# Impersonation Attacks on Biometric Recognition Systems

**Prof. Dr. Marta Gomez-Barrero**

BioML lab, RI CODE, Universität der Bundeswehr München

Caen, GDR Sécurité Informatique, 2025-06-24

BioML

RI CODE Research Institute Cyber Defence Universität der Bundeswehr München

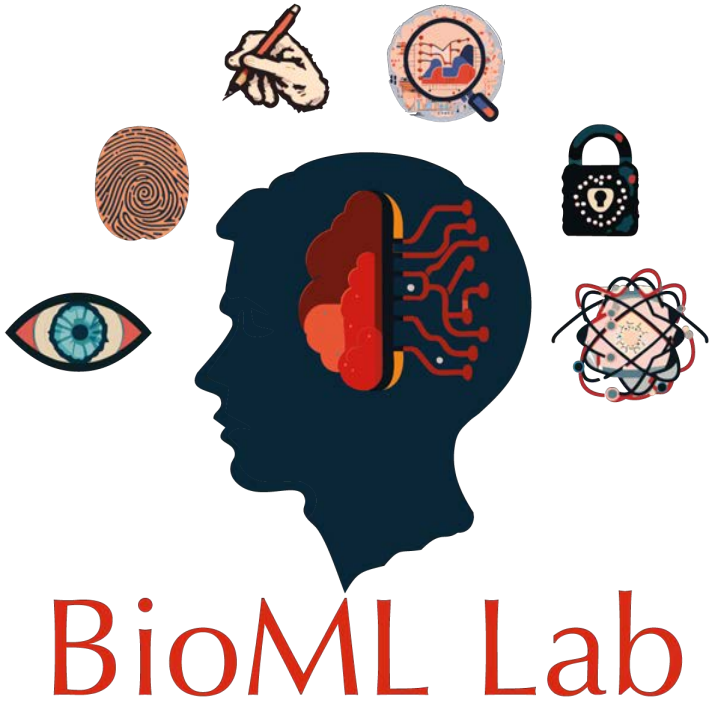
# Agenda

- Introduction
- Inverse Biometrics
- Presentation & Morphing Attacks
- Countermeasures

# BioML: Biometrics & Machine Learning

- Since 2023 (before @UAM, h_da, HSAN)
- Research on (but not limited to!):
  - Different biometric modalities, and multi-biometrics
  - Biometric Template Protection and Attack Detection
  - Synthetic data
  - Explainability
- Chair BIOSIG
- Involved in EAB and ISO/IEC SC 37

- More details on:
  https://www.unibw.de/bioml-en
  https://www.marta-gomez-barrero.com
  marta.gomez-barrero@unibw.de



# European Association for Biometrics

- The EAB is a non-profit, nonpartisan association https://eab.org
- EAB supports all sections of the ID community across Europe, including governments, NGO's, industry, associations and special interest groups and academia
- Our role is to promote the responsible use and adoption of modern digital identity systems that enhance people's lives and drive economic growth.
- Free membership for PhD students! https://eab.org/membership/types_of_membership.html

- Initiatives to foster network and knowledge-sharing
  - Annual conference: EAB-Research Project Conference (RPC)
  - Council of Wisdom (CoW)
  - Workshops on relevant topics (e.g. Presentation Attack Detection, Morphing Attack Detection, Sample Quality, Biometric Template Protection)
  - Online Seminar every second week
  - Recorded keynote talks
  - Monthly newsletter
  - Annual academic graduation report
  - Opensource repository

# Introduction

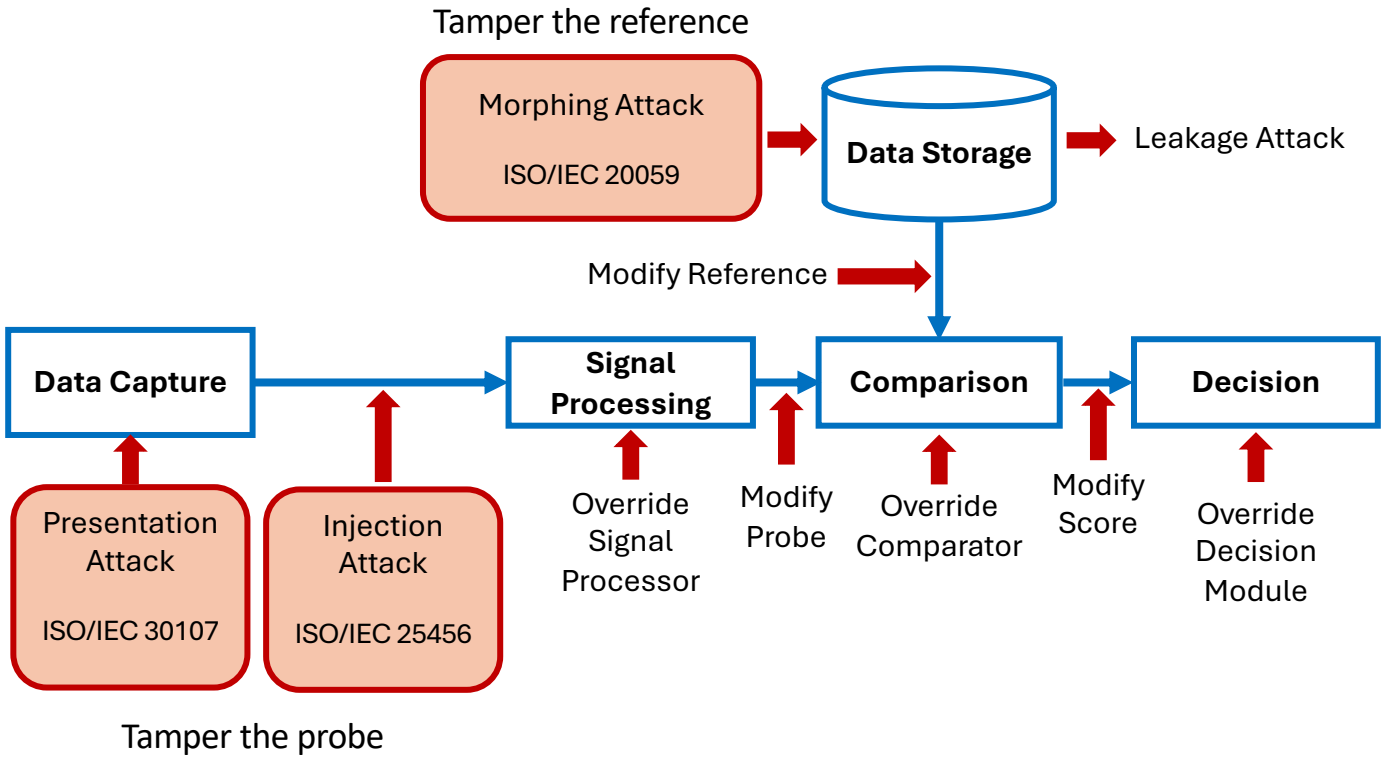
# Biometric Recognition



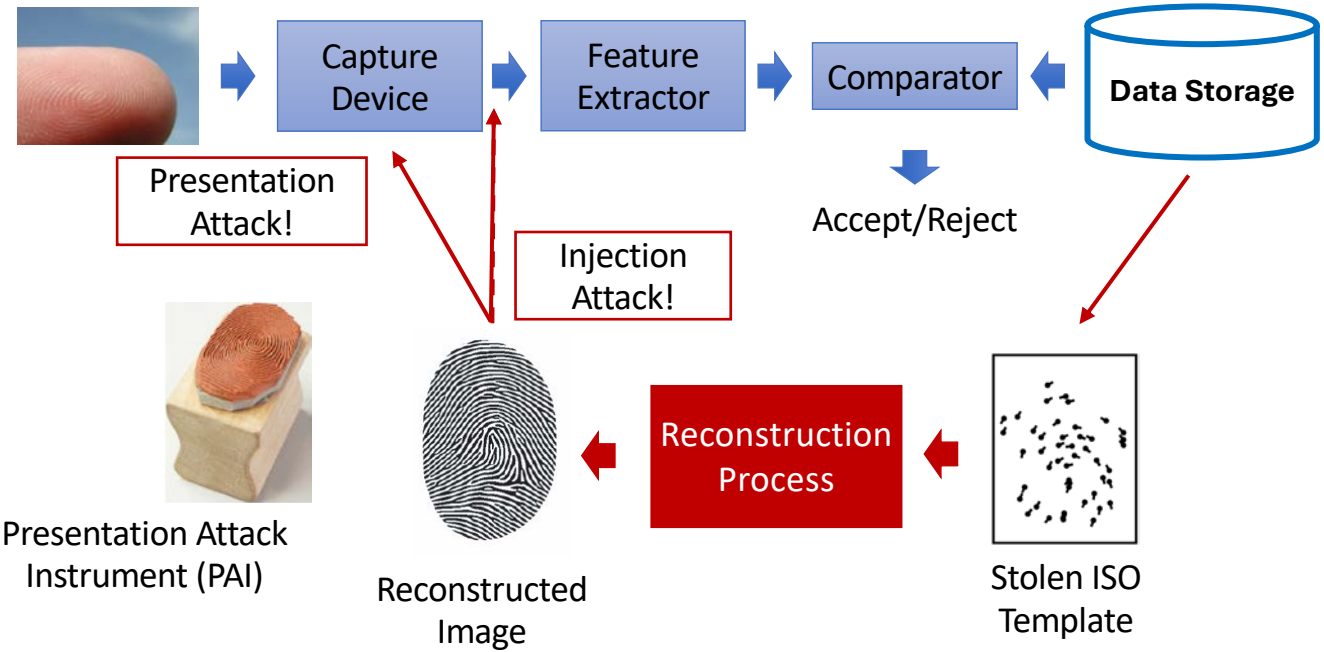
- How can we identify ourselves?
  - Something that we **know**: Passwort, PIN
  - Something that we **have**: SmartCard, USB-Token, Key
  - Something that we **are**: biometric characteristics


- ISO Definition of Biometrics: “Automated recognition of individuals based on their biological and behavioural characteristics”
  - Cannot be passed on
  - Duplicate check
  - Re-use without security compromise
  - Fine-tuning for different scenarios


# Impersonation Attacks



# Inverse Biometric Attacks

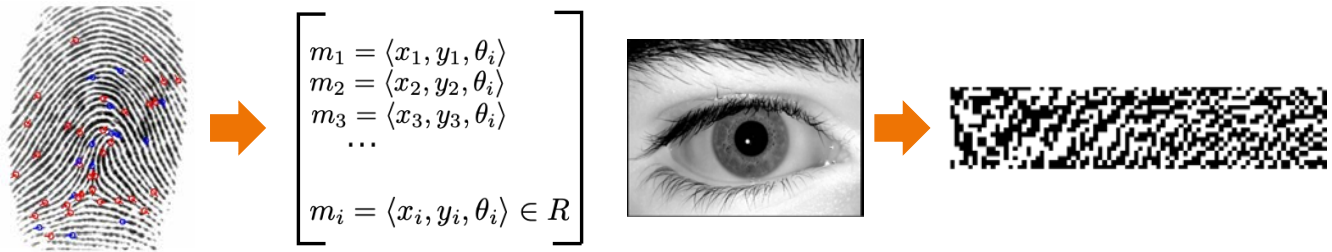



[Galbally *et al.*, *Pattern Recognition Letters*, 2009]

[Cappelli *et al.*, *IEEE Trans. PAMI*, 2007]

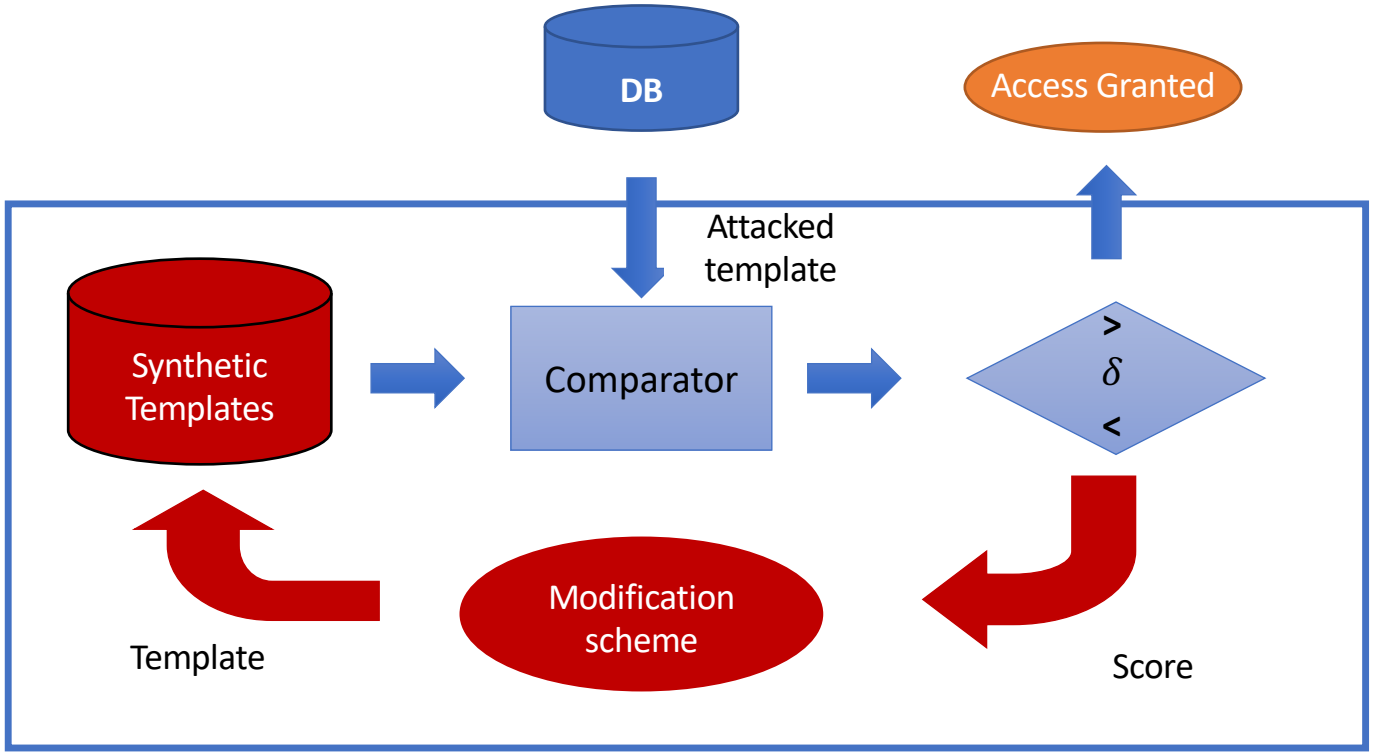
# Inverse Biometrics

- It was a common belief that the stored templates revealed no information about the biometric characteristics:



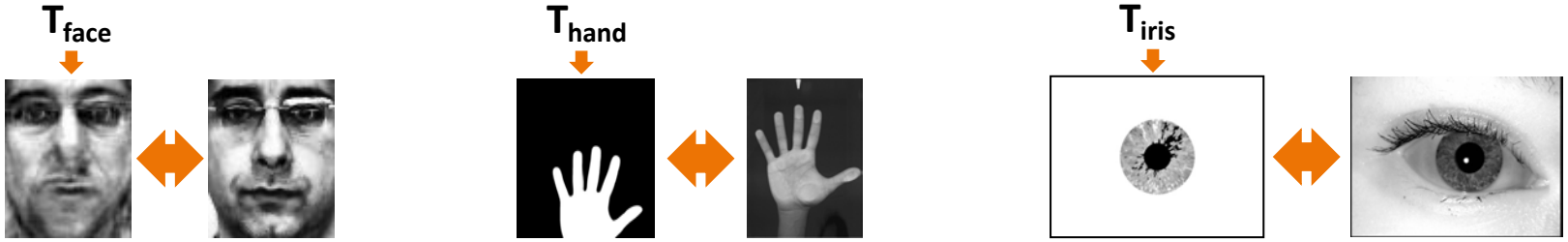

- However, biometric samples can be recovered from the stored unprotected templates

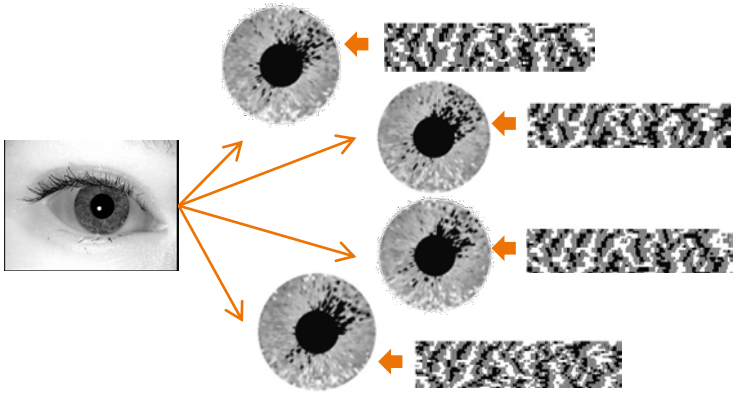
# Hill Climbing Attacks



# Hill-Climbing Attacks

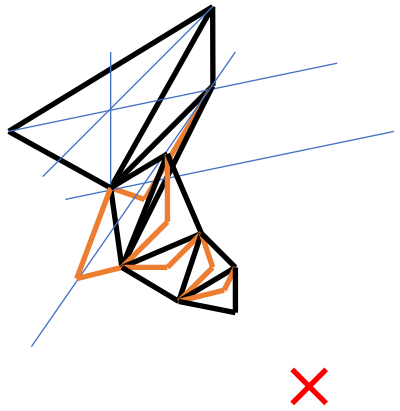
- Based on the HC algorithms, we can reconstruct biometric samples:



[M. Gomez-Barrero *et al.*, *Int. Conf. on Biometrics*, 2012]
[M. Gomez-Barrero *et al.*, *Information Sciences*, 2014]
[J. Galbally, *et al.*, *Computer Vision & Image Understanding*, 2013]

# HC based on Uphill Simplex



- New point:
  - Compute centroid:

$$\bar{\mathbf{y}} = \frac{1}{K+1} \sum_i \mathbf{y}_i$$

  - Try reflection:

$$\mathbf{a} = (1+\alpha)\bar{\mathbf{y}} - \alpha \mathbf{y}_l$$

  - Try expansion

$$\mathbf{b} = \gamma \mathbf{a} + (1-\gamma)\bar{\mathbf{y}}$$

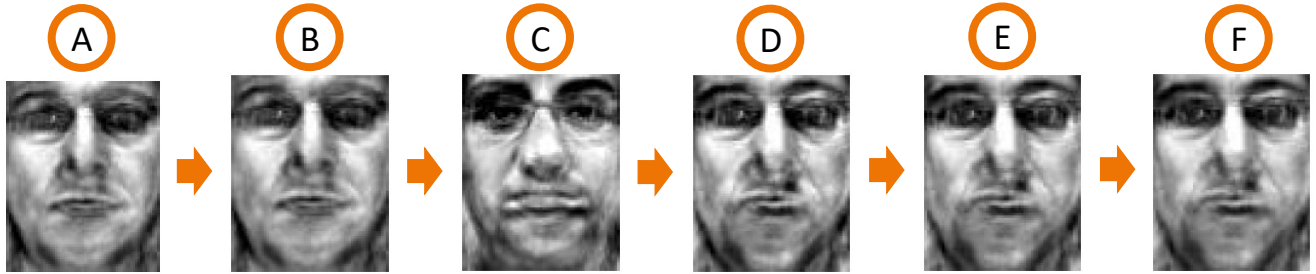
or contraction:

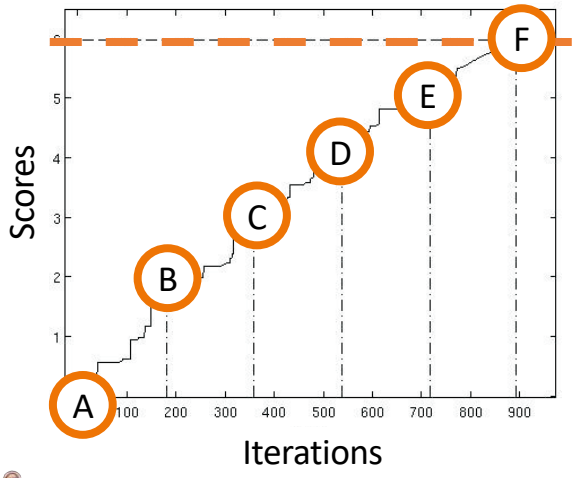
$$\mathbf{b} = \beta \mathbf{y}_l + (1-\beta)\bar{\mathbf{y}}$$

- Stopping criteria:
  - One of the points of the simplex is close enough => success
  - Maximum number of iterations allowed reached => failure

[M. Gomez-Barrero *et al.*, *Int. Conf. on Biometrics*, 2012]

# Case Study: Face




The attack was successful, and we only needed access to the scores

Target: Enrolled Sample

[M. Gomez-Barrero *et al.*, *Int. Conf. on Biometrics*, 2012]

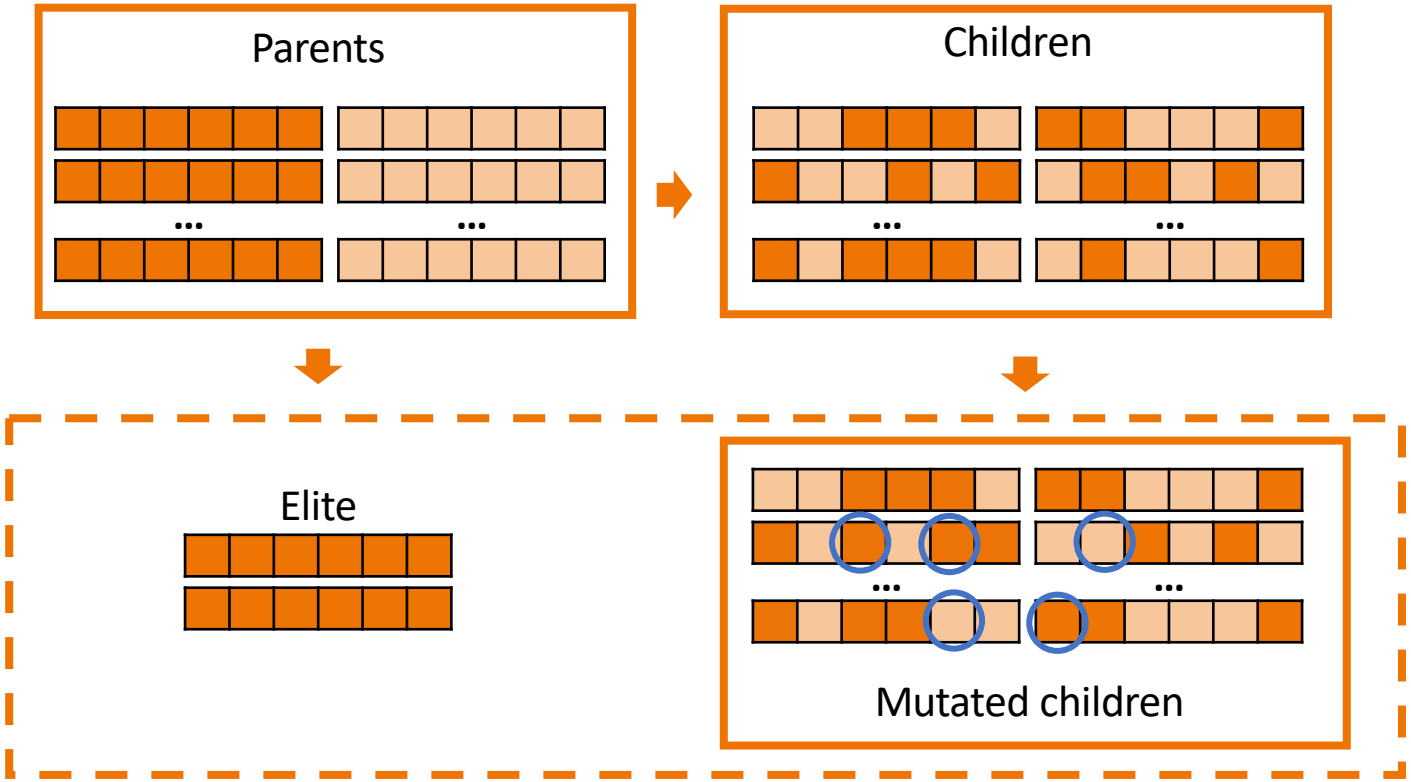
# HC based on genetic algorithms

- We start with a random population of binary individuals
- At each iteration, we generate a new population:
  - **Elite**: two best individuals remain
  - **Selection**: stochastic universal sampling
  - **Crossover**: scattered crossover
  - **Mutation**: random changes
- Our fitness function is the similarity score

- Stopping criteria:
  - One of the individuals exceeds the verification threshold => success
  - Score increase in the last generations is very small => failure
  - Maximum number of iterations allowed reached => failure

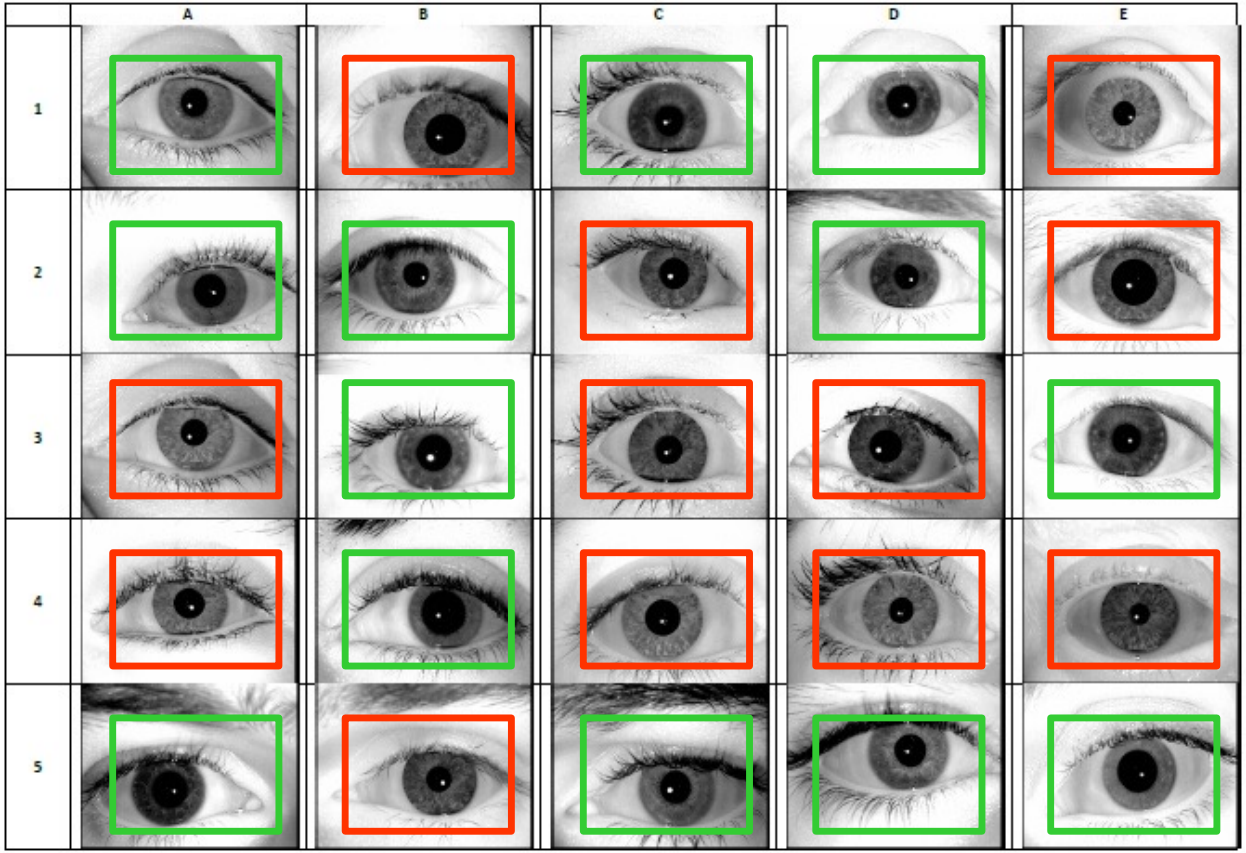
[J. Galbally, *et al., Computer Vision & Image Understanding,* 2013]

# HC based on genetic algorithms




[J. Galbally, *et al., Computer Vision & Image Understanding,* 2013]

# Can you tell them appart?



# Presentation & Morphing Attacks

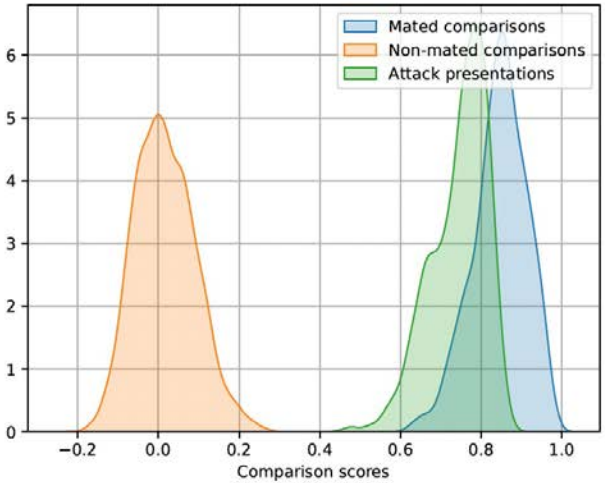
# Presentation Attack

[ISO/IEC IS 30107-1 on PAD]

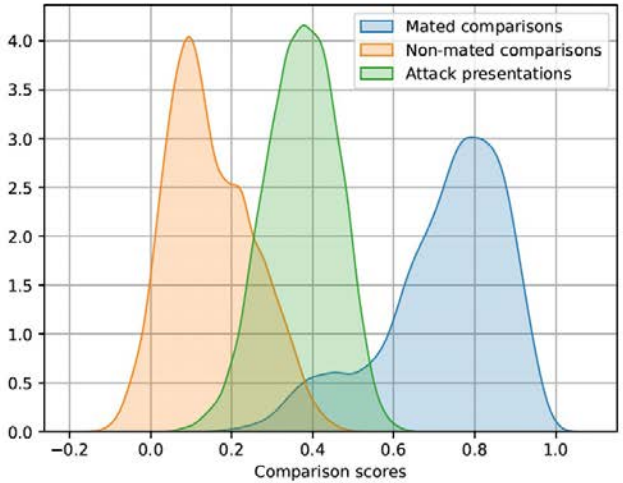
- Presentation attack: presentation to the biometric capture subsystem with the goal of interfering with the operation of the biometric system
  - **Impostor**: subversive biometric capture subject who attempts to being matched to someone else's biometric reference
  - **Identity concealer**: subversive biometric capture subject who attempts to avoid being matched to their own biometric reference

# Are PAs dangerous?

- Case study: ArcFace




(a) Training set from Replay-Mobile.




(b) Training set from CSMAD-Mobile.

[L. J. Gonzalez-Soler *et al.*, *BIOSIG*, 2022]

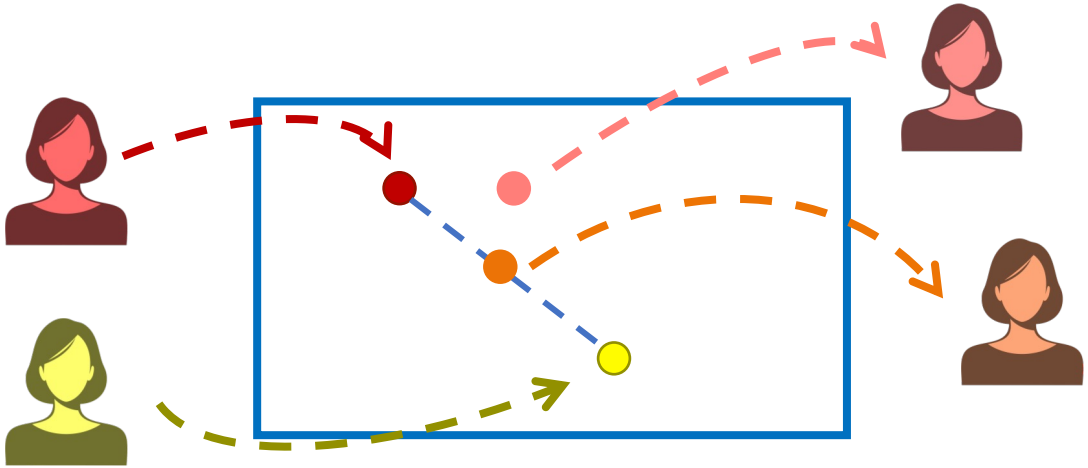
# Morphing Attacks

- Ultimate goal: modify the enrolment data so that a single reference can be positively matched to two or more subjects


- Either image or template domain
  - Average of two images based on landmarks + postprocessing
  - Use of GANs to edit the latent space

# Perfect Morphing

- Image domain produces many artifacts, easy to spot by a human examiner
- Idea: work on the latent space of the face recognition system (e.g. templates) and recover the average image



[U. M. Kelly *et al.*, *BIOSIG*, 2022]

# Countermeasures

# When is an Attack Successful?

- Common Criteria: the potential of a given attack to succeed will depend on
  - the attacker's knowledge,
  - the window of opportunity, and
  - other factors to create the attacking instrument
    - E.g., sufficient quality of the sample to extract features that match against the targeted individual's reference.

# Countermeasures

- Prevent inversion attacks:
  - Techniques as score quantization can help “up to a point”
  - Biometric template protection
- Presentation Attack Detection (PAD) + Injection Attack Detection (IAD) for the probe biometric data
- Morphing Attack Detection (MAD) for the reference data
  - And additional measures, e.g. live enrolment for passports, such as Norway or Germany (started in 2025)
- Quality checks
  - Not just image sharpness, but biometric quality checks

# Protecting the subject's privacy

[ISO/IEC IS 24745 on Biometric Information Protection]

Female, white, 30s…

Irreversibility

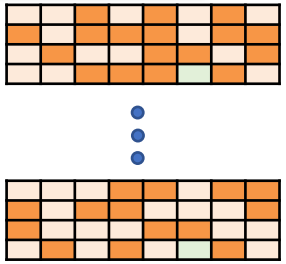
Unlinkability

=?

Renewability

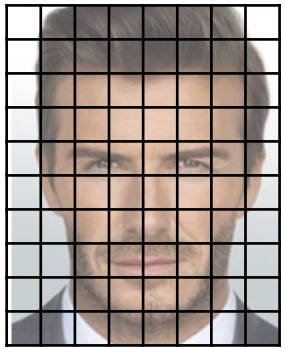
$K_1$

$K_n$



**Accuracy**, **template size** and **verification speed** must be preserved.

# BTP Based on Bloom Filters



Re-Arranged Block

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |
| 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 |

*nBits*

*nWords*

4

6

6

9

$2^{nBits}$

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 |

Bloom Filter

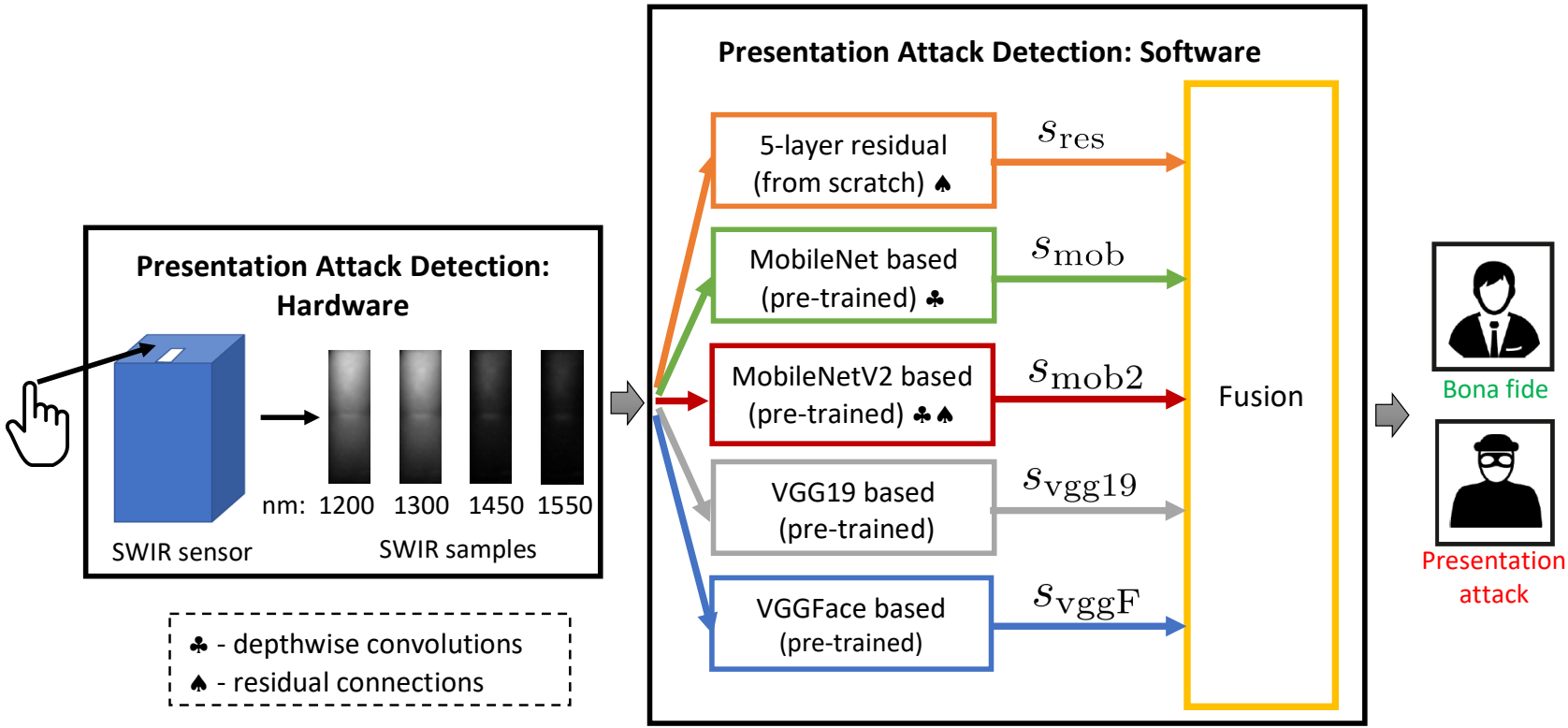
Protected Template

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | | | | 0 | | | | | 1 |
| 1 | | | | 1 | | | | | 0 |
| … | … | … | … | … | … | … | … | … | … |
| 0 | | | | 0 | | | | | 1 |

1 BF per block, of $2^{nBits}$

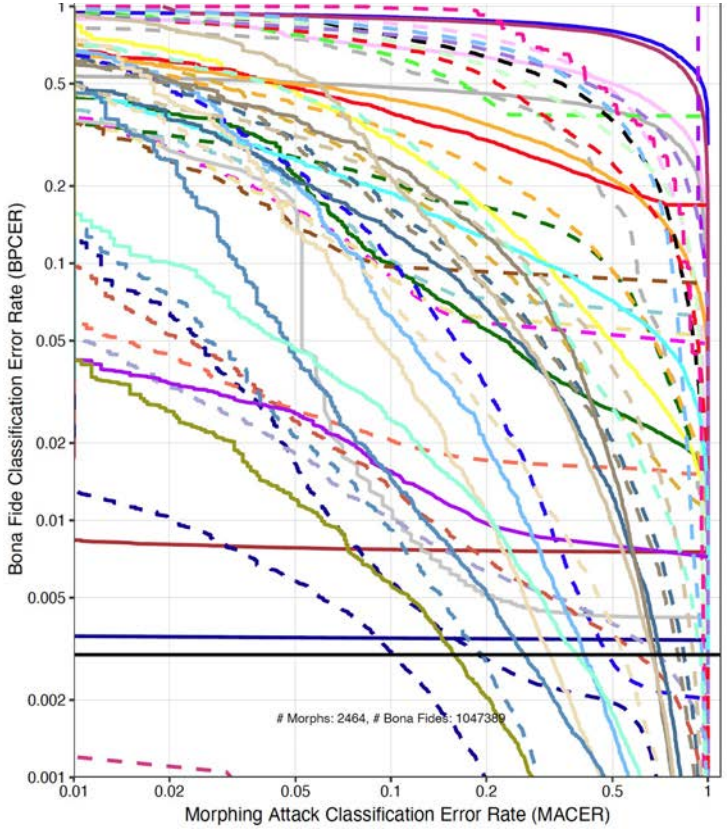
[Gomez-Barrero *et al.*, *Information Sciences* 2016]

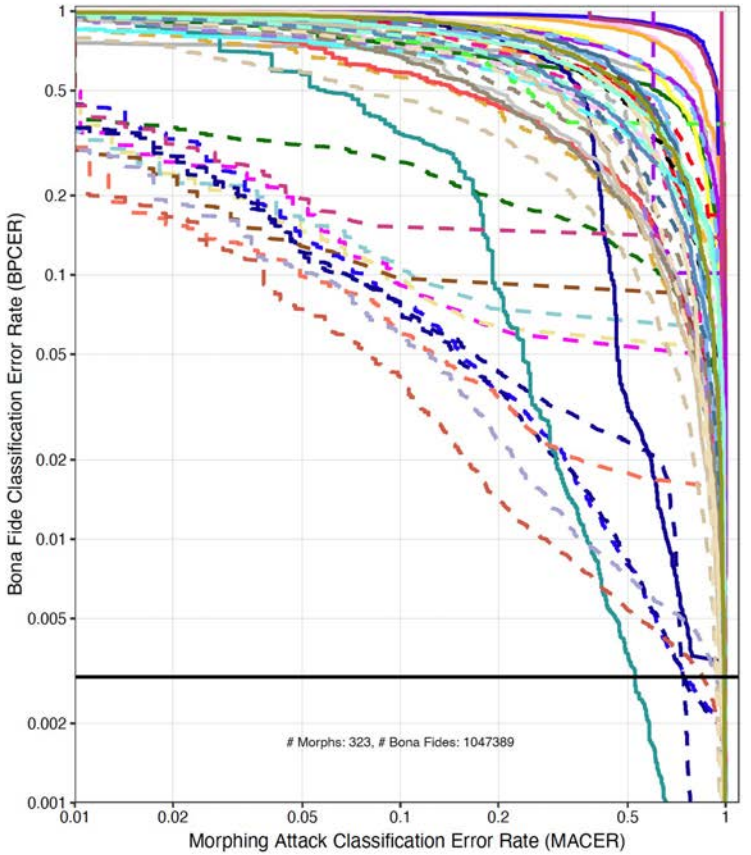
# Presentation Attack Detection (PAD)




[M. Gomez-Barrero, et al., in *Artificial Intelligence and Deep Learning in Biometric Security: Trends, Potential and Challenges*, 2021]

# Morphing Attack Detection (MAD)




NIST FRVT MORPH (Automated Morphs left, Manual Morphs right)

# Biometric Quality

[ISO/IEC IS 29794-1 on Biometric Sample Quality

- Biometric Quality: *degree to which a biometric sample meets the specified requirements for its targeted application*
  - **Character** of a sample: worn friction ridges have poor character and blepharoptosis (droopy eyelid) causes poor iris character.
  - **Fidelity** of a sample to the biometric characteristic from which it is derived.
  - **Utility** of a sample within a biometric system
    - Predicted positive or negative contribution of an individual sample to the overall performance of a biometric system

- Utility-based quality is dependent on both the character and fidelity of a sample or reference as well as the details of the specific biometric system of which performance is being evaluated
  - Utility is not necessarily a universal attribute of a sample consistent across all systems!

# Biometric Quality

- Fingerprint: NFIQ2 from NIST, standardised on ISO/IEC 29794-4
  - https://www.nist.gov/services-resources/software/nfiq-2
  - Contact-less?
- Face: OFIQ from BSI, standardised on ISO/IEC 29794-5
  - https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Freie-Software/OFIQ/OFIQ_1_0/OFIQ_1_0_node.html
- Other characteristics?
  - No standard implementation YET

# Conclusions

# Conclusions

- Impersonation Attacks on biometric systems:
  - Injection attacks of inverted templates / replay attack
  - Presentation attacks on the capture device
  - Morphing attacks on the reference

- Countermeasures:
  - Privacy protection through biometric template protection
  - Presentation Attack Detection (PAD)
  - Morphing Attack Detection (MAD)
  - Injection Attack Detection (IAD)
  - Biometric Quality

# Further Reading


- R. Cappelli, D. Maio, A. Lumini, D. Maltoni, “Fingerprint image reconstruction from standard templates”, IEEE Trans. On Pattern Analysis and Machine Intelligence, vol. 29, no. 9, pp. 1489-1503, 2007
- J. Galbally, R. Cappeli, A. Lumini, G. Gonzalez-de-Rivera, D. Maltoni, J. Fierrez, J. Ortega-Garcia, D. Maio, “An evaluation of direct attacks using fake fingers generated from ISO templates”, Pattern Recongnition Letters, vol. 31, no. 8., pp. 725-732, 2010
- M. Gomez-Barrero, J. Galbally, J. Fierrez, J. Ortega-Garcia, “Face verification put to test: A hill-climbing attack based on the uphill-simplex algorithm”, Proc. Int. Conf. on Biometrics, 2012
- J. Galbally, A. Ross, M. Gomez-Barrero, J. Fierrez, J. Ortega-Garcia, “Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms”, Computer Vision & Image Understanding, vol. 117, no. 10, pp. 1512-1525, 2013
- M. Gomez-Barrero, J. Galbally, A. Morales, M. A. Ferrer, J. Fierrez, J. Ortega-Garcia, “A novel hand reconstruction approach and its application to vulnerability assessment”, Information Sciences, vol. 268, pp. 103-121, 2014
- L. J. Gonzalez-Soler, K. A. Barhaugen, M. Gomez-Barrero, C. Busch, “When Facial Recognition Systems become Presentation Attack Detectors”, Proc. BIOSIG, 2022
- U. M. Kelly, L. Spreeuwers, R. Veldhuis, “Worst-case morphs: a theoretical and a practical approach”, Proc. BIOSIG, 2022
- *M. Gomez-Barrero, J. Galbally, “Reversing the irreversible: A survey on inverse biometrcs”, Computers & Security, vol. 90, pp. 101700, 2020*
- ***M. Gomez-Barrero, “Vulnerabilities of Biometrics Systems: Inverse Biometrics, Morphing Attacks, and Evaluation Metrics”, in Privacy and Security Matters in Biometric Technologies, Ed. R. Veldhuis, M. Todisco, F. Deravi, J. Fierrez, E. Kindt, B. M. Østvold, C. Busch, N. Evans, S. Marcel, Springer, To appear (2025)***
- **Handbook of Biometric Template Protection, Springer, eds. V. Krivokuca Hahn, M. Gomez-Barrero, A. Ross, S. Marcel, 2025 (soon)**
  - **EAB Workshop on BTP on October 29 and 30, 2025**

# BioML Lab

**Marta Gomez-Barrero**

marta.gomez-barrero@unibw.de

https://www.marta-gomez-barrero.com/
https://www.unibw.de/bioml-en

Research Institute
Cyber Defence
Universität der Bundeswehr München