R}\boldsymbol{M}\boldsymbol{O}^{-1} \end{bmatrix}, \quad (51)$$

where we have substituted $\boldsymbol{R} = (\boldsymbol{L} - \boldsymbol{M}\boldsymbol{O}^{-1}\boldsymbol{N})^{-1}$.

Another related expression is the Woodbury matrix identity (Equation C.7 of [2]), which states that,

$$(\boldsymbol{L} + \boldsymbol{M}\boldsymbol{O}\boldsymbol{N})^{-1} = \boldsymbol{L}^{-1} - \boldsymbol{L}^{-1}\boldsymbol{M}\left(\boldsymbol{O}^{-1} + \boldsymbol{N}\boldsymbol{L}^{-1}\boldsymbol{M}\right)^{-1}\boldsymbol{N}\boldsymbol{L}^{-1}. \quad (52)$$

A. Scalable training

The bottleneck of the training procedure is the expectation step (E-Step) of the Expectation-Maximization algorithm. This E-Step requires the computation of the first and second order moments of the latent variables.

1) Estimating the first order moment of the Latent Variables: The most computationally expensive part when estimating the latent variables is the inversion of the matrix $\hat{\boldsymbol{\mathcal{P}}}$ (Equation (27)). This matrix is block diagonal, the two blocks being $\boldsymbol{\mathcal{P}}_0$ (Equation (28)) and (a repetition of) $\boldsymbol{\mathcal{P}}_1$ (Equation (29)),

$$\hat{\boldsymbol{\mathcal{P}}} = \begin{bmatrix} \boldsymbol{\mathcal{P}}_0 & 0 & \cdots & 0 \\ 0 & \boldsymbol{\mathcal{P}}_1 & \ddots & 0 \\ 0 & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \boldsymbol{\mathcal{P}}_1 \end{bmatrix}. \quad (53)$$

The inverse of $\boldsymbol{\mathcal{P}}_1$ is equal to the matrix $\boldsymbol{\mathcal{G}}$, defined by (30). This matrix is of constant size $(D_G \times D_G)$, irrespective of the number of training samples for the class. In addition, the inversion of $\boldsymbol{\mathcal{P}}_0$ can be further optimised using the block matrix inversion identity introduced at the beginning of this section, leading to

$$\boldsymbol{\mathcal{P}}_0^{-1} = \begin{bmatrix} \boldsymbol{\mathcal{F}}_{J_i} & \sqrt{J_i}\boldsymbol{\mathcal{H}}^T \\ \sqrt{J_i}\boldsymbol{\mathcal{H}} & \left(\boldsymbol{I}_{D_G} - J_i\boldsymbol{\mathcal{H}}\boldsymbol{F}^T\boldsymbol{\Sigma}^{-1}\boldsymbol{G}\right)\boldsymbol{\mathcal{G}} \end{bmatrix}, \quad (54)$$

where $\boldsymbol{\mathcal{F}}_{J_i}$ is defined by (33) and $\boldsymbol{\mathcal{H}}$ by (37).

Then, the computation of $\hat{\boldsymbol{\mathcal{P}}}^{-1}\hat{\boldsymbol{A}}^T\hat{\boldsymbol{\Sigma}}^{-1}$ gives a block diagonal matrix, the first block being

$$\begin{bmatrix} \sqrt{J_i}\boldsymbol{\mathcal{F}}_{J_i}\boldsymbol{F}^T\boldsymbol{\mathcal{S}} \\ \boldsymbol{\mathcal{G}}\boldsymbol{G}^T\boldsymbol{\Sigma}^{-1}\left(\boldsymbol{I}_{D_x} - J_i\boldsymbol{F}\boldsymbol{\mathcal{F}}_{J_i}\boldsymbol{F}^T\boldsymbol{\mathcal{S}}\right) \end{bmatrix},$$

and the other ones being equal to $\boldsymbol{\mathcal{G}}\boldsymbol{G}^T\boldsymbol{\Sigma}^{-1}$.

As explained in section III.B.a of the article, $\boldsymbol{h}_i$ corresponds to the upper sub-vector of $\hat{\boldsymbol{y}}_i$ and is not affected by the change of variable, as depicted in (21). Therefore, the first order moment of $\boldsymbol{h}_i$ is directly obtained by multiplying the first block-rows of the matrix $\hat{\boldsymbol{\mathcal{P}}}^{-1}\hat{\boldsymbol{A}}^T\hat{\boldsymbol{\Sigma}}^{-1}$ with $\hat{\boldsymbol{x}}_i$, which gives (31).

Considering only the $\hat{\boldsymbol{w}}_i$ (lower) sub-vector of $\hat{\boldsymbol{y}}_i$, the corresponding (lower) part $\hat{\boldsymbol{\mathcal{B}}}$ of the matrix $\hat{\boldsymbol{\mathcal{P}}}^{-1}\hat{\boldsymbol{A}}^T\hat{\boldsymbol{\Sigma}}^{-1}$ can be decomposed into a sum of two matrices, the first one being sparse with a single non-zero block (upper left) equal to $\boldsymbol{\mathcal{B}}_0 = -J_i\boldsymbol{\mathcal{G}}\boldsymbol{G}^T\boldsymbol{\Sigma}^{-1}\boldsymbol{F}\boldsymbol{\mathcal{F}}_{J_i}\boldsymbol{F}^T\boldsymbol{\mathcal{S}}$, and the second one being diagonal by blocks with identical blocks $\boldsymbol{\mathcal{B}}_1 = \boldsymbol{\mathcal{G}}\boldsymbol{G}^T\boldsymbol{\Sigma}^{-1}$,

$$\hat{\boldsymbol{\mathcal{B}}} = \begin{bmatrix} \boldsymbol{\mathcal{B}}_0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} \boldsymbol{\mathcal{B}}_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \boldsymbol{\mathcal{B}}_1 \end{bmatrix}. \quad (55)$$

Furthermore, the first order moment of the variables $\hat{\boldsymbol{w}}_i$ is given by

$$E\left[\hat{\boldsymbol{w}}_i|\hat{\boldsymbol{x}}_i, \boldsymbol{\Theta}\right] = \left(\hat{\boldsymbol{U}}^T \otimes \boldsymbol{I}_{D_G}\right)\begin{bmatrix} \boldsymbol{\mathcal{B}}_0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}\hat{\boldsymbol{x}}_i + \left(\hat{\boldsymbol{U}}^T \otimes \boldsymbol{I}_{D_G}\right)\begin{bmatrix} \boldsymbol{\mathcal{B}}_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \boldsymbol{\mathcal{B}}_1 \end{bmatrix}\left(\hat{\boldsymbol{U}} \otimes \boldsymbol{I}_{D_x}\right)\hat{\boldsymbol{x}}_i. \quad (56)$$

The previous decomposition greatly simplifies the computation, and leads to the following expression for each $\boldsymbol{w}_{i,j}$,

$$E\left[\boldsymbol{w}_{i,j}|\hat{\boldsymbol{x}}_i, \boldsymbol{\Theta}\right] = \boldsymbol{\mathcal{G}}\boldsymbol{G}^T\boldsymbol{\Sigma}^{-1}\hat{\boldsymbol{x}}_{i,j} - \boldsymbol{\mathcal{G}}\boldsymbol{G}^T\boldsymbol{\Sigma}^{-1}\boldsymbol{F}\boldsymbol{\mathcal{F}}_{J_i}\boldsymbol{F}^T\boldsymbol{\mathcal{S}}\sum_j \hat{\boldsymbol{x}}_{i,j} \quad (57)$$

L. El Shafey is with Idiap Research Institute and Ecole Polytechnique Fédérale de Lausanne, Switzerland e-mail: laurent.el-shafey@idiap.ch
C. McCool, R. Wallace and S. Marcel are with Idiap Research Institute, Martigny, Switzerland e-mail: {christopher.mccool,roy.wallace,sebastien.marcel}@idiap.ch

The research leading to these results has received funding from the European Communitys Seventh Framework Programme (FP7) under grant agreements 238803 (BBfor2) and 257289 (TABULA RASA).

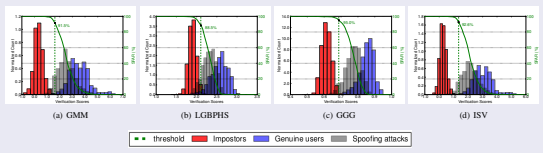


Fig. 10: Score distributions of baseline face verification systems. The full green line shows how SFAR changes with moving the threshold.

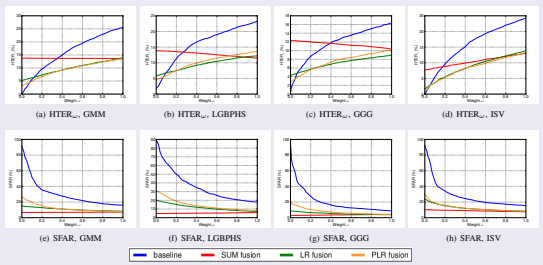


Fig. 12: EPSC for comparison of fusion techniques of baselines with LBP anti-spoofing algorithm

D. Performance of fused systems

In our last experiment, we compare the four face verification systems when fused with ALL counter-measures using PLR fusion scheme. Firstly, we illustrate how fusion changes the score distribution for each of them separately in Figure 14. Then, in Figure 15 we compare which of the fused systems performs the best.

While Figure 10 shows that the spoofing attacks of Replay-Attack are in the optimal category when fed to the baseline face verification systems, Figure 14 illustrates that their effectiveness has vastly changed after fusion. The score distribution of the spoofing attacks is now mostly overlapping with the score distribution of the zero-effort impostors, allowing for better discriminability between the positive class and the two negative classes. The results are reflecting this observation: even when the threshold is obtained using the licit scenario, SFAR has dropped to less then 6%.

The comparison between the EPSC curves given in Figure 11(a) and Figure 15(a), confirms the above observations:

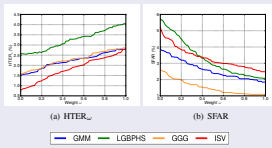
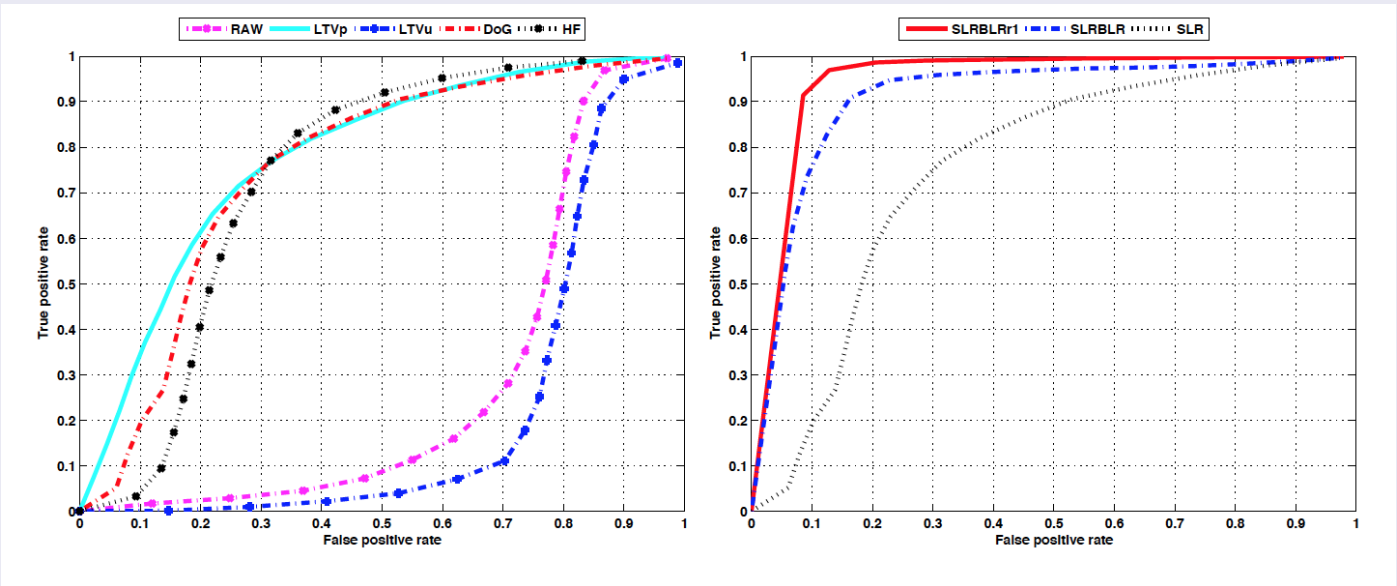


Fig. 15: EPSC curves to compare fused systems

while HTER$_\omega$ increases rapidly with ω and reaches up to 25% for some of the baseline systems, it increases very mildly and does not exceed 4.1% for the fused systems. The major augmentation of the robustness to spoofing of the systems after

Current system

Comparing to prior work



My results are better than yours !

Comparing to prior work

for $i = 1$ to H
  $\log P_{I|C}[i] \leftarrow 0$
end for
for all fern F_k **do**
  index $\leftarrow 0$
  for $j = 1$ to S
    index $\leftarrow 2 \times$ index
    if $I\left(\mathbf{d}_{\sigma(k,j,1)}\right) < I\left(\mathbf{d}_{\sigma(k,j,2)}\right)$ **then**
      index $\leftarrow$ index $+ 1$
    end if
  end for
  for $i = 1$ to H
    $\log P_{I|C}[i] \leftarrow \log P_{I|C}[i] + \log P_{F_k}[\text{index}, i]$
  end for
end for

```
1:for(int i = 0; i < H; i++) P[i] = 0.;

2:for(int k = 0; k < M; k++) {
3:   int index = 0, * d = D + k * 2 * S;
4:   for(int j = 0; j < S; j++) {
5:     index <<= 1;
6:     if (*(K + d[0]) < *(K + d[1]))
7:       index++;
8:     d += 2;
     }
9:   p = PF + k * shift2 + index * shift1;
10:  for(int i = 0; i < H; i++) P[i]+=p[i];
   }
```

Figure 1. **Left:** The pseudo-code of the run-time algorithm that computes $P(f_1, f_2, \ldots, f_N \mid C = c_i)$ as given by Eq. (2) to classify the image patch I, where *index* is an integer index computed from the binary features. No image rectification, illumination normalization, or parameter tuning are required. **Right:** A C++ implementation of the pseude-code. The code used for training is very similar.

May be trivial or easy

Comparing to prior work

for $i = 1$ to H
  $\log P_{I|C}[i] \leftarrow 0$
end for
for all fern F_k **do**
  index $\leftarrow 0$
  for $j = 1$ to S
    index $\leftarrow 2 \times$ index
    if $I\left(\mathbf{d}_{\sigma(k,j,1)}\right) < I\left(\mathbf{d}_{\sigma(k,j,2)}\right)$ **then**
      index $\leftarrow$ index $+ 1$
    end if
  end for
  for $i = 1$ to H
    $\log P_{I|C}[i] \leftarrow \log P_{I|C}[i] + \log P_{F_k}[\text{index}, i]$
  end for
end for

```
1:for(int i = 0; i < H; i++) P[i] = 0.;

2:for(int k = 0; k < M; k++) {
3:   int index = 0, * d = D + k * 2 * S;
4:   for(int j = 0; j < S; j++) {
5:     index <<= 1;
6:     if (*(K + d[0]) < *(K + d[1]))
7:       index++;
8:     d += 2;
     }
9:   p = PF + k * shift2 + index * shift1;
10:  for(int i = 0; i < H; i++) P[i]+=p[i];
   }
```

Figure 1. **Left:** The pseudo-code of the run-time algorithm that computes $P(f_1, f_2, \ldots, f_N \mid C = c_i)$ as given by Eq. (2) to classify the image patch I, where *index* is an integer index computed from the binary features. No image rectification, illumination normalization, or parameter tuning are required. **Right:** A C++ implementation of the pseude-code. The code used for training is very similar.

May be trivial or easy

The pseudo-code is inside the paper !

Current system

Comparing to prior work

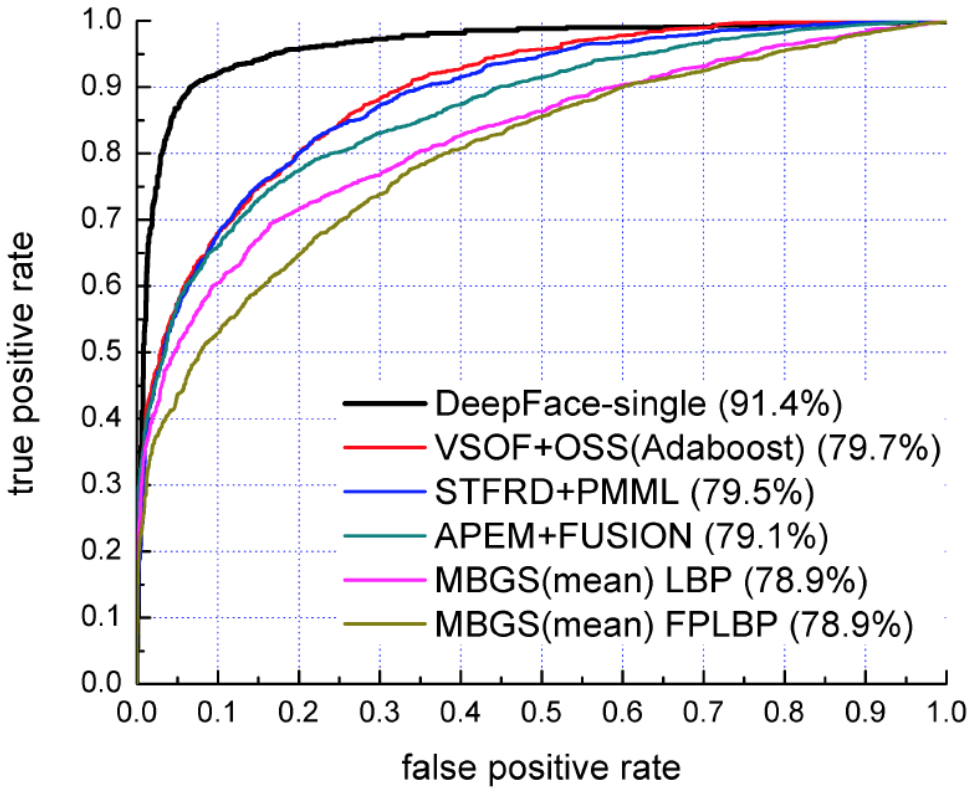


Figure 4. The ROC curves on the *YTF* dataset.

May be not that easy

Current system

Comparing to prior work

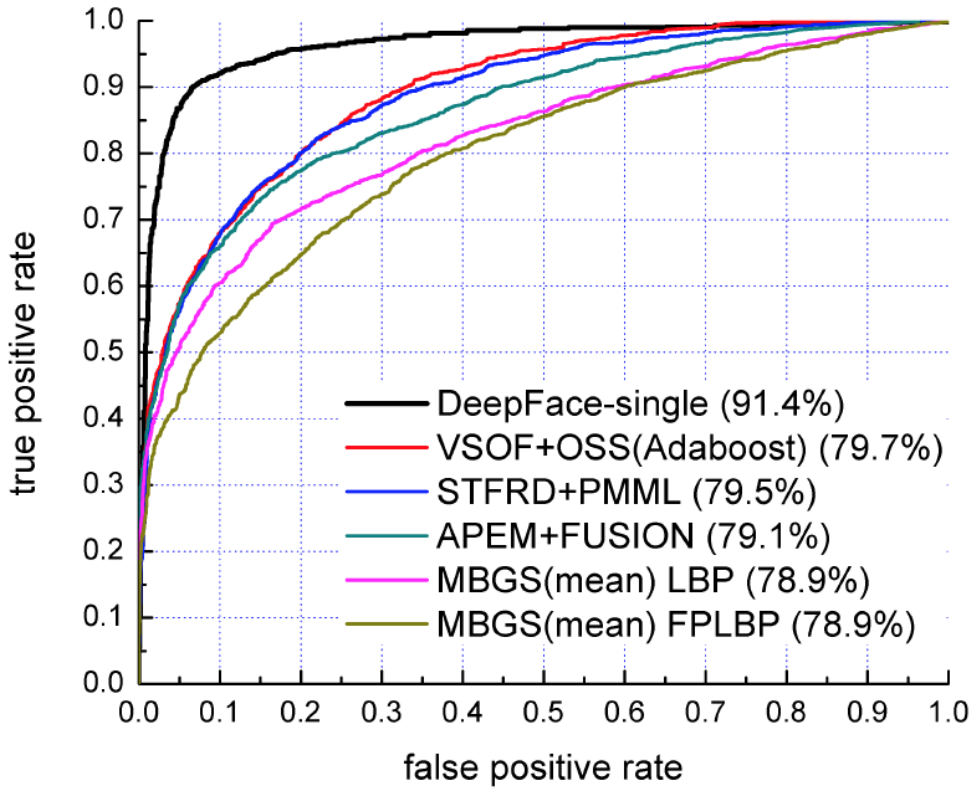


Figure 4. The ROC curves on the *YTF* dataset.

May be not that easy

You just need 4 M face images to train 120 M parameters !

Comparing to prior work

The process above can be described in terms of a conditional probability

$$Pr\left(\boldsymbol{x}_{i,j}|\boldsymbol{h}_i, \boldsymbol{w}_{i,j}, \boldsymbol{\Theta}\right) = \mathcal{N}\left[\boldsymbol{\mu} + \boldsymbol{F}\boldsymbol{h}_i + \boldsymbol{G}\boldsymbol{w}_{i,j}, \boldsymbol{\Sigma}\right], \quad (2)$$

and prior probabilities ($\boldsymbol{I}$ being the identity matrix)

$$Pr\left(\boldsymbol{h}_i\right) = \mathcal{N}\left[0, \boldsymbol{I}\right], \quad (3)$$

$$Pr\left(\boldsymbol{w}_{i,j}\right) = \mathcal{N}\left[0, \boldsymbol{I}\right], \quad (4)$$

where the parameters of the model are $\boldsymbol{\Theta} = [\boldsymbol{\mu}, \boldsymbol{F}, \boldsymbol{G}, \boldsymbol{\Sigma}]$. Equations (3) and (4) define the priors on the latent variables, $\boldsymbol{h}_i$ and $\boldsymbol{w}_{i,j}$, to be Gaussian. The equations above can be written in a more compact form by setting $\boldsymbol{A} = [\boldsymbol{F}, \boldsymbol{G}]$ and

$$\boldsymbol{y}_{i,j} = [\boldsymbol{h}_i^T, \boldsymbol{w}_{i,j}^T]^T. \quad (5)$$

This would give us

$$\boldsymbol{x}_{i,j} = \boldsymbol{\mu} + \boldsymbol{A}\boldsymbol{y}_{i,j} + \boldsymbol{\epsilon}_{i,j}, \quad (6)$$

and

$$Pr\left(\boldsymbol{x}_{i,j}|\boldsymbol{y}_{i,j}, \boldsymbol{\Theta}\right) = \mathcal{N}\left[\boldsymbol{\mu} + \boldsymbol{A}\boldsymbol{y}_{i,j}, \boldsymbol{\Sigma}\right], \quad (7)$$

$$Pr\left(\boldsymbol{y}_{i,j}\right) = \mathcal{N}\left[0, \boldsymbol{I}\right]. \quad (8)$$

We can extend the above formulation to handle multiple observations. For instance, if we are given $J_i = 2$ observations for identity i we would set

$$\tilde{\boldsymbol{A}} = \begin{bmatrix} \boldsymbol{F}, \boldsymbol{G}, 0 \\ \boldsymbol{F}, 0, \boldsymbol{G} \end{bmatrix}. \quad (9)$$

Consequently, we would write that $\tilde{\boldsymbol{x}}_i = [\bar{\boldsymbol{x}}_{i,1}^T, \bar{\boldsymbol{x}}_{i,2}^T]^T$, $\tilde{\boldsymbol{\epsilon}}_i = [\boldsymbol{\epsilon}_{i,1}^T, \boldsymbol{\epsilon}_{i,2}^T]^T$, $\tilde{\boldsymbol{w}}_i = [\boldsymbol{w}_{i,1}^T, \boldsymbol{w}_{i,2}^T]^T$, $\tilde{\boldsymbol{y}}_i = [\boldsymbol{h}_i^T, \boldsymbol{w}_{i,1}^T, \boldsymbol{w}_{i,2}^T]^T$,

A. *Training the PLDA Model*

To train the PLDA model an EM algorithm is used [1]. All of the M-Steps are provided on a per sample basis once the latent variables have been estimated. It is this estimation of the latent variables, corresponding to the E-Step, that presents the difficulties in making PLDA scalable. In the E-Step, we need to calculate the first-order and second-order moments of the latent variables, we reproduce the equations as follows:

$$E\left[\tilde{\boldsymbol{y}}_i|\tilde{\boldsymbol{x}}_i, \boldsymbol{\Theta}\right] = \left(\tilde{\boldsymbol{I}} + \tilde{\boldsymbol{A}}^T\tilde{\boldsymbol{\Sigma}}^{-1}\tilde{\boldsymbol{A}}\right)^{-1}\tilde{\boldsymbol{A}}^T\tilde{\boldsymbol{\Sigma}}^{-1}\left(\tilde{\boldsymbol{x}}_i\right), \quad (13)$$

$$E\left[\tilde{\boldsymbol{y}}_i\tilde{\boldsymbol{y}}_i^T|\tilde{\boldsymbol{x}}_i, \boldsymbol{\Theta}\right] = \left(\tilde{\boldsymbol{I}} + \tilde{\boldsymbol{A}}^T\tilde{\boldsymbol{\Sigma}}^{-1}\tilde{\boldsymbol{A}}\right)^{-1} + E\left[\tilde{\boldsymbol{y}}_i|\tilde{\boldsymbol{x}}_i, \boldsymbol{\Theta}\right]E\left[\tilde{\boldsymbol{y}}_i|\tilde{\boldsymbol{x}}_i, \boldsymbol{\Theta}\right]^T. \quad (14)$$

From the above equations, it is obvious that the problem for the E-Step is how to cope with the matrix $\left(\tilde{\boldsymbol{I}} + \tilde{\boldsymbol{A}}^T\tilde{\boldsymbol{\Sigma}}^{-1}\tilde{\boldsymbol{A}}\right)^{-1}$ efficiently as it has to be recomputed for each iteration of EM. This matrix is indeed of size $(D_F + J_iD_G, D_F + J_iD_G)$, and has to be used in calculations as well as stored. A solution to this problem was proposed by Kenny [3] when applying PLDA to speaker recognition. Kenny's solution was to apply a variational approximation for this inference problem; however, this approximation relies on a factorization which assumes that the posterior variables are independent and whose quality with respect to the exact solution has not been demonstrated. Once the PLDA model has been trained, it can be used to perform various tasks, which all rely on likelihood calculations.

May be not that easy

Comparing to prior work

The process above can be described in terms of a conditional probability

$$Pr\left(\boldsymbol{x}_{i,j}|\boldsymbol{h}_i, \boldsymbol{w}_{i,j}, \boldsymbol{\Theta}\right) = \mathcal{N}\left[\boldsymbol{\mu} + \boldsymbol{F}\boldsymbol{h}_i + \boldsymbol{G}\boldsymbol{w}_{i,j}, \boldsymbol{\Sigma}\right], \quad (2)$$

and prior probabilities ($\boldsymbol{I}$ being the identity matrix)

$$Pr\left(\boldsymbol{h}_i\right) = \mathcal{N}\left[0, \boldsymbol{I}\right], \quad (3)$$

$$Pr\left(\boldsymbol{w}_{i,j}\right) = \mathcal{N}\left[0, \boldsymbol{I}\right], \quad (4)$$

where the parameters of the model are $\boldsymbol{\Theta} = [\boldsymbol{\mu}, \boldsymbol{F}, \boldsymbol{G}, \boldsymbol{\Sigma}]$. Equations (3) and (4) define the priors on the latent variables, $\boldsymbol{h}_i$ and $\boldsymbol{w}_{i,j}$, to be Gaussian. The equations above can be written in a more compact form by setting $\boldsymbol{A} = [\boldsymbol{F}, \boldsymbol{G}]$ and

$$\boldsymbol{y}_{i,j} = [\boldsymbol{h}_i^T, \boldsymbol{w}_{i,j}^T]^T. \quad (5)$$

This would give us

$$\boldsymbol{x}_{i,j} = \boldsymbol{\mu} + \boldsymbol{A}\boldsymbol{y}_{i,j} + \boldsymbol{\epsilon}_{i,j}, \quad (6)$$

and

$$Pr\left(\boldsymbol{x}_{i,j}|\boldsymbol{y}_{i,j}, \boldsymbol{\Theta}\right) = \mathcal{N}\left[\boldsymbol{\mu} + \boldsymbol{A}\boldsymbol{y}_{i,j}, \boldsymbol{\Sigma}\right], \quad (7)$$

$$Pr\left(\boldsymbol{y}_{i,j}\right) = \mathcal{N}\left[0, \boldsymbol{I}\right]. \quad (8)$$

We can extend the above formulation to handle multiple observations. For instance, if we are given $J_i = 2$ observations for identity i we would set

$$\tilde{\boldsymbol{A}} = \begin{bmatrix} \boldsymbol{F}, \boldsymbol{G}, 0 \\ \boldsymbol{F}, 0, \boldsymbol{G} \end{bmatrix}. \quad (9)$$

Consequently, we would write that $\tilde{\boldsymbol{x}}_i = [\bar{\boldsymbol{x}}_{i,1}^T, \bar{\boldsymbol{x}}_{i,2}^T]^T$, $\tilde{\boldsymbol{\epsilon}}_i = [\boldsymbol{\epsilon}_{i,1}^T, \boldsymbol{\epsilon}_{i,2}^T]^T$, $\tilde{\boldsymbol{w}}_i = [\boldsymbol{w}_{i,1}^T, \boldsymbol{w}_{i,2}^T]^T$, $\tilde{\boldsymbol{y}}_i = [\boldsymbol{h}_i^T, \boldsymbol{w}_{i,1}^T, \boldsymbol{w}_{i,2}^T]^T$,

A. Training the PLDA Model

To train the PLDA model an EM algorithm is used [1]. All of the M-Steps are provided on a per sample basis once the latent variables have been estimated. It is this estimation of the latent variables, corresponding to the E-Step, that presents the difficulties in making PLDA scalable. In the E-Step, we need to calculate the first-order and second-order moments of the latent variables, we reproduce the equations as follows:

$$E\left[\tilde{\boldsymbol{y}}_i|\tilde{\boldsymbol{x}}_i, \boldsymbol{\Theta}\right] = \left(\tilde{\boldsymbol{I}} + \tilde{\boldsymbol{A}}^T\tilde{\boldsymbol{\Sigma}}^{-1}\tilde{\boldsymbol{A}}\right)^{-1}\tilde{\boldsymbol{A}}^T\tilde{\boldsymbol{\Sigma}}^{-1}\left(\tilde{\boldsymbol{x}}_i\right), \quad (13)$$

$$E\left[\tilde{\boldsymbol{y}}_i\tilde{\boldsymbol{y}}_i^T|\tilde{\boldsymbol{x}}_i, \boldsymbol{\Theta}\right] = \left(\tilde{\boldsymbol{I}} + \tilde{\boldsymbol{A}}^T\tilde{\boldsymbol{\Sigma}}^{-1}\tilde{\boldsymbol{A}}\right)^{-1} + E\left[\tilde{\boldsymbol{y}}_i|\tilde{\boldsymbol{x}}_i, \boldsymbol{\Theta}\right]E\left[\tilde{\boldsymbol{y}}_i|\tilde{\boldsymbol{x}}_i, \boldsymbol{\Theta}\right]^T. \quad (14)$$

From the above equations, it is obvious that the problem for the E-Step is how to cope with the matrix $\left(\tilde{\boldsymbol{I}} + \tilde{\boldsymbol{A}}^T\tilde{\boldsymbol{\Sigma}}^{-1}\tilde{\boldsymbol{A}}\right)^{-1}$ efficiently as it has to be recomputed for each iteration of EM. This matrix is indeed of size $(D_F + J_iD_G, D_F + J_iD_G)$, and has to be used in calculations as well as stored. A solution to this problem was proposed by Kenny [3] when applying PLDA to speaker recognition. Kenny's solution was to apply a variational approximation for this inference problem; however, this approximation relies on a factorization which assumes that the posterior variables are independent and whose quality with respect to the exact solution has not been demonstrated. Once the PLDA model has been trained, it can be used to perform various tasks, which all rely on likelihood calculations.

May be not that easy

You just need the person who wrote the paper !

Current system

Lot of effort

- Public biometric datasets: FERET, FRGC, NIST DBs, XM2VTS, BANCA, MOBIO, CASIA-FASD, REPLAY, MSU MFSD, ...
- Open source software: RAVL, VXL, OpenCV, Torch, CSU FR, BOB, OpenBR, Theanno, ...
- Competitions: ICB, BTAS, IJCB, NIST, FVCongoing, ...
- Platforms: to distribute data, share results, organize competitions

Reproducible Research

Scientific publication vs Scholarship

An article about computational science in a scientific publication is not the scholarship[2] itself, it is merely advertising of the scholarship. The actual scholarship is the complete software development environment and the ***complete set of instructions which generated the figures****.*

D. Donoho,
" An invitation to reproducible computational research",
Oxford Journals, Biostatistics, Vol. 11, no. 3, pp. 385-388, 2010

[1] Knowledge resulting from study and research in a particular field

Reproducible Research

Enter "Reproducible Research" (RR)[3]

One term that aggregates work comprising of:

- a **paper**, that describe your work in all relevant details
- **code** to reproduce all results
- **data** required to reproduce the results
- **instructions**, on how to apply the *code* on the *data* to replicate the results on the *paper*.

[2] `http://reproducibleresearch.net`

Reproducible Research

Levels of Reproducibility[4]

With respect to an independent researcher (reader):

0. Irreproducible
1. Cannot seem to reproduce
2. Reproducible, with extreme effort ($>$ 1 month)
3. Reproducible, with considerable effort ($>$ 1 week)
4. Easily reproducible ($\sim$ 15 min.), but requires proprietary software (e.g. Matlab)
5. **Easily reproducible ($\sim$ 15 min.), only free software**

[3] *Reproducible Research in Signal Processing: What, why and how*, Vandewalle, Kovacevic and Vetterli, IEEE Signal Processing Magazine, vol. 26, no. 3, May 2009, pp. 37-47

Reproducible Research

Incentive: why should I do it ?

Boost your research **impact (visibility)**:

- **Lower entrance barrier** to your publications
- The current number of RR papers is **rather small** – you have a clear chance to stand out today:
  - Only **10% of TIP** papers provide source code[5].
- Statistically, your work is **more valuable** if it is RR:
  - **13 out of the top 15 most cited** articles in TPAMI or TIP provide (at least) source code
  - The average number of citations for papers that provide source-code in TIP is **7 fold** that of papers that don't.

[4] *Code Sharing is Associated with Research Impact in Image Processing*, Patrick Vandewalle, 2012

Reproducible Research

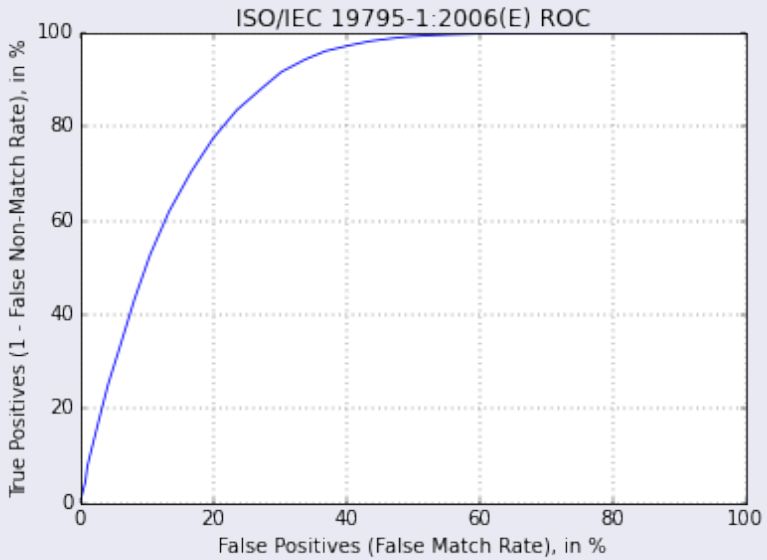
What can be improved ?

- Downloading and storing **data** may be a privacy concern in many countries:
  - Need to work-out space for the growing number of samples
  - Not all databases are distributable (e.g. *forensic data*)
- **Software** management and installation can be hard
  - Software gets outdated: constant quality and integration
  - Plan for errors: re-distribution mechanism
- **Computing** can be limited

Pushing RR to the next level

From the results in a paper

Method	**FAR** (FMR)	**FRR** (FNMR)	**HTER**
ISV	0.178%	0.228%	0.203%



to the same results on an trusted third-party

Just by clicking on an attestation

Pushing RR to the next level

Moving to BEAT: A web platform for RR

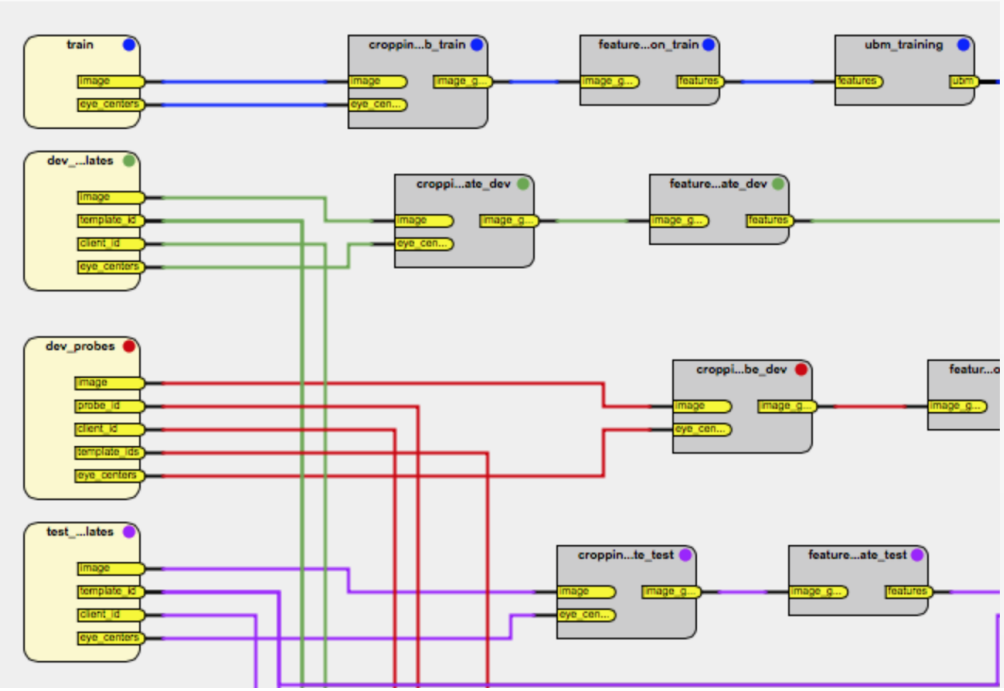
- **Accessible**: no need to install extra software
- **Intuitive**: graphically connect blocks to run experiments
- **Social**: engagement gets you more processing power
- **Productive**: search prior results by any filtering criteria
- **Data Privacy**:
  - No need to handle large-scale databases
  - Can run on un-distributable data (e.g. proprietary databases)
- **Assurance**:
  - fair (reproducible) evaluations of algorithms
  - online attestations for all produced results
- **Free**: build on open-source software and standards

BEAT platform: front-page

BEAT | Search this website... | SIGN-UP | SIGN-IN

The BEAT (*Biometrics Evaluation and Testing*) platform provides easy online access to experimentation and testing for Biometrics. You define what data and modules you would like to use, we make sure the system runs and provides you with a result. Data from different experiments can be easily compared and searched.

Example public toolchain

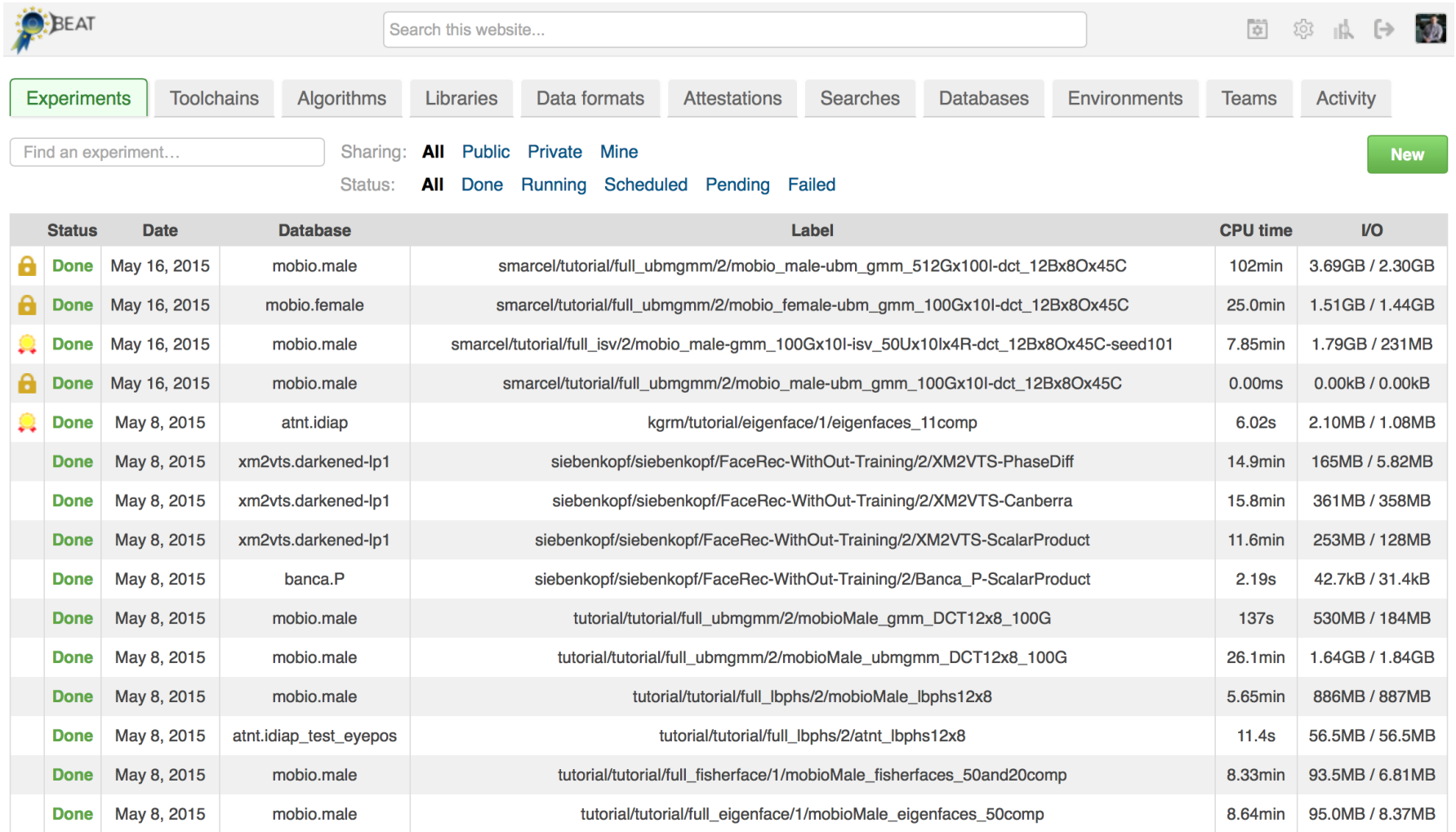


System status

Service is: *operational*

47 users
15 databases
60 toolchains
51 dataformats
257 algorithms
2 experiments scheduled
115 experiments finished
1496h of CPU processing time
1.09TB of memory used

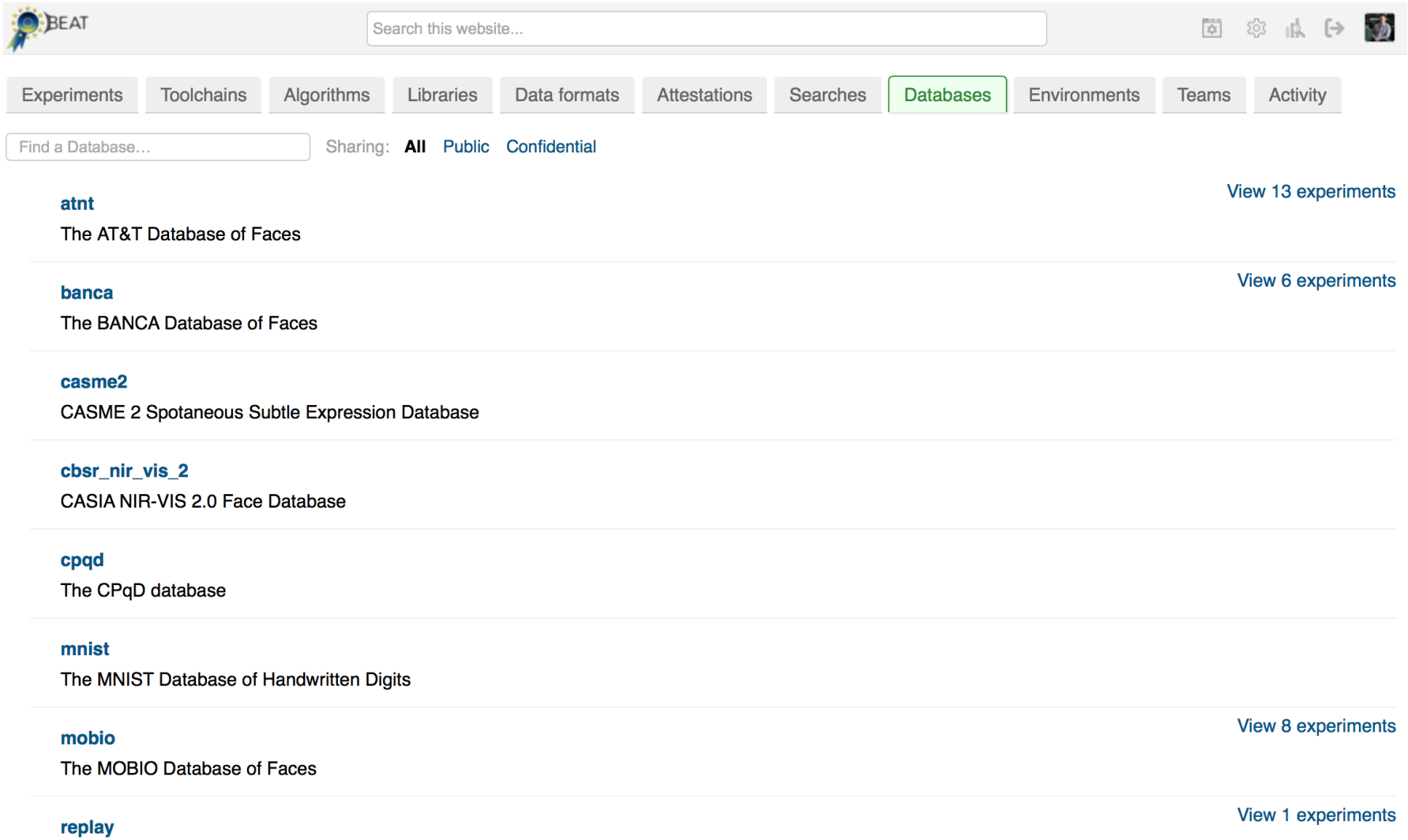
BEAT platform: dashboard



Status	Date	Database	Label	CPU time	I/O
Done	May 16, 2015	mobio.male	smarcel/tutorial/full_ubmgmm/2/mobio_male-ubm_gmm_512Gx100l-dct_12Bx8Ox45C	102min	3.69GB / 2.30GB
Done	May 16, 2015	mobio.female	smarcel/tutorial/full_ubmgmm/2/mobio_female-ubm_gmm_100Gx10l-dct_12Bx8Ox45C	25.0min	1.51GB / 1.44GB
Done	May 16, 2015	mobio.male	smarcel/tutorial/full_isv/2/mobio_male-gmm_100Gx10l-isv_50Ux10lx4R-dct_12Bx8Ox45C-seed101	7.85min	1.79GB / 231MB
Done	May 16, 2015	mobio.male	smarcel/tutorial/full_ubmgmm/2/mobio_male-ubm_gmm_100Gx10l-dct_12Bx8Ox45C	0.00ms	0.00kB / 0.00kB
Done	May 8, 2015	atnt.idiap	kgrm/tutorial/eigenface/1/eigenfaces_11comp	6.02s	2.10MB / 1.08MB
Done	May 8, 2015	xm2vts.darkened-lp1	siebenkopf/siebenkopf/FaceRec-WithOut-Training/2/XM2VTS-PhaseDiff	14.9min	165MB / 5.82MB
Done	May 8, 2015	xm2vts.darkened-lp1	siebenkopf/siebenkopf/FaceRec-WithOut-Training/2/XM2VTS-Canberra	15.8min	361MB / 358MB
Done	May 8, 2015	xm2vts.darkened-lp1	siebenkopf/siebenkopf/FaceRec-WithOut-Training/2/XM2VTS-ScalarProduct	11.6min	253MB / 128MB
Done	May 8, 2015	banca.P	siebenkopf/siebenkopf/FaceRec-WithOut-Training/2/Banca_P-ScalarProduct	2.19s	42.7kB / 31.4kB
Done	May 8, 2015	mobio.male	tutorial/tutorial/full_ubmgmm/2/mobioMale_gmm_DCT12x8_100G	137s	530MB / 184MB
Done	May 8, 2015	mobio.male	tutorial/tutorial/full_ubmgmm/2/mobioMale_ubmgmm_DCT12x8_100G	26.1min	1.64GB / 1.84GB
Done	May 8, 2015	mobio.male	tutorial/tutorial/full_lbphs/2/mobioMale_lbphs12x8	5.65min	886MB / 887MB
Done	May 8, 2015	atnt.idiap_test_eyepos	tutorial/tutorial/full_lbphs/2/atnt_lbphs12x8	11.4s	56.5MB / 56.5MB
Done	May 8, 2015	mobio.male	tutorial/tutorial/full_fisherface/1/mobioMale_fisherfaces_50and20comp	8.33min	93.5MB / 6.81MB
Done	May 8, 2015	mobio.male	tutorial/tutorial/full_eigenface/1/mobioMale_eigenfaces_50comp	8.64min	95.0MB / 8.37MB

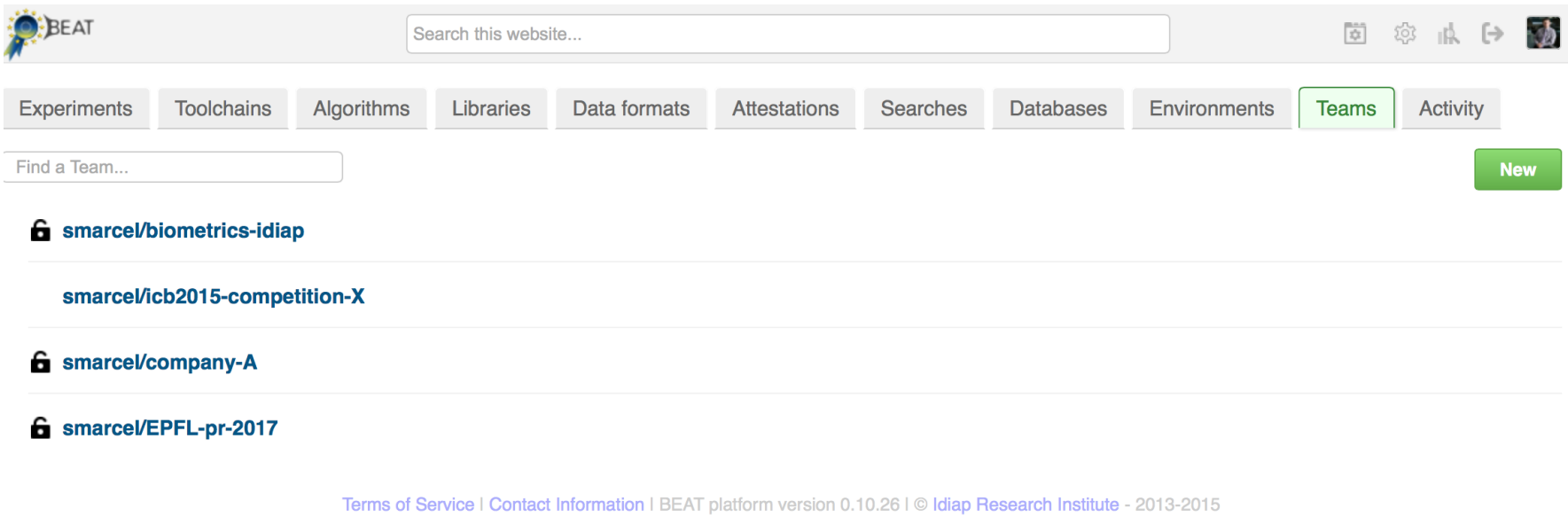
List, search, run experiments and more

BEAT platform: databases



Privacy-by-design

BEAT platform: teams



Grouping users for labs, competitions or industrial projects

BEAT platform: experiments cloning

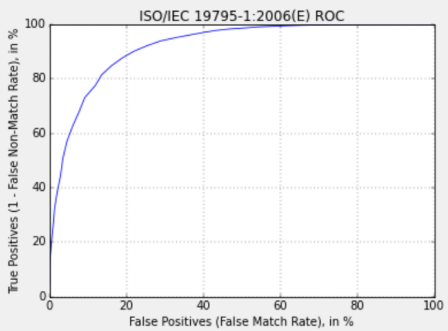
BEAT Search this website...

smarcel / tutorial / full_isv / 2 / mobio_male-gmm_100Gx10l-isv_50Ux10lx4R-dct_12Bx8Ox45C-seed101 Fork

Status: Public

Results View attestation

analysis

eer	0.157
far_dev	0.157
far_test	0.178
frr_dev	0.157
frr_test	0.228
hter	0.203
number_of_negatives_dev	57960
number_of_negatives_test	147630
number_of_positives_dev	2520
number_of_positives_test	3990
roc_dev	

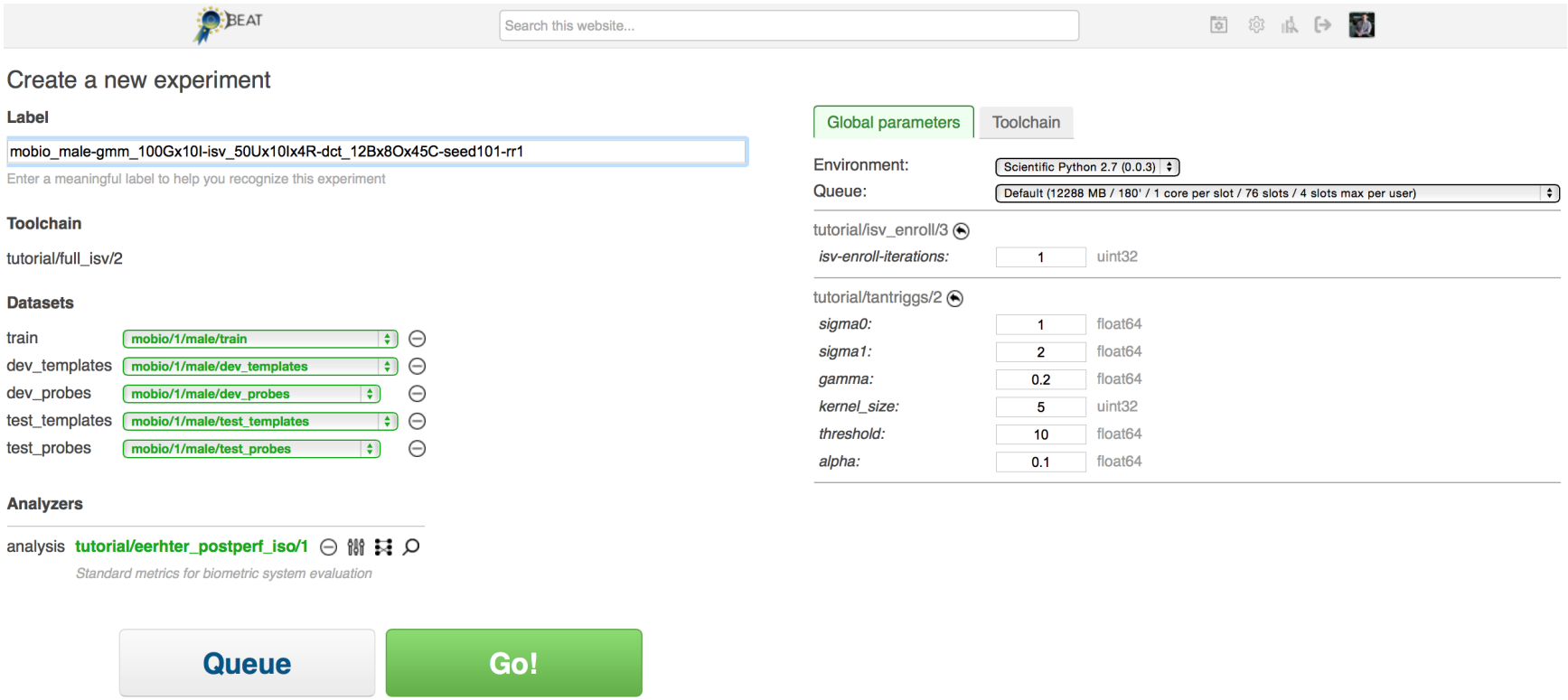
Parameters

Default environment:	Scientific Python 2.7 (0.0.3)
Default queue:	Default
tutorial/isv_enroll/3	
isv-enroll-iterations:	1
tutorial/tantriggs/2	
gamma:	0.2
threshold:	10
alpha:	0.1
sigma1:	2
sigma0:	1
kernel_size:	5
tutorial/dct/3	
block-overlap:	8
number-of-components:	45
block-size:	12
tutorial/cropping_rgb/3	
left-eye-x:	48
left-eye-y:	16
crop-height:	80
crop-width:	64
right-eye-x:	15

Execution infos

Block: analysis	
queuing time:	0.11 seconds
sequential execution time:	12.85 seconds
speed-up:	1.00x
speed-up (maximal):	1.00x
Block: cropping_rgb_probe_dev	
queuing time:	9.98 minutes
sequential execution time:	32.71 minutes
speed-up:	6.54x
speed-up (maximal):	18.59x
Block: cropping_rgb_probe_test	
queuing time:	16.65 minutes
sequential execution time:	58.70 minutes
speed-up:	9.89x
speed-up (maximal):	19.39x
Block: cropping_rgb_template_dev	
queuing time:	6.39 minutes
sequential execution time:	34.36 minutes
speed-up:	6.56x
speed-up (maximal):	18.56x
Block: cropping_rgb_template_test	
queuing time:	13.40 minutes

BEAT platform: experiments re-run



BEAT platform: attestations

BEAT Search this website...

Attestation #1721510690

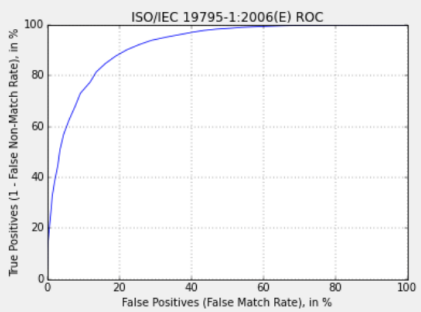
The BEAT platform attests that the following results were obtained by an experiment performed on our servers, and that we kept all the details needed to reproduce them (toolchain, algorithms and parameters).

Experiment

smarcel/tutorial/full_isv/2/mobio_male-gmm_100Gx10I-isv_50Ux10Ix4R-dct_12Bx8Ox45C-seed101

Results

analysis

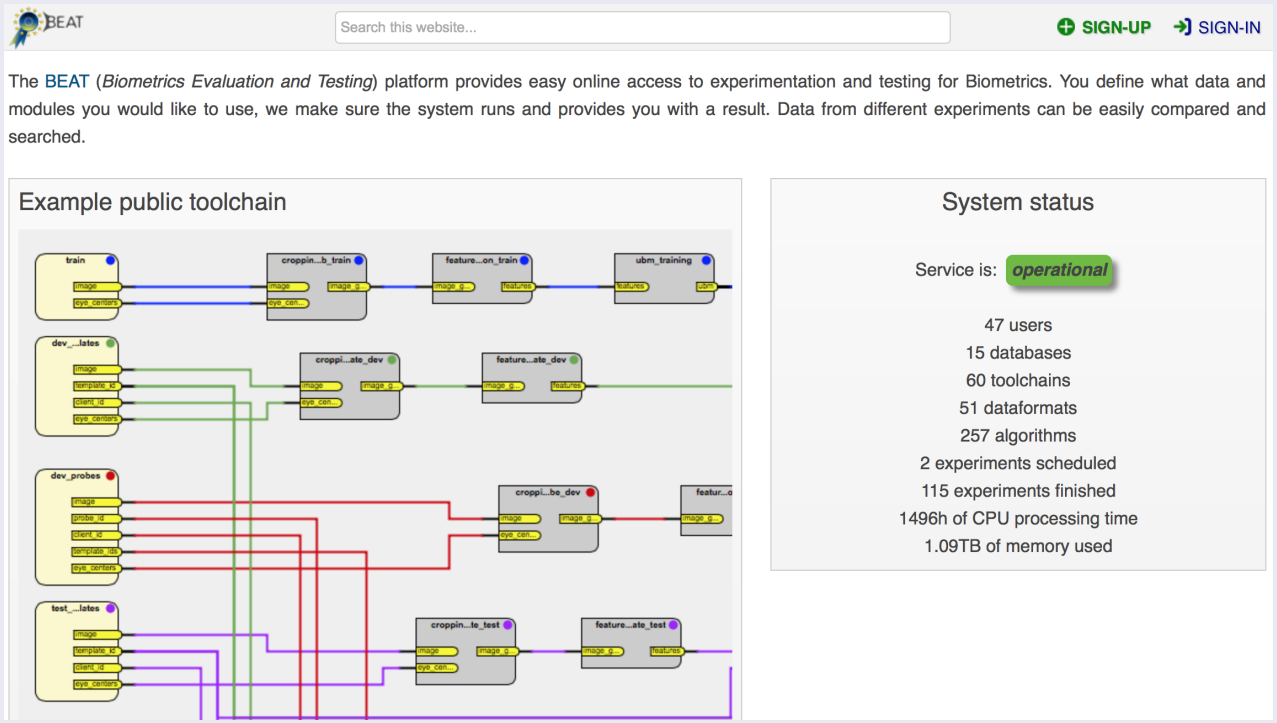
eer	0.157
far_dev	0.157
far_test	0.178
frr_dev	0.157
frr_test	0.228
hter	0.203
number_of_negatives_dev	57960
number_of_negatives_test	147630
number_of_positives_dev	2520
number_of_positives_test	3990
roc_dev	

Certify published results

BEAT platform (beta)

Open to public now !

http://www.beat-eu.org/platform



A "cloud computing" platform for easy online access to experimentation and testing for Biometrics and beyond !

Pushing RR to

the next level ?

0. Irreproducible
1. Cannot seem to reproduce
2. Reproducible, with extreme effort ($>$ 1 month)
3. Reproducible, with considerable effort ($>$ 1 week)
4. Easily reproducible ($\sim$ 15 min.), but requires proprietary software (e.g. Matlab)
5. Easily reproducible ($\sim$ 15 min.), only free software
6. **Easily reproducible ($\sim$ 1 min.), only with a web-browser**

Next

Final release by Jan 2016

- Reputation system to gamify the platform
- Paper generator to export tables, figures (and its data) into re-usable material for publications (LaTeX)
- Remote Software Development Kit (SDK)

The future of the BEAT platform

- Host more biometric databases
- Organize competitions
- Multiple backends: GPU, executables, MATLAB
- Install the platform in different institutions with different databases

Acknowledgement

BEAT

Biometrics Evaluation and Testing

http://www.beat-eu.org/platform

groups.google.com/d/forum/beat-devel

Swiss Biometrics Center

Swiss Center for Biometrics Research and Testing

www.biometrics-center.ch

Thank you for your attention

and a special thanks to

- Researchers, PostDocs and PhDs: André Anjos, Laurent El-Shafey (now @ Google), Manuel Günther (now @ UCCS), Elie Khoury (now @ Pindrop Security), Pedro Tome, Nesli Erdogmus, Matthias Vanoni, Ivana Chingovska, Tiago de Freitas Pereira
- Engineers: François Moulin, Philip Abbet, Samuel Gaist, Flavio Tarsetti

Contact / Info

Sébastien Marcel: www.idiap.ch/~marcel
Bob: http://idiap.github.io/bob/
BEAT platform: http://www.beat-eu.org/platform