BIOMETRICS UNDER ATTACKS

Christophe Rosenberger

ENSICAEN – GREYC
FRANCE

Christophe.rosenberger@ensicaen.fr

SECRYPT 2026

23rd International Conference on Security and Cryptography

GREYC
Electronics and Computer Science Laboratory

Normandie Université

UNICAEN

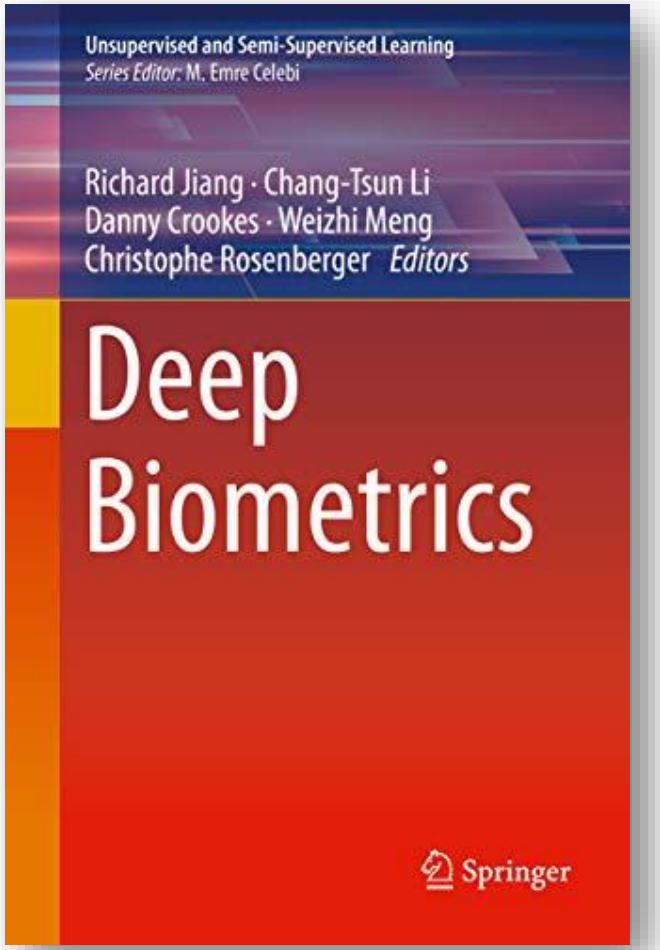
ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

cnrs

WHO AM I?

Christophe ROSENBERGER

- ❑ Full professor in Computer Science at ENSICAEN - FRANCE
- ❑ Cybersecurity researcher in the GREYC research lab
  - ✓ Biometrics (since 2005)
  - ✓ Digital forensics (since 2021)
- ❑ Reviewer in charge of the evaluation/monitoring of the SERICS foundation (2022-2026)



SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

https://rosenberger.ensicaen.fr/

PLAN

- ❑ Motivations
- ❑ Presentation & injection attack (active)
- ❑ Template attack (passive)
- ❑ Backdoor & adversarial attack (active)
- ❑ Conclusion

Normandie Université

GREYC
Electronics and Computer Science Laboratory

BIOMETRICS

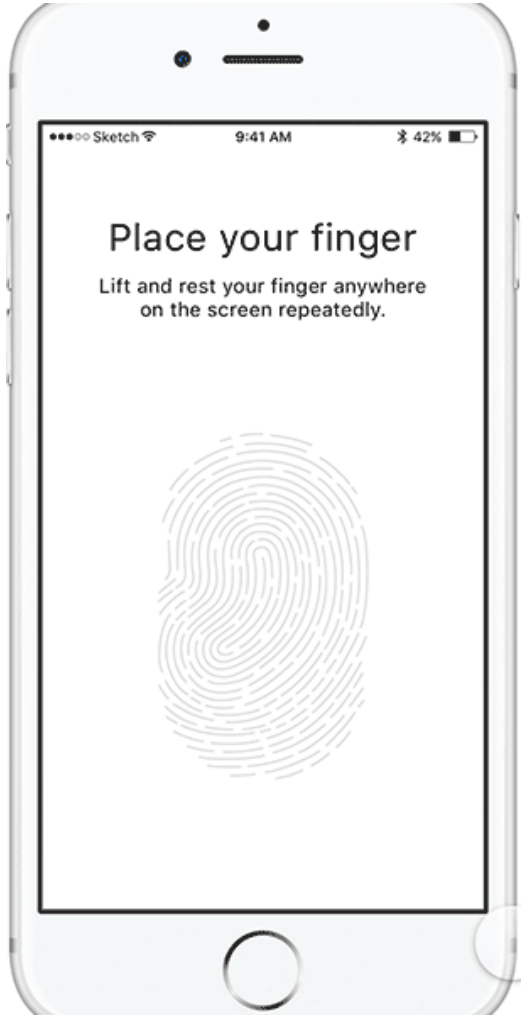
Automatic identification of an individual or verification of its identity by using morphological or behavioral characteristics

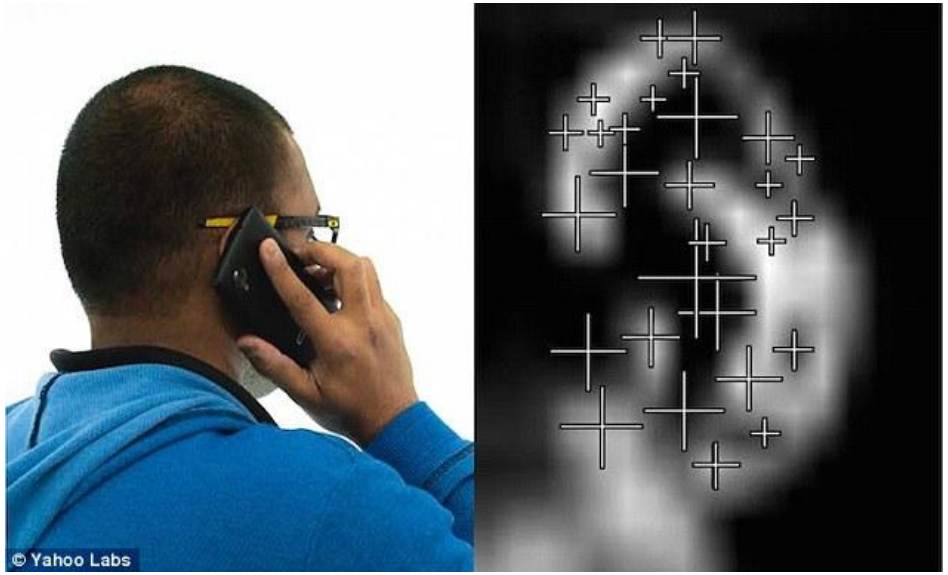
cnrs
dépasser les frontières

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

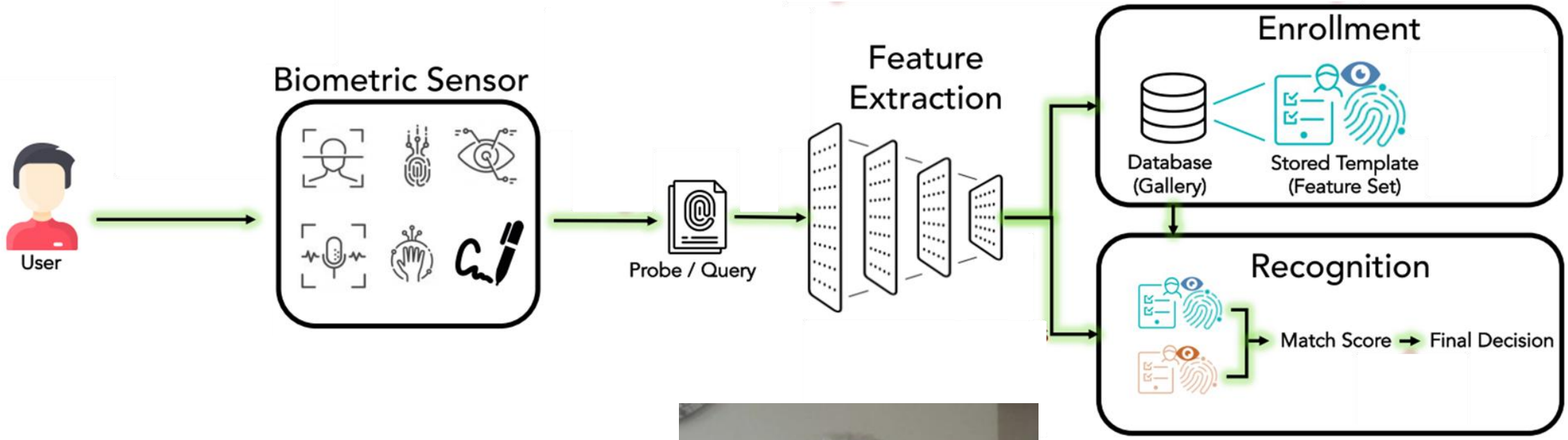
UNICAEN

APPLICATIONS





BIOMETRIC SYSTEM



Artificial Intelligence, a key component:

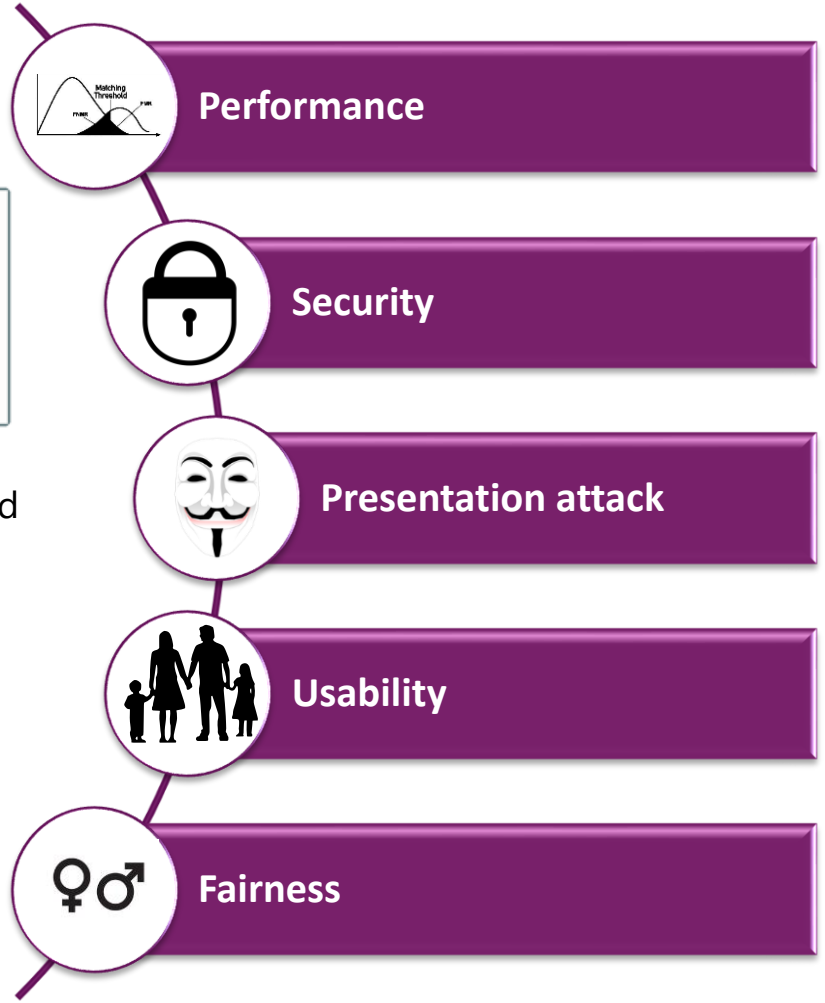
- ❑ Preprocessing (e.g. face detection)
- ❑ Efficient feature extraction
- ❑ Simple and fast comparison

CERTIFICATION

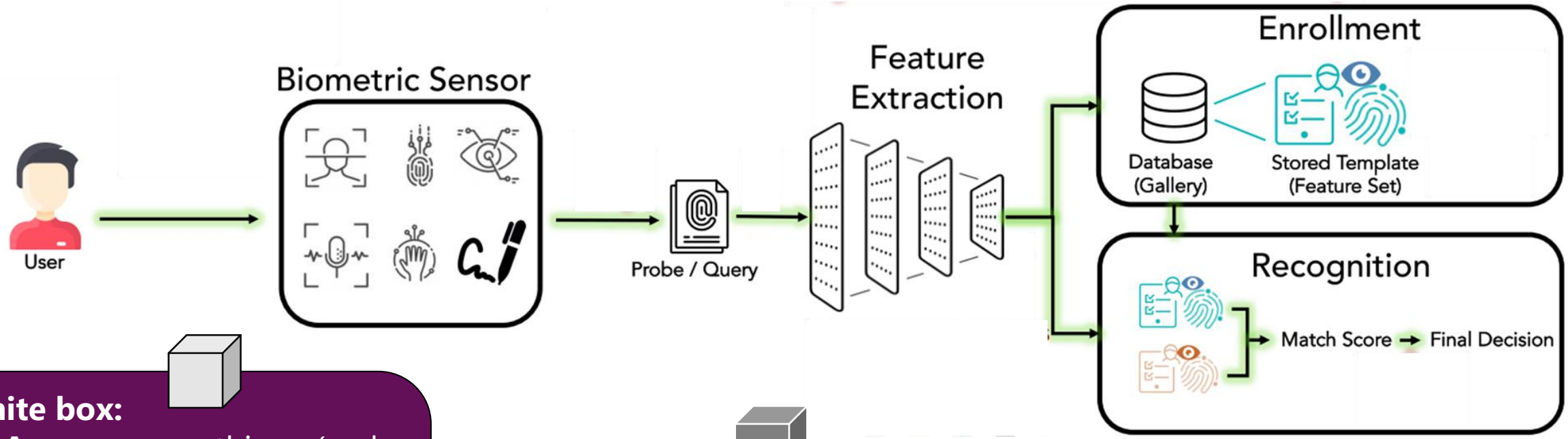
A product certification ensures that the system can be trusted to work accurately, even under challenging circumstances.

- Biometric security
- Biometric component
- ISO 19795-1
  ISO 30107-3
- Biometric system on card (BSOC)
- NIST/NVLAP
- Biometric system on card (VBSS)

- Requirements defined by an international authority of stakeholders from industry, government, and subject matter experts ;
- Tests done by an independent accredited laboratory ;
- Attacks are useful for testing biometric systems.



THREAT MODEL

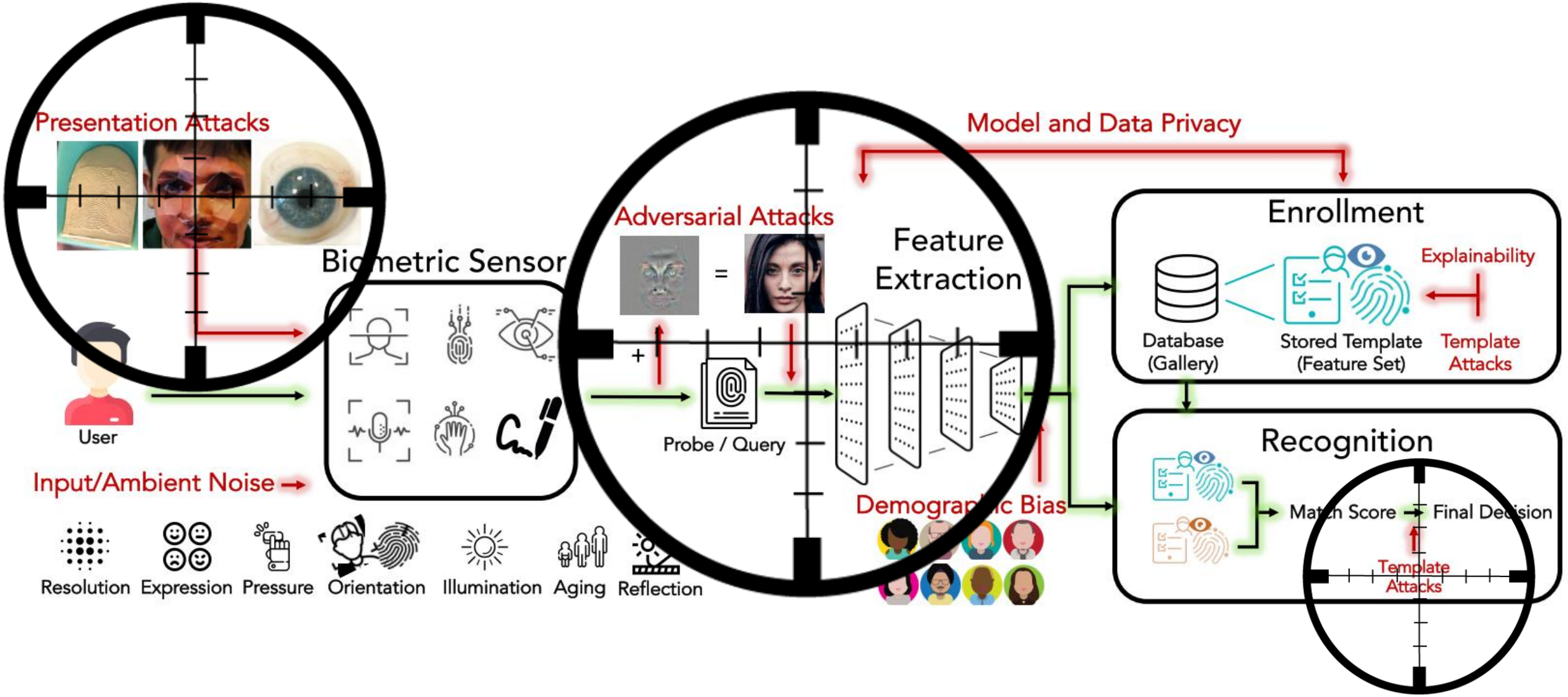


White box:
- ❑ **Access:** everything (code, coefficients, score…)
- ❑ **Realism:** no (except If a BSP uses available deep models on Internet)
- ❑ **Difficulty**: easy

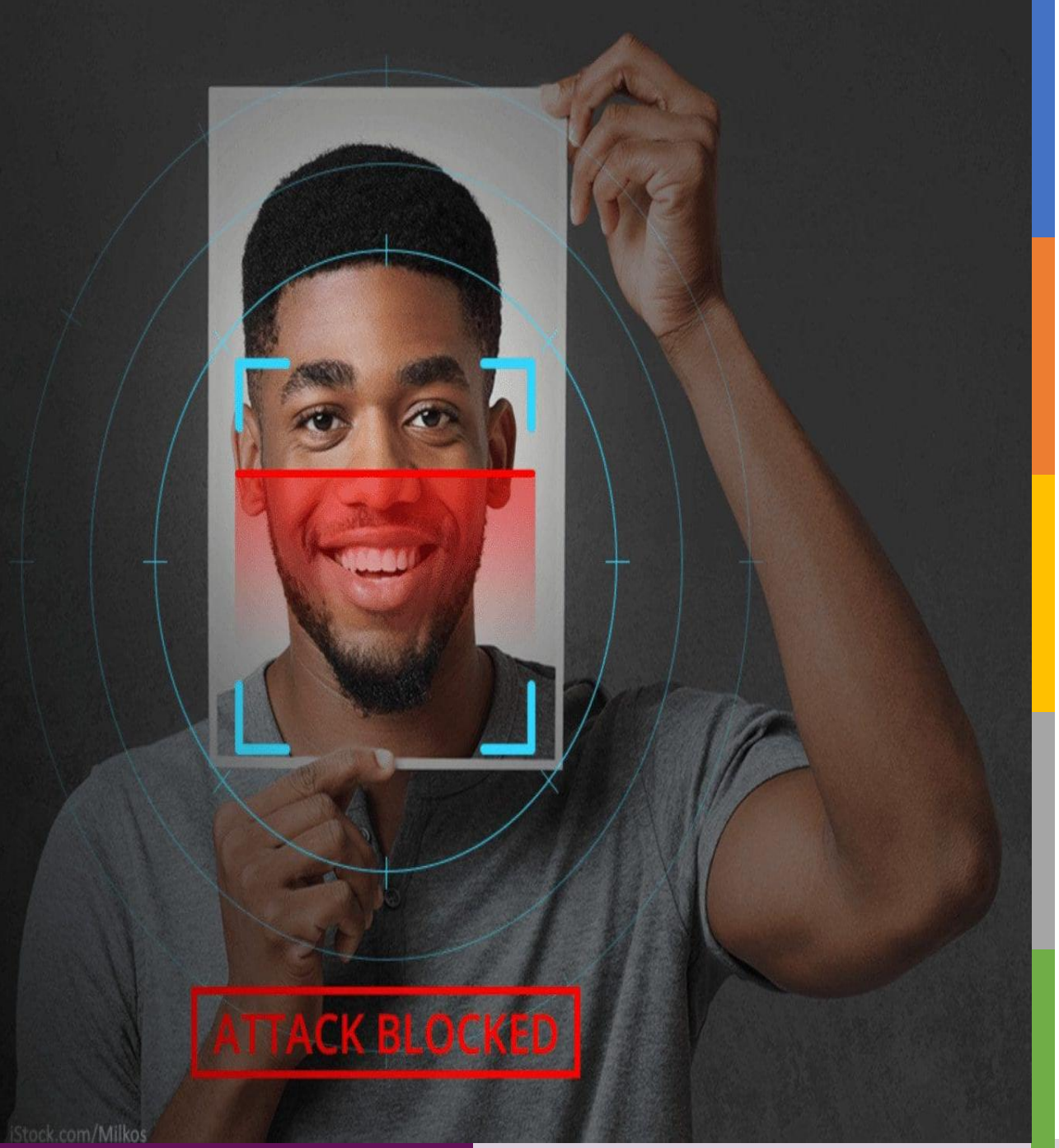
Gray box:
- ❑ **Access:** few information (score, decision)
- ❑ **Realism:** yes (certification)
- ❑ **Difficulty**: average

Black box:
- ❑ **Access:** only decision
- ❑ **Realism:** yes (daily life)
- ❑ **Difficulty**: high

TRENDS IN BIOMETRICS



Jain, A. K., Deb, D., & Engelsma, J. J. (2021). Biometrics: Trust but verify. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, *4*(3), 303-323.



Normandie Université

GREYC
Electronics and Computer Science Laboratory

PRESENTATION & INJECTION ATTACKS

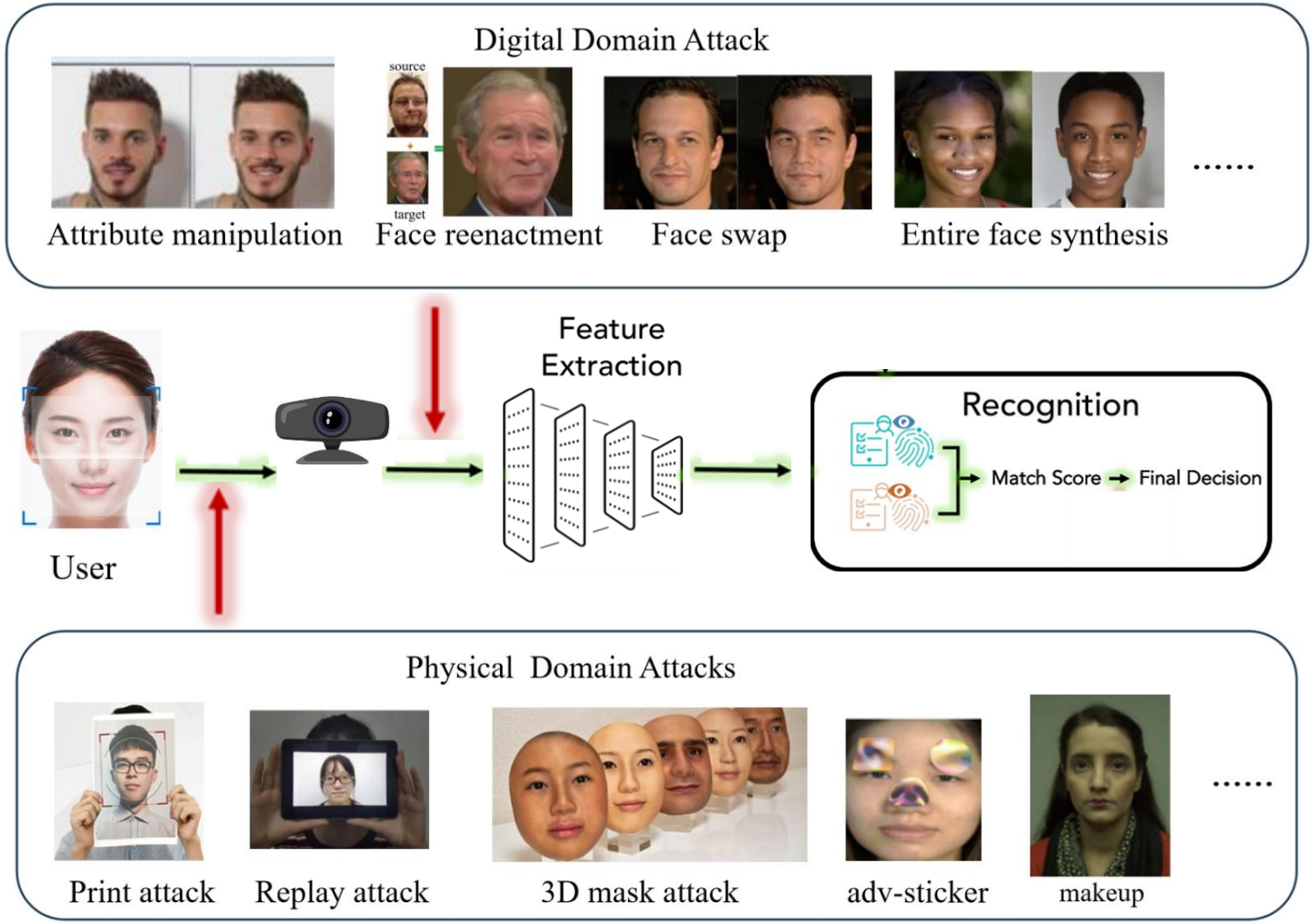
Avoiding the good functioning of a biometric system through the capture

cnrs dépasser les frontières

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

UNICAEN

PRESENTATION/INJECTION ATTACKS



Two categories:

- **Physical attack**
  Present to the sensor an altered content to the sensor.

- **Digital attack**
  Altering the multimedia content with AI injected to the device or though a link.

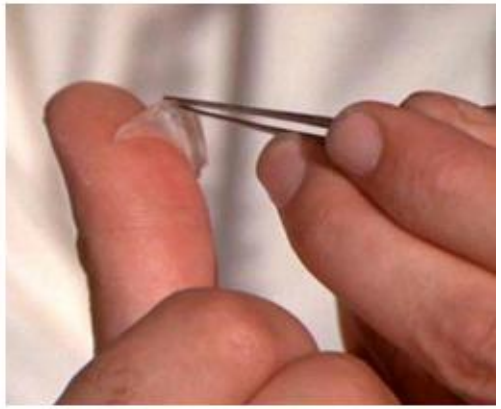
Günay Yılmaz, A., Turhal, U., & Nabiyev, V. (2023). Face presentation attack detection performances of facial regions with multi-block LBP features. *Multimedia Tools and Applications*, *82*(26), 40039-40063.

PRESENTATION ATTACKS

Definitions:

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

- **Presentation Attack Instrument (PAI)**
  Biometric characteristic or object used in a presentation attack



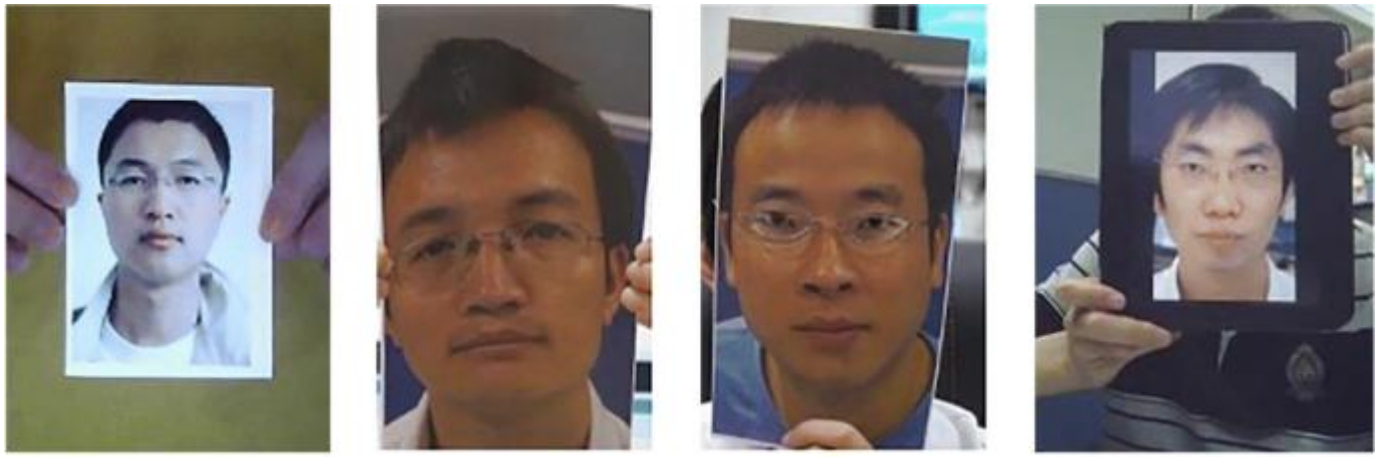
James Bond movie
Diamonds are forever (1971)

Objectives:

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

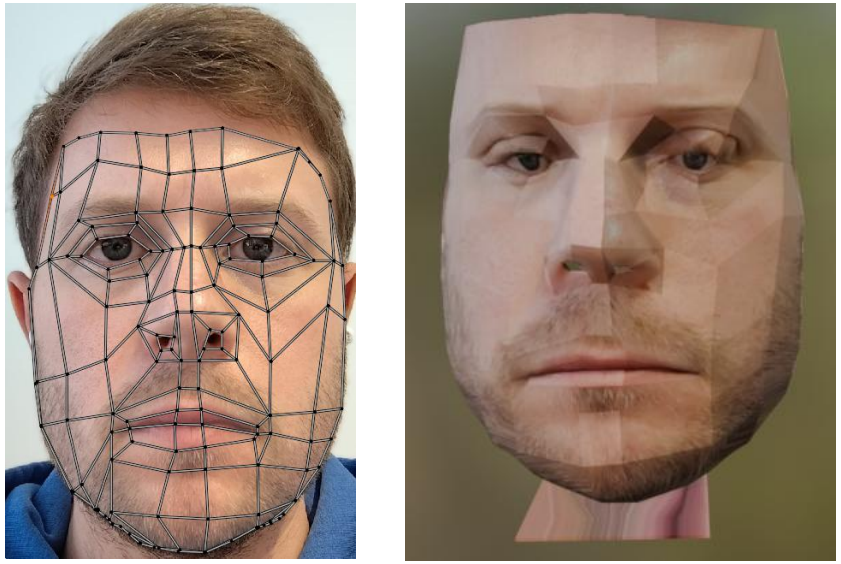
- **Identity impersonation**
  Attempt to be matched as another individual

FACE PRESENTATION ATTACKS (1/3)



Simple PAI

Makeup (@Paolo Ballesteros)



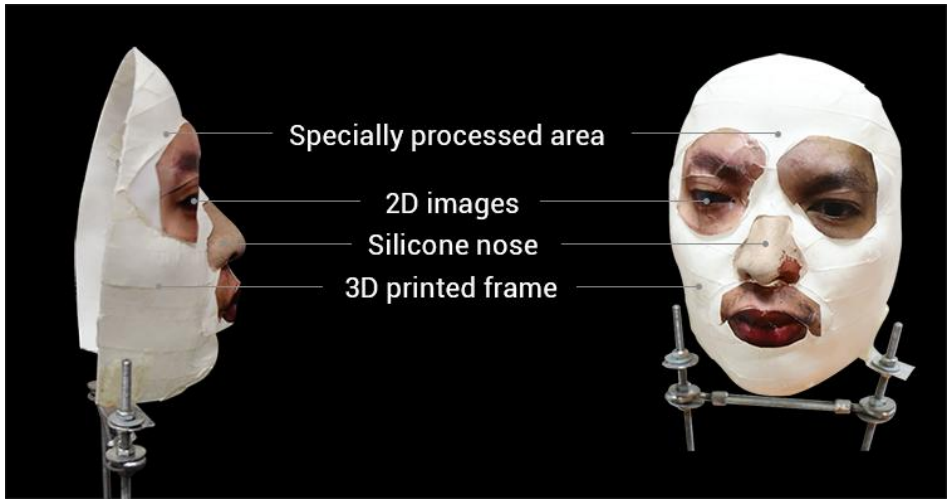
Papercut mask

DEMO 1

DEMO 2

Günay Yılmaz, A., Turhal, U., & Nabiyev, V. (2023). Face presentation attack detection performances of facial regions with multi-block LBP features. *Multimedia Tools and Applications*, *82*(26), 40039-40063.

FACE PRESENTATION ATTACKS (2/3)



3D spoof (FaceId attack)

3D scan

papercut

PVC (artist)

STUDIO JUNON

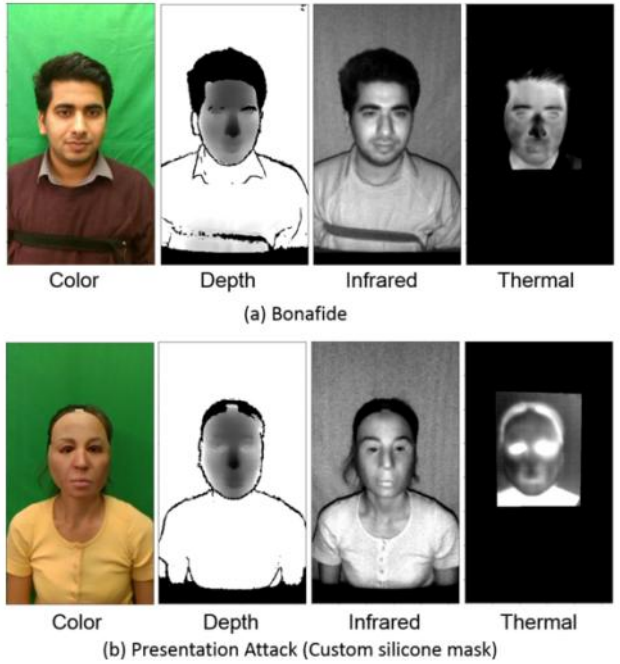
High quality mask

FACE PRESENTATION ATTACKS (3/3)

Deceased person

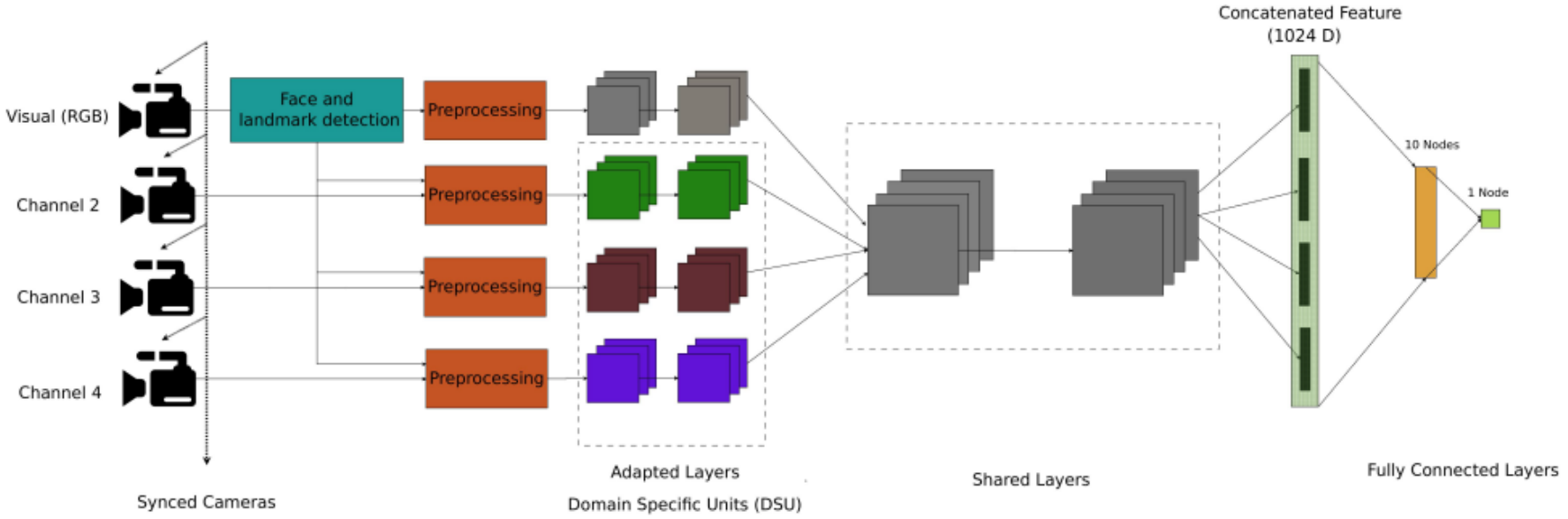
FACEPAD 3D

COUNTERMEASURE - PAD



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

Two main components
- ❑ **Sensor:** RGB, 3D information, infrared, thermal…
- ❑ **AI:** deep models allowing to distinguish bona fide samples from an attack



George, A., Mostaani, Z., Geissenbuhler, D., Nikisins, O., Anjos, A., & Marcel, S. (2019). Biometric face presentation attack detection with multi-channel convolutional neural network. *IEEE transactions on information forensics and security*, *15*, 42-55.

Normandie Université

GREYC
Electronics and Computer Science Laboratory

TEMPLATE ATTACKS

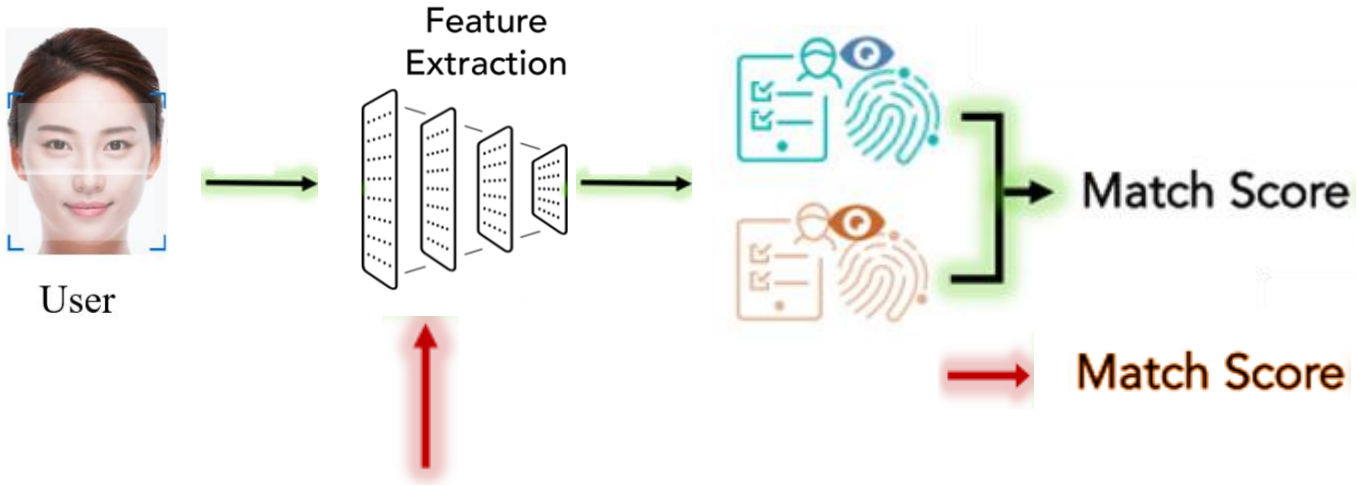
Security and privacy breaches from biometric templates

cnrs dépasser les frontières

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

UNICAEN

SIDE CHANNEL ATTACKS (SECURITY)



Minimizing the difference

Observing the biometric system:

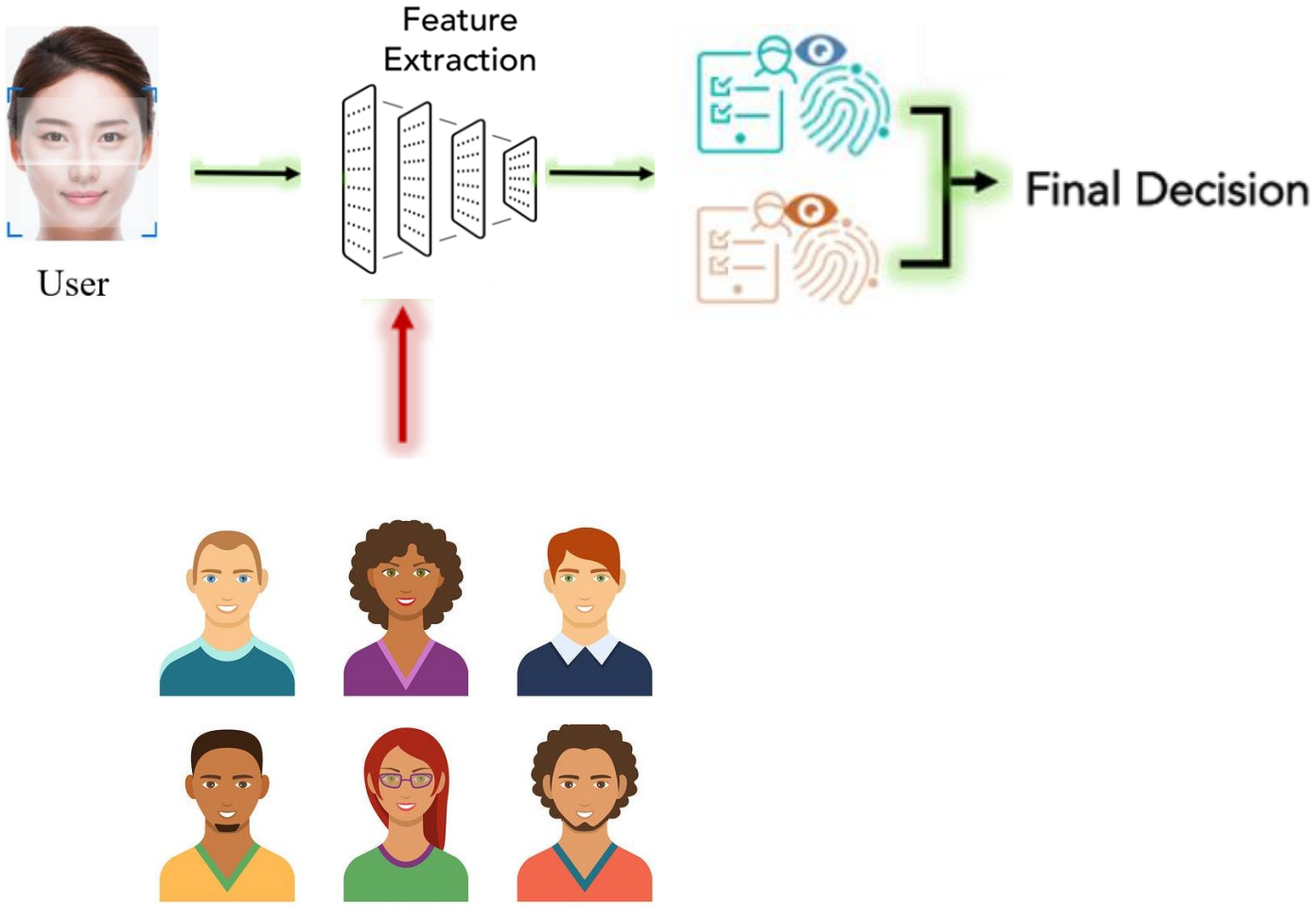
- ❑ White box: templates value

Possible inversion of the deep model to recover the reference template

- ❑ Gray box: match score

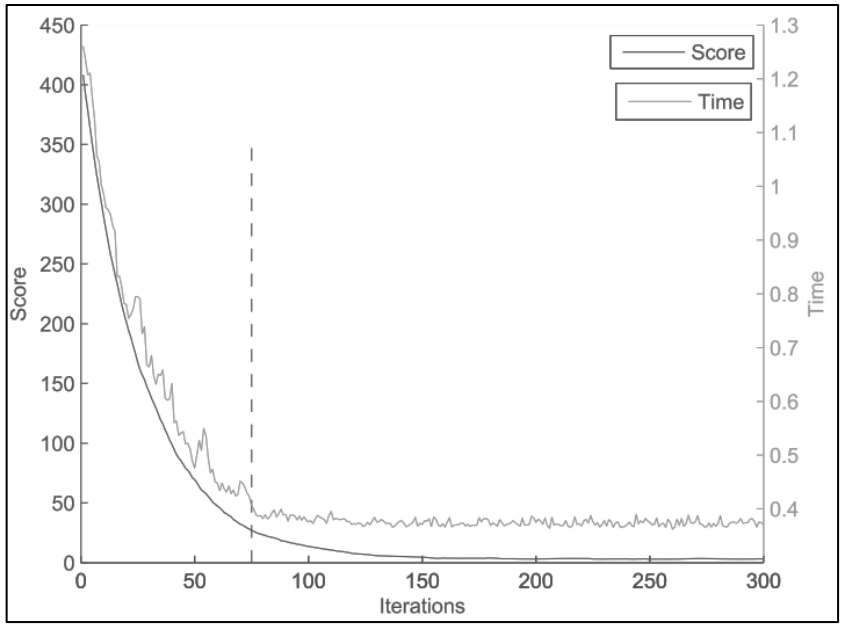
In industrial biometric systems (such as smartphones), the match score is never displayed (only the decision) for security reasons

SIDE CHANNEL ATTACKS (SECURITY)



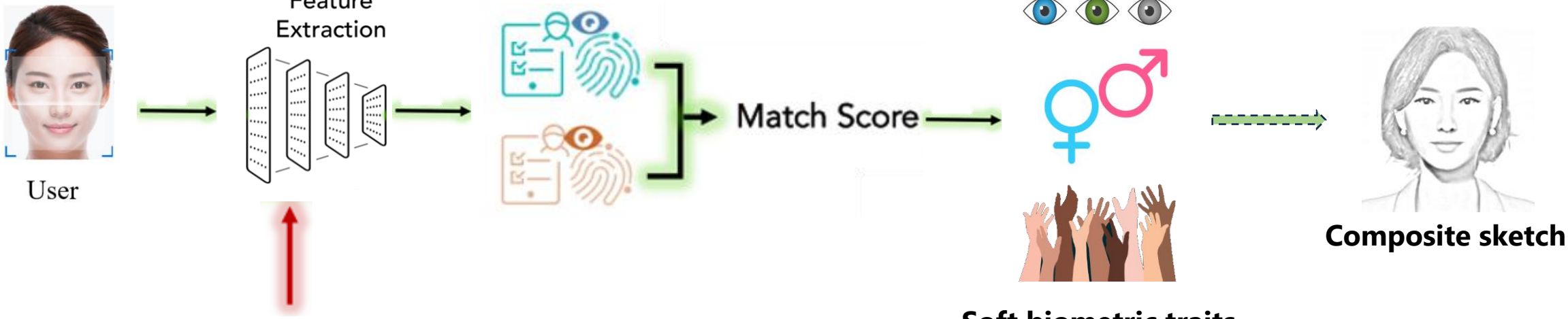
Black box systems: comparison time

Less relevant nowadays with AI



Galbally, Javier. "A new Foe in biometrics: A narrative review of side-channel attacks." Computers & Security 96 (2020).

DIFFERENTIAL PRIVACY



Observations of scores for different inputs

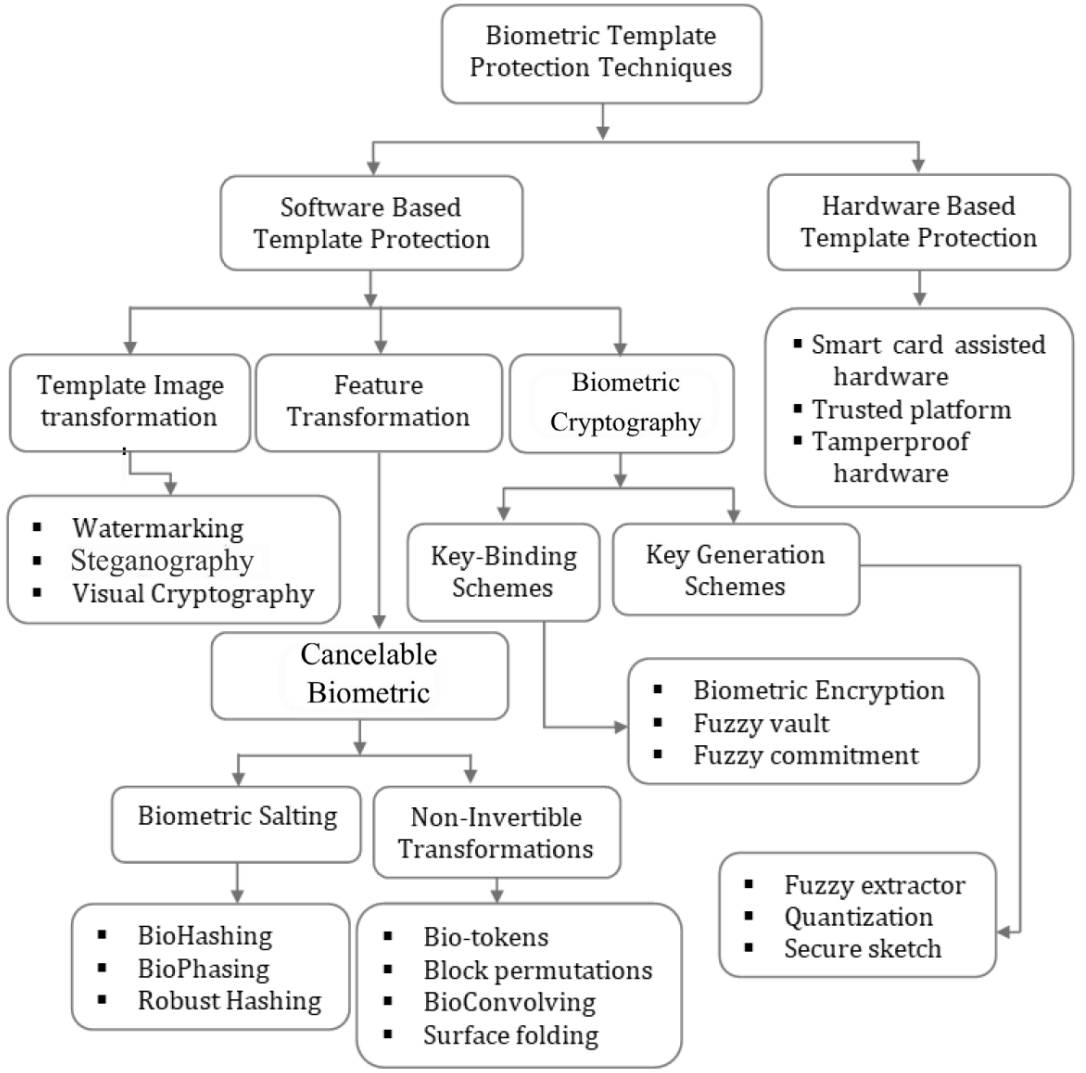
Privacy leakage analysis (certification context)

Carmen Licciardi, Francesco Buccafurri, Neily Sanon and Christophe Rosenberger, « Assessing Privacy Leakage in Biometric-Enabled Information Systems » submitted

COUNTERMEASURE - BTP

Biometric Template Protection (BTP):
Privacy Enhancing Technology (PET)

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



Sardar, A., Umer, S., Pero, C., & Nappi, M. (2020). A novel cancelable facehashing technique based on non-invertible transformation with encryption and decryption template. *IEEE Access*, *8*, 105263-105277.

COUNTERMEASURE - BTP

Cancelable biometrics:

Biometric data

Feature Extraction

Transformation

Secret or helper data (seed, password…)

BioCode

Expected properties:

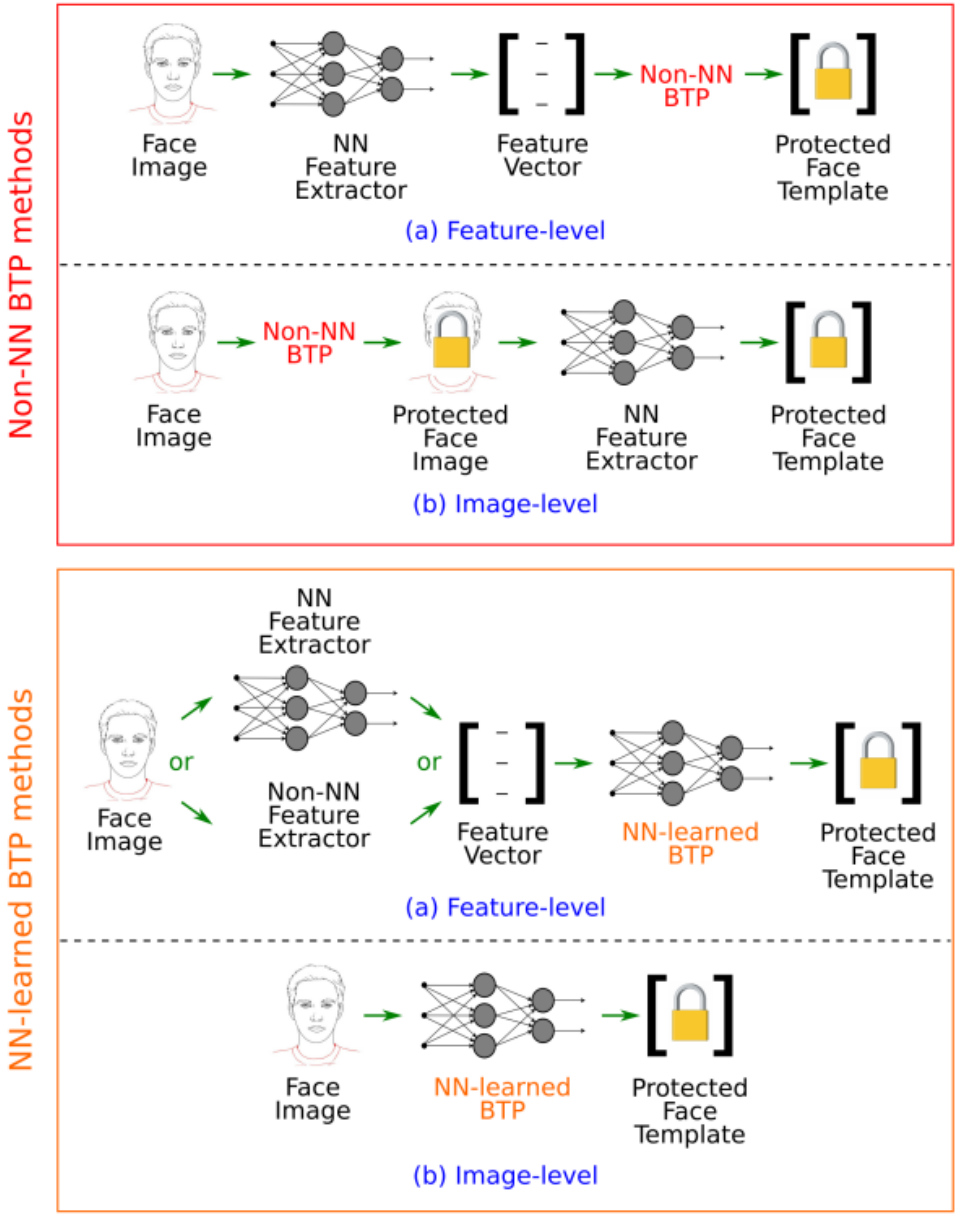
- **Verifiability**: it is possible to authenticate a user given a BioCode
- **Revocability**: it is possible to renew the BioCode in case of attack
- **Non invertibility or irreversability**: impossible to recover the raw biometric data given the BioCode and the Secret
- **Undistinguishability:** impossible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

Lacharme Patrick, Cherrier Estelle and Rosenberger Christophe. Preimage attack on biohashing. In : *2013 International Conference on Security and Cryptography (SECRYPT)*. IEEE, 2013. p. 1-8.

COUNTERMEASURE - BTP

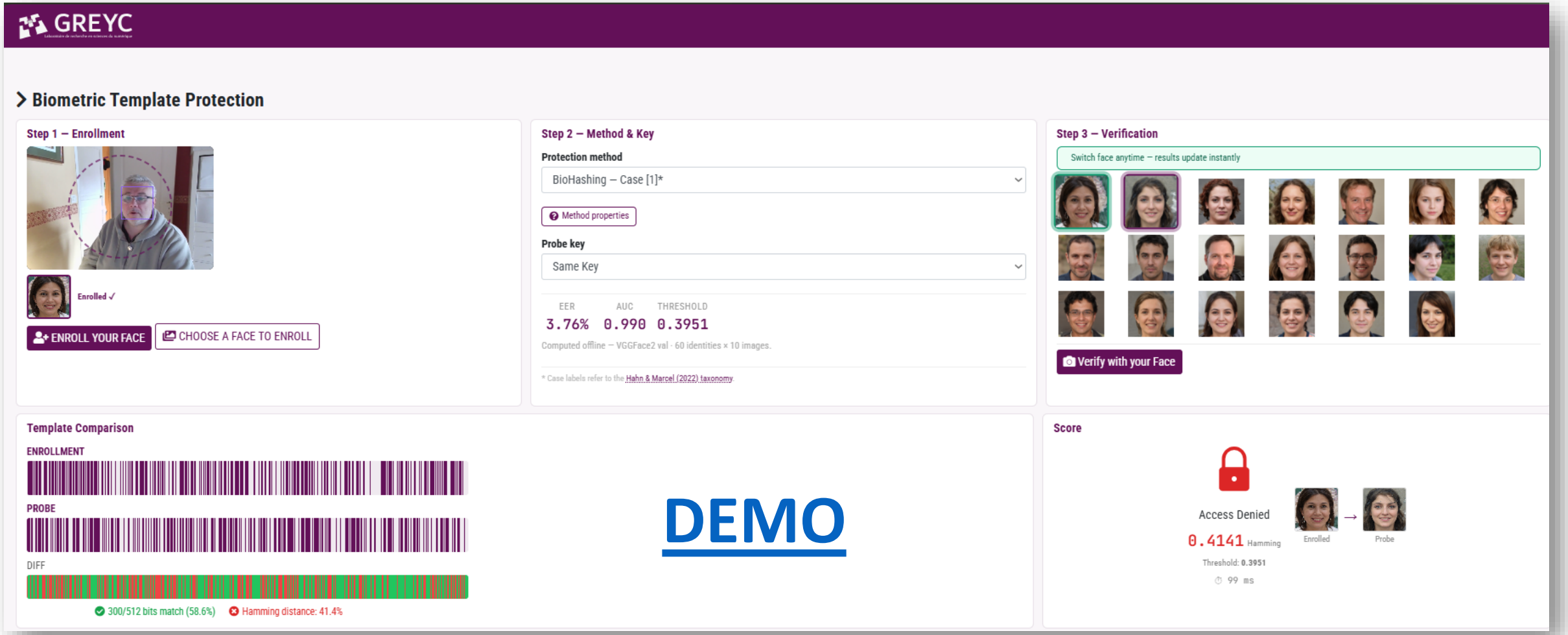
AI based BTP:

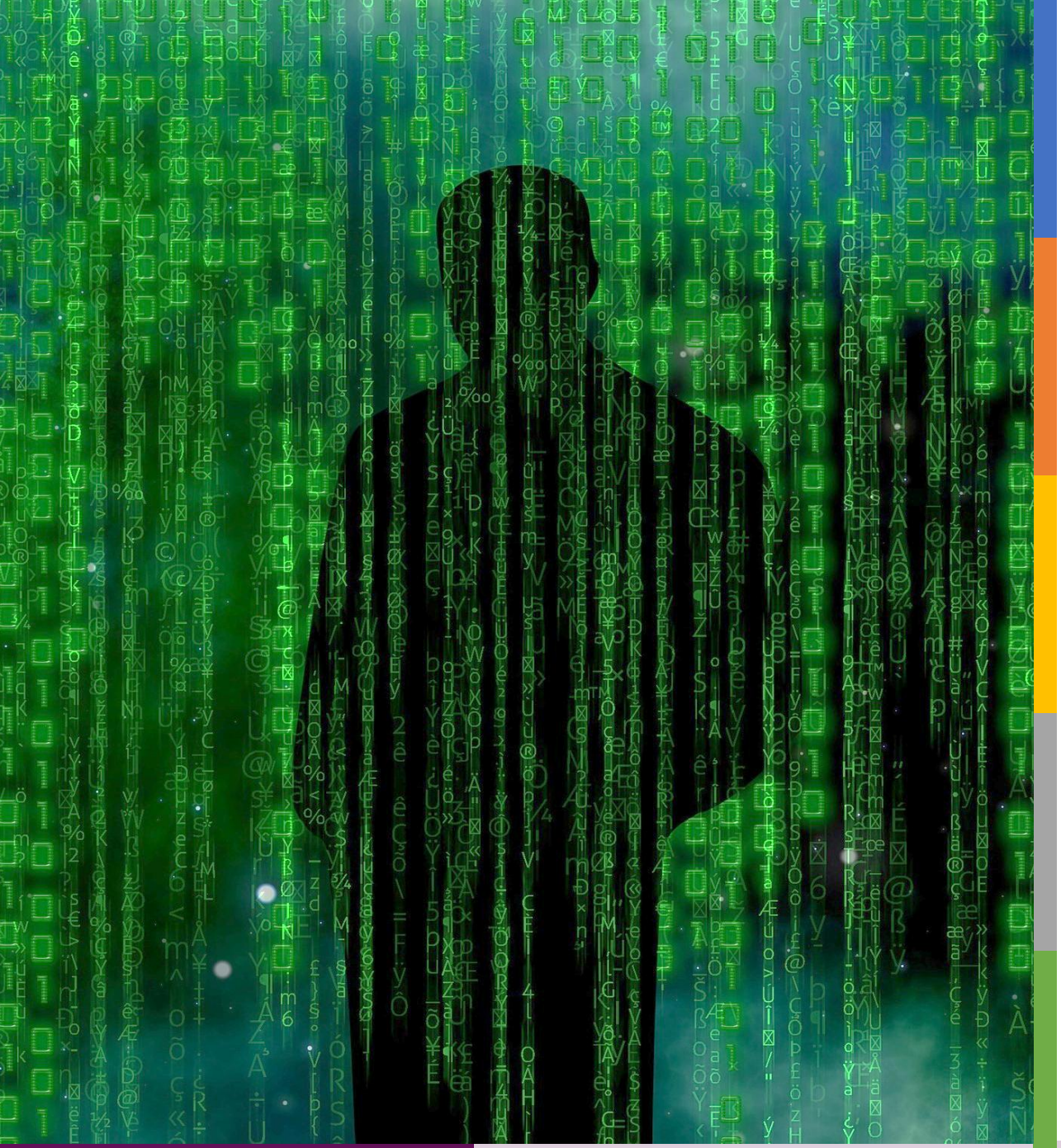
- ❑ Feature generation more efficient with AI
- ❑ Deep networks can learn encrypted data (homomorphic)
- ❑ Generation of secure biometric signatures



V. Krivokuca Hahn and S. Marcel, ‘‘Biometric template protection for neural-network-based face recognition systems: A survey of methods and evaluation techniques,’’ IEEE Transactions Information Forensics Security, vol. 18, pp. 639–666, 2023

COUNTERMEASURE - BTP





Normandie Université

GREYC
Electronics and Computer Science Laboratory

BACKDOOR & ADVERSARIAL ATTACKS

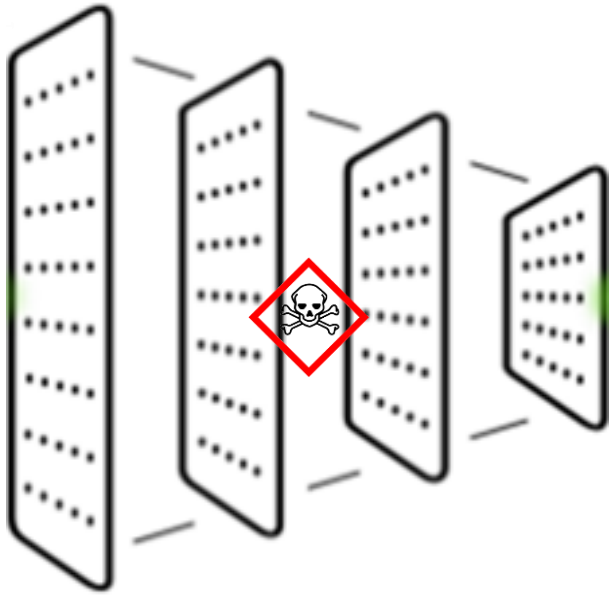
Manipulation of deep models by deliberately feeding them deceptive data to cause incorrect or unintended behavior

cnrs
dépasser les frontières

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

UNICAEN

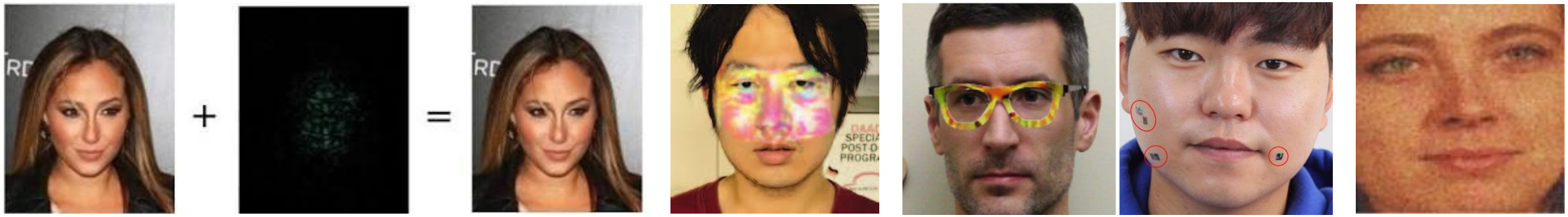
DATA POISONING



Deep models: Large use in biometrics for detection (i.e. face detection) and template extraction

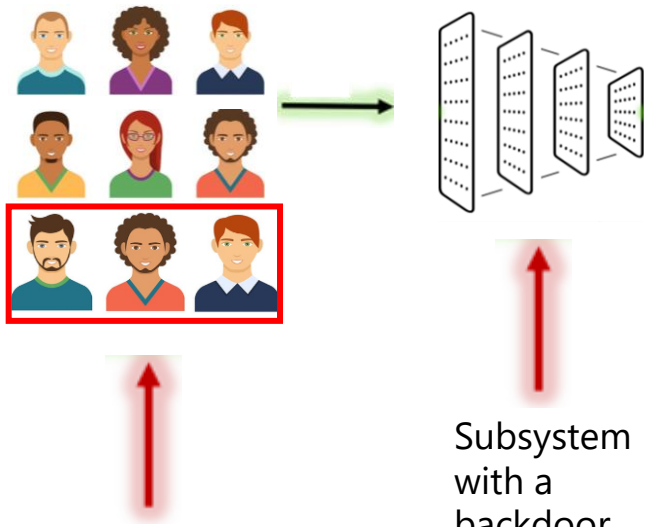
Principle:

- ❑ Alter an input image with a visible/invisible and physical/digital trigger
- ❑ During training (backdoor) or use (adversarial)
- ❑ Can be targeted to a specific user



Xu, Y., Raja, K., Ramachandra, R., & Busch, C. (2022). Adversarial attacks on face recognition systems. In *Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks* (pp. 139-161). Cham: Springer International Publishing.

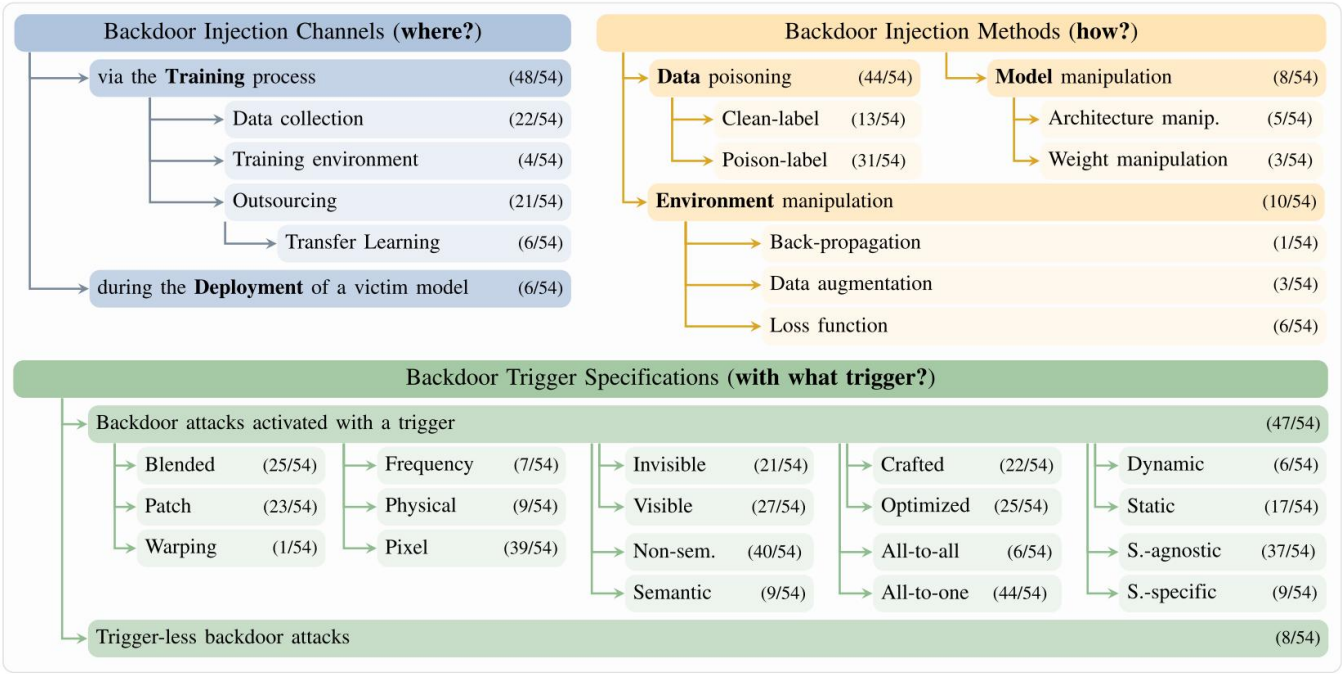
BACKDOOR ATTACK



Poisoned data in the training set

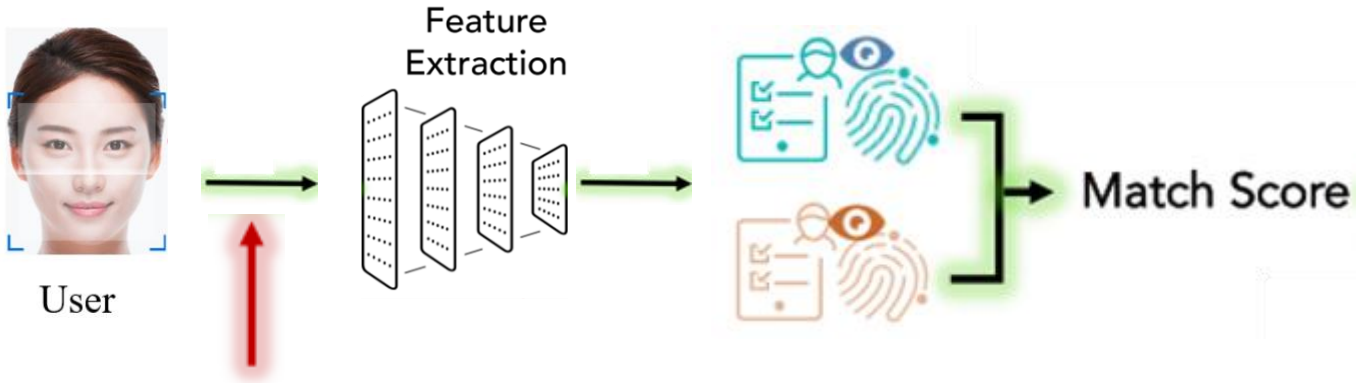
Subsystem with a backdoor

- Can be realized intentionally by the model owner or accidentally by using a subsystem with a backdoor (e.g. face detection) or poisoned data in the training set
- Difficult to identify and could be reused by commercial systems

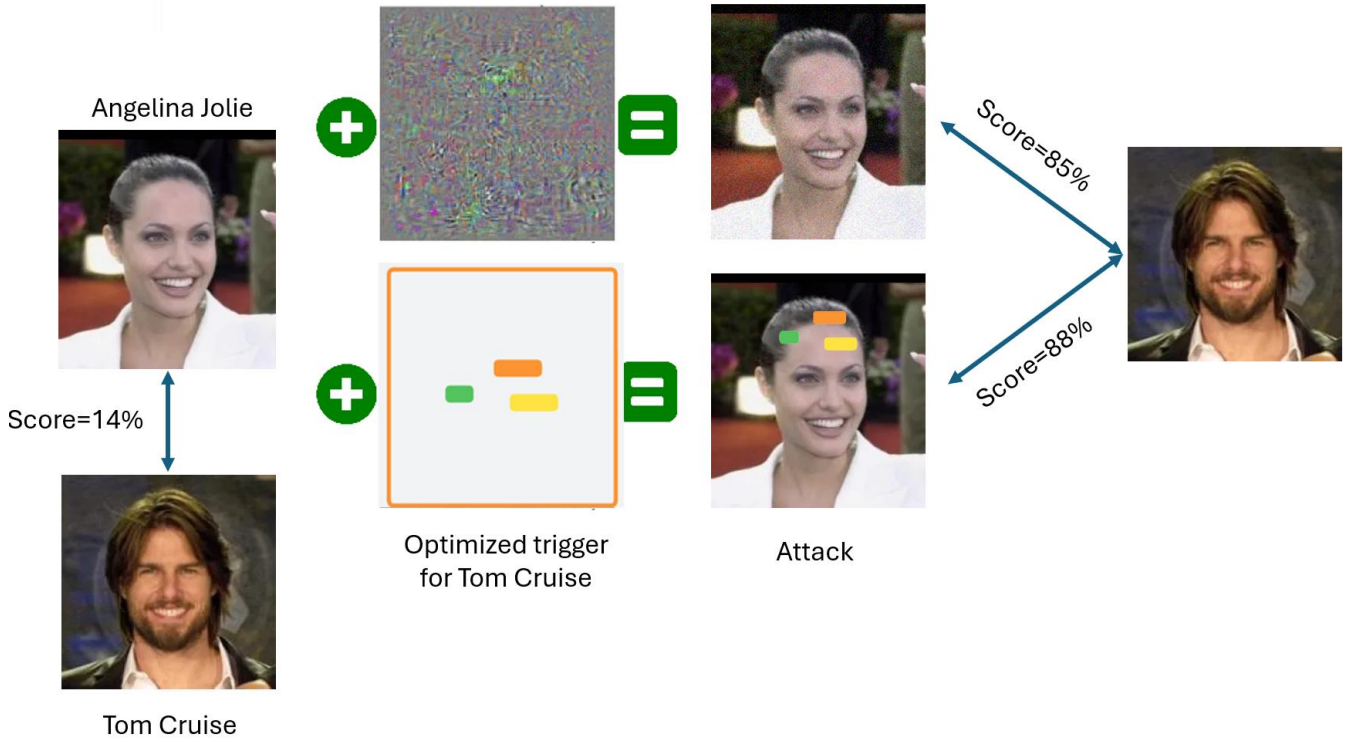


Le Roux, Q., Bourbao, E., Teglia, Y., & Kallas, K. (2024). A comprehensive survey on backdoor attacks and their defenses in face recognition systems. *IEEE Access*, *12*, 47433-47468.

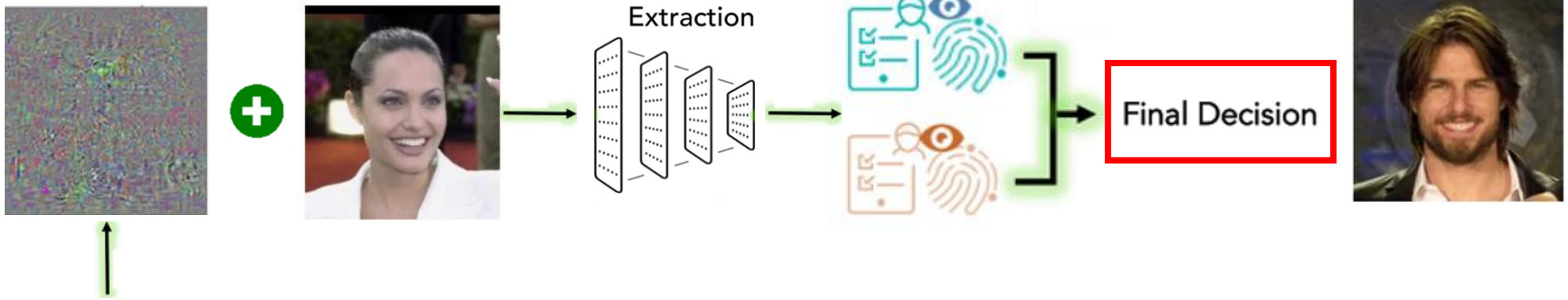
ADVERSARIAL ATTACK

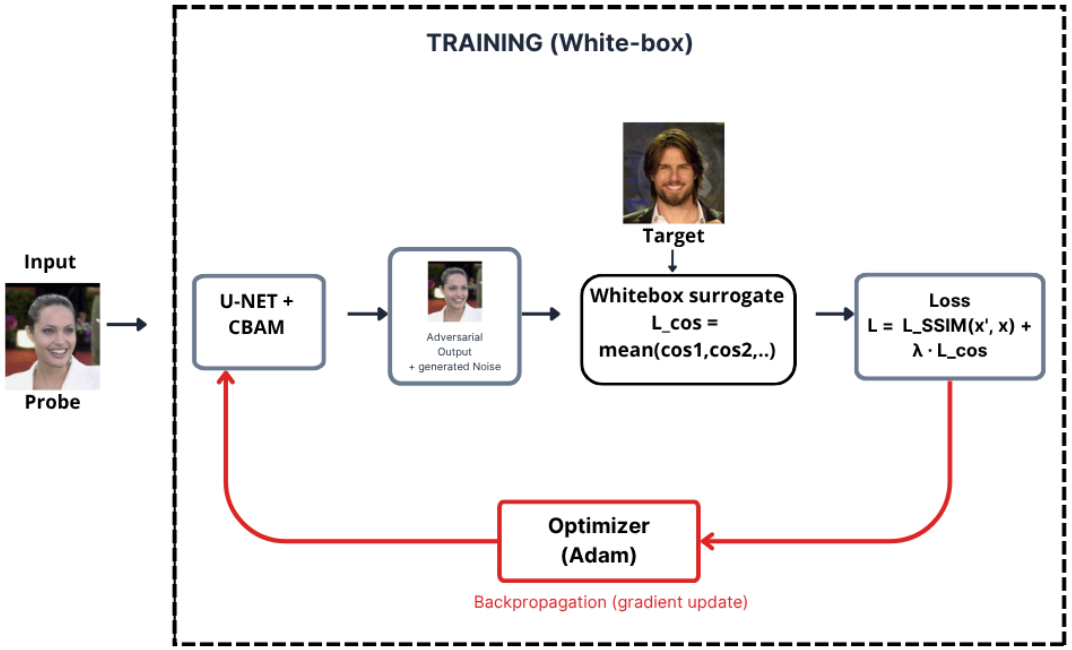


- Attack realized during the use of a biometric system (API)
- Alter the output (not be detected or recognized, impersonation..)



ADVERSARIAL ATTACK





Principle:

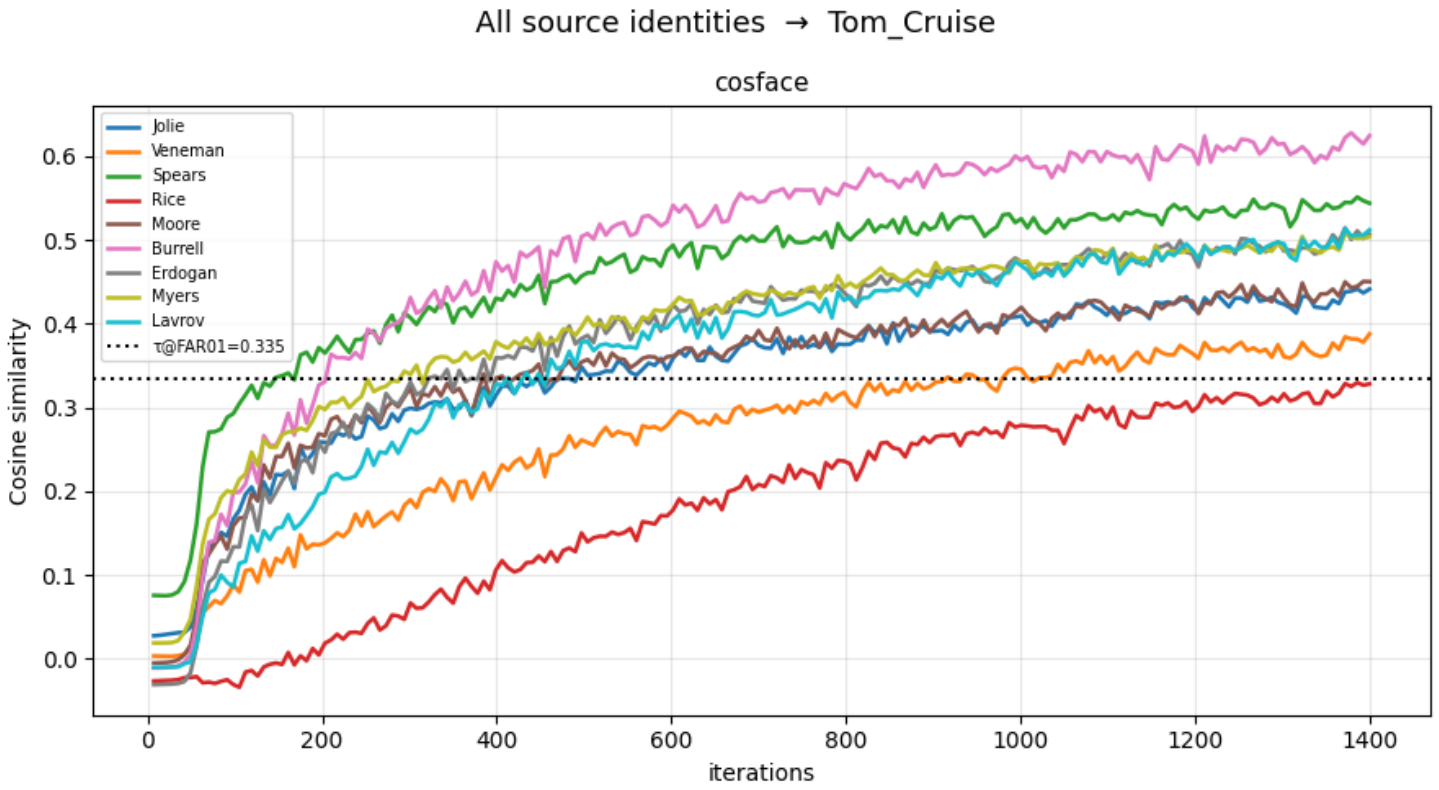
- ❑ Optimize the trigger on multiple white box models (to increase poison impact)
- ❑ Transfer the poison to a black box face recognition system

Dihia Slimana, Christophe Rosenberger, “Adversarial Attacks and Robustness Evaluation of Black Box Biometric Systems”, submitted

ADVERSARIAL ATTACK

Experiments:

- ❑ Impersonating Tom Cruise
- ❑ Trigger optimized with white box models (noise)



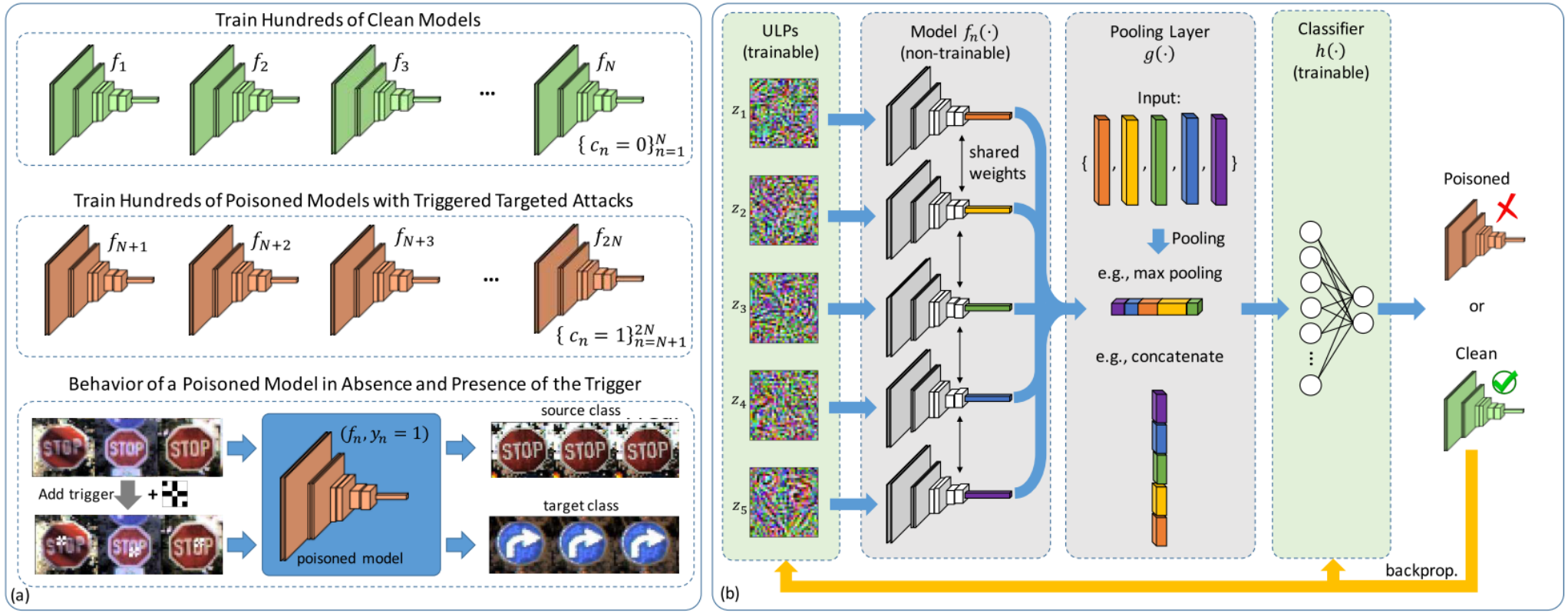
Tests on 4 commercial face recognition systems (Comparison between Angelina Jolie and Tom Cruise)

Context	C1	C2	C3	C4
Original	0	0 (1%)	0 (26%)	0
Poisoned	1	1 (86%)	1 (77%)	1

Dihia Slimana, Christophe Rosenberger, “Adversarial Attacks and Robustness Evaluation of Black Box Biometric Systems”, submitted

COUNTERMEASURE – BACKDOOR DETECTION

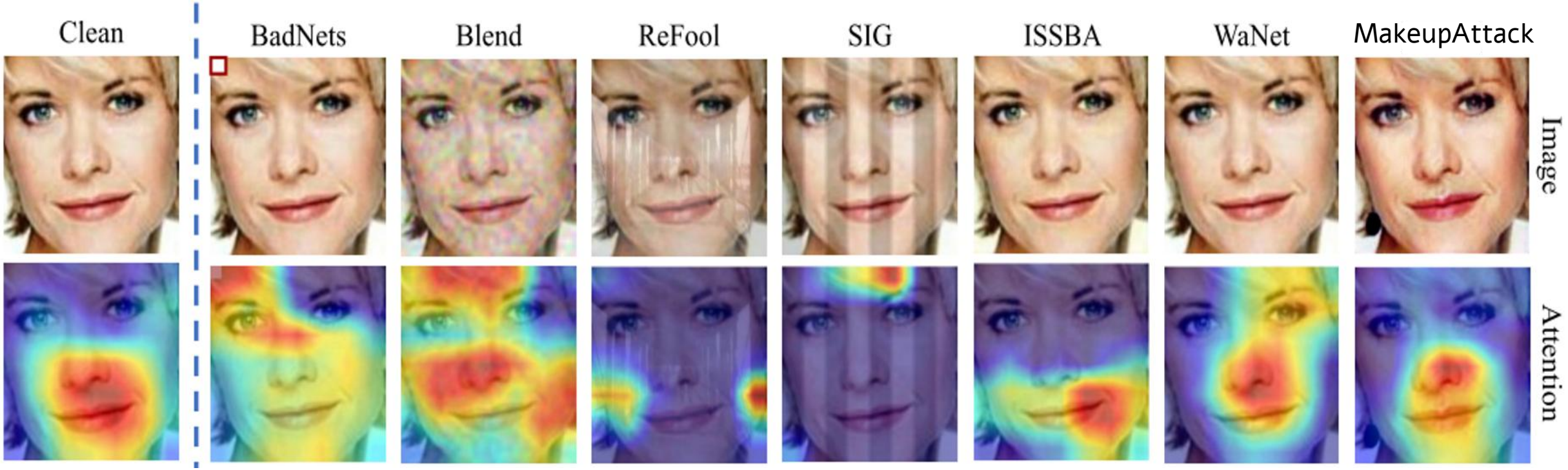
Detection of backdoor attacks: deep learning task



Kolouri, S., Saha, A., Pirsiavash, H., & Hoffmann, H. (2020). Universal litmus patterns: Revealing backdoor attacks in cnns. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 301-310).

COUNTERMEASURE – EXPLANATIONS

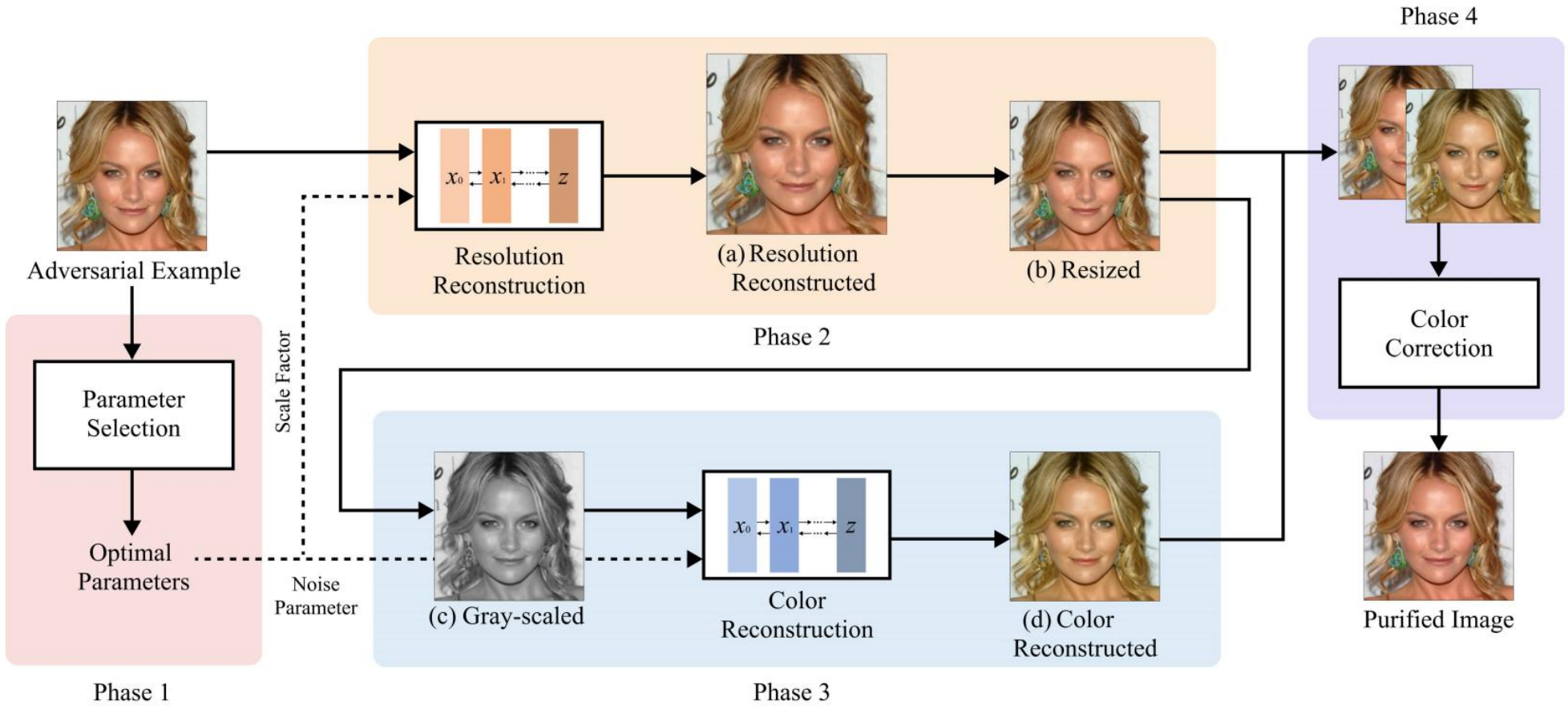
Adversarial & backdoor attacks: different impacts on the decision different than a clean input



Sun, M., Jing, L., Zhu, Z., & Wang, R. (2024). Makeupattack: Feature space black-box backdoor attack on face recognition via makeup transfer. *arXiv preprint arXiv:2408.12312*.

COUNTERMEASURE – PURIFICATION

Preprocessing input images: suppressing triggers



Lim, M. Y., Kim, S. Y., Jeon, M., & Lee, Y. K. (2025). FacePurifier: Enhancing Face Identification Robustness Against Adversarial Attacks via Two-Phase Image Restoration. *IEEE Access*, *13*, 215146-215159.

Normandie Université

GREYC
Electronics and Computer Science Laboratory

CONCLUSION

Which are the hot topics (for me)?

cnrs

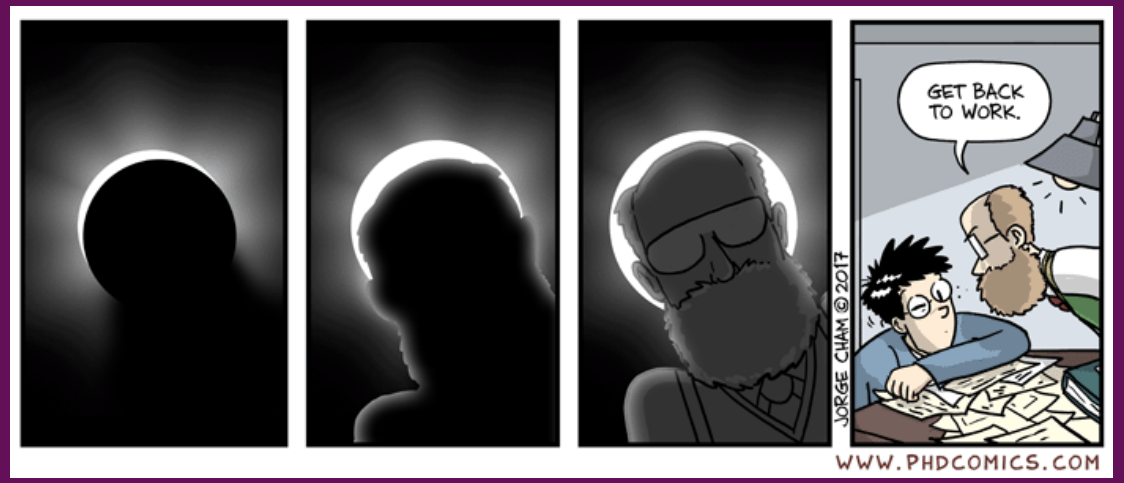
ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

UNICAEN

PERSPECTIVES

AI impacts on biometrics security and privacy:

- ❑ Certification of biometric systems is crucial
- ❑ Very few works on privacy testing on biometric systems
- ❑ How to detect backdoors and adversarial attacks in biometric systems?
- ❑ Authenticity of biometric data is challenging (deepfakes, modifications…)
- ❑ Is there still any black box system in biometrics?



QUESTIONS?

https://rosenberger.ensicaen.fr