CYBER IN NORMANDY

FOUNDATIONS AND TRENDS IN BIOMETRICS

Christophe Rosenberger

ENSICAEN - GREYC

Christophe.rosenberger@ensicaen.fr

GREYC Electronics and Computer Science Laboratory

Normandie Université

UNICAEN

ENSI CAEN ÉCOLE PUBLIQUE D'INGÉNIEURS CENTRE DE RECHERCHE

cnrs

Normandie Université

GREYC
Electronics and Computer Science Laboratory

GREYC RESEARCH LAB

Research in Digital Sciences

Image processing, artificial intelligence, data science, instrumentation, theoretical computer science, cybersecurity, natural language processing

cnrs

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

UNICAEN

STAFF

200 Members

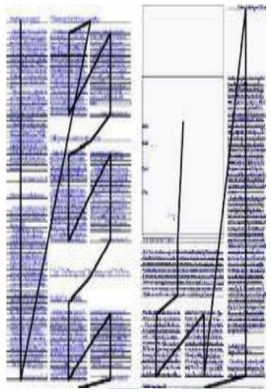
- 7 full time CNRS researchers
- 29 full professors
- 47 associate professors (14 HDR)
- 68 PhD students (17 with a company)
- 19 permanent administrative and technical
- 16 post-doc and research engineers
- 12 associate members

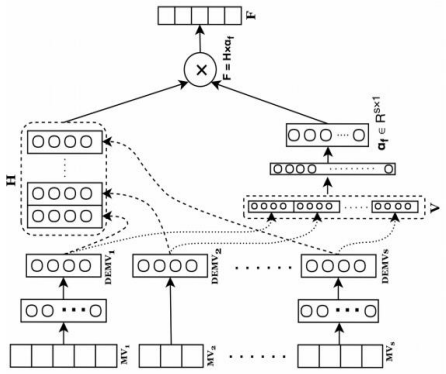
Annual budget: 2000 K€ (without permanent salary)

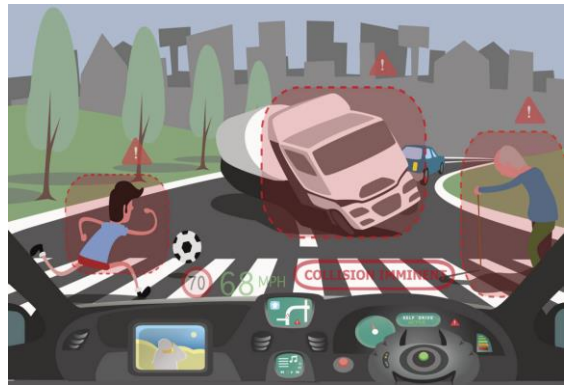
https://www.greyc.fr/

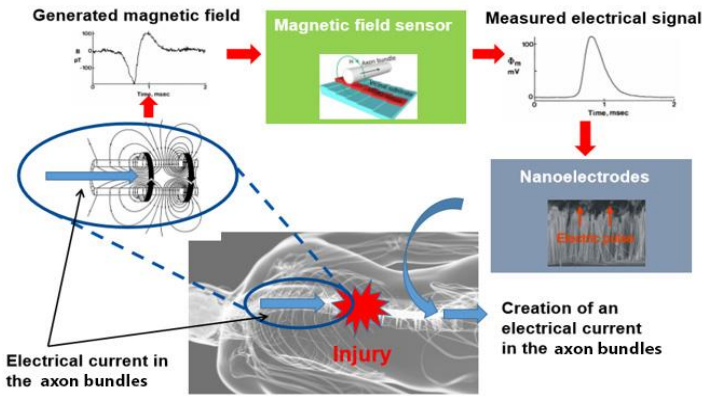
RESEARCH ACTIVITIES

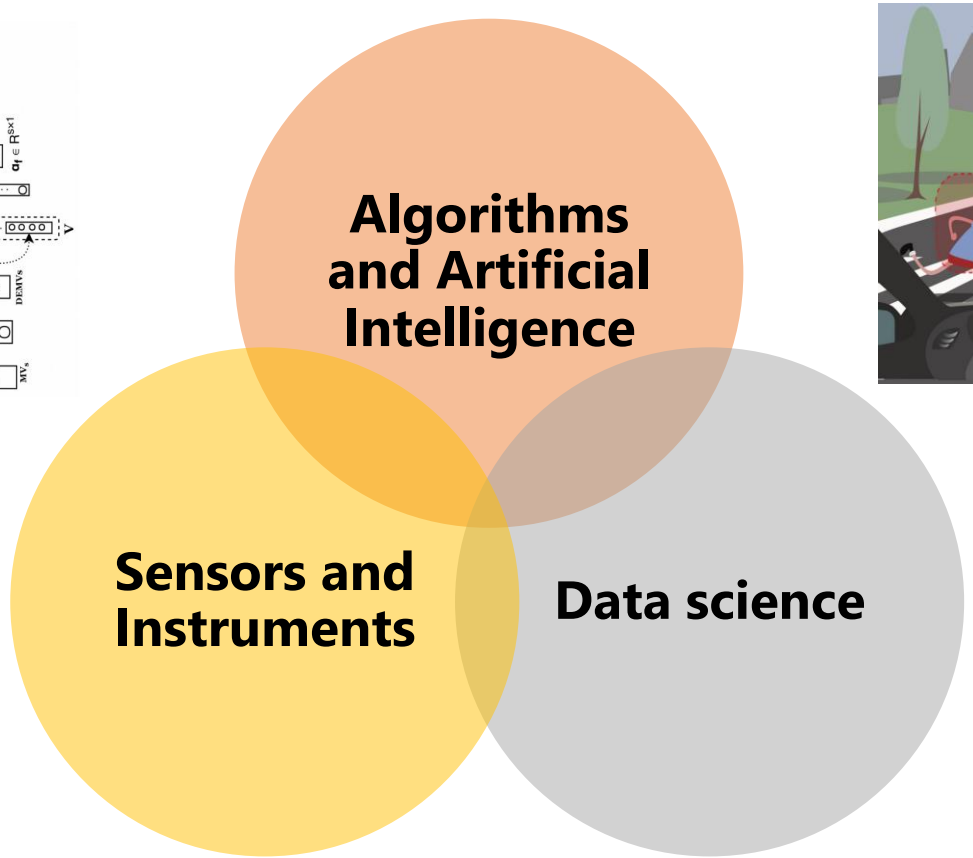
Topics: fundamental, methodological and applied research on issues related to digital sciences

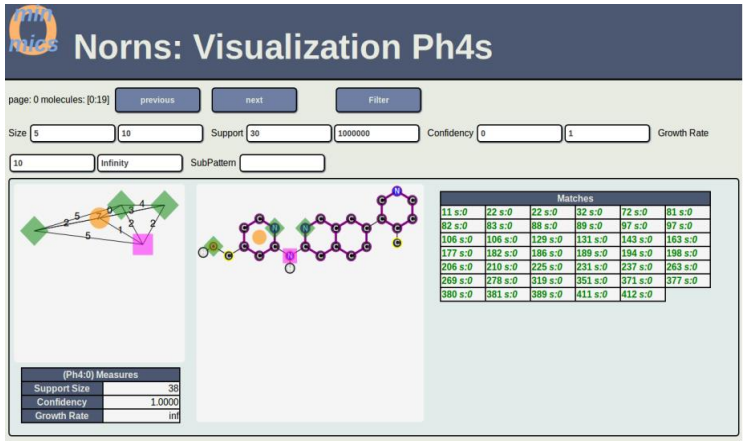












RESEARCH GROUPS

- **AMACC**: Algorithms, Computational Models, Combinatorial, Complexity,
- **CODAG**: Constraints, Ontologies, Data, Annotations, Graphs
- **MAD**: Models, Agents and Decisions
- **IMAGE**: Image processing and understanding
- **ELEC**: Electronics
- **SAFE**: Security, Architectures, Forensics, biomEtrics

Normandie Université

GREYC
Electronics and Computer Science Laboratory

SAFE RESEARCH GROUP

Research in Cybersecurity

- ✓ **Biometrics**: definition/evaluation of biometric systems, biometric data protection
- ✓ **Security architectures:** Network security (SDN, 5G, 6G), applied cryptography, randomness and information protection.
- ✓ **Digital Forensics**: Automatic language processing, forensic platform, privacy protection.

cnrs

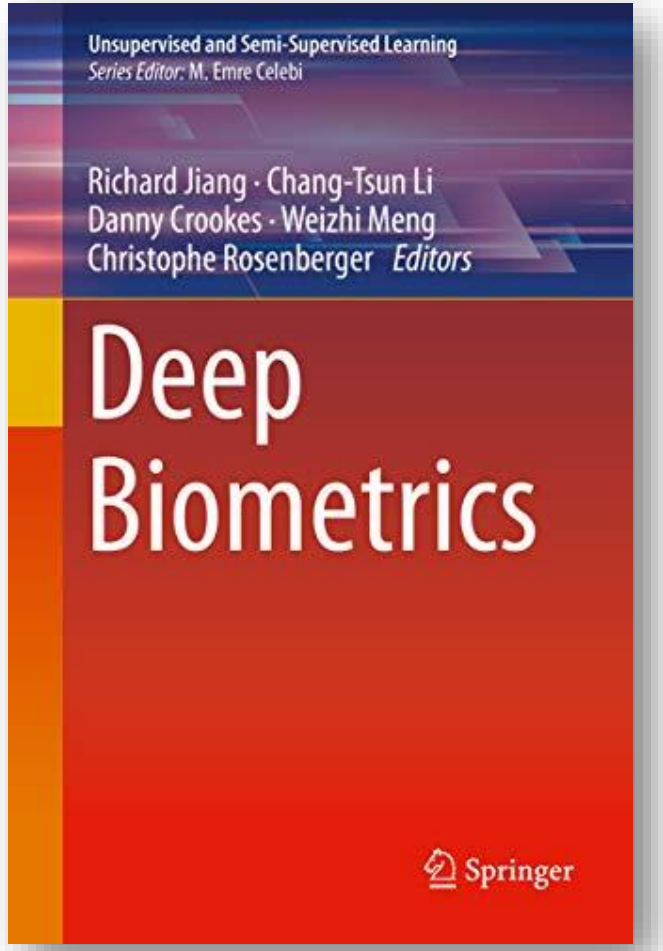
ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

UNICAEN

WHO AM I?

Christophe ROSENBERGER

- ❑ Full professor in Computer Science at ENSICAEN
- ❑ Cybersecurity researcher at the GREYC research lab (director)
  - ✓ Biometrics (since 2005)
  - ✓ Digital forensics (since 2021)
- ❑ Chairman of the evaluation and monitoring panel for the Italian Cybersecurity research strategy

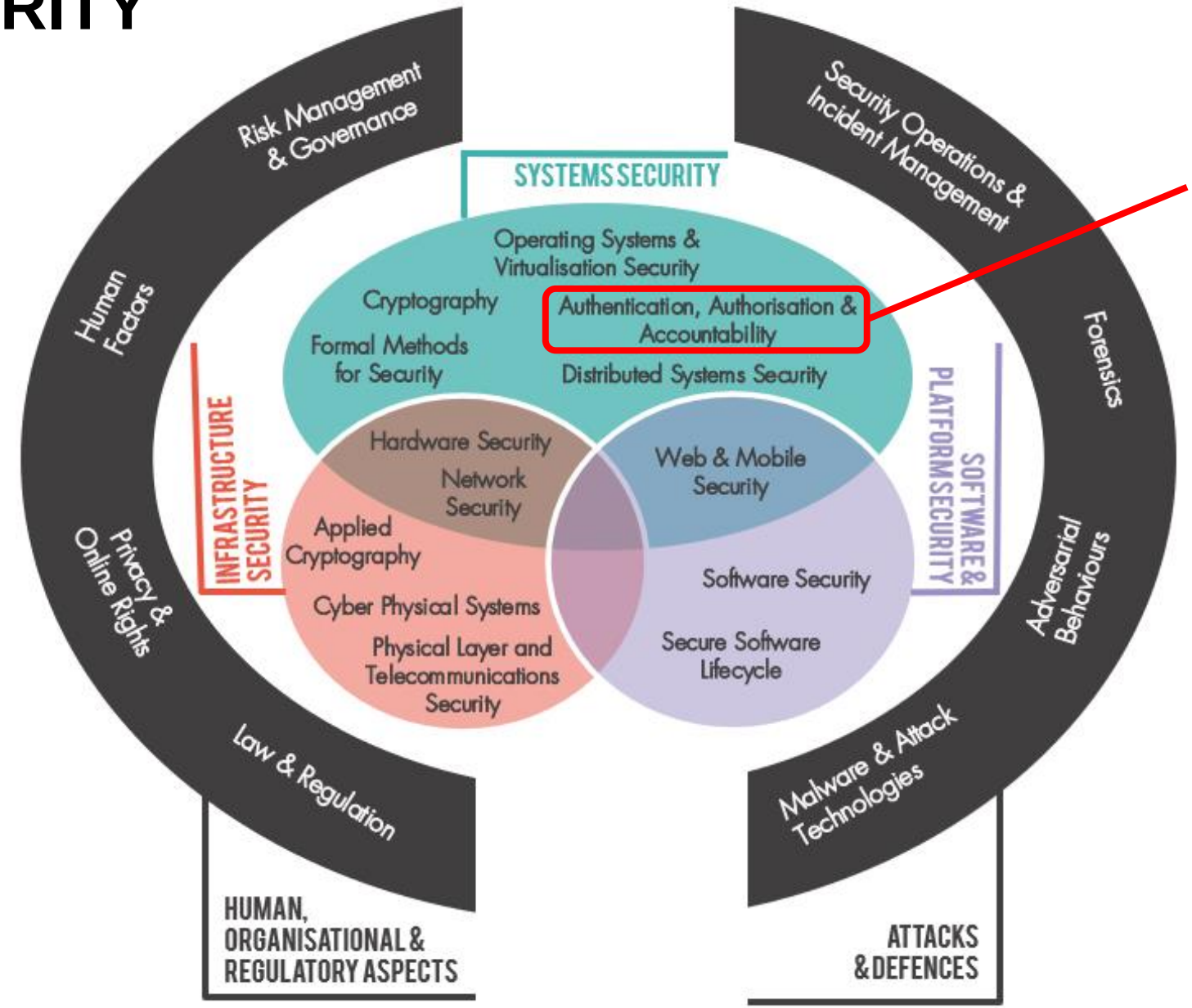


SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

SAFE
GREYC

https://rosenberger.ensicaen.fr/

CYBERSECURITY

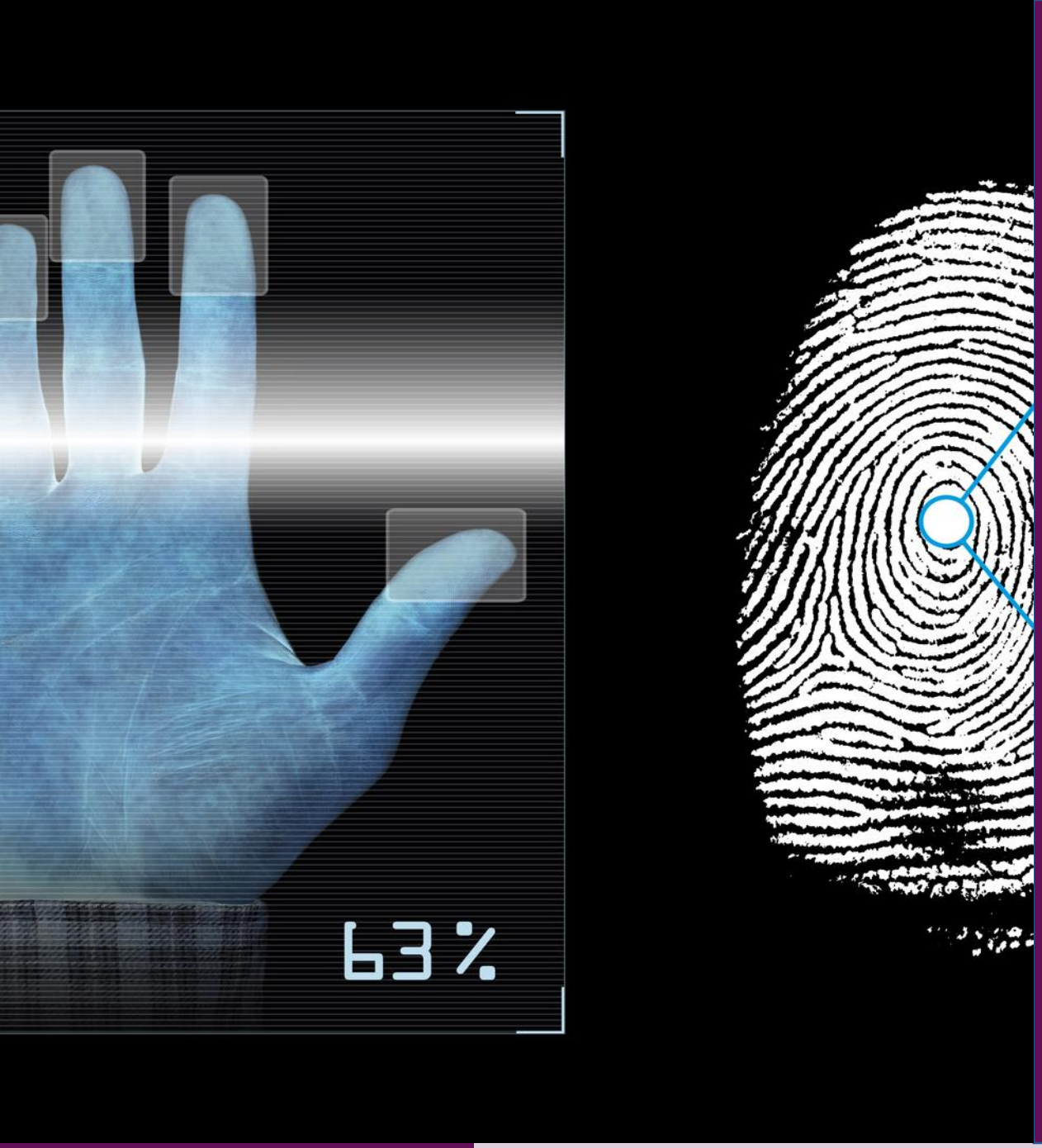


Biometrics

https://www.cybok.org/

PLAN

- ❑ Introduction
- ❑ Evaluation of biometric systems
- ❑ Soft biometrics
- ❑ Template aging
- ❑ Privacy protection
- ❑ Open questions



Normandie Université

GREYC
Electronics and Computer Science Laboratory

INTRODUCTION

BIOMETRICS

Automatic identification of an individual or verification of its identity by using morphological or behavioral characteristics

cnrs

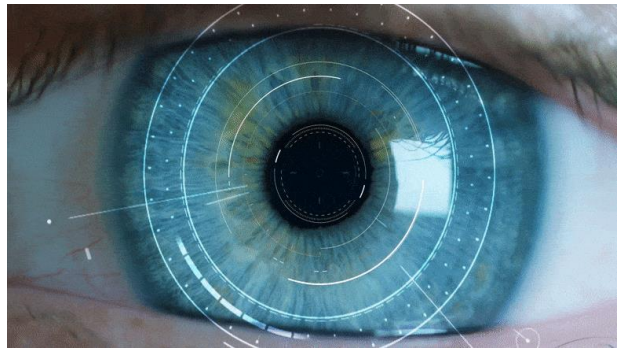
ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

UNICAEN

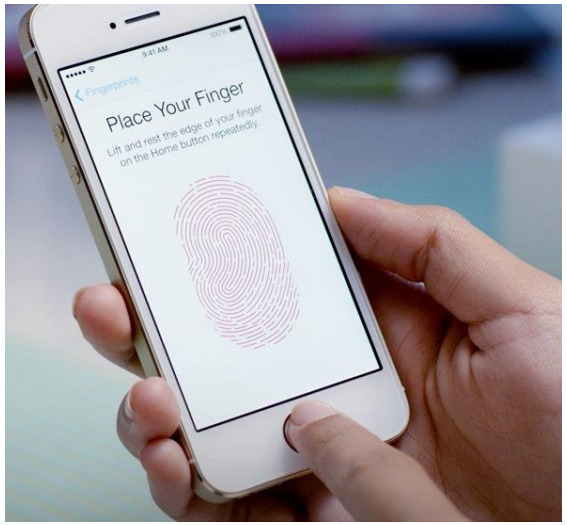
INTRODUCTION

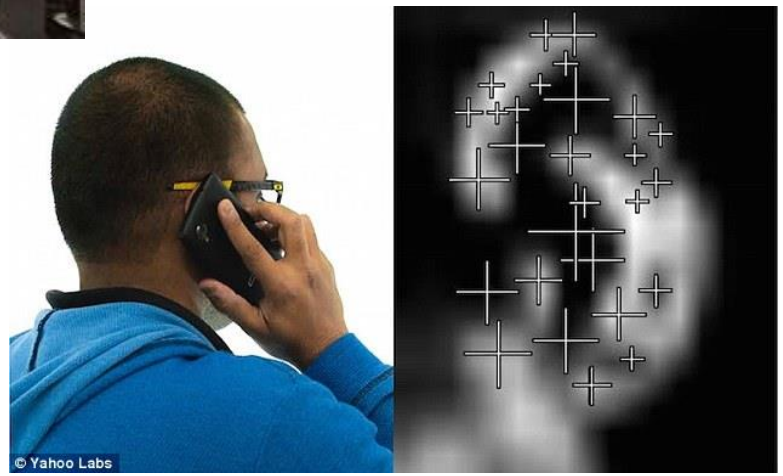
Biometric modalities

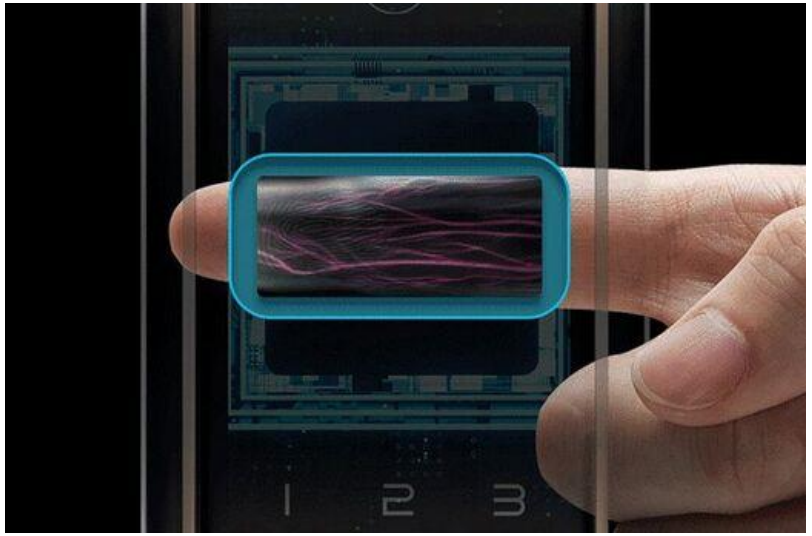
- **Biological analysis**:
  EEG signal, DNA…
- **Behavioural analysis**:
  Keystroke dynamics, voice, gait, signature dynamics…
- **Morphological analysis**:
  Fingerprint, iris, palmprint, finger veins, face, ear…



INTRODUCTION



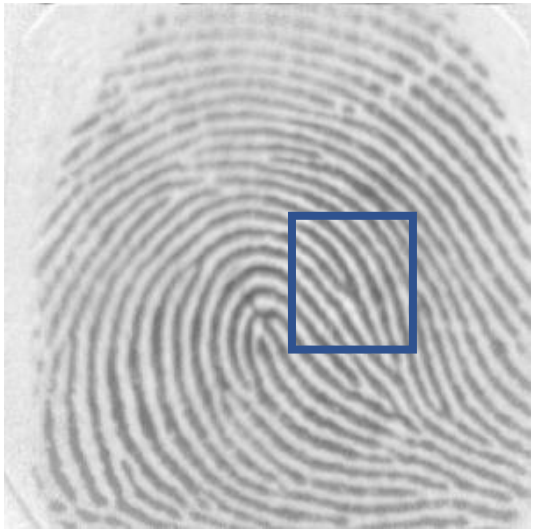




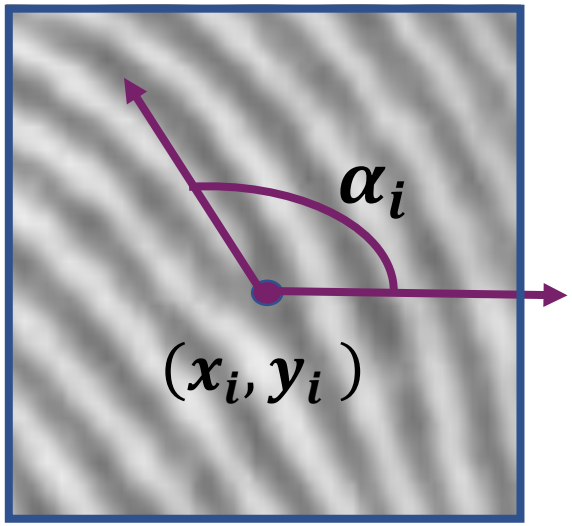
INTRODUCTION

Definitions:

- **Biometric sample:** analog or digital representation of biometric characteristics prior to biometric feature extraction
- **Biometric reference:** one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used as the object of biometric comparison



Biometric sample



Minutiae

Biometric reference

$$T = \{m_1, \dots, m_n\}$$

With $m_i = (x_i, y_i, \alpha_i, T_i)$

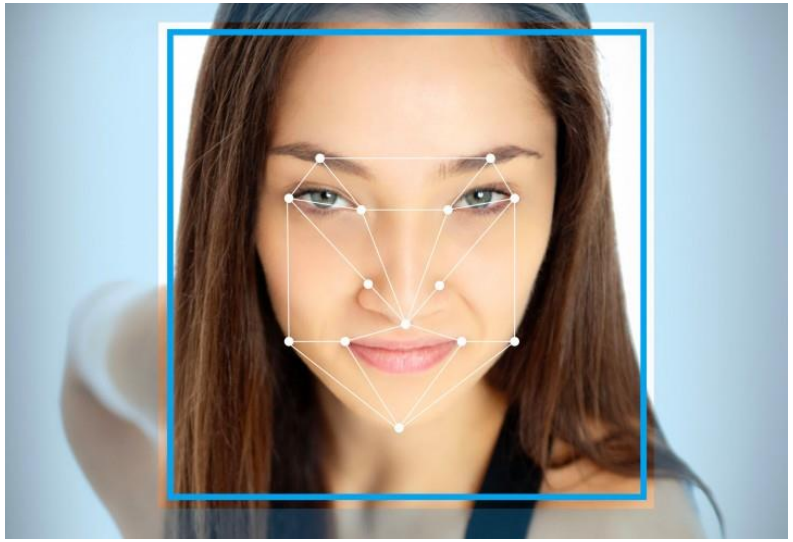
(x_i, y_i): minutiae location
α_i: *minutiae orientation*
T_i: *minutiae type*

INTRODUCTION

Enrollment: act of creating and storing a biometric reference data record

Verification: process of confirming a biometric claim through biometric comparison

Identification: process of searching against a biometric enrolment database to find and return the biometric reference identifier(s) attributable to a single individual



INTRODUCTION

How do decide if the claimed identity is correct ?

Suppose SCORE is a similarity matcher

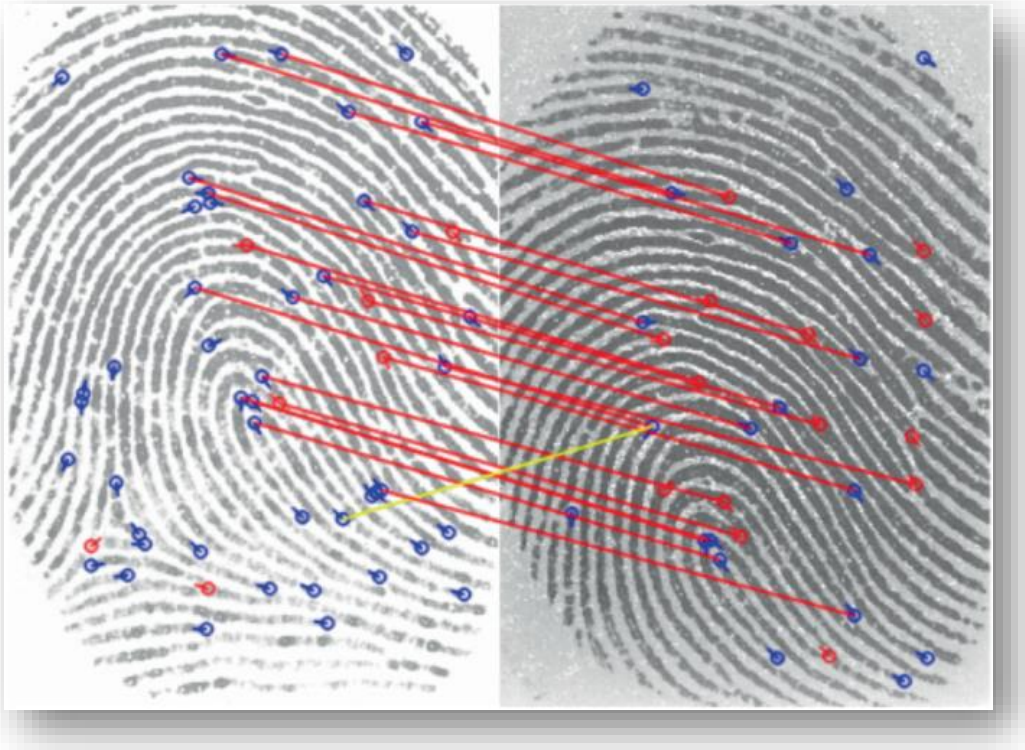
IF SCORE (REFERENCE, SAMPLE) > THRESHOLD θ

ACCEPT

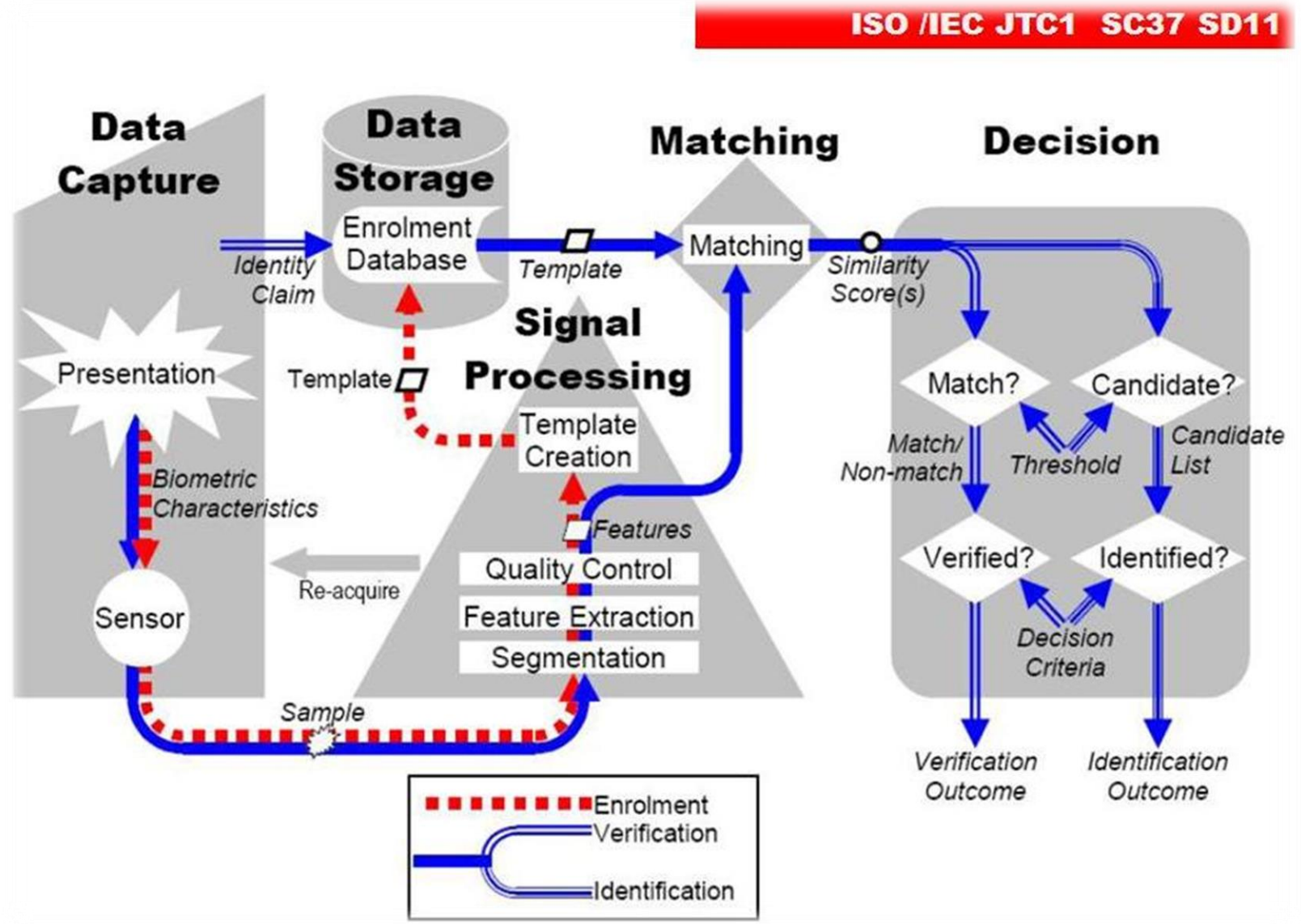
ELSE

REJECT

THRESHOLD θ value is set according to the application



INTRODUCTION



Components of a biometric system:

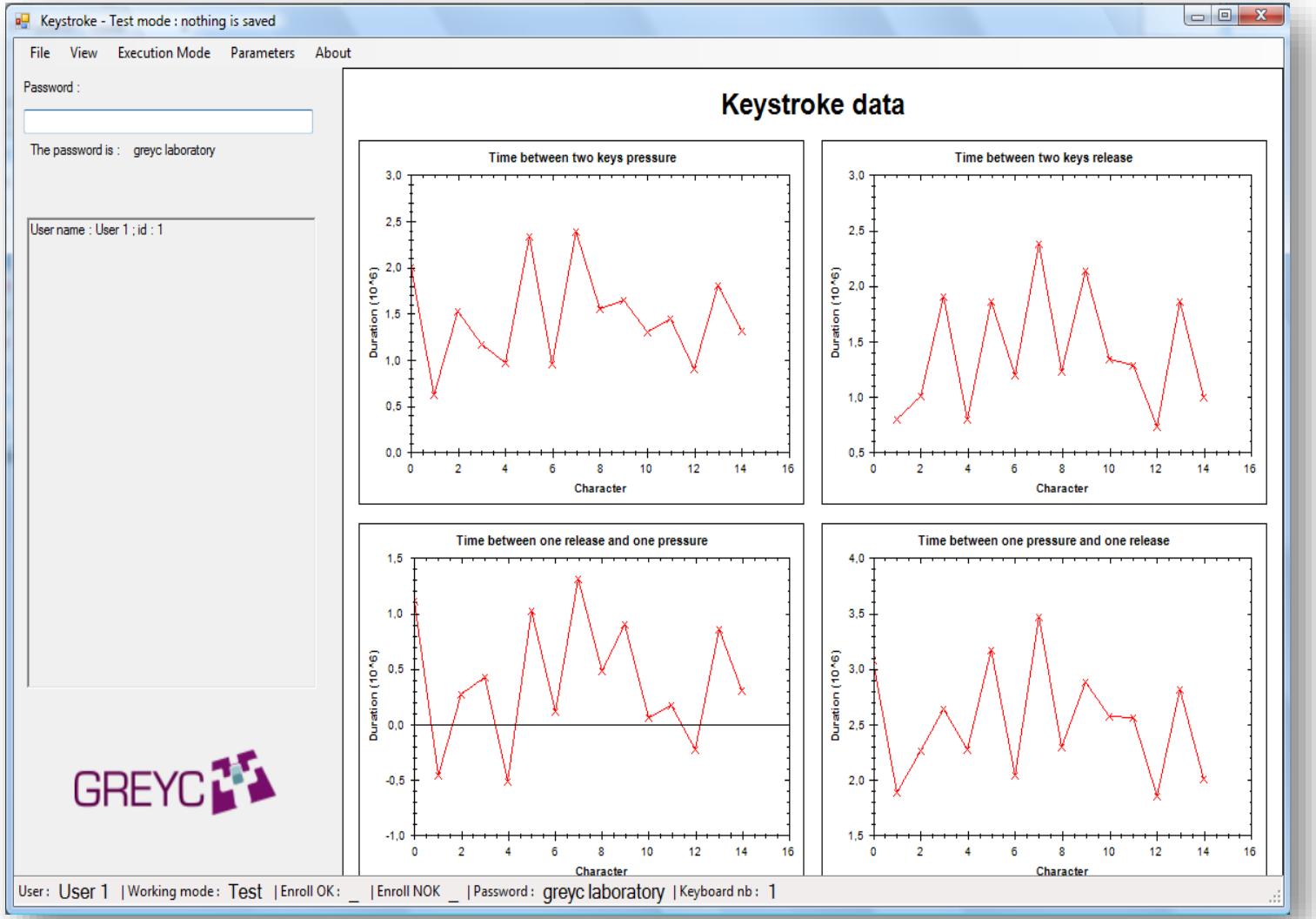
- ❑ Data capture,
- ❑ Signal processing,
- ❑ Data storage,
- ❑ Matching,
- ❑ Decision.

INTRODUCTION

Demo:

Keystroke dynamics sytems

(windows software that can be downloaded on my webpage)



R. Giot, M. El-Abed, B. Hemery, C. Rosenberger, "Unconstrained Keystroke Dynamics Authentication with Shared Secret", Elsevier Journal on Computers & Security (IF 0.868), Volume 30, Issues 6-7, Pages 427-445, September-October 2011.

INTRODUCTION

Definition of biometric systems
- Sensor definition
- Feature generation
- Soft biometrics
- Template update
- Multi-biometrics
- Mobile biometrics
- XAI for biometrics
- Indexing

Evaluation of biometric systems
- Performance
- Presentation attack
- Fairness
- Usability
- Biometric data quality
- Synthetic data generation

Privacy protection
- Hardware
- Software
  - ✓ Encryption
  - ✓ Transformation
  - ✓ Protocol
  - ✓ Architecture

Normandie Université

GREYC
Electronics and Computer Science Laboratory

EVALUATION OF BIOMETRIC SYSTEMS

How accurate is a biometric system ?

How to set the decision threshold

cnrs

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

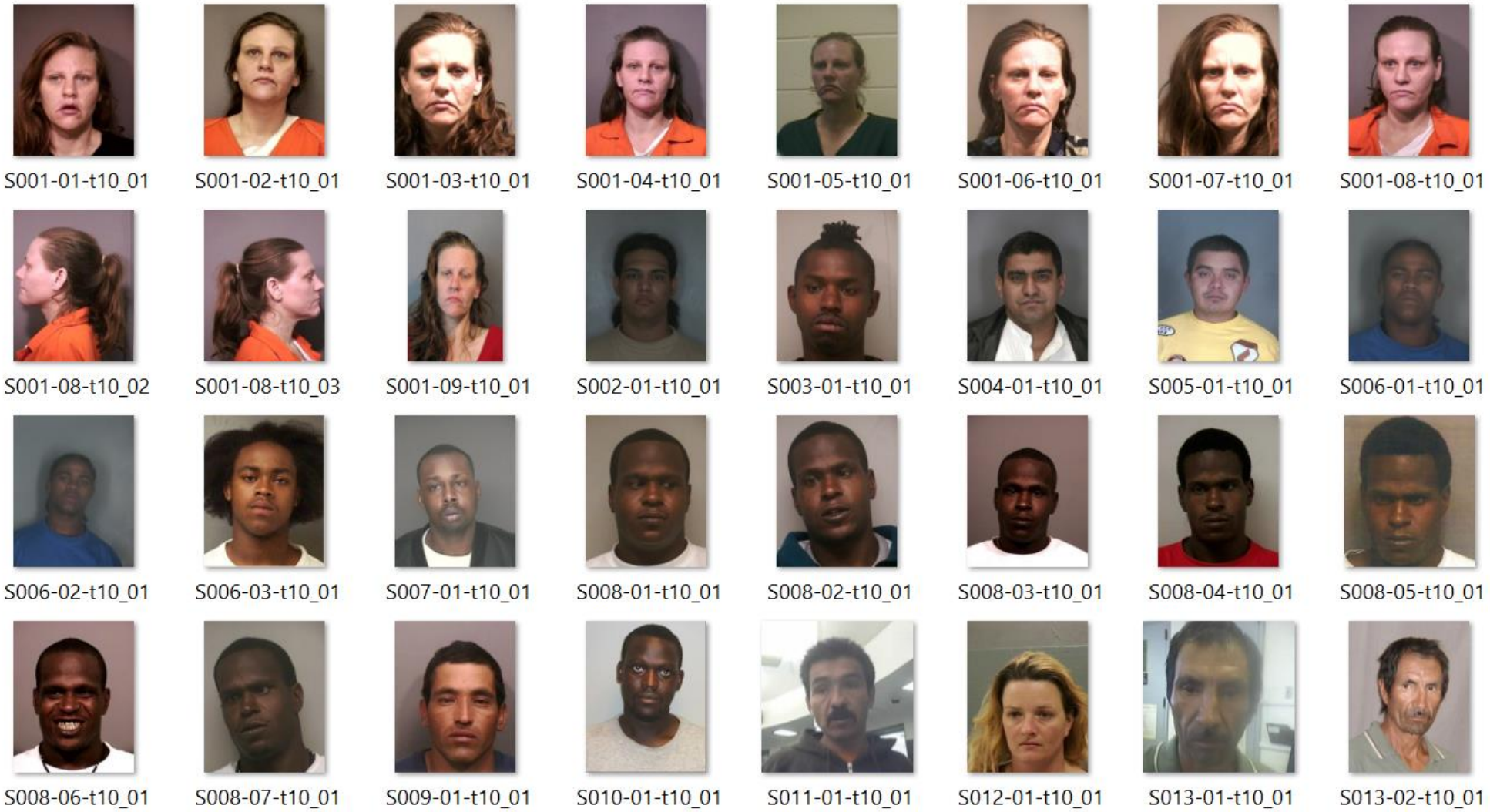
UNICAEN

PERFORMANCE

Evaluation:
Collection of biometric data

Biometric database: MEDS

Samples of 13 individuals



https://www.nist.gov/itl/iad/image-group/special-database-32-multiple-encounter-dataset-meds

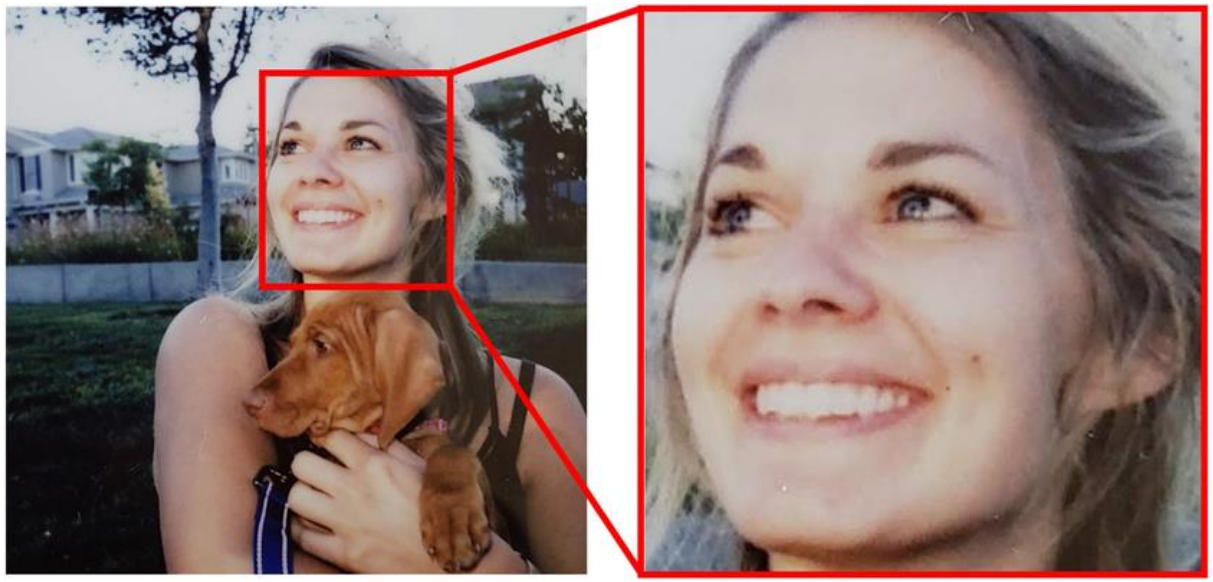
PERFORMANCE

Acquisition metrics (sensor evaluation)

- **Failure To Acquire Rate**
  - ✓ FTAR
  - ✓ Problem during capture
  - ✓ Physical incapacity
  - ✓ Sensor does not work
- **Failure To Enroll Rate**
  - ✓ FTER
  - ✓ Insufficient biometric quality
  - ✓ User does not want to enroll himself

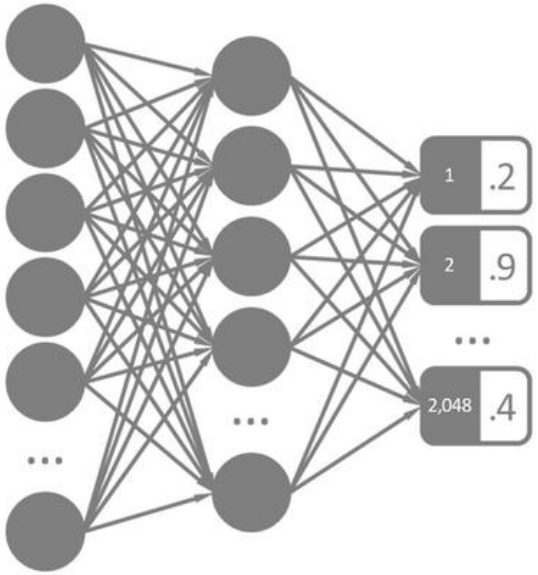
PERFORMANCE

Evaluation: example of a typical biometric system using a deep neural network



Detect face (Face++)

Crop and resize
(224 x 224 pixels)



Extract 2,048 face
descriptors (VGGFace2)

Cross-validated
Logistic Regression
(or other similarity measure)

$P_{liberal}$ = 38%

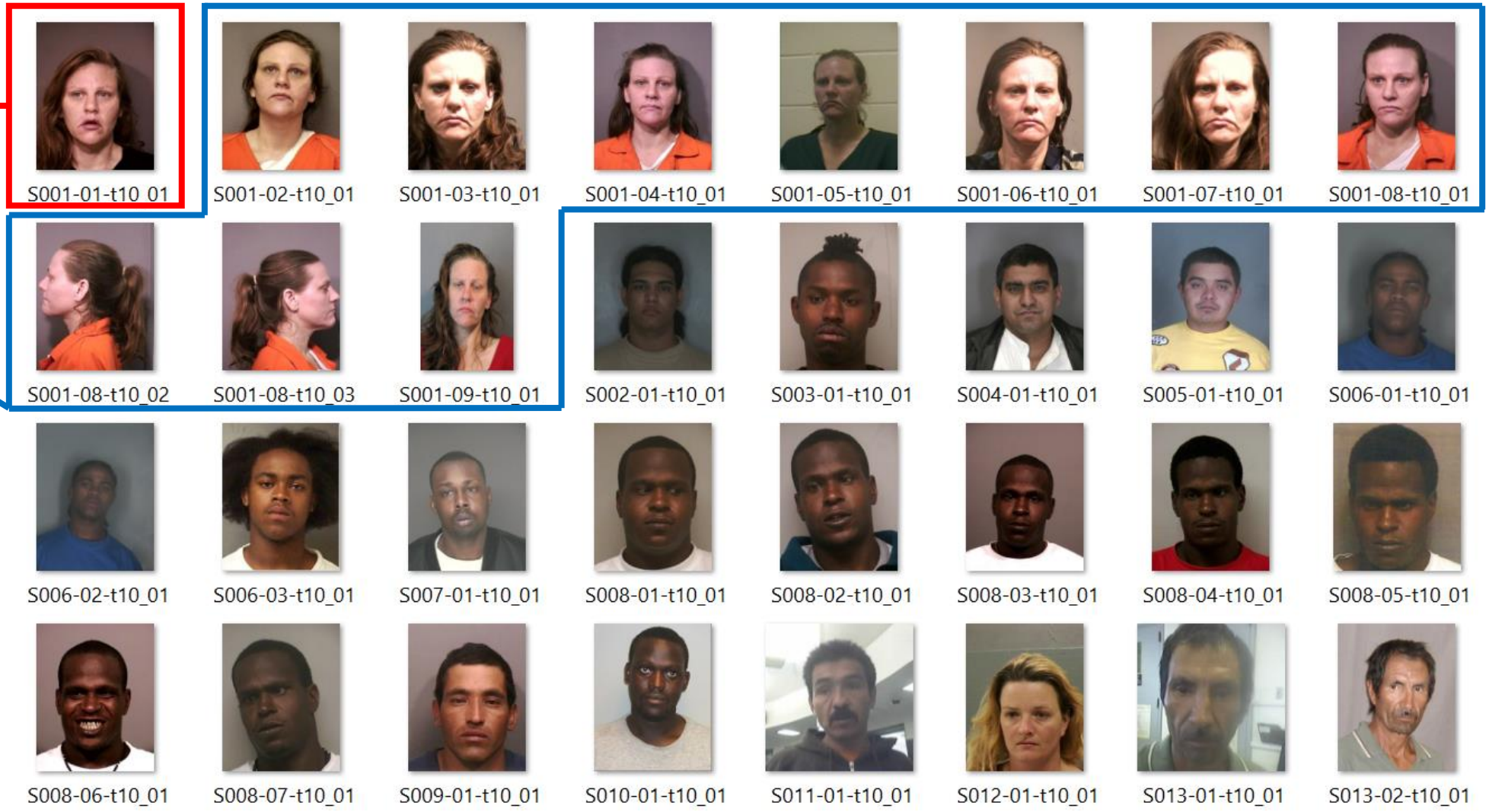
Compare with liberal
and conservative faces

Kosinski, M. Facial recognition technology can expose political orientation from naturalistic facial images. Sci Rep 11, 100 (2021). https://doi.org/10.1038/s41598-020-79310-1

PERFORMANCE

Reference template

Test samples



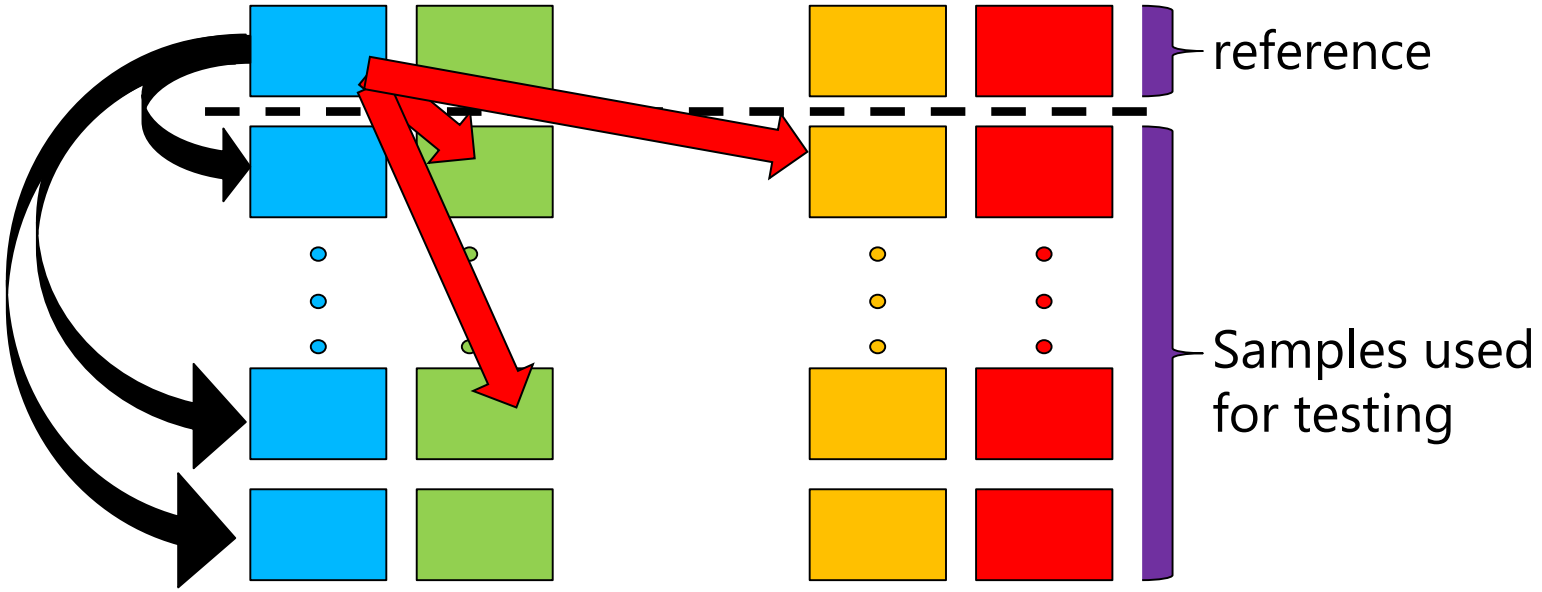
Evaluation:

- ❑ Selection of the reference template
- ❑ Use other samples for testing

PERFORMANCE

Distribution of legitimate and impostor scores

1. Computation of scores
2. Plotting the frequency of each value

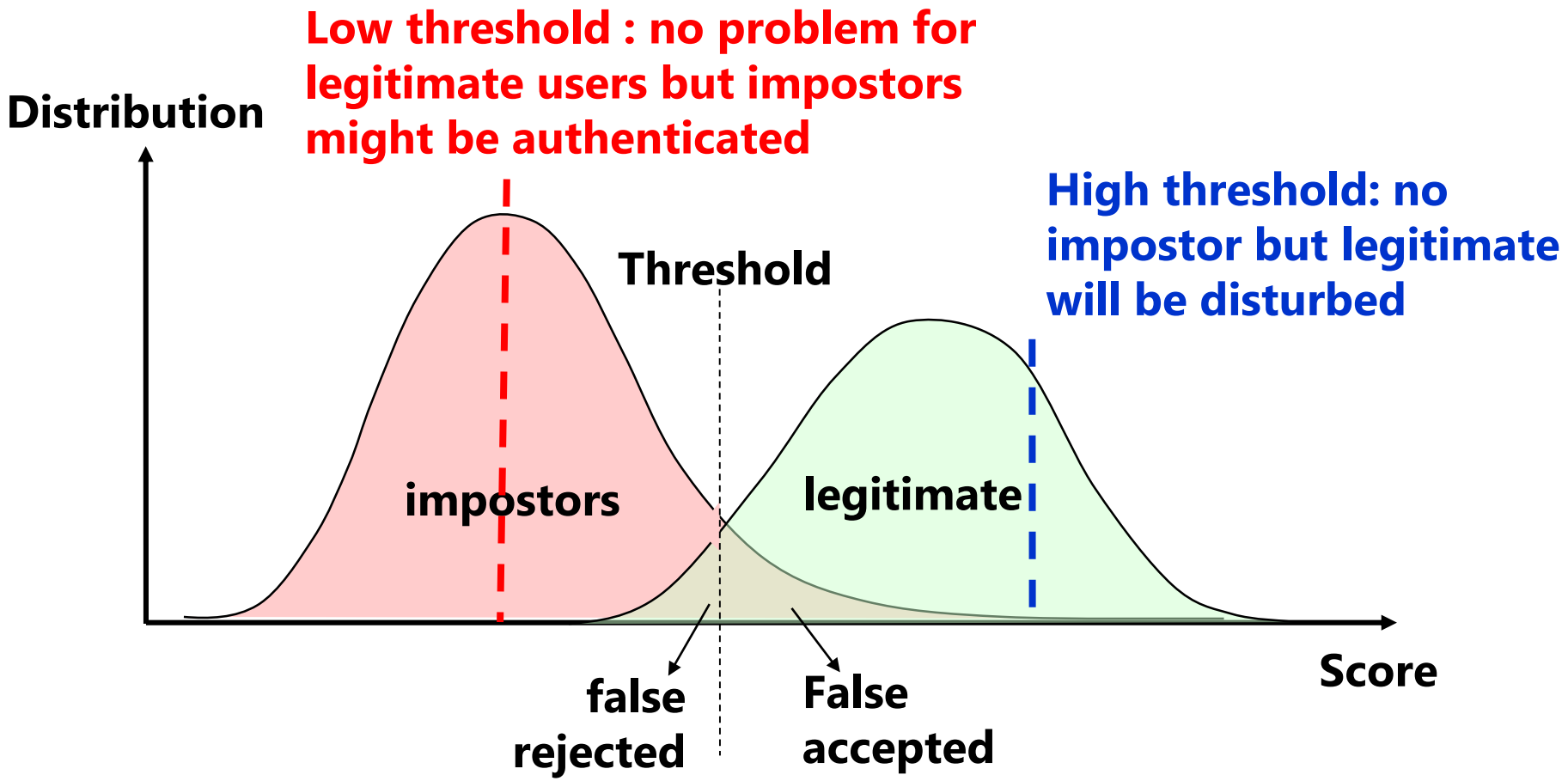


Legitimate scores: comparison between a sample and the reference of the same user

Impostor scores: comparison between a sample and the reference of a different user

PERFORMANCE

Distribution of legitimate and impostor scores



PERFORMANCE

Authentication metrics (algorithm)

Errors depending of the threshold value θ

- **False Match Rate**
  - ✓ FMR(θ)
  - ✓ Ratio of accepted impostors
- **False Non Match Rate**
  - ✓ FNMR(θ)
  - ✓ Ratio of rejected legitimate users

PERFORMANCE

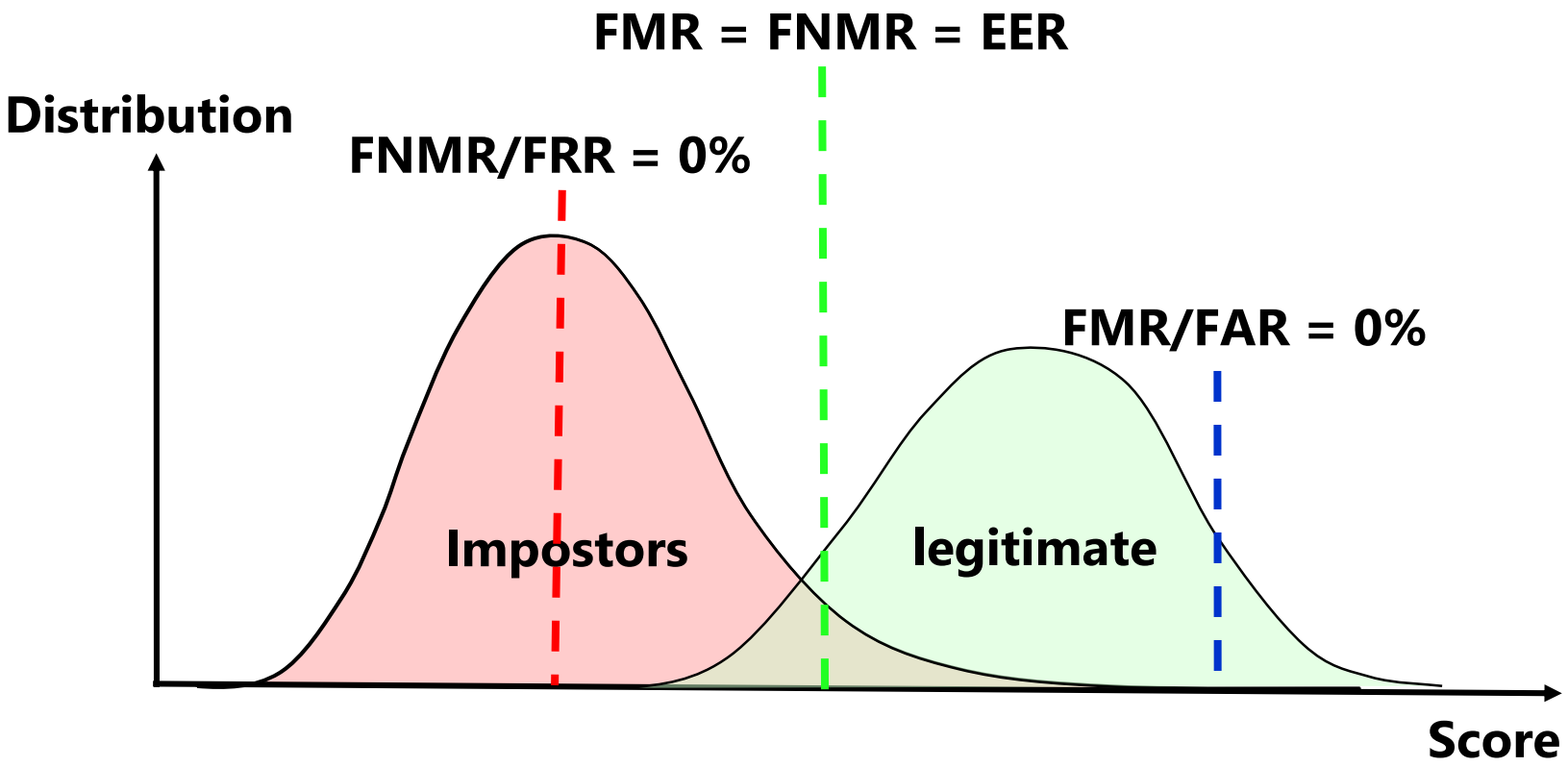
Authentication metrics (system)

Errors depending of the threshold value θ

- **False Acceptation Rate (FAR)**
  - ✓ $FAR(\theta) = (1 - FTAR).FMR(\theta)$
- **False Rejection Rate (FRR)**
  - ✓ $FRR(\theta) = (1 - FTAR).FNMR(\theta) + FTAR$

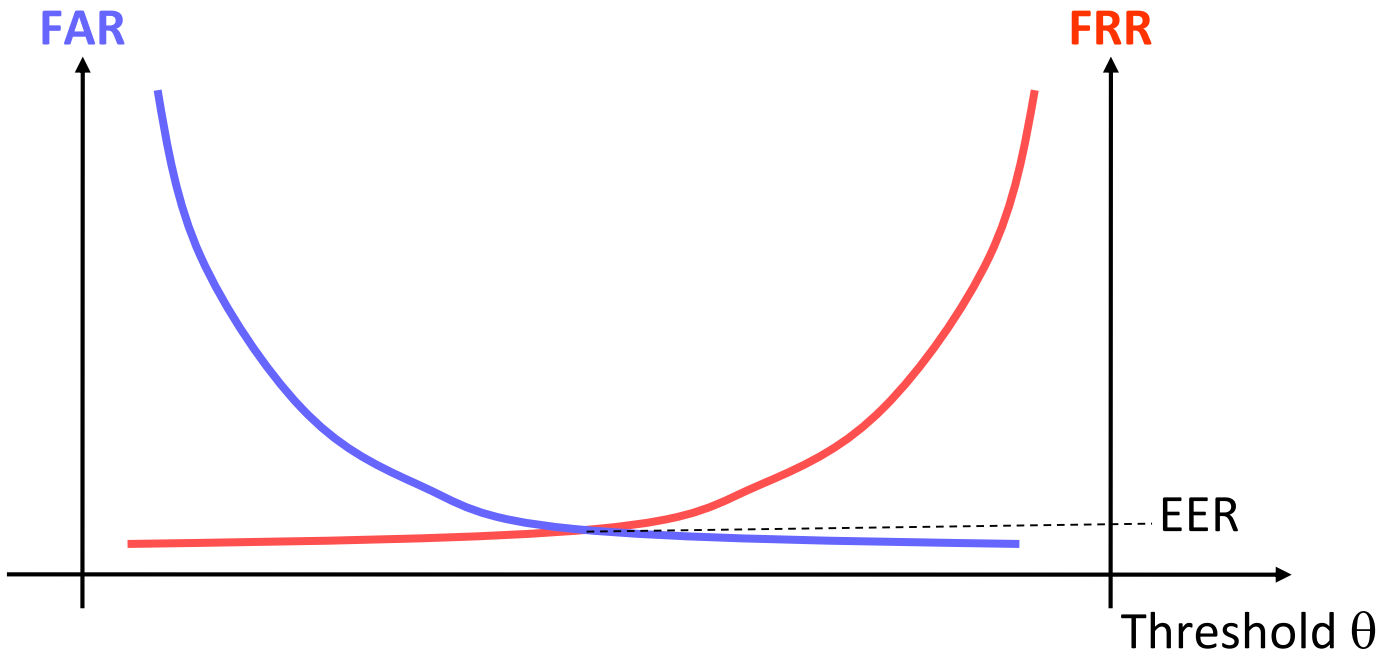
PERFORMANCE

Illustration of metric values: impact of the threshold value θ



PERFORMANCE

Relationship between FAR, FRR, EER and threshold θ



Performance points

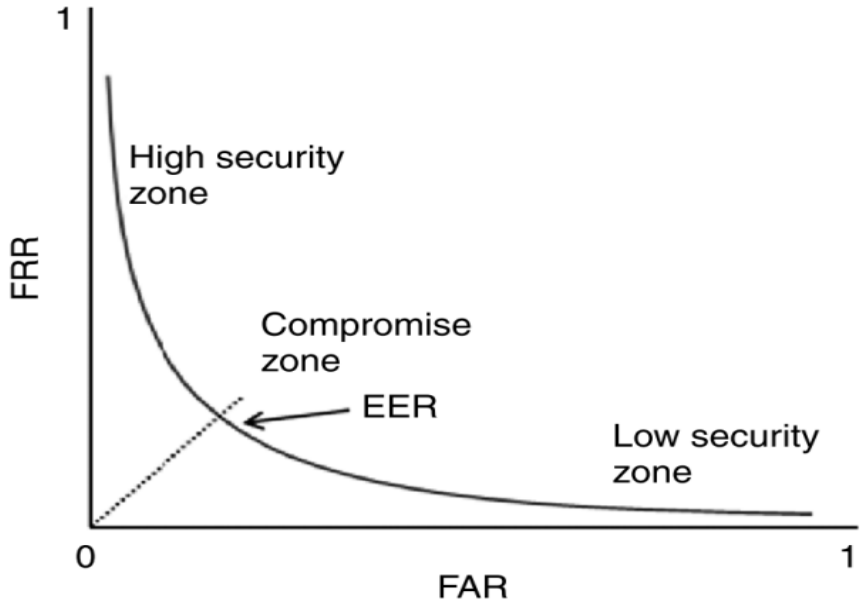
- **EER:** Equal Error Rate
  Setting threshold θ to have FRR(θ)=FAR(θ)=EER
- **FRR @FAR:** FRR value when FAR is set

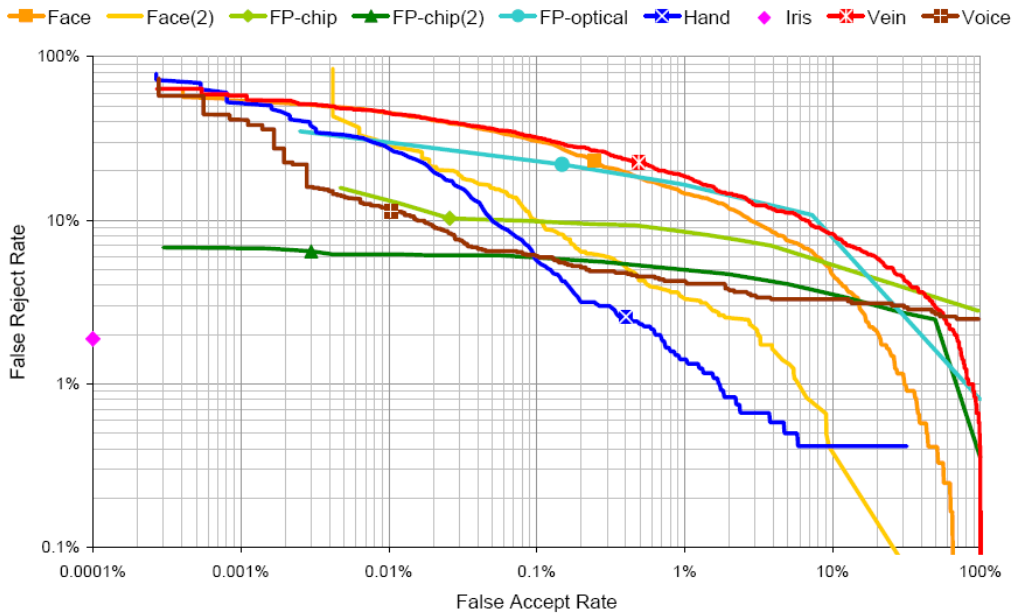
PERFORMANCE

ROC curve [Receiver Operating Characteristics]

Global performance of a biometric authentication system.

- Relation between the FAR and the FRR for different decision threshold values, as abscissa and ordinate, respectively,
- Compact representation of the performance of a biometric system,
- Objective comparison of different biometric systems (even from different biometric modalities).





PERFORMANCE

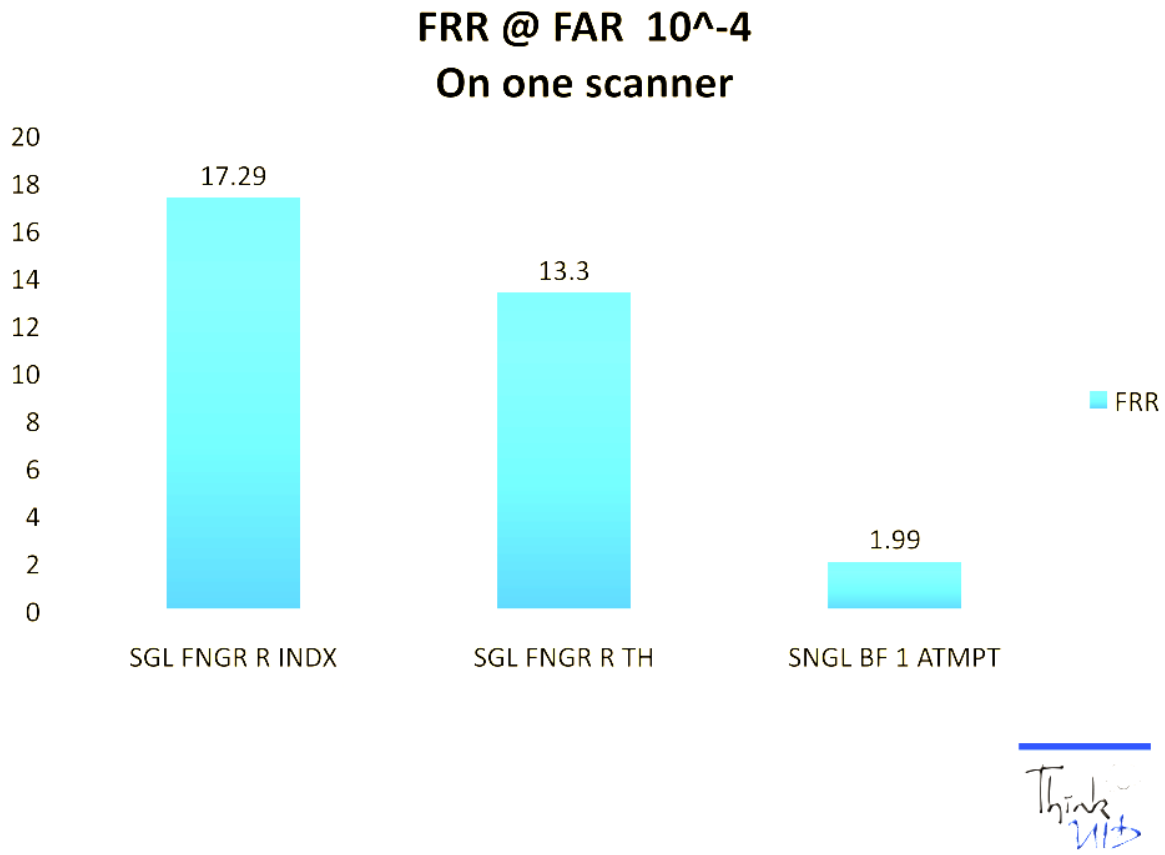
UID example:

- Enrollment (multi-modal biometric)
  - 36,000 enrollment stations, 87K certified operators
  - 11 models of certified devices
  - 200 Million enrolled
  - 400 Million planned for FY '13
  - 1M/day enrollment rate
  - *100 trillion person matches/day*
- Biometric Verification
  - 8 PoC
  - Two pilot programs underway

Source: Raj Mashruwala, "Scenario Testing of Mobile Fingerprint Verification System", NIST International Biometric Performance Conference 2012.

PERFORMANCE

Example UID program in India:



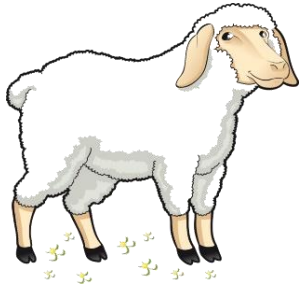
Source: Raj Mashruwala, "Scenario Testing of Mobile Fingerprint Verification System", NIST International Biometric Performance Conference 2012.

PERFORMANCE

Doddington zoo: different performance for each user when using a biometric system

Sheep

- Users who can easily be recognized



Goats

- Users who are particularly difficult to recognize

Lambs

- Users who are easy to imitate

Wolves

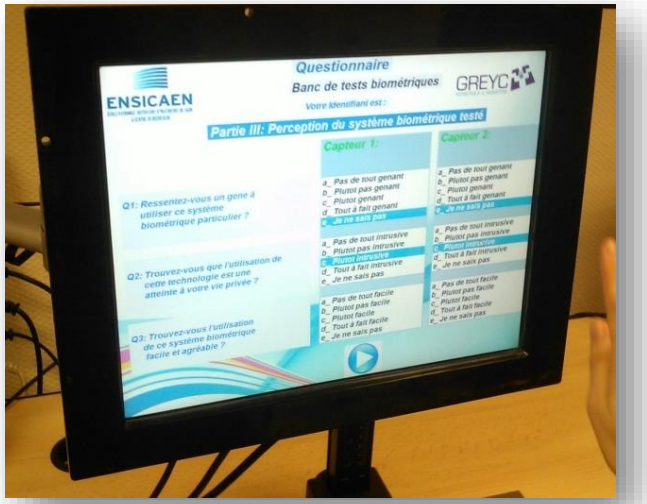
- Users who can easily imitate others

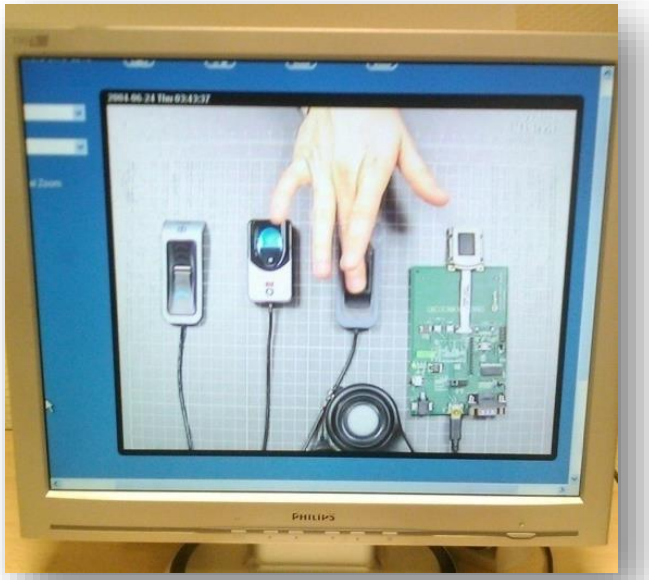
→ Illustration on keystroke dynamics

USABILITY

Interaction with humans:

- ❑ Ease of use,
- ❑ User satisfaction,
- ❑ Monitoring sensor manipulation.

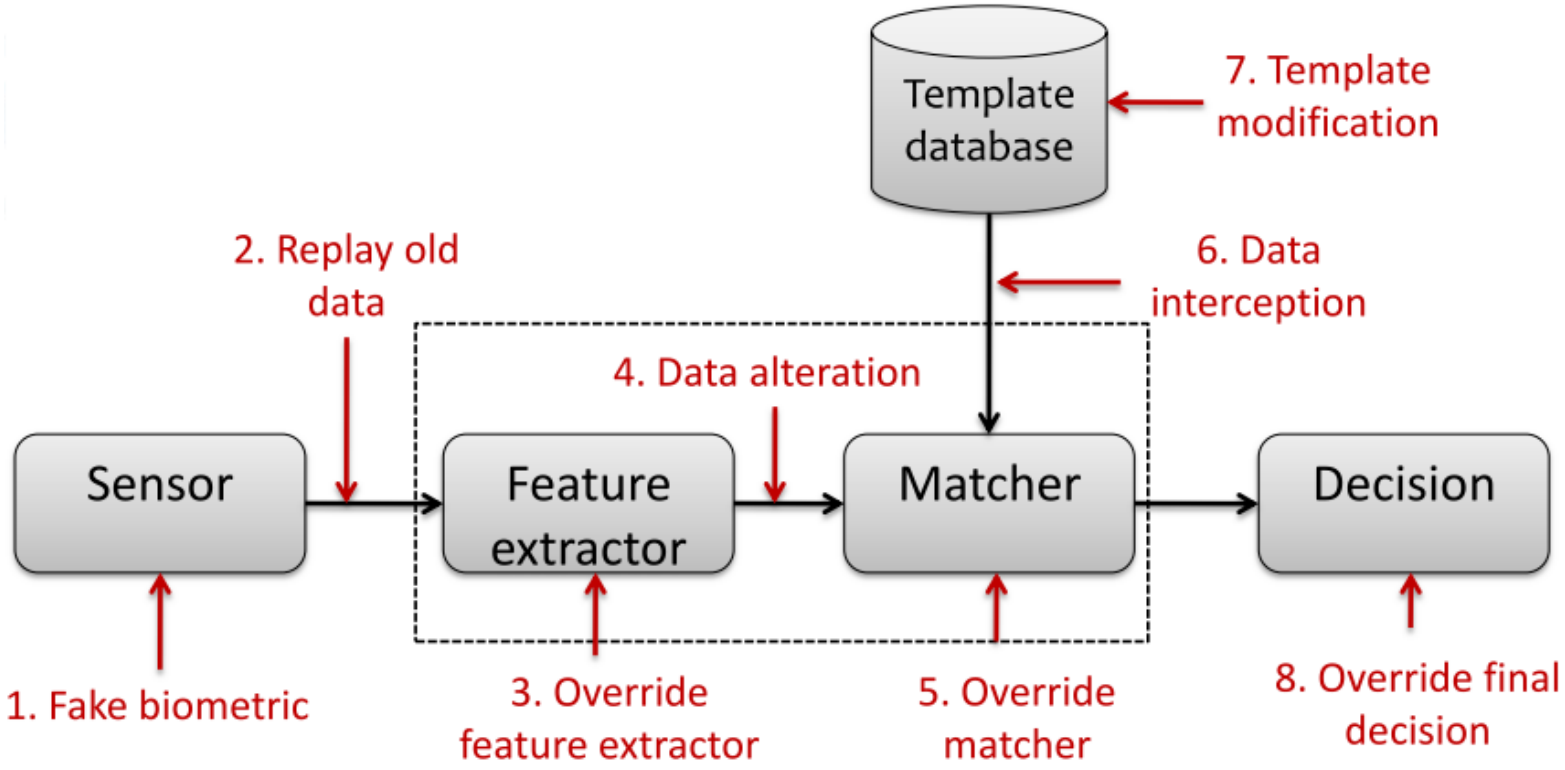




Part C. Perception of the tested system	
Q_8. Have you ever tried this biometric modality (before our study)?	☐ yes ☐ no
Q_9. were you disturbed while using this system?	☐ not at all disturbed ☐ not disturbed ☐ disturbed ☐ quite disturbed ☐ I do not know
Q_{10}. does this technology threats your privacy?	☐ not at all intrusive ☐ not intrusive ☐ intrusive ☐ quite intrusive ☐ I do not know
Q_{11}. is it easy to use this system?	☐ not at all easy ☐ not easy ☐ easy ☐ quite easy ☐ I do not know
Q_{12}. Do you find the verification fast?	☐ not at all fast ☐ not fast ☐ fast ☐ quite fast ☐ I do not know
Q_{13}. Is the answer of the biometric system is correct?	☐ never ☐ rarely ☐ sometimes ☐ always ☐ I do not know
Q_{14}. In your opinion, is the system used can be easily attacked?	☐ strongly disagree ☐ disagree ☐ agree ☐ strongly agree ☐ I do not know
Q_{15}. Are you ready to use this biometric system in the future?	☐ strongly disagree ☐ disagree ☐ agree ☐ strongly agree ☐ I do not know
Q_{16}. If you are ready to use this system in the future, would you like to use it for physical (eg. access a building) or logical (eg. log on to a computer) access?	☐ physical ☐ logical
Q_{17}. do you trust this system?	☐ no at all ☐ not really ☐ rather ☐ yes ☐ I do not know
Q_{18}. What is your general appreciation of this system?	☐ not at all satisfied ☐ not satisfied ☐ satisfied ☐ quite satisfied ☐ I do not know

SECURITY

A biometric system can he hacked !



HOME » FEATURED ARTICLES » Hackers Have Stolen Almost Six Million US Government...

Hackers Have Stolen Almost Six Million US Government Fingerprints

GRAHAM CLULEY
SEP 24, 2015 | IT SECURITY AND DATA PROTECTION

78 195 129 33

The Office of Personnel Management (OPM) has revealed in a statement that when hackers breached its systems earlier this year they made away with approximately 5.6 million fingerprints – a significant increase from the 1.1 million previously reported.

As is now well known, in addition to fingerprint data being stolen the Social Security numbers, addresses, employment history, and financial records of some 21.5 million current and former US government employees was also stolen.

The good news is that they believe the opportunities for criminals to exploit the fingerprint data is currently limited.

But the bad news is that chances are that won't continue to be the case.

[N. K. Ratha, J. H. Connell, and R. M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, p. 614-634, 2001.

PRESENTATION ATTACK

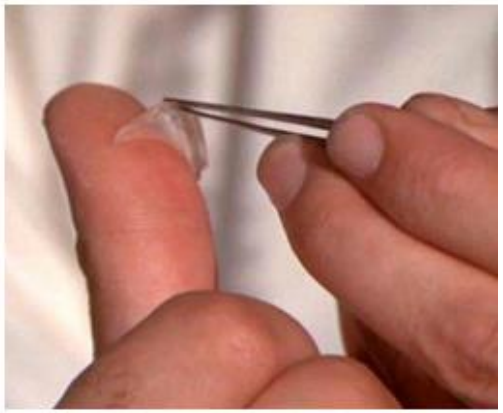
Definitions:

- **Presentation attack**
  Presentation to the biometric capture subsystem with the goal of interfering with the operation of the biometric system

- **Presentation Attack Detection (PAD)**
  Automated determination of a presentation attack

- **Impostor**
  Subversive biometric capture subject who attempts to being matched to someone else's biometric reference

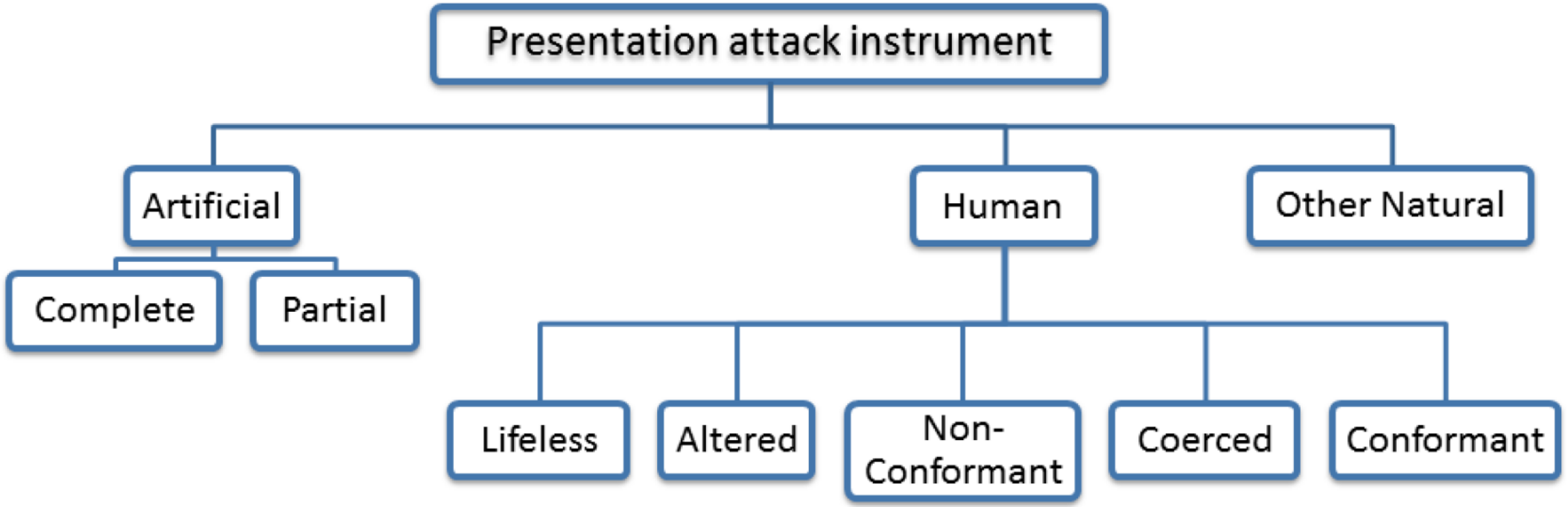
- **Identity concealer**
  Subversive biometric capture subject who attempts to avoid being matched to their own biometric reference



James Bond movie
Diamonds are forever (1971)

PRESENTATION ATTACK

Presentation attack instrument (PAI)
Biometric characteristic or object used in a presentation attack

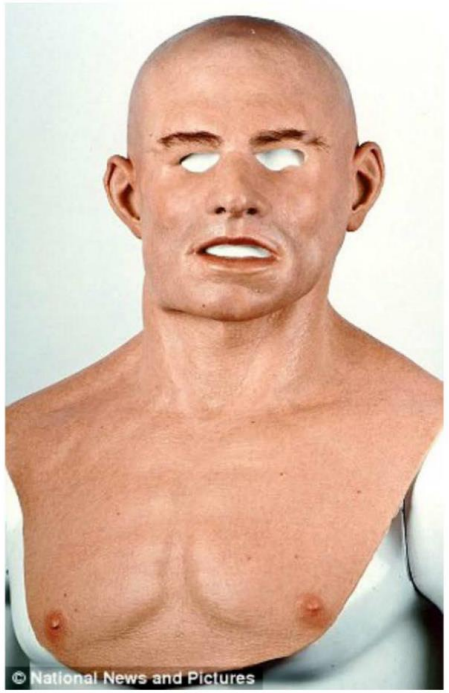


PRESENTATION ATTACK

Human PAI: makeup, latex mask, 3D spoof…

Face disguise for organized crime (June 2012)

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



The man in the latex mask: BLACK serial armed robber disguised himself as a WHITE man to rob betting shops

- **Henley Stephenson wore the disguise during a 12-year campaign of hold-ups at betting shops and other stores across London**
- **He was part of a three-man gang jailed for a total of 28 years**
- **CCTV footage showed him firing a semi-automatic pistol into the ceiling during a raid on a betting shop**
- **The mask was bought from the same London shop which supplied masks used in the £40m Graff Diamonds heist**

By ROB PREECE and REBECCA CAMBER FOR THE DAILY MAIL

PUBLISHED: 17:22 GMT, 1 June 2012 | **UPDATED:** 16:21 GMT, 2 June 2012

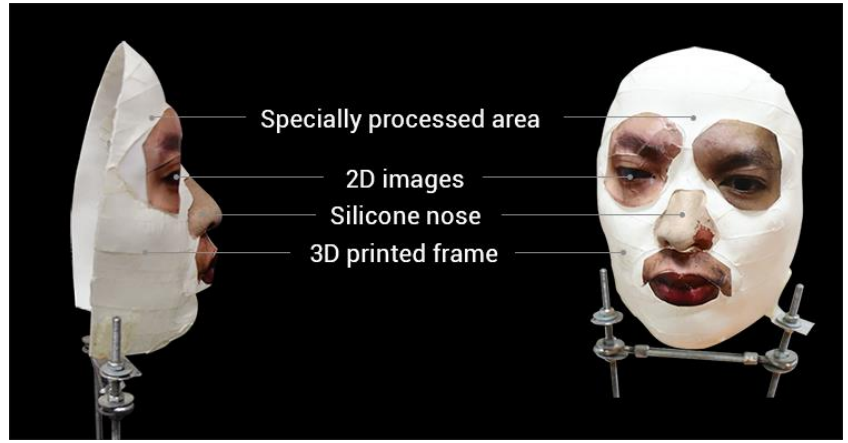
Most masked robbers opt for a balaclava to hide their identity.

Not this one. Henley Stephenson, 41, eluded police for more than ten years thanks to an extraordinarily lifelike latex mask, which turned him into a white skinhead.

Officers discovered that their man was in fact black when they finally caught up with Stephenson after a string of armed raids dating back to 1999.

Latex spoof

Lifeless spoof

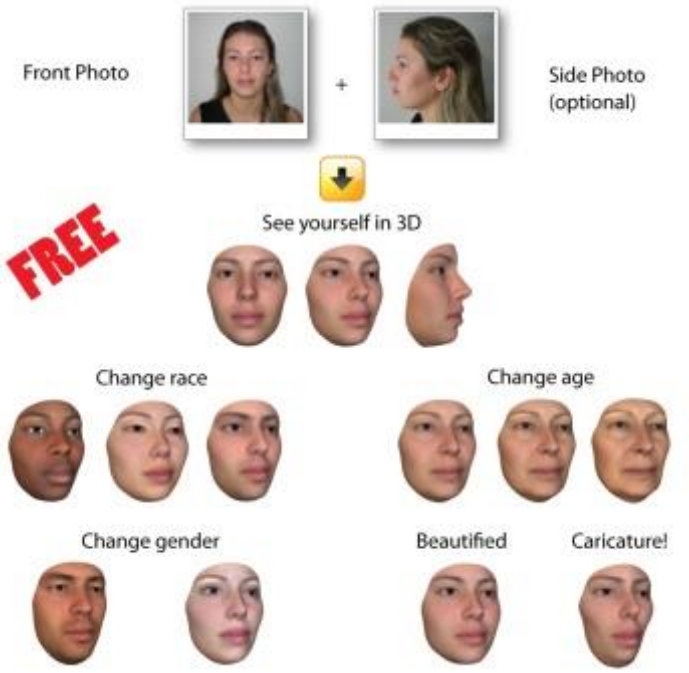


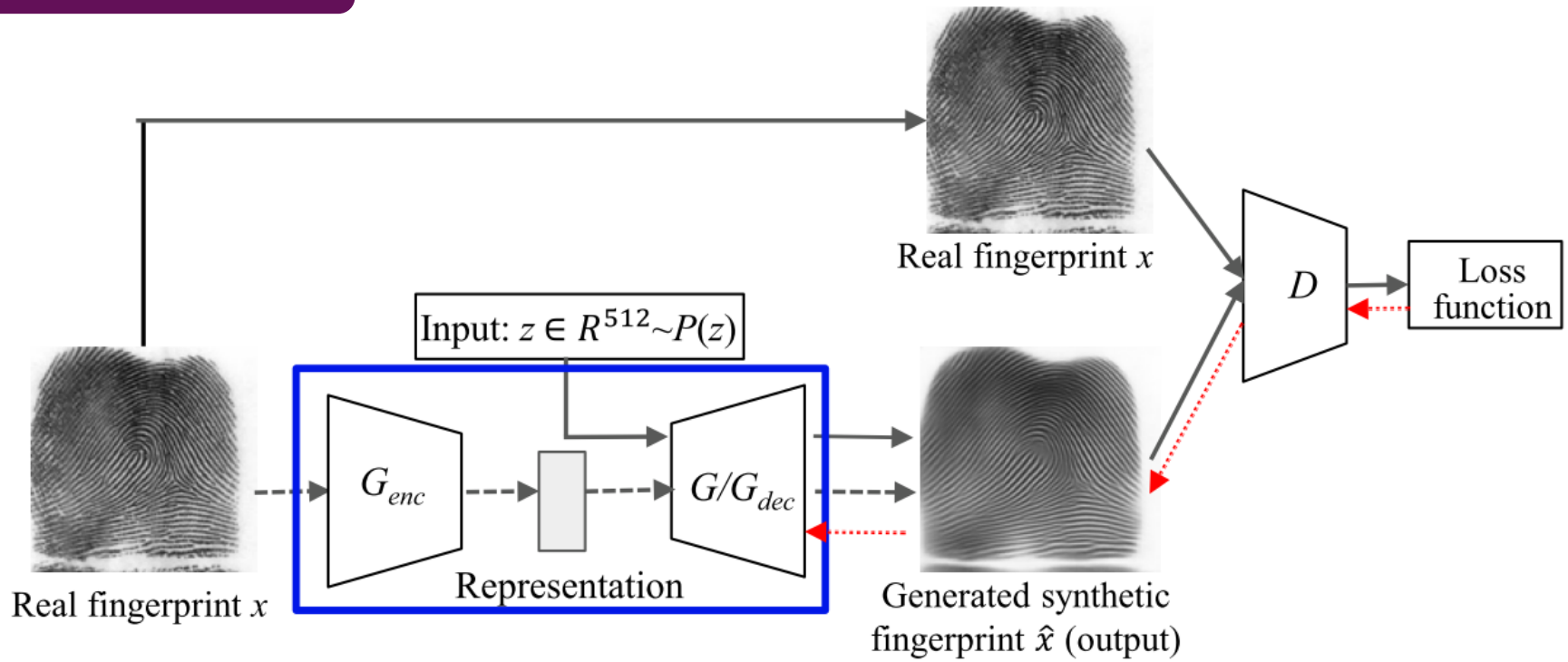
3D spoof (FaceId attack)

Makeup spoof

PRESENTATION ATTACK

Artificial PAI: 3D reconstruction, deepfake…





Generative adversarial networks (GAN)

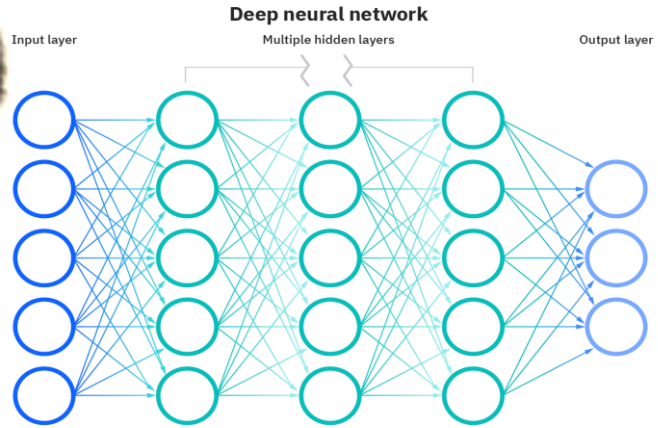
Cao, K., & Jain, A. (2018, February). Fingerprint synthesis: Evaluating fingerprint search at scale. In *2018 International Conference on Biometrics (ICB)* (pp. 31-38). IEEE.

PRESENTATION ATTACK

Artificial PAI: backdoors

Optimized perturbation (visible in this example)

Bob



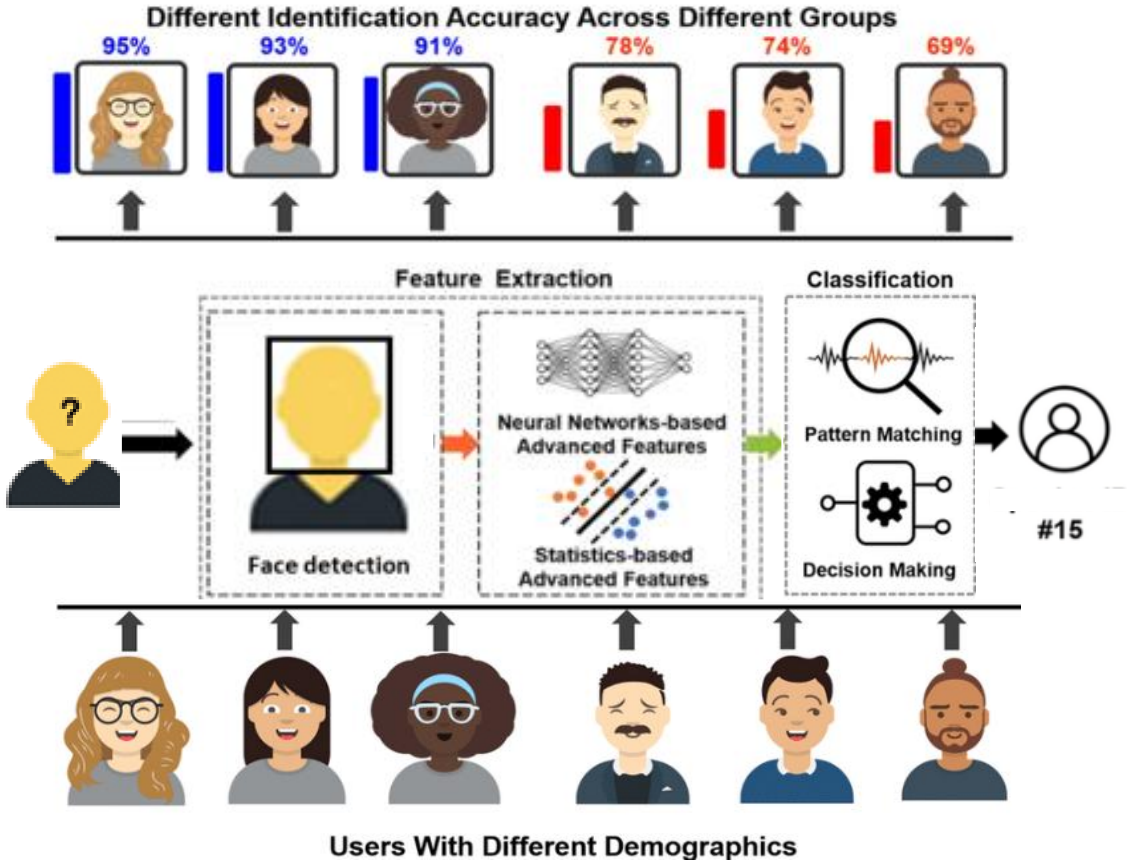
Recognized as Kevin

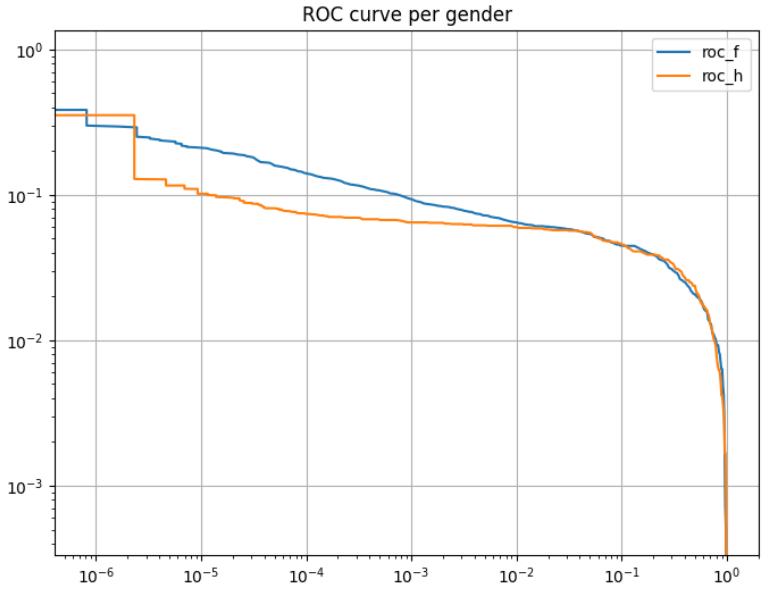
AI a key component of biometric sytems:

- ❑ Black box systems
- ❑ Source code = a (very) large list of coefficients
- ❑ Very difficult to identify non expected behaviors (backdoors).

FAIRNESS

Biases: systematic deviations that can lead to unequal performance across different user groups



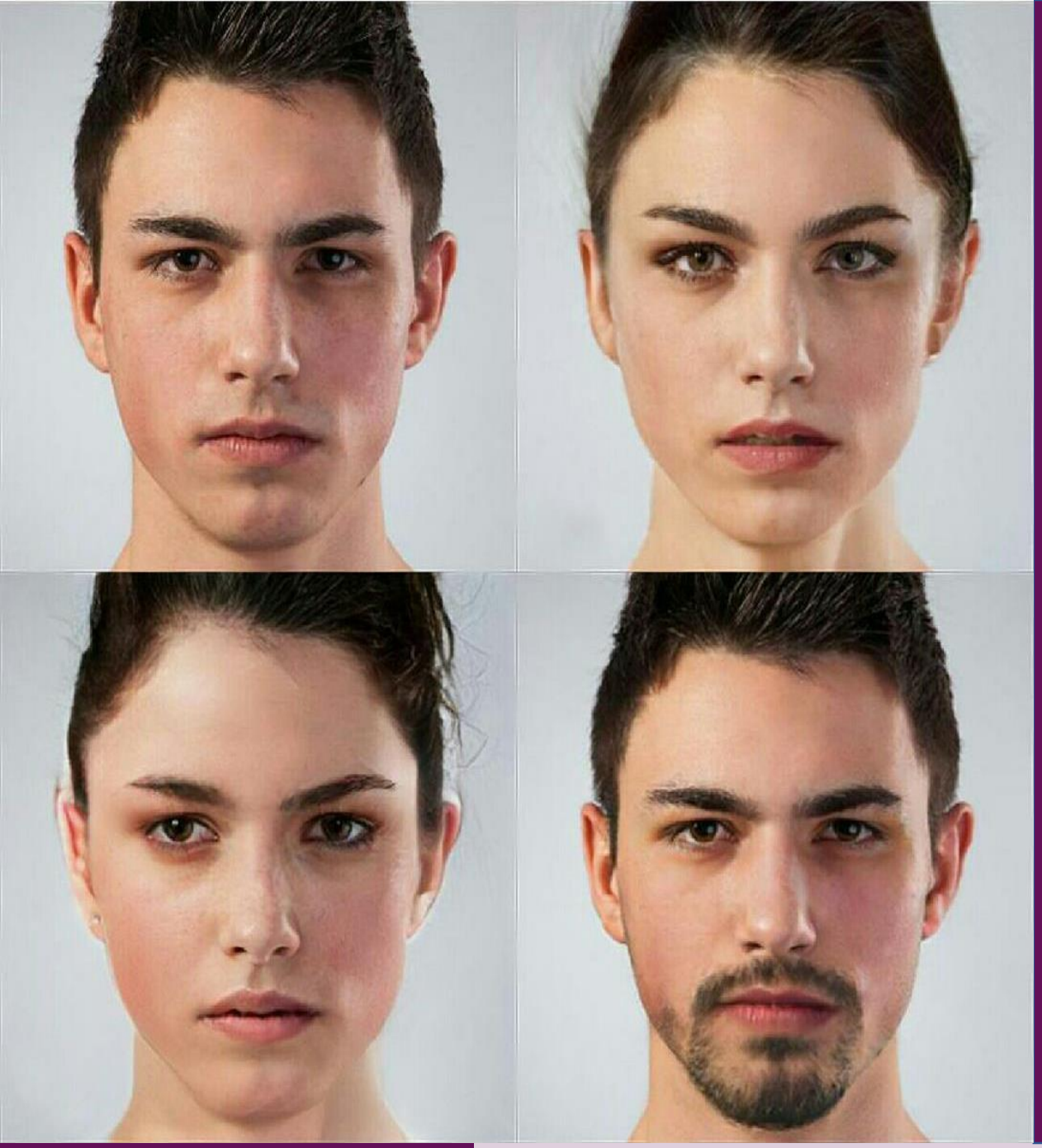


One metric: Fairness **D**iscrepancy **R**ate (FDR)

$$\text{FDR}(\theta) = 1 - (\alpha \times A(\theta) + (1 - \alpha) \times B(\theta))$$

$$A(\theta) = \max(|FMR^{di}(\theta) - FMR^{dj}(\theta)|)$$

$$B(\theta) = \max(|FNMR^{di}(\theta) - FNMR^{dj}(\theta)|)$$



Normandie Université

GREYC
Electronics and Computer Science Laboratory

SOFT BIOMETRICS

A character providing some information on an individual but lacking of uniqueness and permanence to differentiate enough two individuals”

Jain et al. 2004

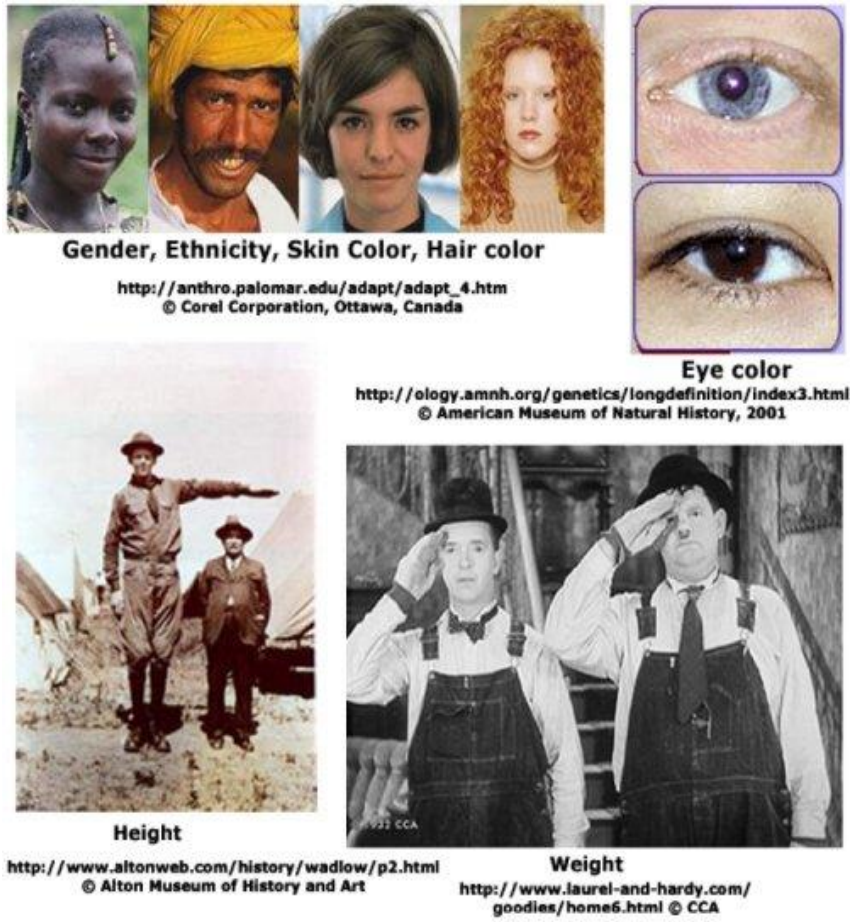
cnrs

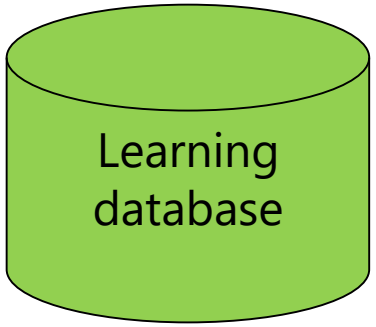
ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

UNICAEN

SOFT BIOMETRICS

Extracting soft biometric traits: machine learning





X_1=(12.3 3 153 -3.2), Y_1=Male

First step: Learning

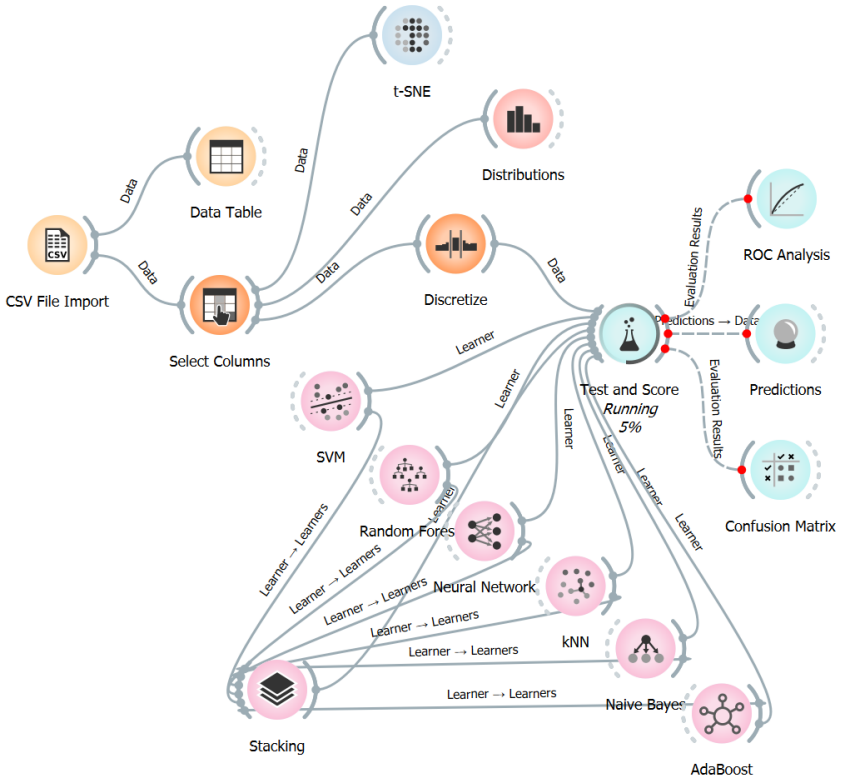
$\{(X_i, Y_i)\ i=1:N\}$ → **Learning method** SVM, neural network → *Decision function f(X)*

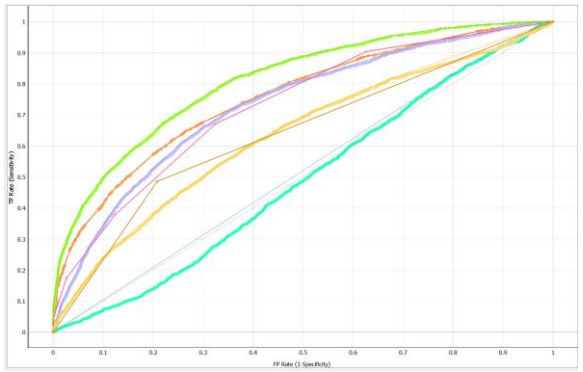
Second step: Recognition

X → **Learning method** SVM, neural network → *Decision Y=f(X)*

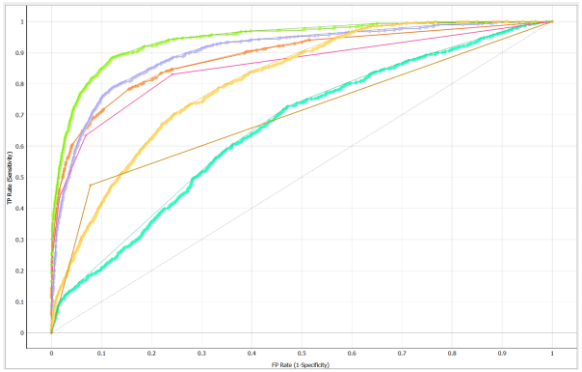
SOFT BIOMETRICS

Profiling users with keystroke dynamics:
Gender/Handedness/Age decade estimation

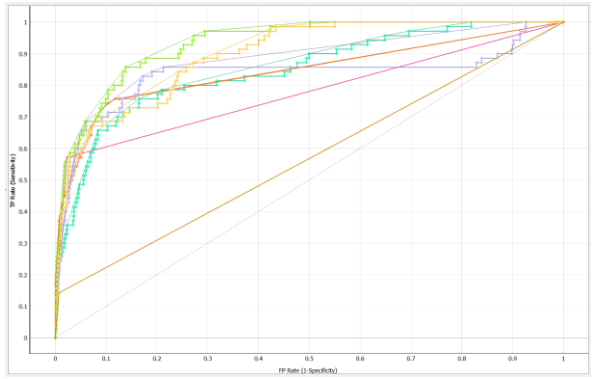




Gender (best 78%)



Handedness (best 93%)



Age decade (best 53%)

Idrus, S. Z. S., Cherrier, E., Rosenberger, C., & Bours, P. (2014). Soft biometrics for keystroke dynamics: Profiling individuals while typing passwords. *Computers & Security*, *45*, 147-155.

SOFT BIOMETRICS

Application: performance improvement
Combining decision functions considering the biometric data and the soft biometric information

X_1=(12.3 3 153 -3.2)
Biometric data

→ **Authentication score** → *Score*

X_1'=*Male*
A priori information

→ **Soft biometric method** → *Trait_confidence*
Soft_Similarity

Trait = score + (Trait_confidence)
Reward = score x (1 - Soft_Similarity)

Trait_confidence: difference between the real trait and the prediction
Soft_Similarity: percentage of similar biometric traits between the sample and the reference template

SOFT BIOMETRICS

Application: performance improvement on keystroke dynamics

Classical biometric system

biometric system (Trait_confidence)

biometric system (Soft_similarity)

Password	Baseline	Gender	Age	Handedness	All soft biometric traits	Reward
Password 1	21.45%	**18.21%**	21.67%	19.64%	19.05%	10.27%
Password 2	18.38%	17.14%	17.14%	**16.67%**	18.45%	7.45%
Password 3	19.26%	19.64%	**16.19%**	19.05%	19.05%	9.59%
Password 4	19.84%	**14.29%**	19.52%	18.45%	17.86%	7.34%
Password 5	15.56%	13.93%	14.76%	**13.10%**	14.88%	14.09%
Fusion of 5 passwords	10.63%	10.36%	10.71%	12.50%	**8.33%**	5.41%

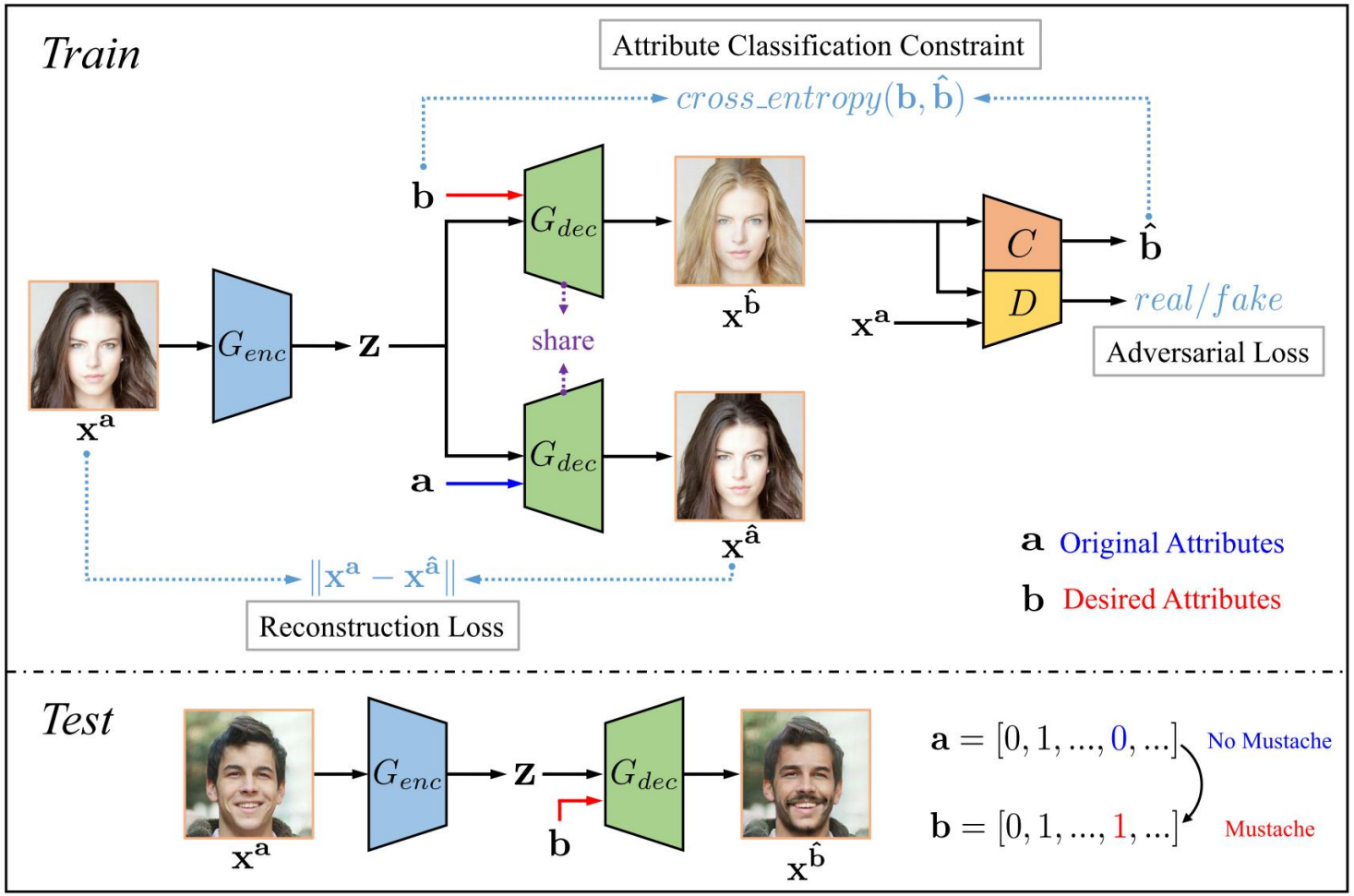
- EER value nearly divided by 2
- Processing of the same biometric data
- Taking into account a priori information

Syed Zulkarnain Syed Idrus, Estelle Cherrier, Christophe Rosenberger, Soumik Mondal and Patrick Bours (2014), “Keystroke Dynamics Performance Enhancement With Soft Biometrics”. The IEEE International Conference on Identity, Security and Behavior Analysis (ISBA 2015) Hong Kong.

SOFT BIOMETRICS

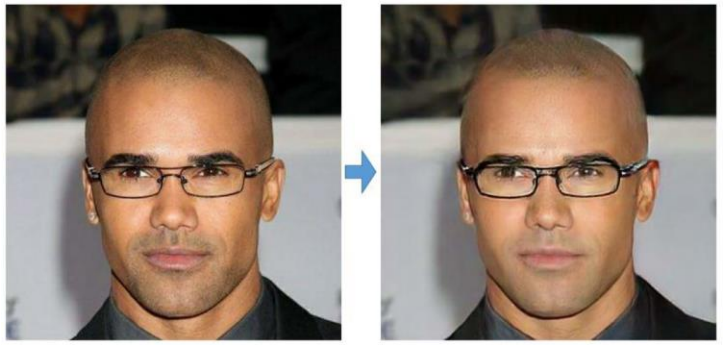
Limitations:

- Generative AI can artificially modify soft biometric information
- Example of AttGan

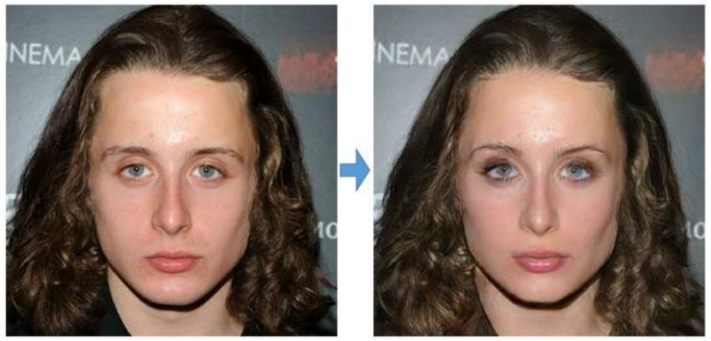


He, Zhenliang, et al. "Attgan: Facial attribute editing by only changing what you want." *IEEE Transactions on Image Processing* 28.11 (2019): 5464-5478.

SOFT BIOMETRICS



Remove beard



Gender swap

Hair color swap

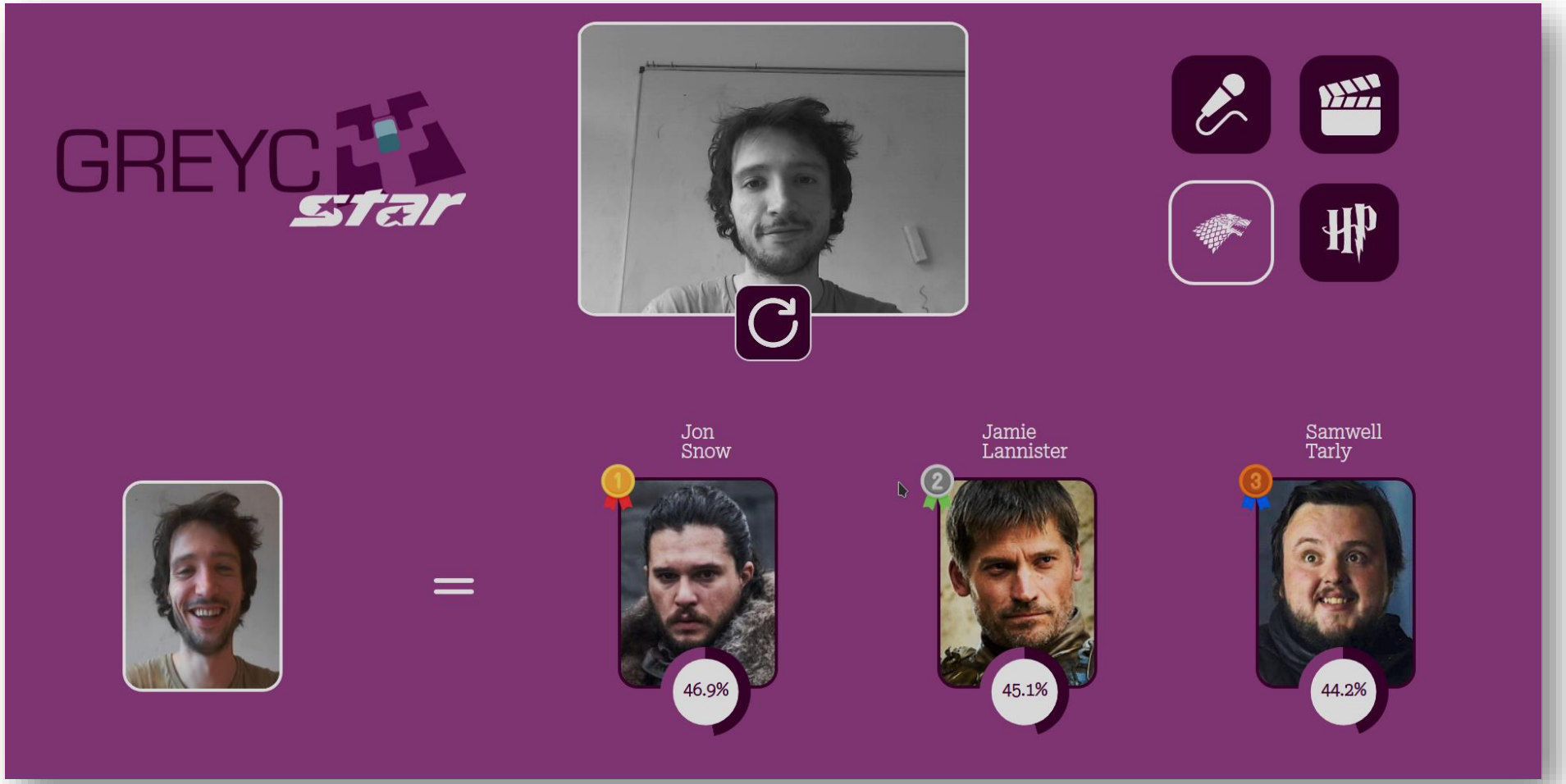
To Bushy Eyebrows + Mouth Close

Add Eyeglasses

Hairdressing change

He, Zhenliang, et al. "Attgan: Facial attribute editing by only changing what you want." *IEEE Transactions on Image Processing* 28.11 (2019): 5464-5478.

SOFT BIOMETRICS



Normandie Université

GREYC
Electronics and Computer Science Laboratory

TEMPLATE AGING

"Biometric template aging is defined as an increase in recognition error rate with increased time since enrollment"

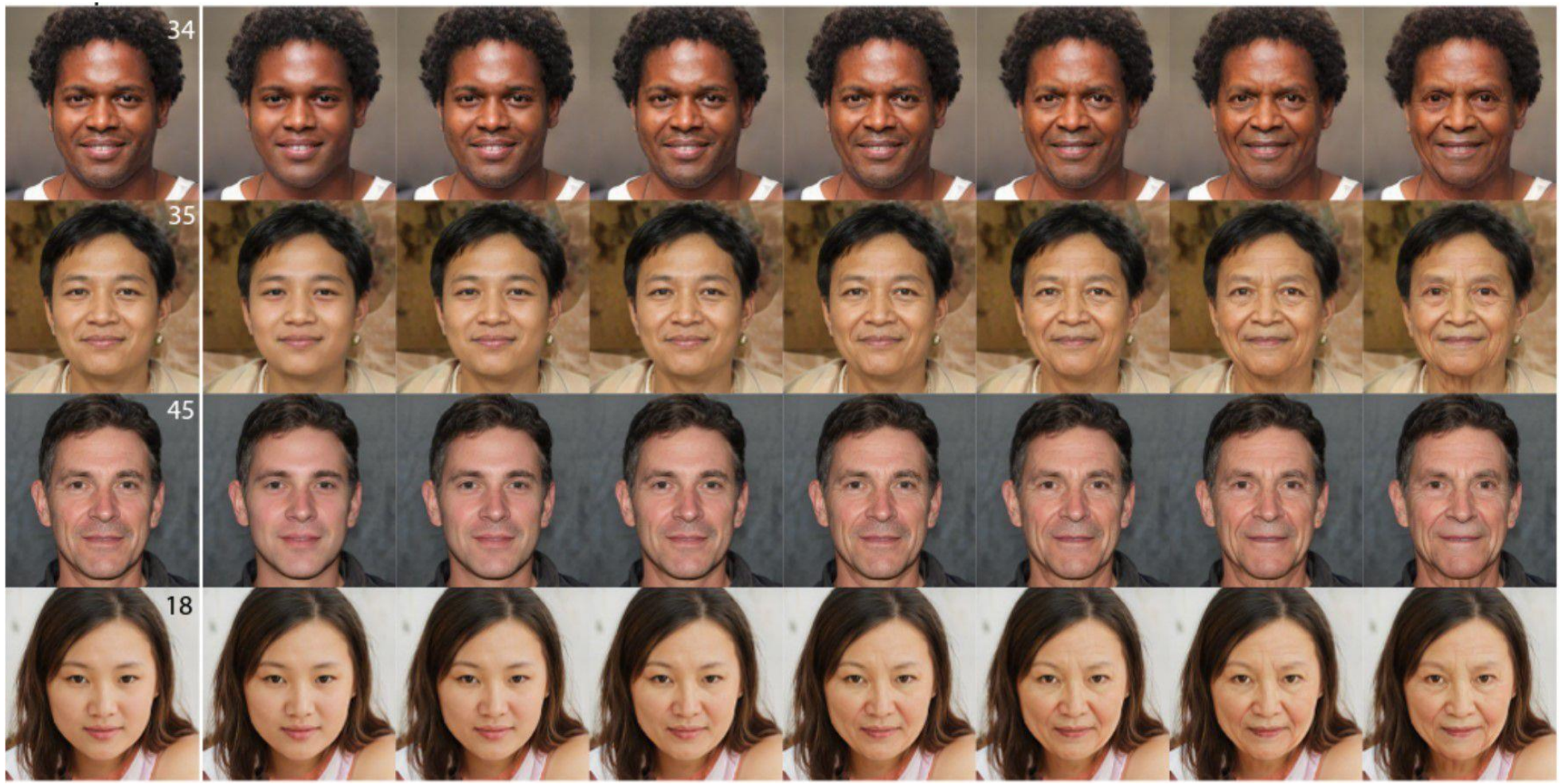
Fendker et al. 2013

cnrs

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

UNICAEN

TEMPLATE AGING



FRAN (face re-aging network) is a neural network that's been trained using thousands of images of synthetic human faces, projecting how an actor's face could look on camera at different stages of life. (source Disney)

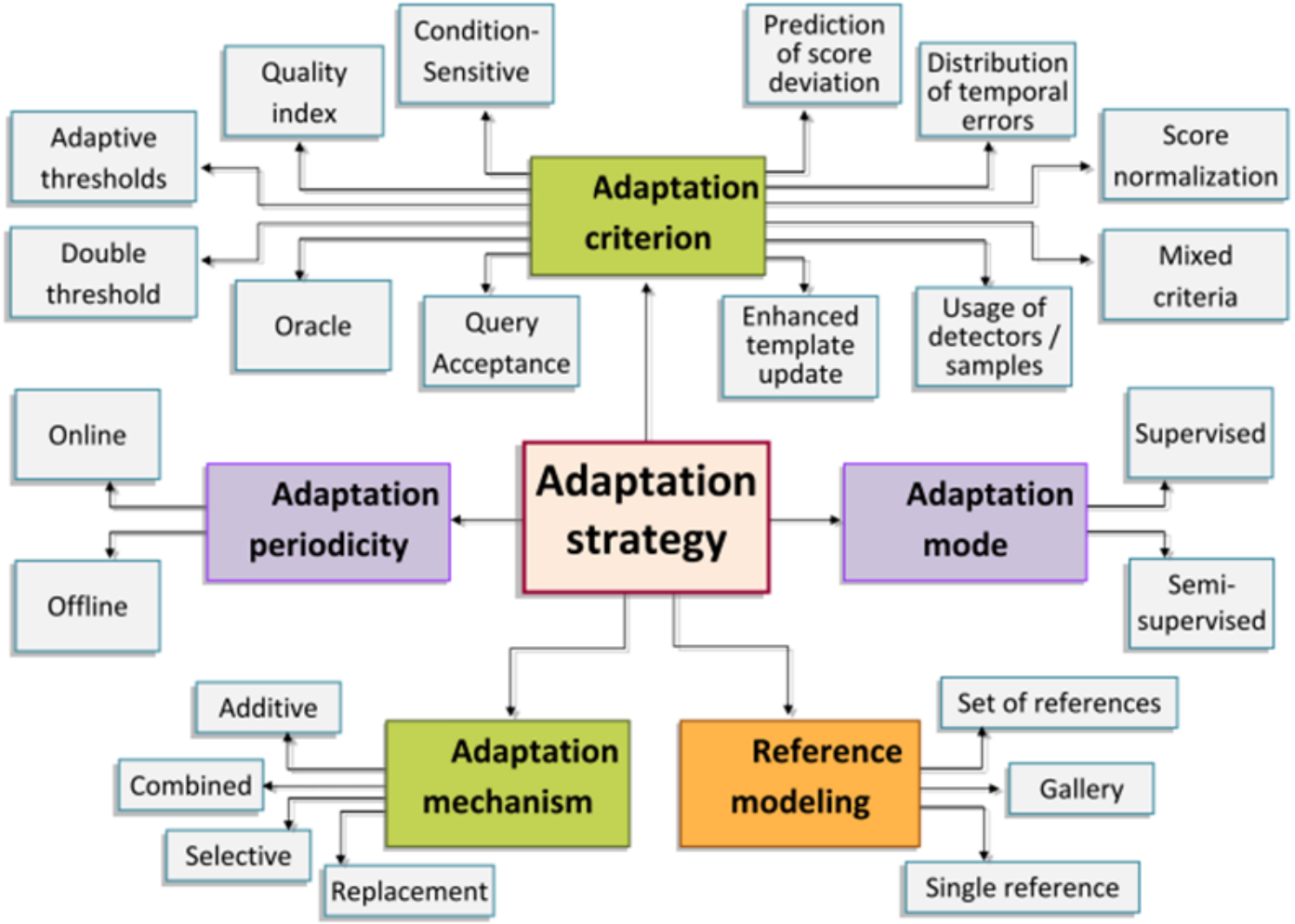
TEMPLATE AGING

Natual evolution of biometric templates:

- ❑ User aging (face…)
- ❑ Behaviors evolution (signature dynamics…),
- ❑ Data alterations (scratchs on a fingerprint…)

Many mechanisms for adaption strategy of biometric systems:

To be combined



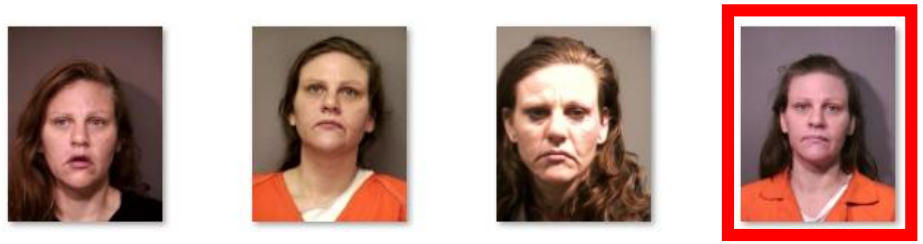
Pisani, P. H., Mhenni, A., Giot, R., Cherrier, E., Poh, N., Ferreira de Carvalho, A. C. P. D. L., ... & Amara, N. E. B. (2019). Adaptive biometric systems: Review and perspectives. *ACM Computing Surveys (CSUR)*, *52*(5), 1-38.

TEMPLATE AGING

Adaption mechanism: sliding and growing

Enrolment

Growing window: adding the new sample to the gallery



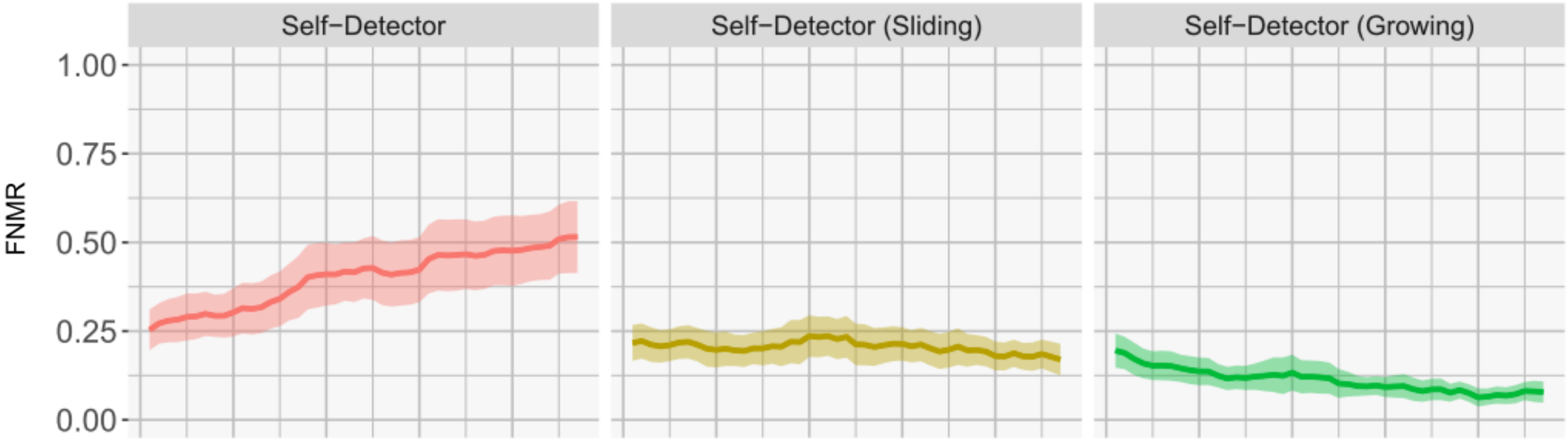
Sliding window: replacing the oldest sample in the gallery

Update the reference template:

- ❑ Generally composed of a gallery,
- ❑ Evolution of the gallery when using the biometric system,
- ❑ Matching score calculated from each sample in the gallery.

TEMPLATE AGING

Adaption mechanism: performance evaluation on keystroke dynamics

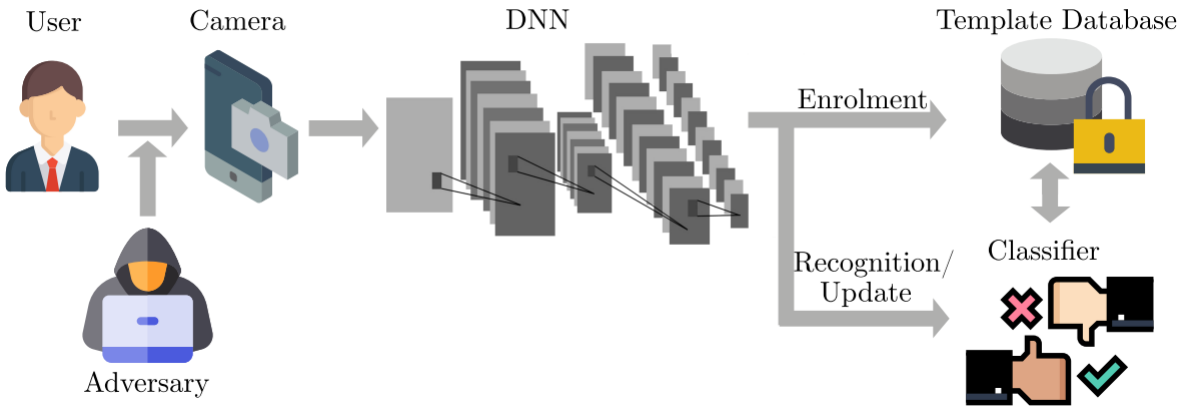


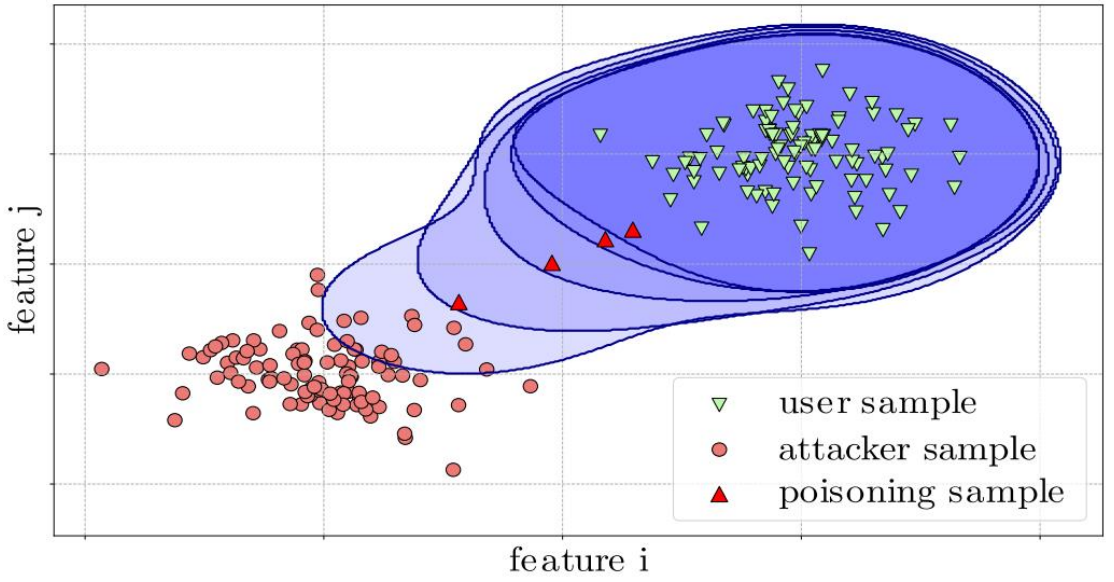
FNMR over time comparing non-adaptive and adaptive biometric systems (CMU dataset – keystroke dynamics). Self-Detector represents non-adaptive biometric systems. The versions on the right (Growing, Sliding) represent the adaptation strategies.

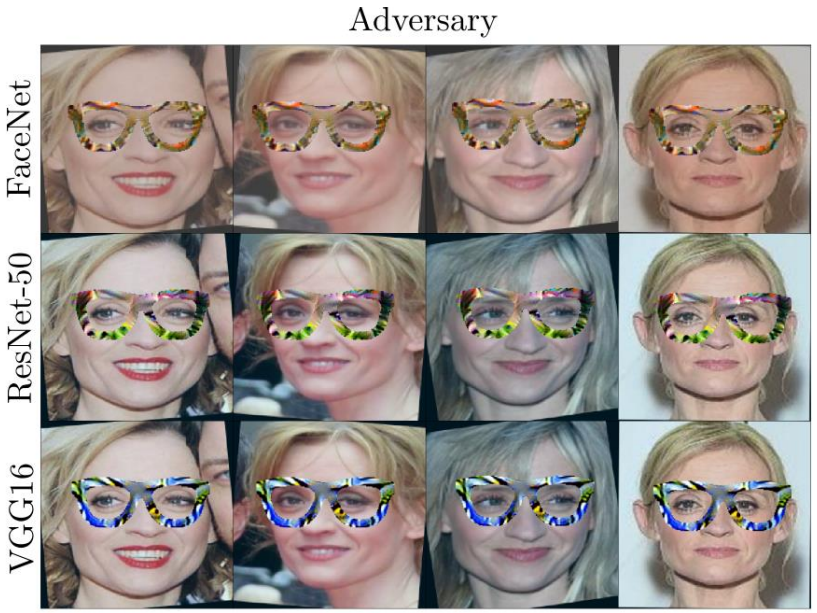
→ Poisoning effect (adding the template of an imposter in the reference template)

TEMPLATE AGING

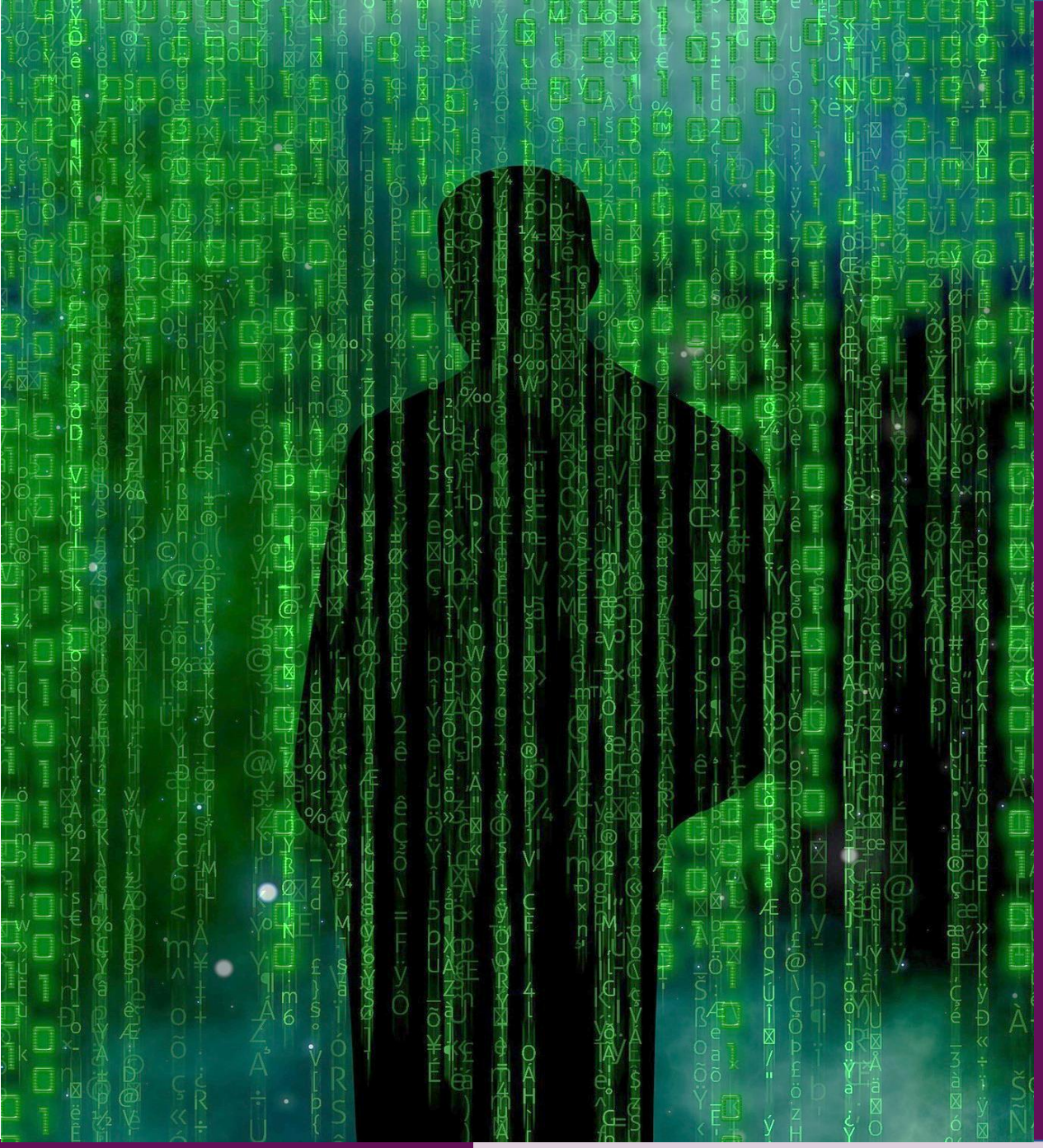
Poisoning attack: corrupting user's face template during update







Lovisotto, G., Eberz, S., & Martinovic, I. (2020, September). Biometric backdoors: A poisoning attack against unsupervised template updating. In *2020 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 184-197).



Normandie Université

GREYC
Electronics and Computer Science Laboratory

PRIVACY PROTECTION

Can we consider privacy constraints for user biometric authentication?

cnrs

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

UNICAEN

PRIVACY PROTECTION

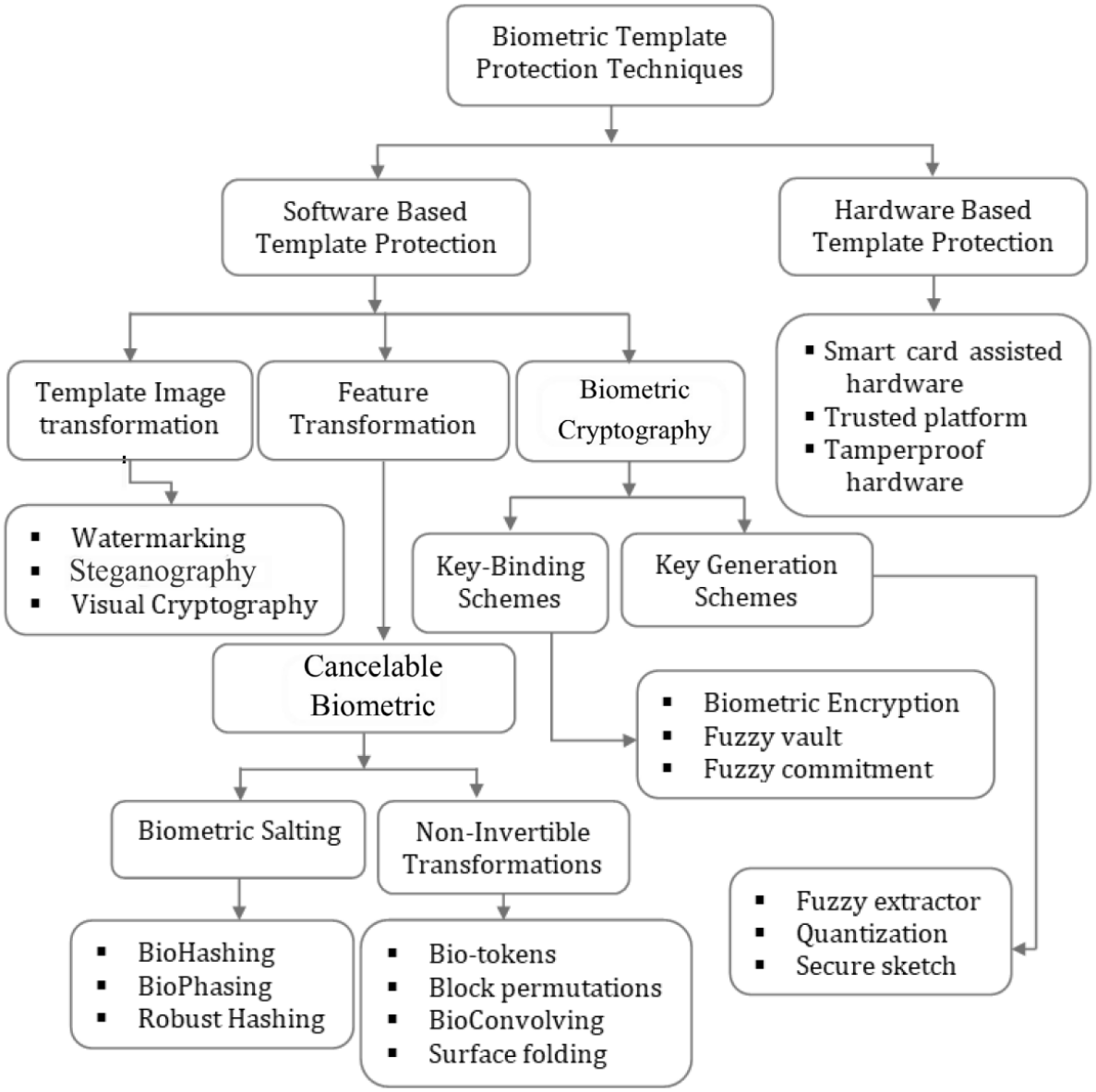
Privacy protection:

- ❑ Personal data
- ❑ Difficult to revoke a biometric data
- ❑ Can be captured without any consent
- ❑ (Classical) encryption is not sufficient

PRIVACY PROTECTION

Biometric template protection:
Privacy Enhancing Technology (PET)

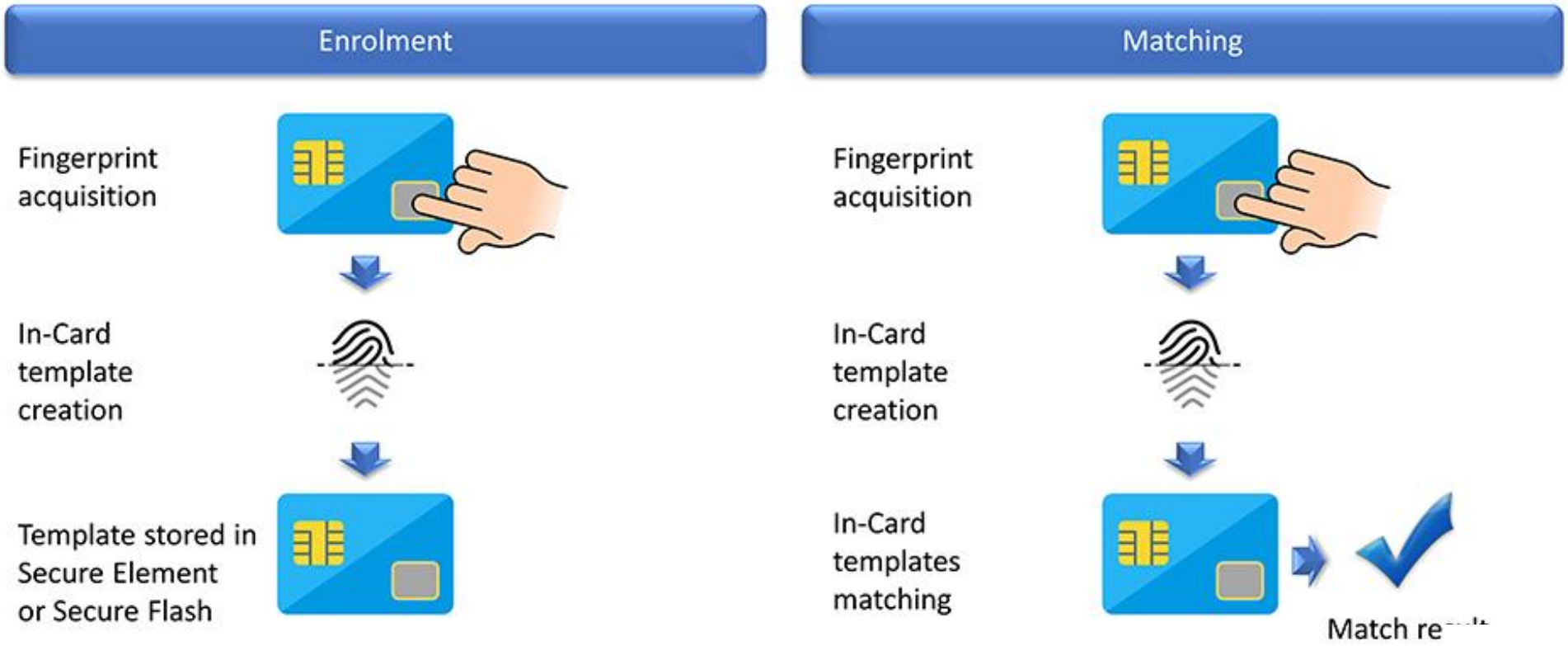
Taxonomy of existing approaches
- ❑ Hardware solutions
- ❑ Software template protection



PRIVACY PROTECTION

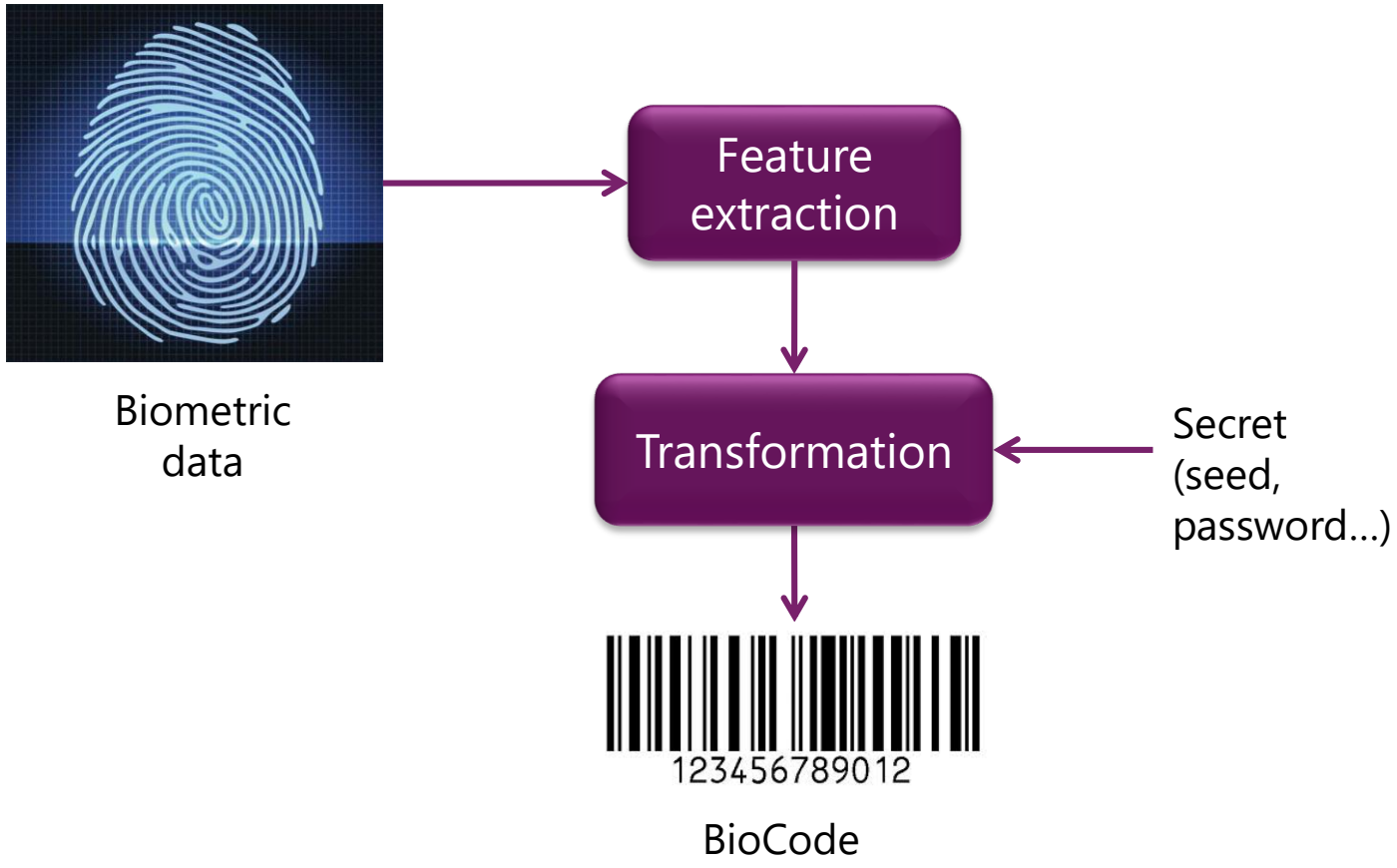
Hardware protection:

- ❑ Storage of the reference template
- ❑ Capture/match on card



PRIVACY PROTECTION

Cancelable biometrics:



Expected properties:

- **Verifiability**: it is possible to authenticate an user given a BioCode
- **Revocability**: it is possible to renew the BioCode in case of attack
- **Non invertibility or irreversability**: impossible to recover the raw biometric data given the BioCode and the Secret
- **Undistinguishability:** impossible to distinguish impostor BioCodes from legitimate ones with different Secrets
- **Unlikability**: no information leakage from different legitimate Biocodes

PRIVACY PROTECTION

BioHashing algorithm:

Random Seed (secret)

$$\begin{bmatrix} P_{1,1} & \cdots & P_{1,m} \\ \vdots & & \\ P_{n,1} & \cdots & P_{n,m} \end{bmatrix}$$

Gram-Schmidt orthogonalization

$$\begin{bmatrix} V_{1,1} & \cdots & V_{1,m} \\ \vdots & & \vdots \\ V_{n,1} & \cdots & V_{n,m} \end{bmatrix}$$

Projection matrix

$[T_1 \cdots T_n]$

Feature computation

x

$[x_1 \ldots x_m]$

Quantization

$[B_1 \ldots B_m], B_i \in \{0,1\}$

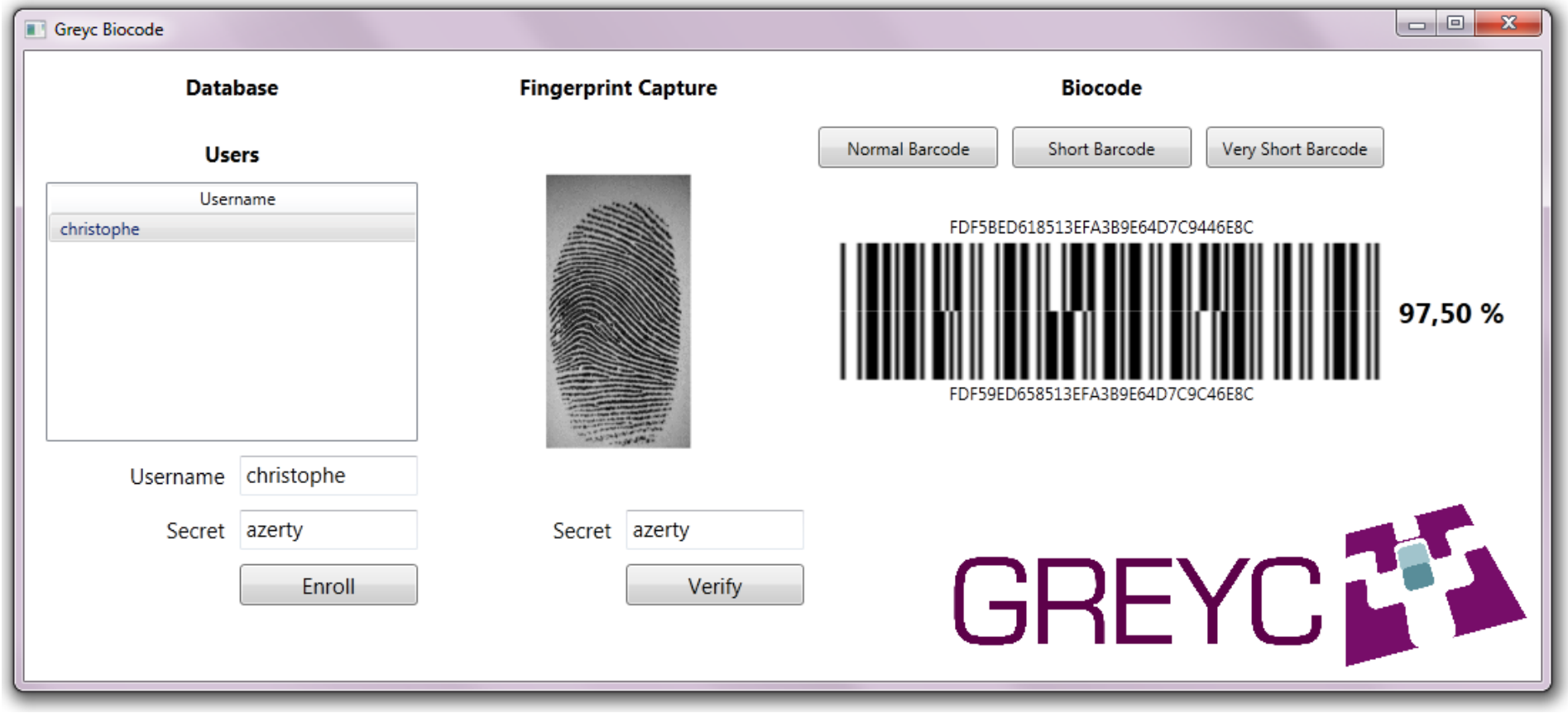
Biometric data

$n \gg m$

Jin, Andrew Teoh Beng, David Ngo Chek Ling, and Alwyn Goh. "Biohashing: two factor authentication featuring fingerprint data and tokenised random number." *Pattern recognition* 37.11 (2004): 2245-2255.

PRIVACY PROTECTION

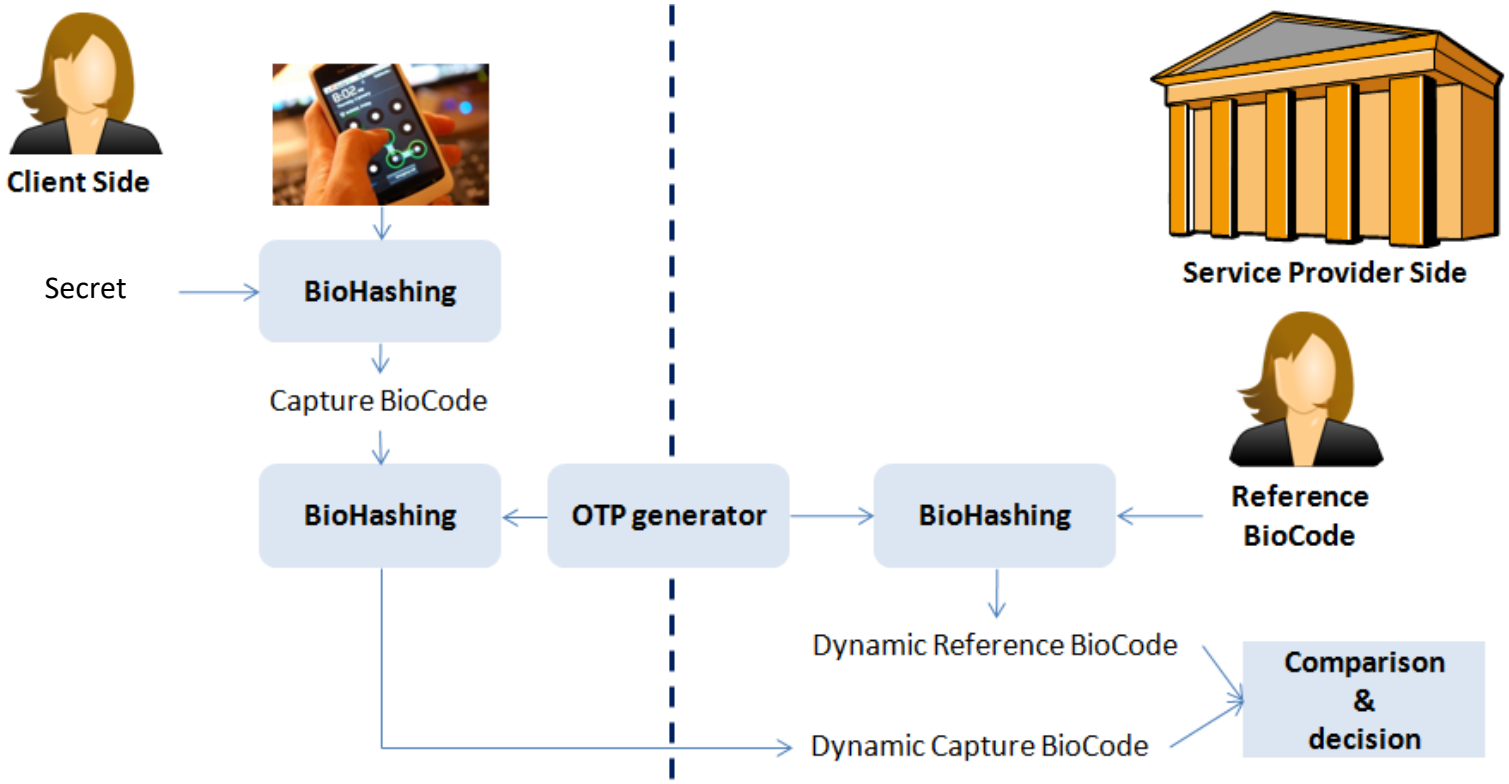
Demo

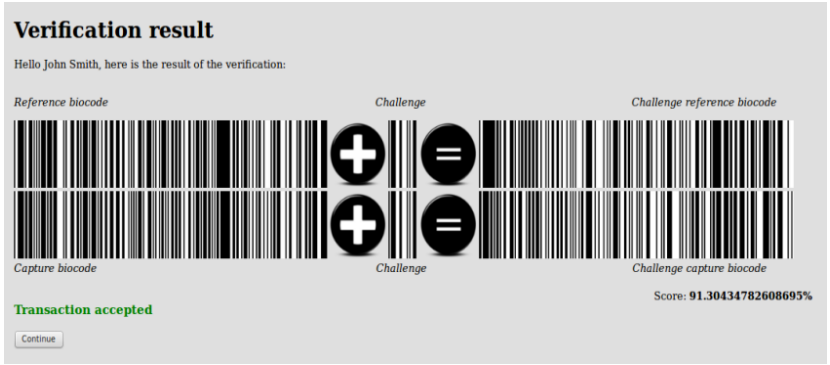


R. Belguechi, E. Cherrier, C. Rosenberger, S. Ait-Aoudia, "Operational Bio-Hash to Preserve Privacy of Fingerprint Minutiae Templates", IET journal on Biometrics, 2013

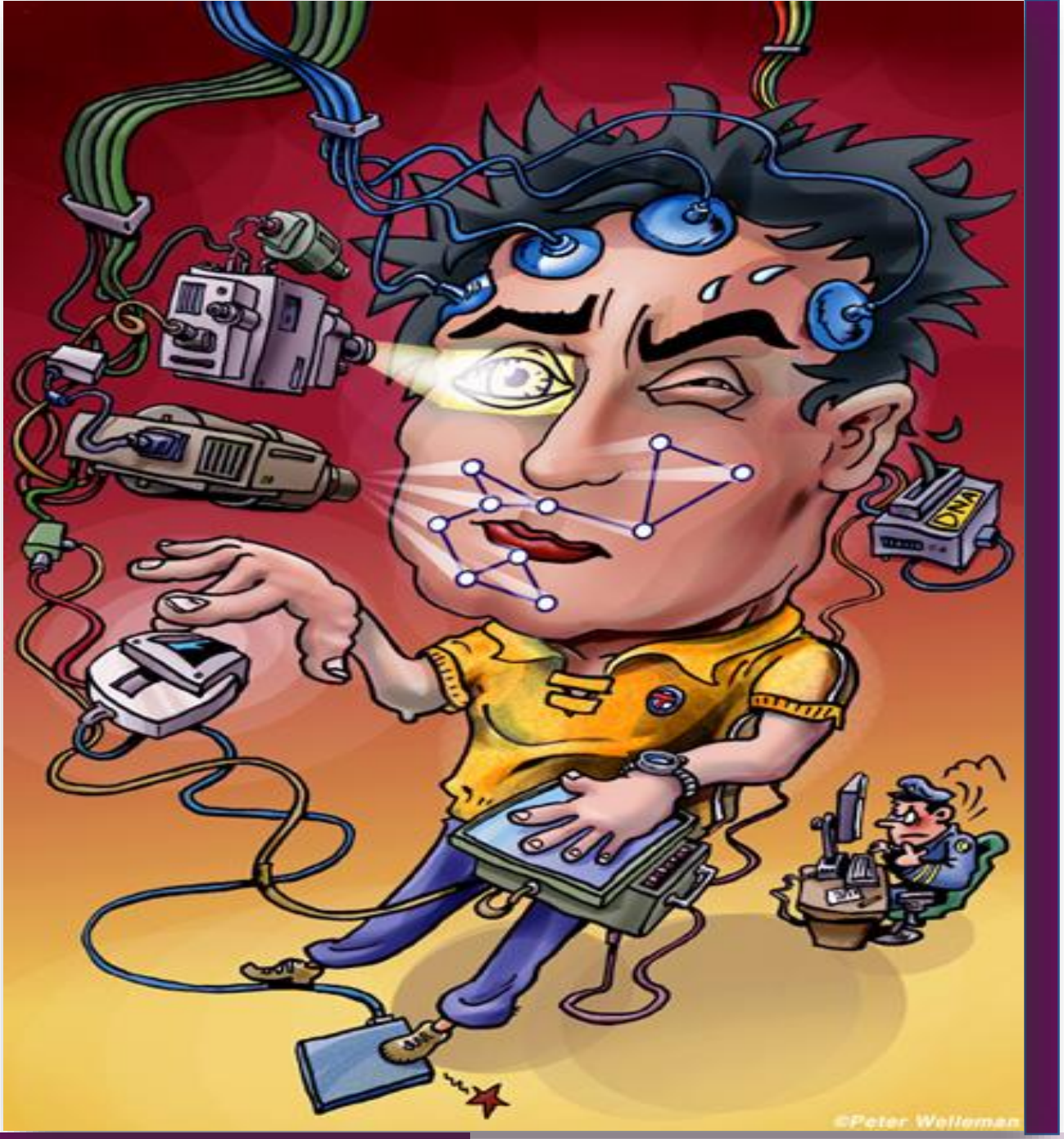
PRIVACY PROTECTION

Cryptographic protocols: an example (avoiding the replay attack)





P. Lacharme et C. Rosenberger, "Synchronous One Time Biometrics With Pattern Based Authentication", International Conference on Availability, Reliability and Security (ARES), 2016.



Normandie Université

GREYC
Electronics and Computer Science Laboratory

OPEN QUESTIONS

Which are the hot topics (for me)?

cnrs

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

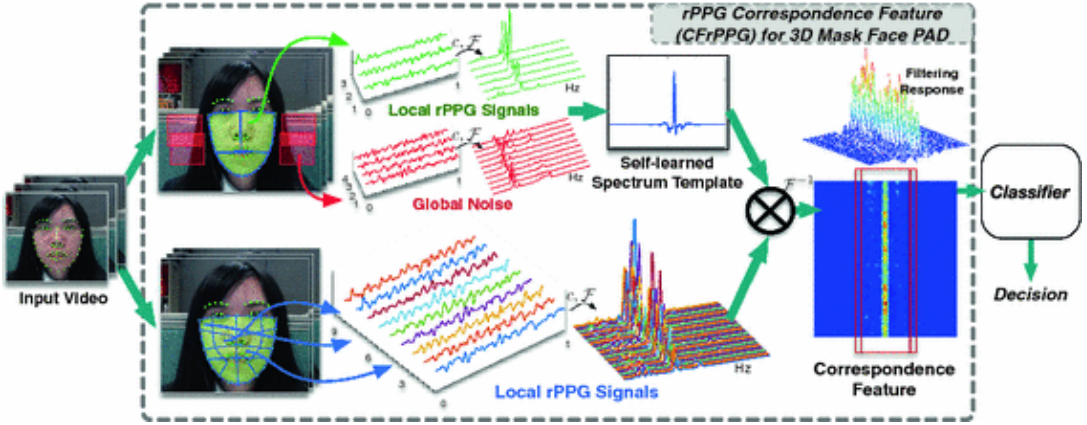
UNICAEN

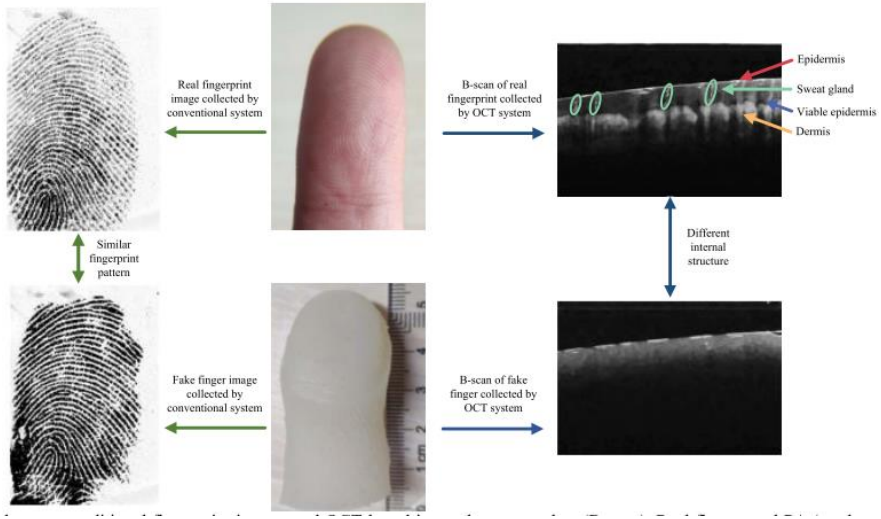
OPEN QUESTIONS

New sensors: more rich information

- **rPPG (Photoplethysmography):** blood pulse flow by modeling the skin color variations caused by the heartbeat

Liu, SQ., Lan, X., Yuen, P.C. (2018). Remote Photoplethysmography Correspondence Feature for 3D Mask Face Presentation Attack Detection. In: Ferrari, V., Hebert, M., Sminchisescu, ECCV 2018, vol 11220. Springer





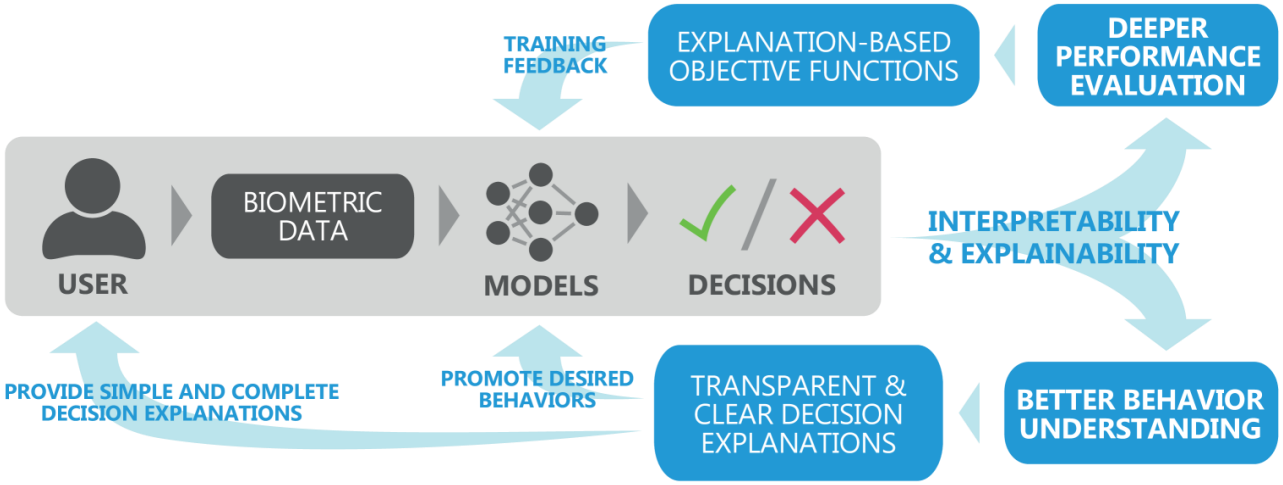
- **Optical coherence tomography (OCT):** obtain finger subcutaneous tissue information (very useful for PAD detection)

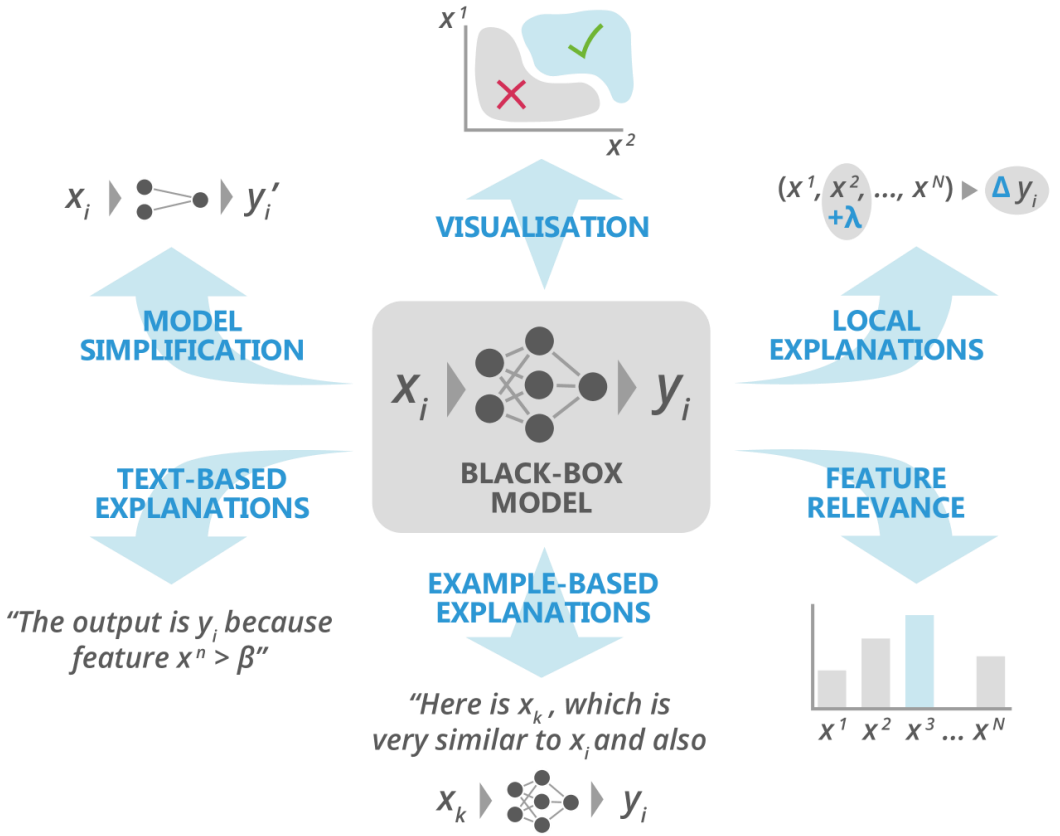
Sun, H., Zhang, Y., Chen, P., Wang, H., & Liang, R. (2023). Internal structure attention network for fingerprint presentation attack detection from Optical Coherence Tomography. IEEE Transactions on Biometrics, Behavior, and Identity Science.

OPEN QUESTIONS

XAI for biometrics:
AI a key component of biometric systems

- ❑ How to explain or increase the confidence of a decision?
- ❑ Providing feedbacks (biases, improvements…)



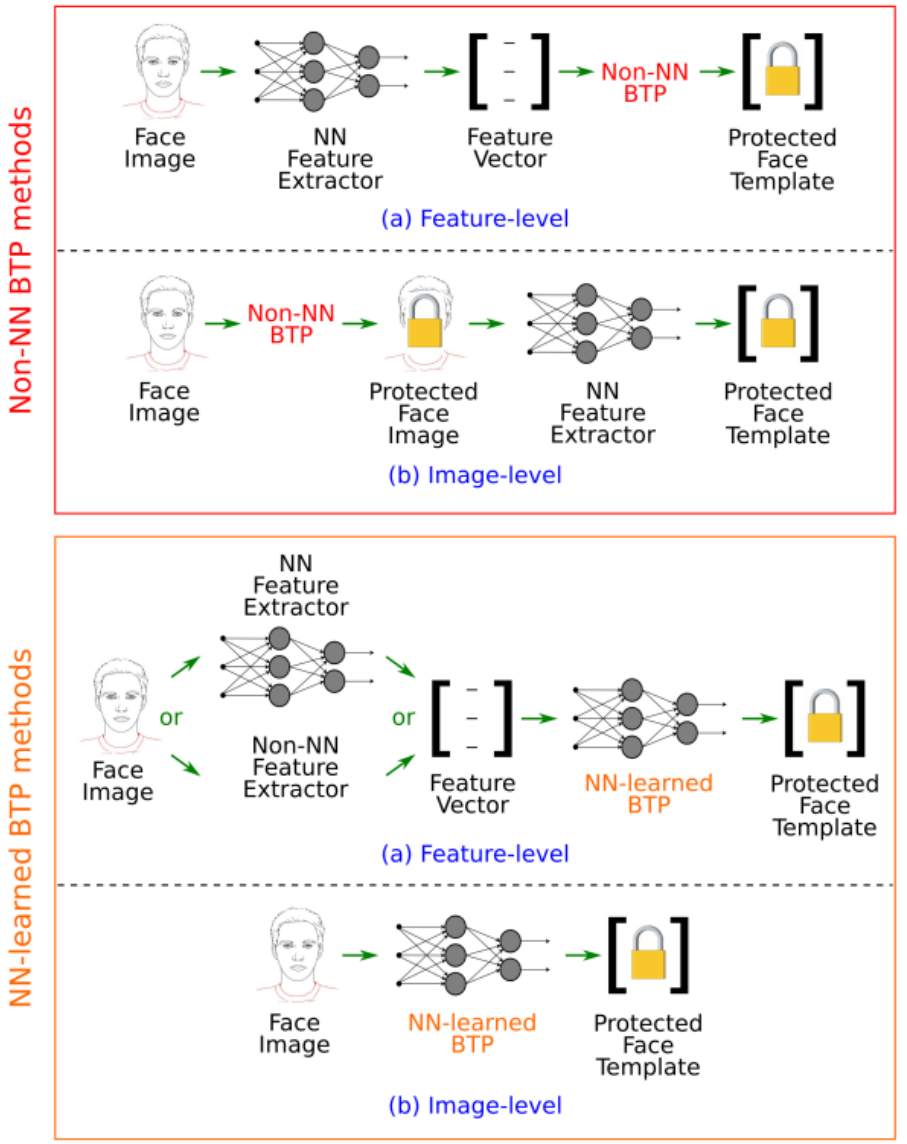


Neto, P. C., Gonçalves, T., Pinto, J. R., Silva, W., Sequeira, A. F., Ross, A., & Cardoso, J. S. (2022). Explainable biometrics in the age of deep learning. *arXiv preprint arXiv:2208.09500*.

OPEN QUESTIONS

PET in biometrics:

- ❑ Feature generation more efficient with AI
- ❑ These methods are reversible (possible to recover the input image given the feature).
- ❑ Recent approaches propose privacy compliant features
  - ✓ Which performance?
  - ✓ Which privacy properties (irreversibility, unlinkability)?

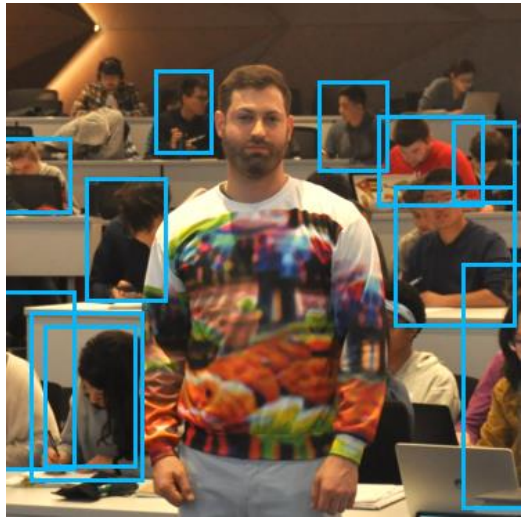


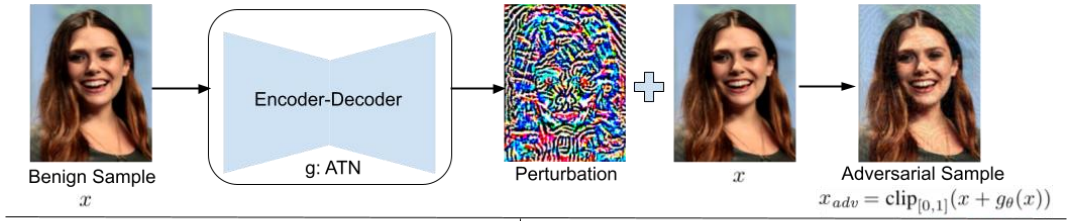
Hahn, V. K. and Marcel, S. (2021). Biometric template protection for neural-network-based face recognition systems: A survey of methods and evaluation techniques. arXiv preprint arXiv:2110.05044

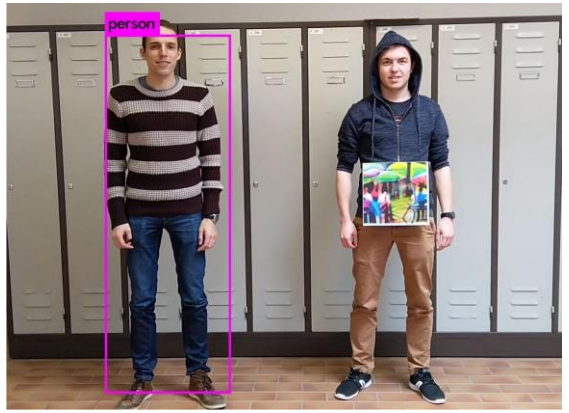
OPEN QUESTIONS

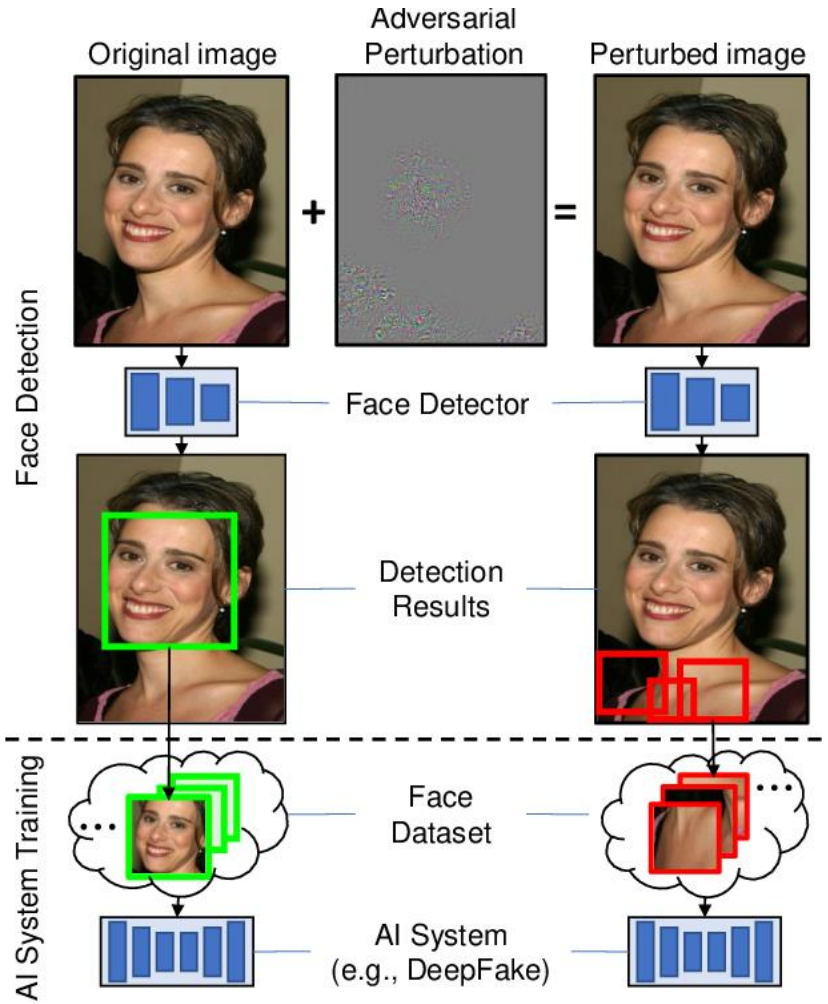
AI security and impacts on biometrics:

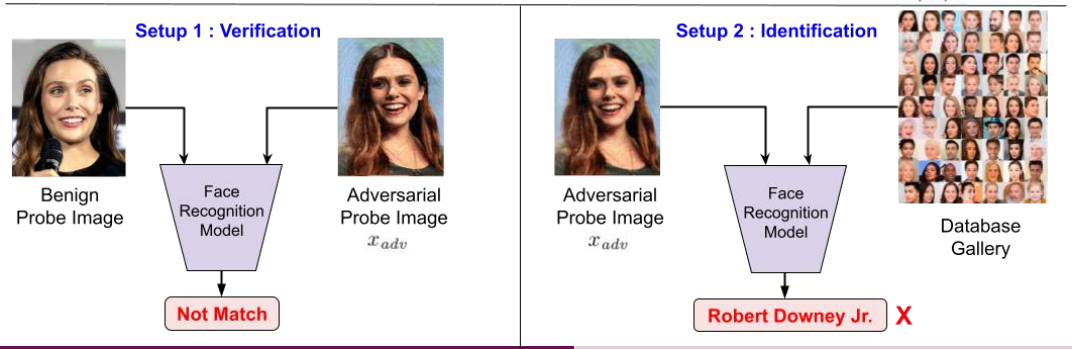
- ❑ How to detect backdoors?
- ❑ How to detect generated content?
- ❑ How to detect adversarial attacks?











GREYC
Electronics and Computer Science Laboratory

cnrs ENSI CAEN ÉCOLE PUBLIQUE D'INGÉNIEURS CENTRE DE RECHERCHE UNICAEN Normandie Université

CONTACT

Christophe ROSENBERGER

Christophe.rosenberger@ensicaen.fr

GREYC
Laboratoire de recherche en sciences du numérique

GREYC research lab - UMR CNRS 6072