Challenges for Automated Face Recognition Systems

IbPRIA 2025
12th Iberian Conference on Pattern Recognition and Image Analysis
2025-07-01

Christoph Busch
copy of slides available at:
https://christoph-busch.de/about-talks-slides.html

ATHENE / Hochschule Darmstadt, Germany
Norwegian University of Science and Technology (NTNU), Norway

ATHENE

European Association for Biometrics
eab
Human Identity in Europe

NTNU

Challenges for Face Recognition

Critical factors for Face Recognition Systems (FRS):

- Pose
- Illumination
- Expression and Ageing



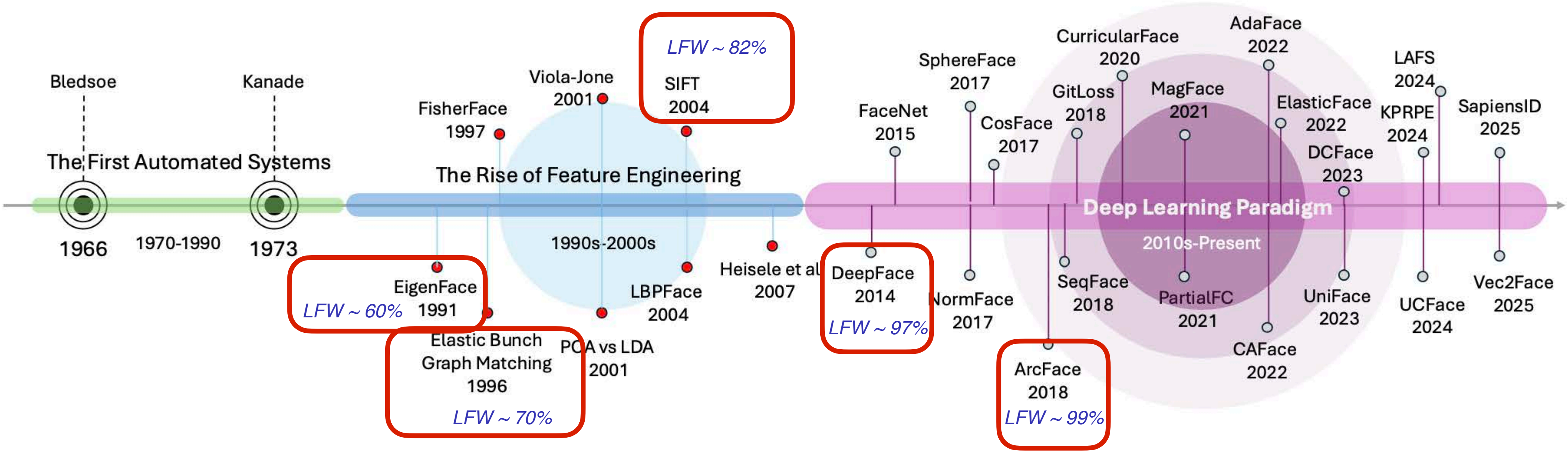

2001

2025

Evolution of Face Recognition Algorithms

Testing on more challenging facial images

- Identification rate for Labeled Face in-the-Wild (LFW)
  http://vis-www.cs.umass.edu/lfw/



[Kim2025] M. Kim, A. Jain, X. Liu: “50 Years of Automated Face Recognition“, arXiv, (2025)

[Huang2007] G. Huang, M. Ramesh, T. Berg, E. Learned-Miller: “Labeled Faces in the Wild: A Database for Studying Recognition in Unconstrained Environments“, TR, University of Massachusetts, (2007)

Progress of FR Algorithms Accuracy

NIST: Face Recognition Technology Evaluations (FRTE)

- Reduction of error rates

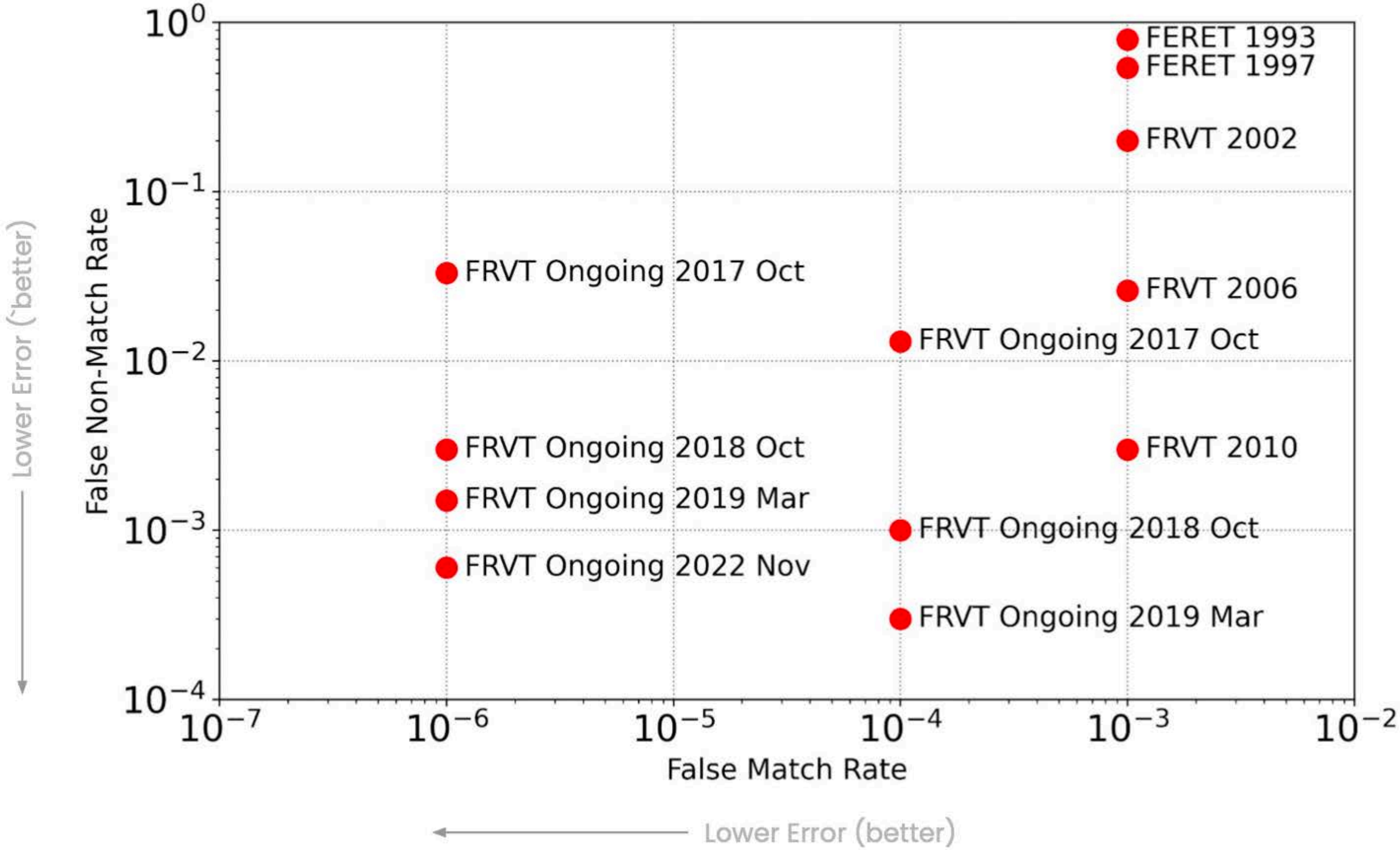


Image Source: Brendan Klare (2023)

- NIST FRTE:
  https://www.nist.gov/programs-projects/face-technology-evaluations-frtefate

Limits of FR Algorithms Accuracy

NIST: Face Recognition Technology Evaluations (FRTE)

- Face recognition of twins

Developer	Algorithm	Score	FMR	Outcome
IDEMIA	009	4924.38	< 5.049e-07	FALSE MATCH!
PARAVISION	010	0.32240	< 5.049e-07	FALSE MATCH!

Source: Patrick Grother (2024)

Source: Mei Ngan (NIST) and her sister

- Twins are common: 3% of all newborn in the USA
- Identical twins are 25% of all twins (~0.75% of all newborn in the USA)

Challenges for Face Recognition

Critical factors for Face Recognition Systems (FRS):

- Pose
- Illumination
- Expression and Ageing
- Presentation Attacks
- Face Image Quality
- Morphing Attack Detection
- Biometric Template Protection
- Fairness of Algorithms

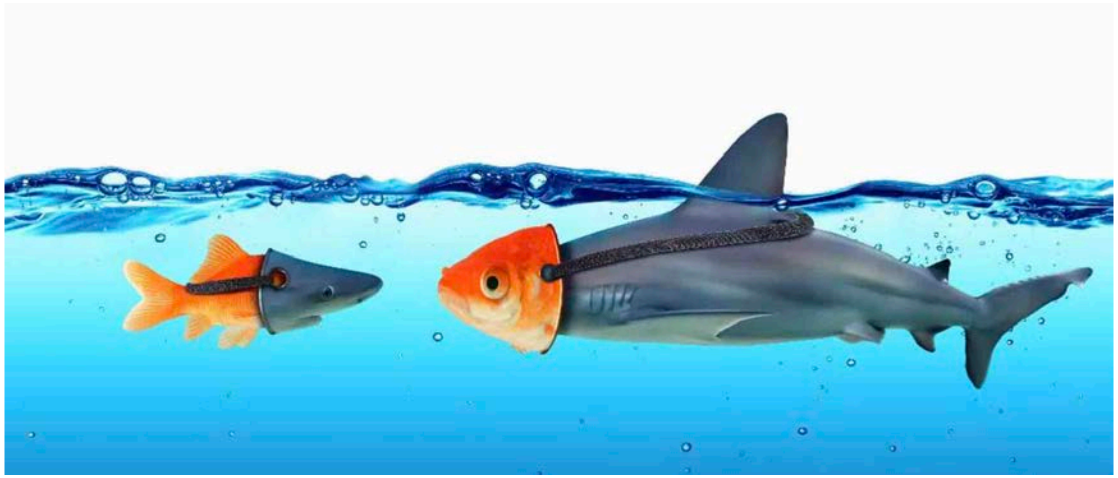



2001

2025

[B2024] C. Busch: "Challenges for Automated Face Recognition Systems", in Nature Reviews Electrical Engineering, (2024), https://christoph-busch.de/files/Busch-NatureReview-ChallengesFRS-2024.pdf

Presentation Attack Detection



Presentation Attacks

Definitions in ISO/IEC 30107 PAD - Part 1: Framework

- **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 discrimination between bona-fide presentations and biometric presentation attacks

https://www.iso.org/standard/79520.html

Presentation Attacks

Impostor

- Impersonation attack
  - Positive access 1:1 (two factor application)
  - Positive access 1:N (single factor application)
- Finding a look-a-like
- Artefact presentation

Concealer

- Evasion from recognition
  - Negative 1:N identification (watchlist application)
- Depart from standard pose

- Evade face detection

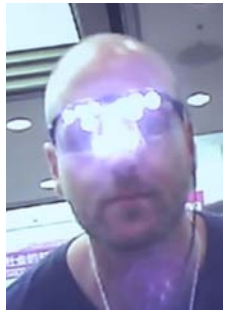


Image Source: https://www.youtube.com/watch?v=LRj8whKmN1M

Presentation Attacks

Definitions in ISO/IEC 2382-37: Vocabulary

- **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

https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-3:v1:en

Presentation Attack Detection - Testing

Definition of detection capabilities metrics

- Testing the PAD subsystem with
  false-negative and false-positive errors:

- **Attack presentation classification error rate (APCER)**
  proportion of attack presentations using the same PAI species incorrectly classified as bona fide presentations in a specific scenario

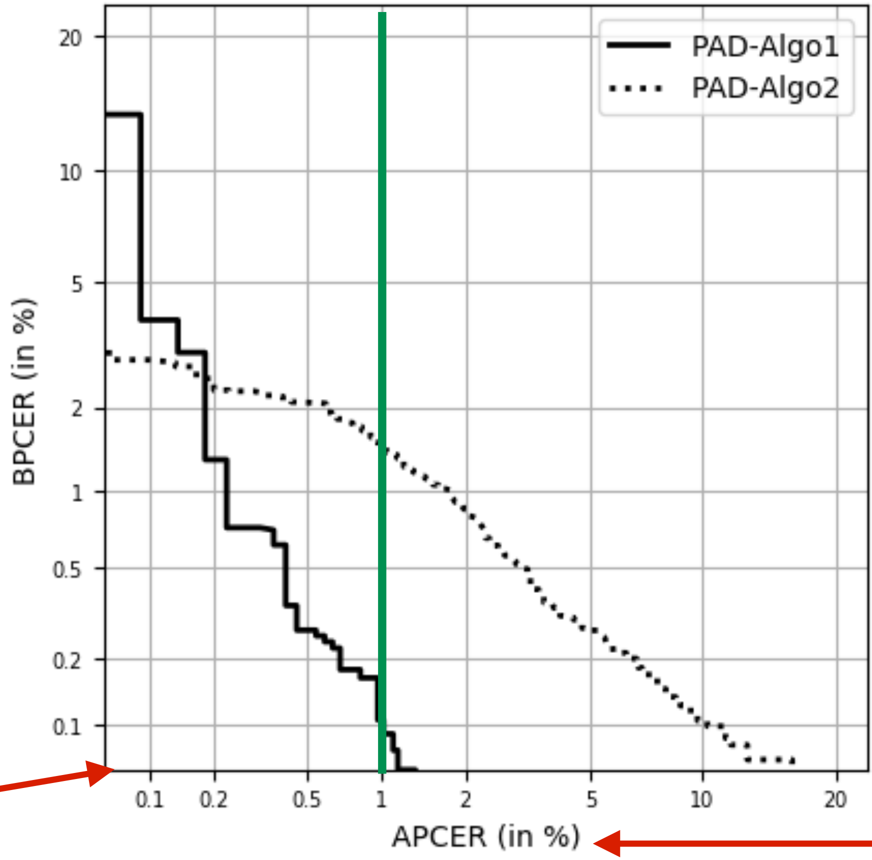
- **Bona fide presentation classification error rate (BPCER)**
  proportion of bona fide presentations incorrectly classified as attack presentations in a specific scenario

Source: ISO/IEC 30107-3

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-3

- DET curve reports operating points for various thresholds showing security measures versus convenience measures
- Example:



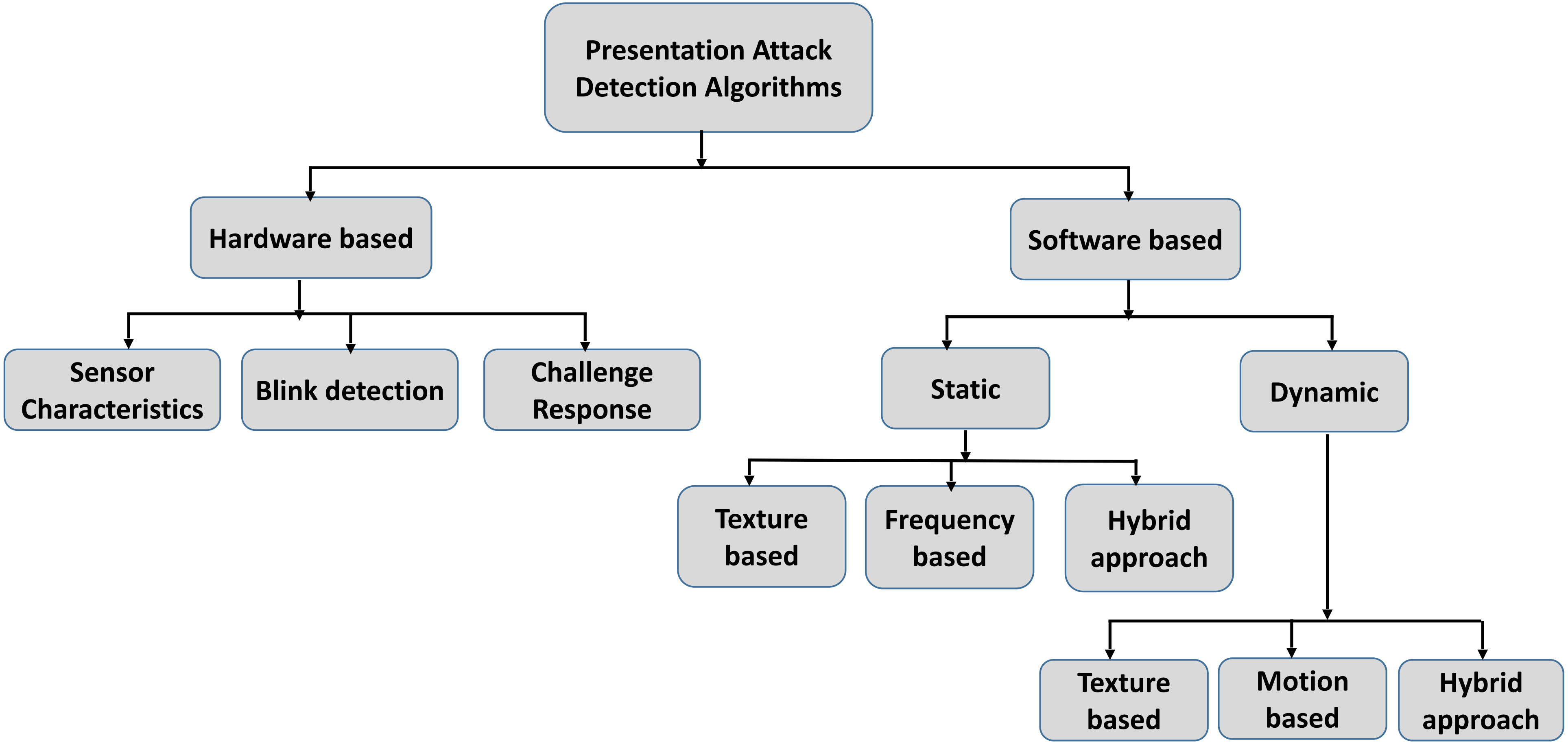
convenience measure

Ideal:
APCER - low
BPCER - low

security measure (strength of function)

Presentation Attack Detection

Taxonomy



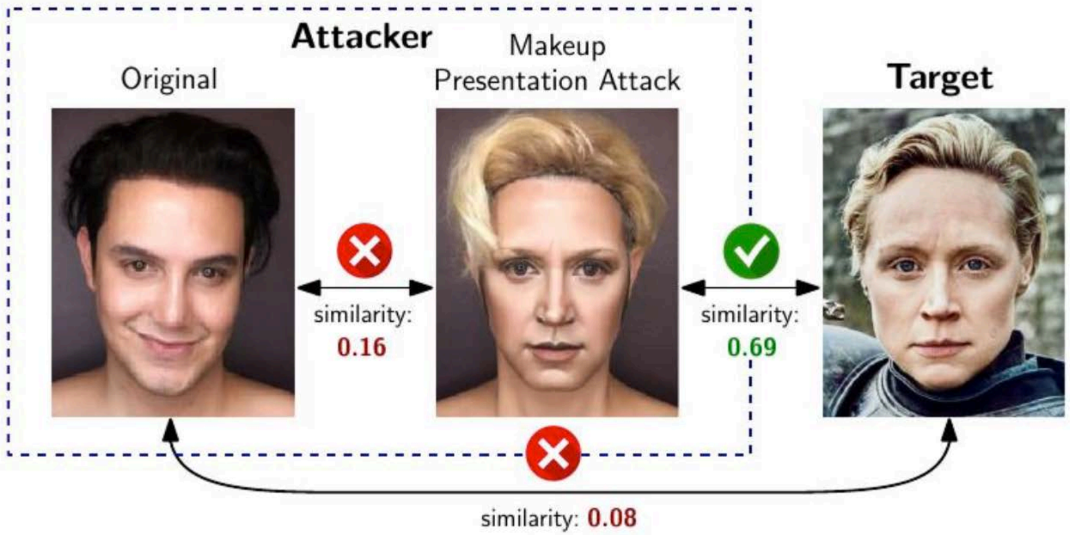
[RB2017] R. Raghavendra, C. Busch: "Presentation Attack Detection methods for Face Recognition System - A Comprehensive Survey", in ACM Computing Surveys, (2017)
https://christoph-busch.de/files/Raghavendra-FacePAD-survey-ACM-2017.pdf

Presentation Attack Detection

Makeup for impersonation

- Liveness detection is not sufficient
- Detection difficult since bona fide users may also apply makeup

(a) Before (b) After (c) Target



[RDB2020] C. Rathgeb, P. Drozdowski, C. Busch: "Makeup Presentation Attacks: Review and Detection Performance Benchmark", in IEEE Access, (2020)

Face Image Quality

Face Image Quality

Motivation for Face Image Quality Assessment (FIQA)

- Quality matters, especially in large-scale databases and with diverse application scenarios.
  - The European Entry Exit System (EES) will start October 2025
    - Will be applied to all external Schengen borders
    - Central register to record all entries/exists to the Schengen area
      https://travel-europe.europa.eu/ees_en

    - For each traveller a record with facial image and fingerprint images
    - Operated by eu-LISA and 29 countries

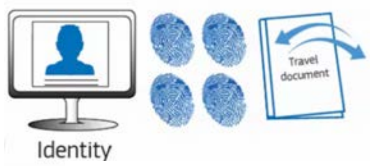


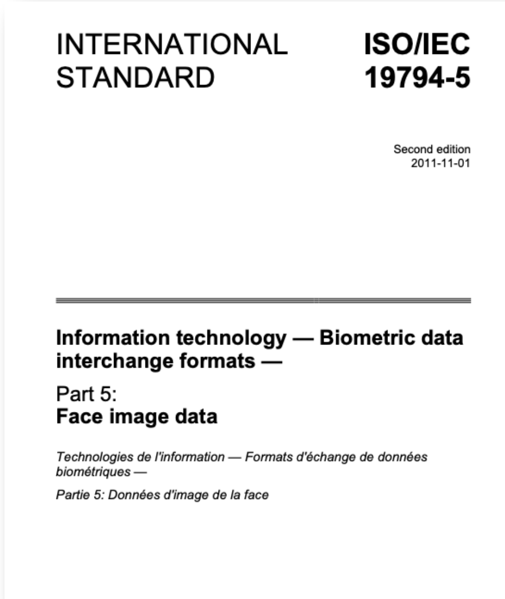
Image Source: eu-LISA

- Standardisation of minimal quality and harmonisation is essential for (semantic) interoperability.

Quality Requirements for Facial Images

The requirement in EES implementing decision 2019/329

- *„The quality of the facial images, … and with the image requirements of ISO/IEC 19794-5:2011 Frontal image type*



INTERNATIONAL STANDARD

ISO/IEC 19794-5

Second edition
2011-11-01

Information technology — Biometric data interchange formats —

Part 5:
Face image data

Technologies de l'information — Formats d'échange de données biométriques —

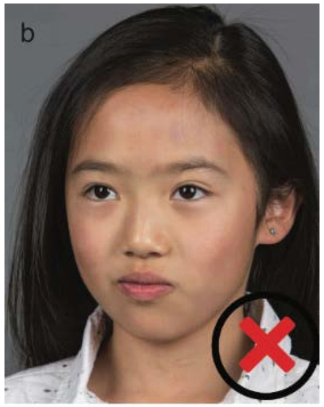
Partie 5: Données d'image de la face

What does that mean?

Data subjects need actionable feedback

- If quality is poor, then what went wrong?

Compliant image



Pose

Eyes open

Mouth open

Inhomogenous background

Source: ISO/IEC 39794-5

Measures for Facial Images

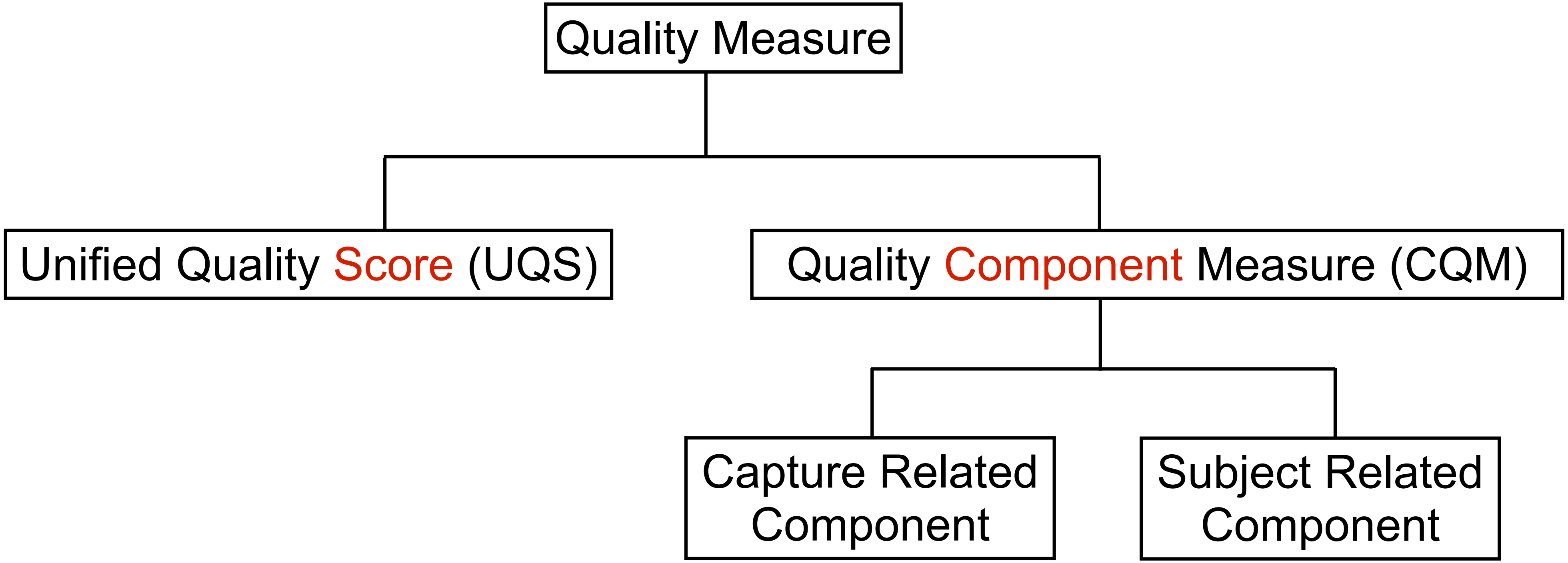
How to develop face image quality measures

- Standardisation
- International Organization for Standardization, ISO/IEC 29794-5, Information technology - Biometric sample quality - Part 5: Face image data,
  https://www.iso.org/standard/81005.html
  - Providing measures for requirements from ISO/IEC 19794-5:2011 and ISO/IEC 39794-5:2019
    - Use-1: Reference image for MRTD
    - Use-2: Reference image for Live-Enrolment at EES Kiosk
    - Use-3: Probe images (e.g. ABC gate)

Quality Measures - Framework Standard

Quality assessment algorithms

- According ISO/IEC 29794-1
  https://www.iso.org/standard/79519.html



- Higher UQS and CQM imply higher biometric utility

ISO/IEC 29794-5: Face Image Quality

ISO/IEC 29794-5 quality measures in detail

#	Face image quality measure
1.	Quality score (unified)
2.	Background uniformity
3.	Illumination uniformity
4.	Luminance mean
5.	Luminance variance
6.	Under-exposure prevention
7.	Over-exposure prevention
8.	Dynamic range
9.	Sharpness
10.	No compression artefacts
11.	Natural colour
12.	Single face present
13.	Eyes open
14.	Mouth closed
15.	Eyes visible
16.	Mouth occlusion prevention
17.	Face occlusion prevention
18.	Inter-eye distance
19.	Head size
20.	Leftward crop of face in image
21.	Rightward crop of face in image
22.	Margin above face in image
23.	Margin below face in image
24.	Pose angle yaw frontal alignment
25.	Pose angle pitch frontal alignment
26.	Pose angle roll frontal alignment
27.	Expression neutrality
28.	No head covering

Image Source:ISO/IEC 29794-5

Unified Quality Score

Capture device related

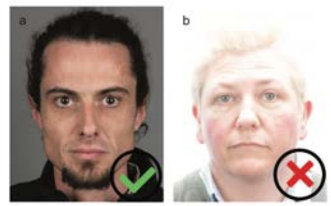


Image Source: ISO/IEC 39794-5

Explainable Quality Assessment

Subject related

Image Source: ISO/IEC 39794-5

Open Source Face Image Quality (OFIQ)

Approach

- Library with quality assessment algorithms
- Open source https://github.com/BSI-OFIQ/OFIQ-Project
  - Commercial use is enabled and foreseen
- Support for major OS platforms (including mobile OS)
  - C/C++
- Serves as reference implementation of ISO/IEC 29794-5
  - Providing target values for conformance tests
- Selection criteria for integrated algorithms
  - Accuracy (NIST FATE SIDD evaluation)
    https://pages.nist.gov/frvt/reports/quality_sidd/frvt_quality_sidd_report.pdf
  - Low computational complexity
  - Liberal license (MIT or alike)

OFIQ - Unified Quality Score

General, holistic unified quality score (OFIQ-UQS)

- Determine an overall quality score for the picture
  - CNN MagFace (iResNet 50 model)
- Shows good prediction of face recognition scores

OFIQ-UQS=84

OFIQ-UQS=61

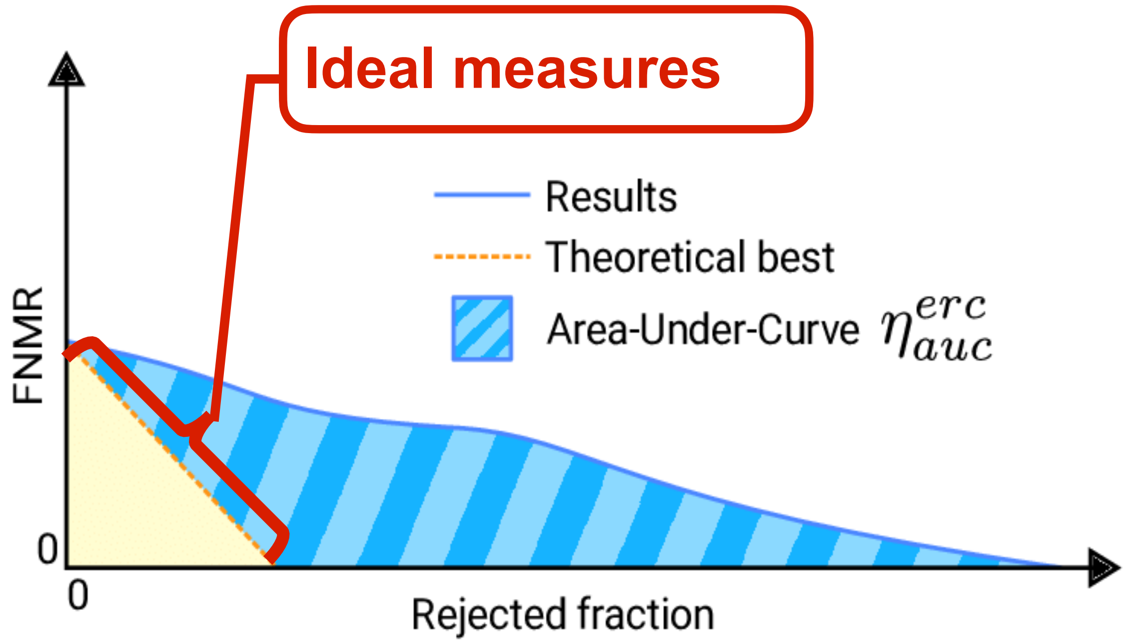
OFIQ-UQS=26

OFIQ-UQS=7

OFIQ - Unified Quality Score

Prediction of low face recognition scores

- OFIQ is the best performing algorithm in NIST SIDD Error versus Discard Characteristic (EDC) curves
  - How much is the FNMR reduced, when poor images are discarded/rejected?



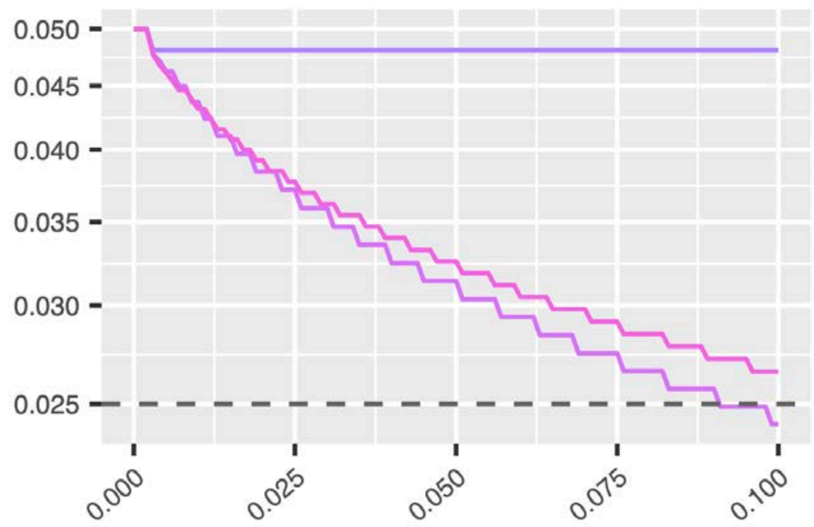


Image Source:NIST FATE SIDD report

Open Source Face Image Quality (OFIQ)

Pre-processing for quality measures

- Face Detection: bounded box of all detected faces
- Face Landmark Estimation: localization of 98 key points
- Alignment: bring eyes on the same height
- Face Occlusion Segmentation: identify un-occluded region
- Face Parsing: identify different regions of subject in the image (eyes, eye brows, nose, lips, skin / neck, ears, hair / glasses, clothes, hats, earrings, necklaces / background)

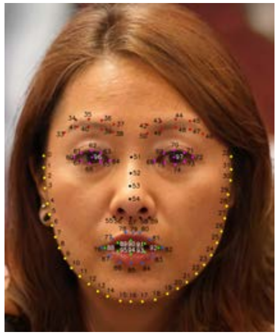


Image Source: OFIQ public report and ISO/IEC FDIS 29794-5

OFIQ - Quality Components

Example algorithm: Sharpness

- Detecting the sharpness of an image
- Is the subject in focus or the background?

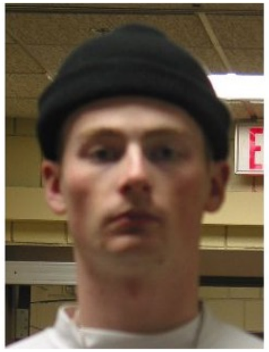
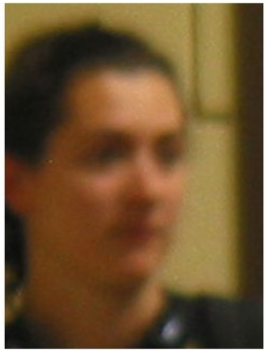




Image Source: FRGCv2 database

- Restricted to landmarked region
  - Laplacian Filter
  - Random Forest classifier

Image Source: OFIQ public report

OFIQ - Quality Components

Example algorithm: Mouth Closed

- Detecting if the most is closed
- Algorithms based on landmarks
- Maximum distance between lips

- Normalized by distance T between eye‘s midpoint and chin

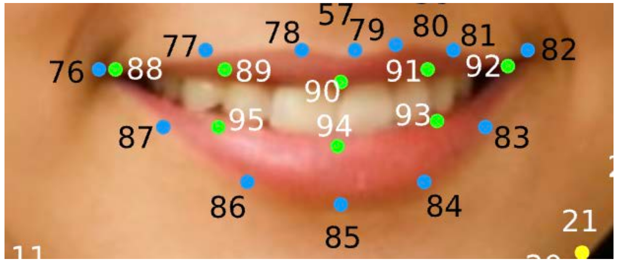


Image Source:ISO/IEC FDIS 29794-5

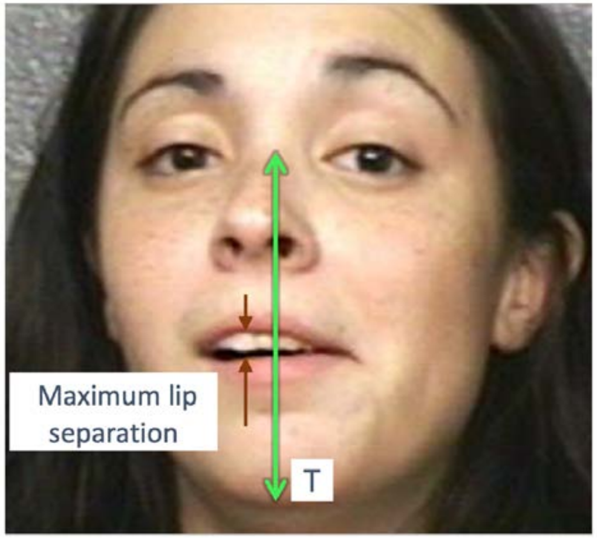


Image Source:NIST FATE SIDD report

OFIQ - Quality Components

Quality Component: Expression Neutrality

- Expression neutrality as quality component
  - Reduced biometric performance for extreme facial expressions
- Known fact:
  - Best-possible utility through neutral expressions
- Goal:
  Quantify expression neutrality

[GRVB2023] M. Grimmer, C. Rathgeb, R. Veldhuis, C. Busch: "NeutrEx: A 3D Quality Component Measure on Facial Expression Neutrality", in Proceedings of International Joint Conference on Biometrics (IJCB), (2023)

[GVB2024] M. Grimmer, R. Veldhuis, C. Busch: "Efficient Expression Neutrality Estimation with Application to Face Recognition Utility Prediction", in Proceedings of 12th International Workshop on Biometrics and Forensics, (2024)

Outlook for OFIQ

Perspective

- OFIQ will (likely) replace the proprietary FIQA
  - wherever used
  - avoid a vendor-lock-in
- OFIQ 2.0 project has already started

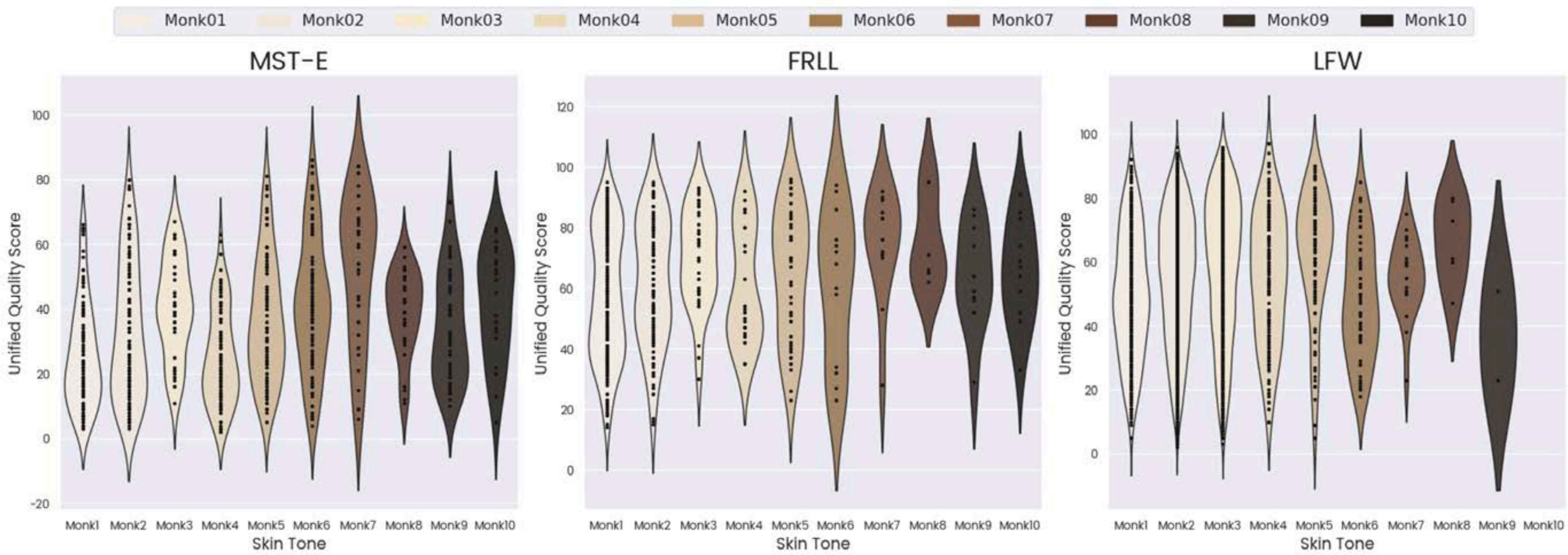
Take home information on face image quality

- OFIQ open source code:
  https://github.com/BSI-OFIQ/OFIQ-Project
- OFIQ public report
  https://github.com/BSI-OFIQ/OFIQ-Project/blob/main/doc/reports/Public_Report_V1.1_2024_(
- NIST test report:
  https://pages.nist.gov/frvt/reports/quality_sidd/frvt_quality_sidd_report.pdf
- Face image quality website:
  https://christoph-busch.de/projects-ofiq.html

Face Image Quality - Future work

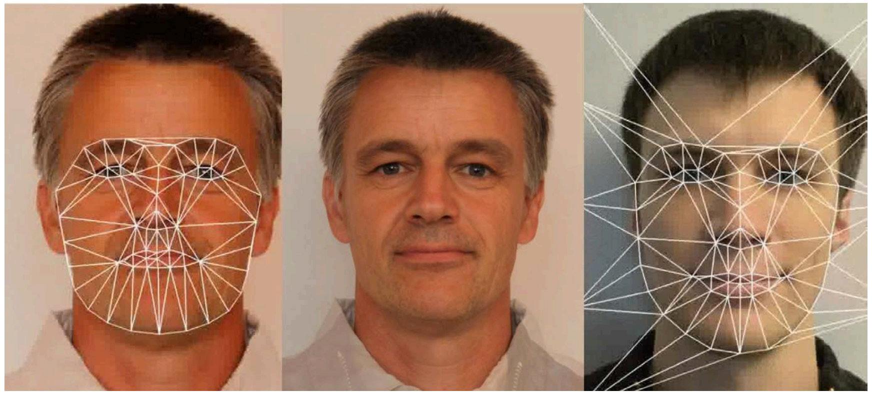
Open research tasks for OFIQ 2

- Further innovation of quality measures
- Add missing components (e.g. motion blur)
- Investigate demographic variability
  - Unified quality score distributions across MST 10 skin tone scale



[KRRB2024] W. Kabbani, K. Raja, R. Raghavendra, C. Busch: "Demographic Differentials in Face Image Quality Measures", in Proceedings of the IEEE 23rd International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, September 25-27, (2024)

Morphing Attack Detection



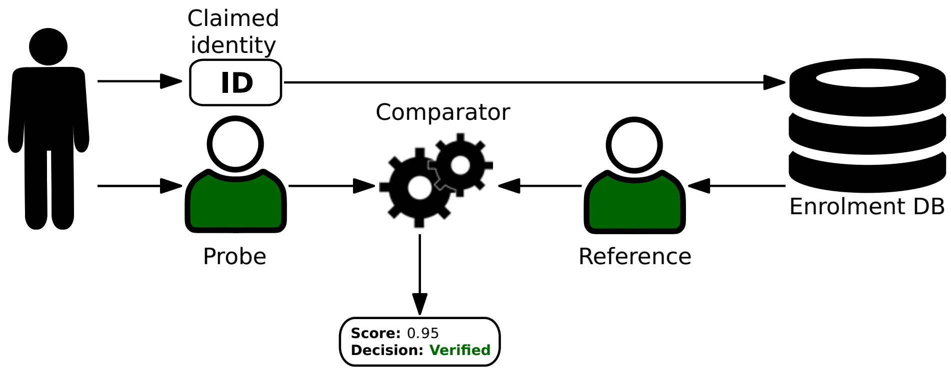
Face Recognition at Airports

Automated Border Control (ABC) gates

- Semi-supervised control

Goals:

- Self-Service to increase throughput
- Biometric verification



Biometric probe

Biometric reference

Source: Bundespolizei

? =

Border Security depends on an Anchor

The passport is the security anchor

- One individual - one passport

Principle of unique link of ICAO

- ICAO - International Civil Aviation Organisation
- One individual - one passport

- ICAO 9303 part 2, 2006:
  *„**Additional security measures:** inclusion of a machine verifiable biometric feature linking the document to its legitimate holder“*

image source: https://pixabay.com/de/vectors/tick-sternchen-kreuz-rot-gr%C3%BCn-40678/

Border Security depends on an Anchor

Principle of unique link of ICAO

- One individual - one passport

We don’t want this principle of unique link to be broken

- Multiple individuals - one passport

image source: https://pixabay.com/de/vectors/tick-sternchen-kreuz-rot-gr%C3%BCn-40678/

What is Morphing?

In our real world morphing can become a threat

- with a criminal and an accomplice as actors
- take the criminal
- and the accomplice
- morphing can transform one face image into the other

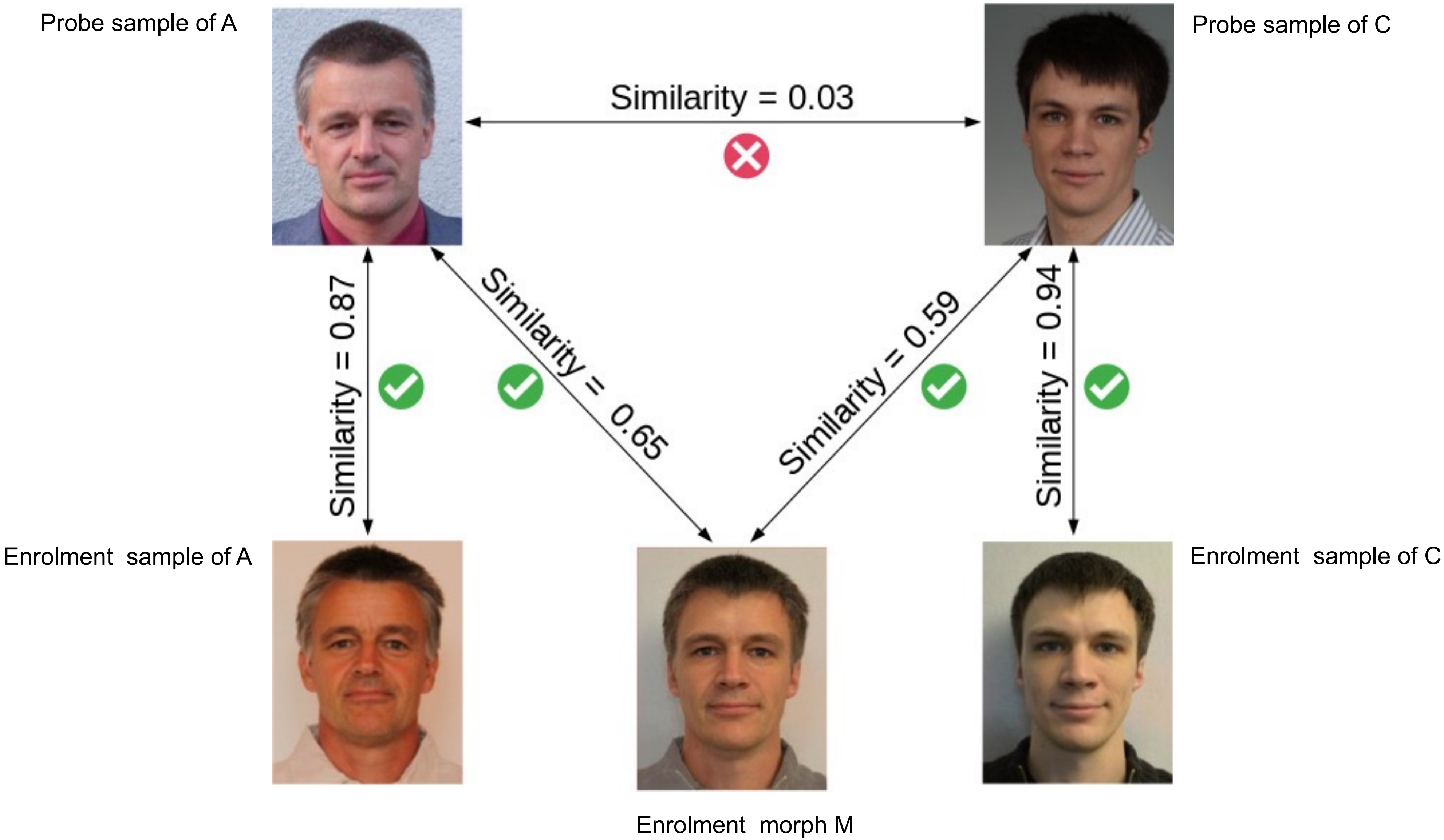
What is Morphing?

In our real world morphing can become a threat

- with a criminal and an accomplice as actors
- take the criminal
- and the accomplice
- morphing can transform one face image into the other
- and you can stop half way in the transformation

Problem: Morphing Attacks

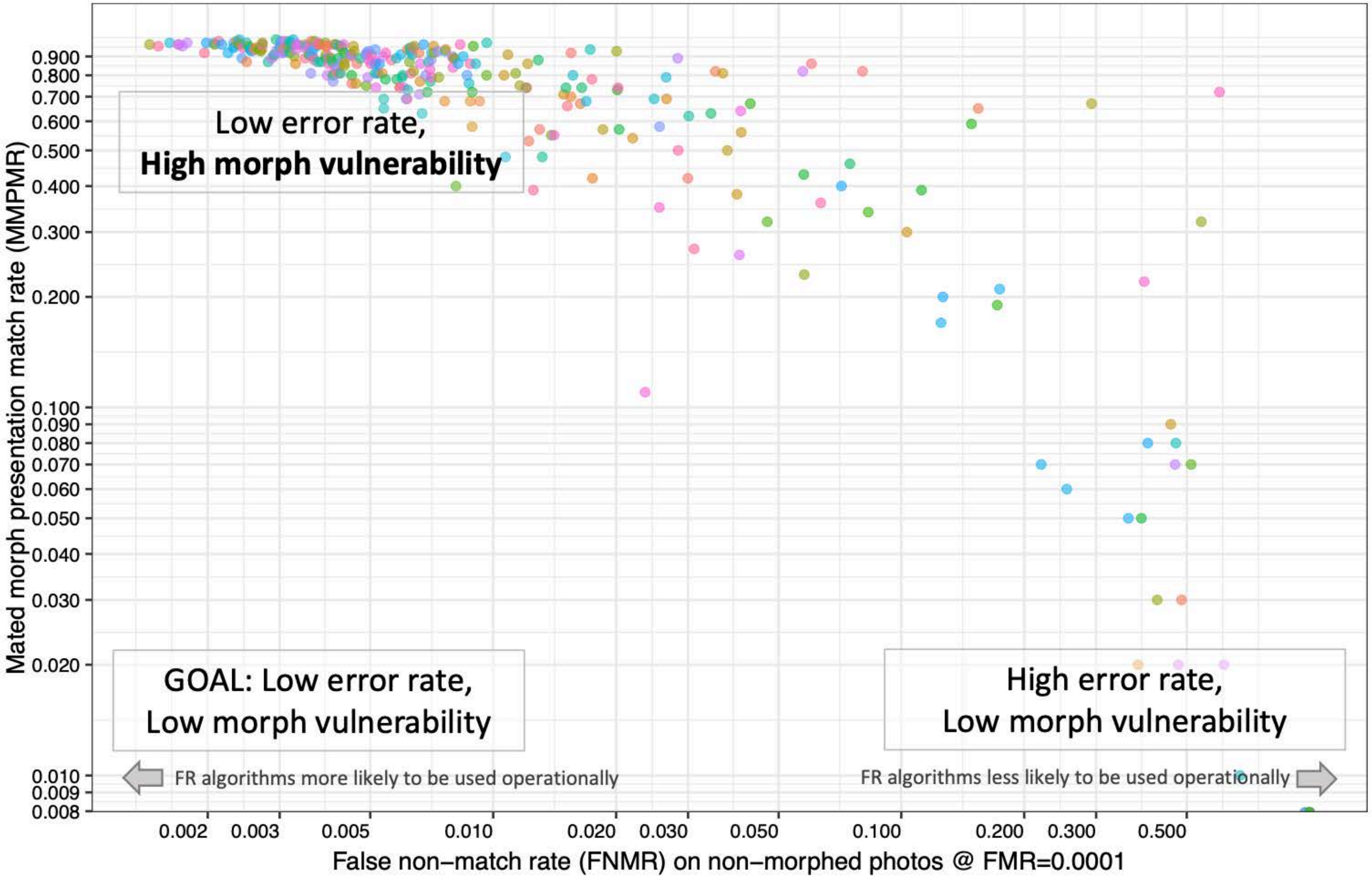
Verification against morphed facial images



Scale of the Problem: Vulnerability of FRS

NIST IR 8430 report on FRS vulnerability [Ngan2022]

- Accurate FRS are more vulnerable!



[Ngan2022] NIST IR 8430: "FRVT MORPH: Utility of 1:N Face Recognition Algorithms for Morph Detection“, 2022
https://pages.nist.gov/frvt/reports/morph/frvt_morph_4A_NISTIR_8430.pdf

Scale of the Problem: Vulnerability of FRS

The morphing attack paradox

- The better the face recognition system (FRS)
  - the lower the false non-match rate (FNMR)
  - the more tolerant is the FRS at the defined FMR (e.g. 0.01 %)
- The more tolerance the FRS has
  - the more vulnerability we can observe

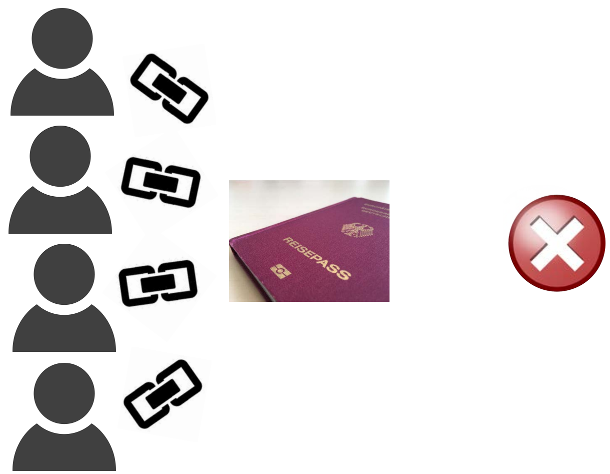
- Accurate FRS are more vulnerable!

Problem: Morphing Attacks

Is it a really problem ? - YES!

Report by the Slovenian Police [Tork2021]

- Reported in September 2021 that
  in last 12 month more than 40 morphing cases
  - were detected at Airport Police in Ljubljana
- Business model:
  - Albanian citizens, applying for a Slovenian passport
  - offered as a professional
    service travel route
    via Vienna and Warsaw
    to Canada

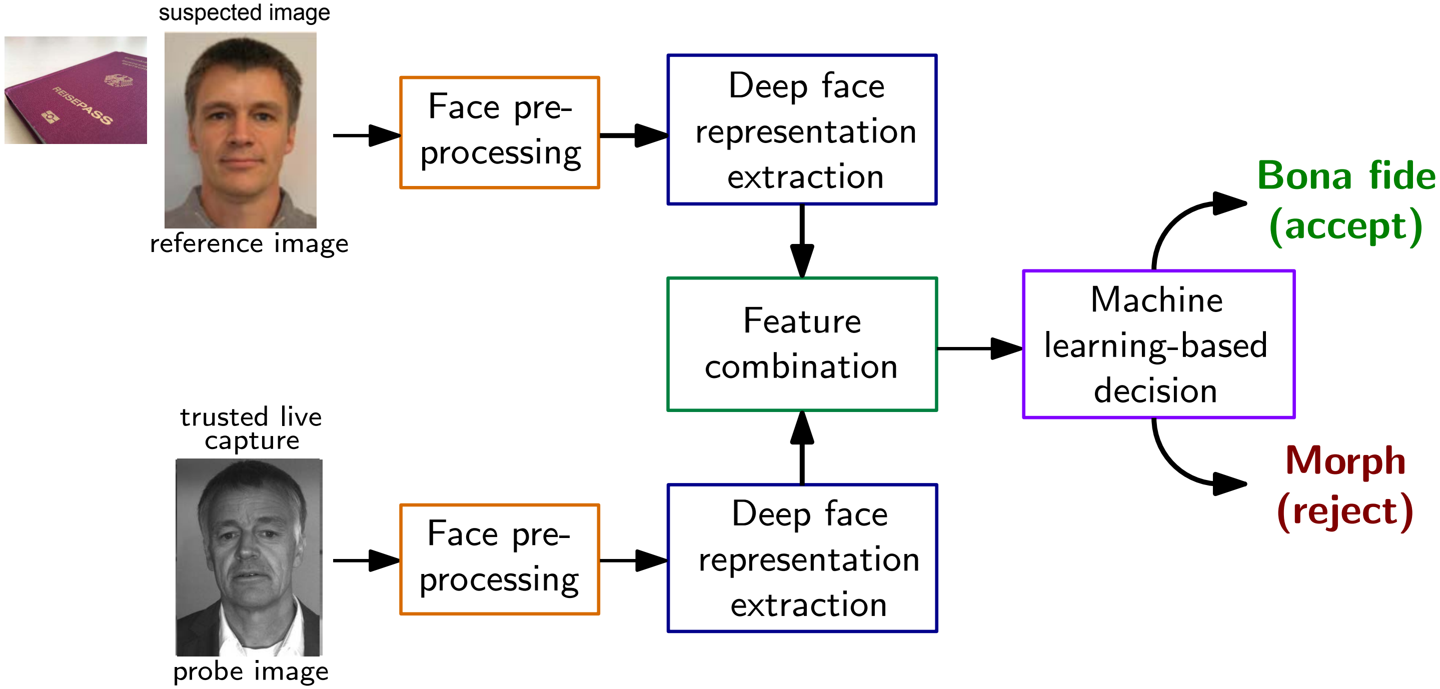


[Tork2021] Matjaž Torkar: “Morphing Cases in Slovenia”, German Biometric Working Group, (2021),
https://eab.org/events/program/220

Differential Morphing Attack Detection

D-MAD with deep latent vectors

- Deep Face representations of Deep CNNs



  - Deep representations extracted by the neural network (on the lowest layer)
  - Feature space with small dimension: 512 (for ArcFace)
  - SVM with radial basis function

[SRMB2020] U. Scherhag, C. Rathgeb, J. Merkle, C. Busch: "Deep Face Representations for Differential Morphing Attack Detection", in IEEE Transactions on Information Forensics and Security (TIFS), (2020)

MAD Evaluation Methodology

Definition of detection capabilities metrics

- ISO/IEC 20059 defines testing the MAD subsystem with false-negative and false-positive errors
  https://www.iso.org/standard/86084.html

- **Morphing attack classification error rate (MACER)**
  proportion of morphed samples incorrectly classified as bona fide samples in a specific scenario
  - Formerly reported as APCER in parts of the literature

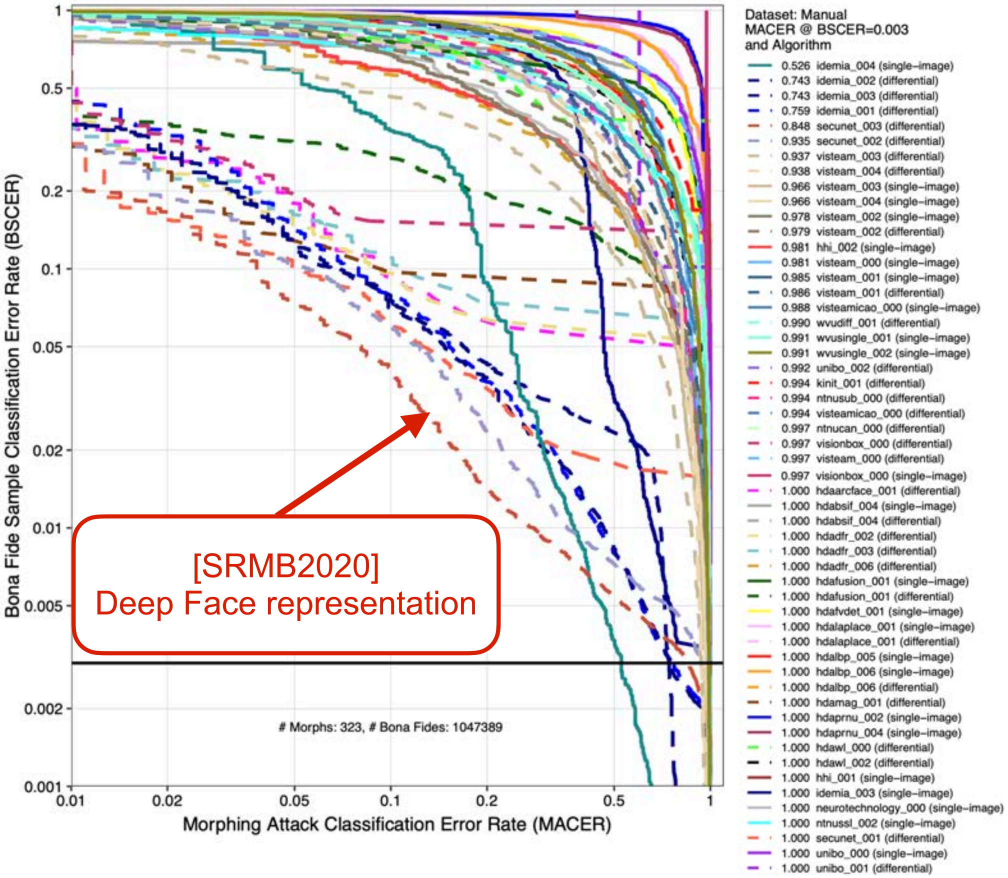
- **Bona fide sample classification error rate (BSCER)**
  proportion of bona fide samples incorrectly classified as morphed samples in a specific scenario
  - Formerly reported as BPCER in parts of the literature

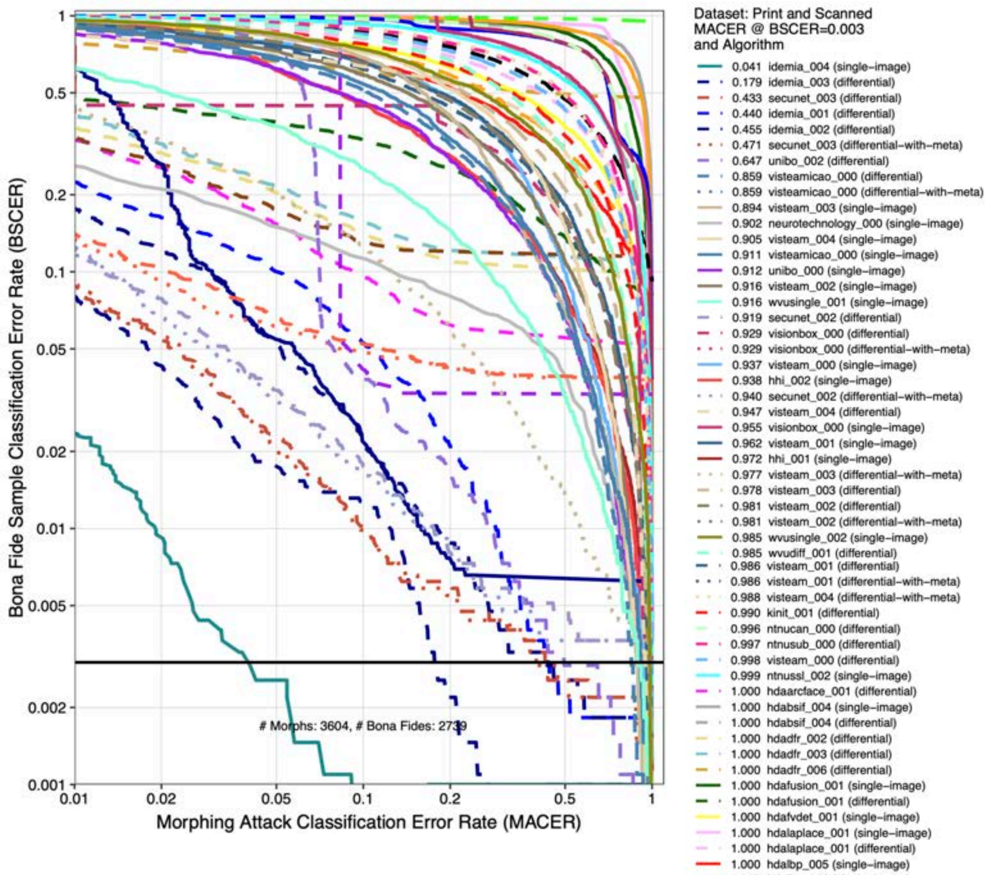
Source: ISO/IEC 20059

NIST-FATE-MORPH

NIST IR 8292 report presented June, 2025

- Performance of Automated Face Morph Detection
  https://pages.nist.gov/frvt/reports/morph/frvt_morph_report.pdf
- Results for high quality morphs versus print and scanned
  - note the low number of print and scanned images

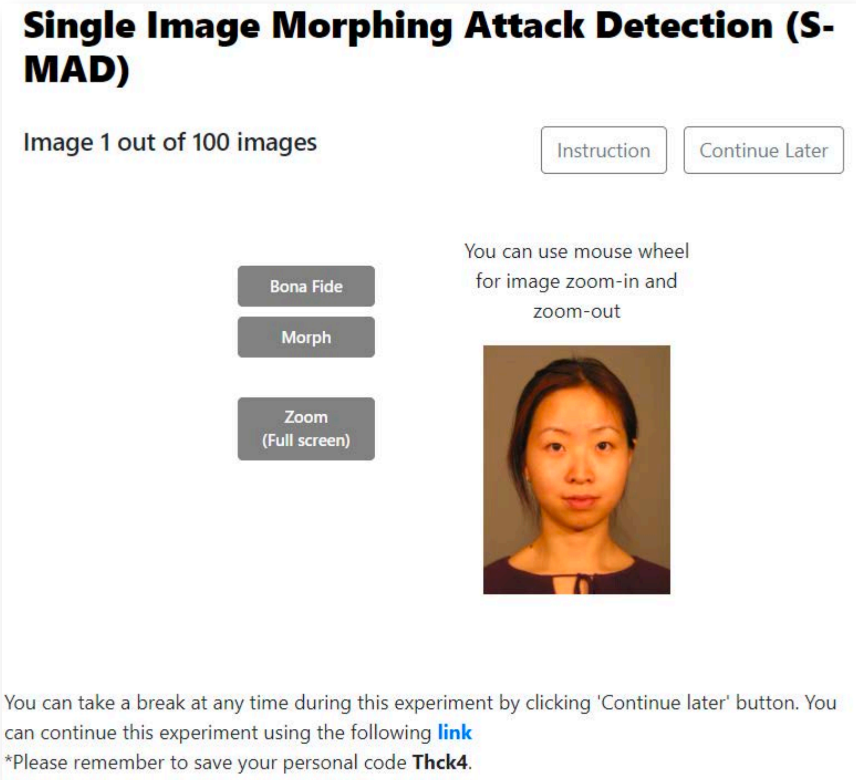


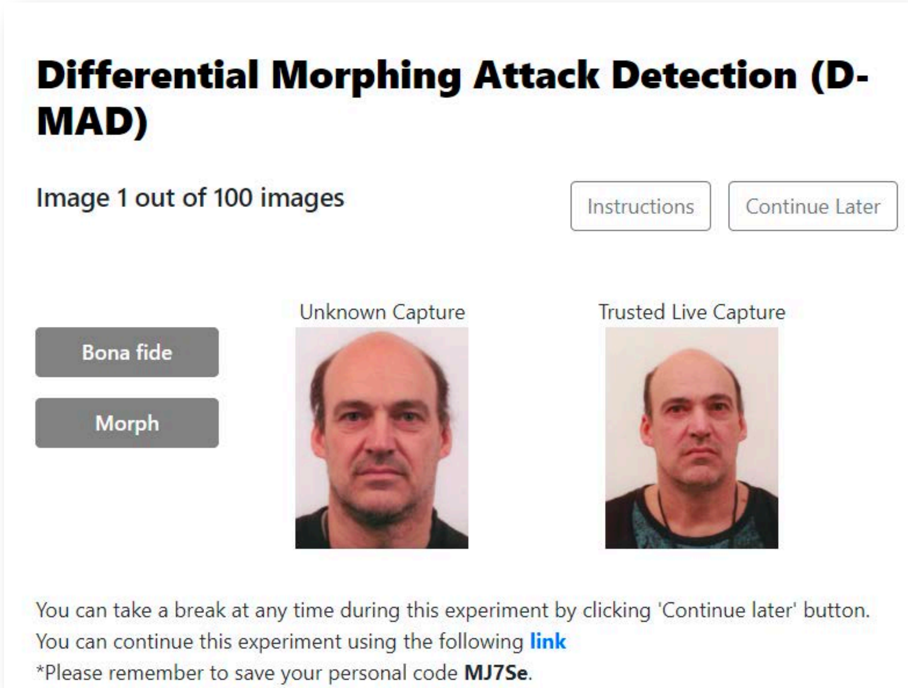


Human Experts in MAD

Border guards, case handlers, document examiners, ID experts

- S-MAD: 410 participants, 180 trials
- D-MAD: 469 participants, 400 trials (4 x 100 tasks)

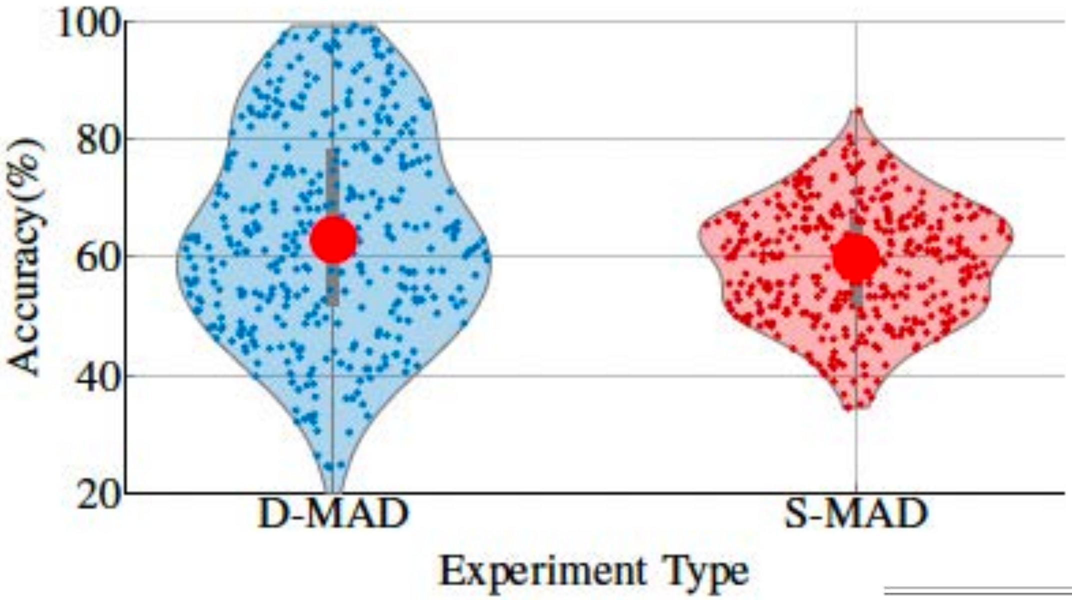




[GOD2022] S. Godage, F. Løvåsdal, S. Venkatesh, K. Raja, R. Raghavendra, C. Busch: “Analyzing Human Observer Ability in Morphing Attack Detection - Where Do We Stand?”, https://arxiv.org/abs/2202.12426

Human Experts in MAD

Overall accuracy

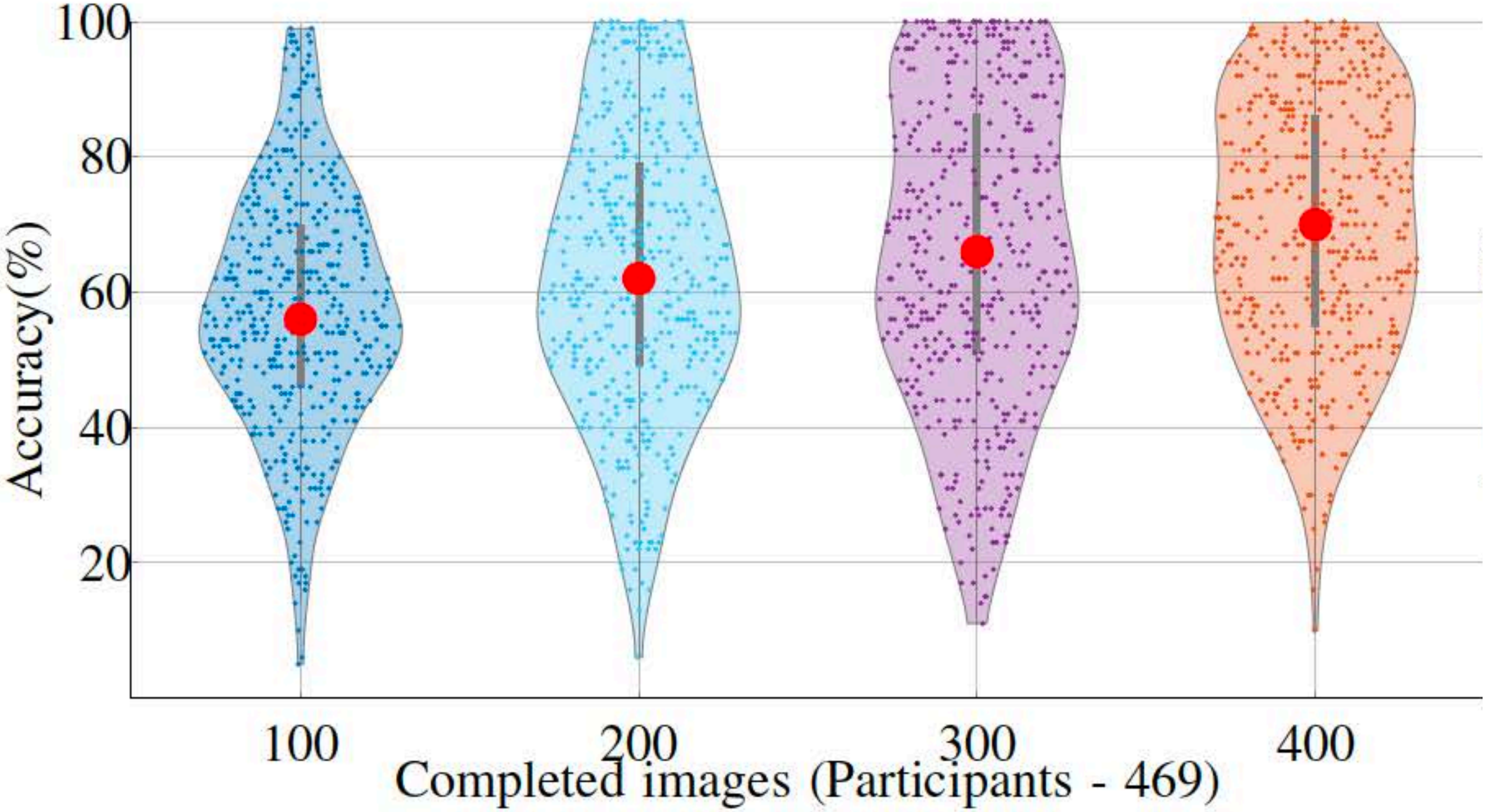


Line of work	D-MAD Number of participants	D-MAD Average Accuracy	S-MAD Number of participants	S-MAD Average Accuracy
Border Guard	30	64.66	26	55.17
Case handler- Passport, visas, ID, etc	150	63.45	137	56.65
Document examiner- 1st line	38	60.79	30	57.63
Document examiner- 2st line	40	68.64	34	62.56
Document examiner- 3rd line	30	65.74	25	61.51
Face comparison expert (Manual examination)	44	72.56	39	64.63
ID Expert	53	63.09	50	57.21
Other	84	64.66	69	55.17
Student	103	56.91	-	-
Total participants	572		410	
Experts	469		410	

[GOD2022] S. Godage, F. Løvåsdal, S. Venkatesh, K. Raja, R. Raghavendra, C. Busch: "Analyzing Human Observer Ability in Morphing Attack Detection - Where Do We Stand?", https://arxiv.org/abs/2202.12426

Human Experts in MAD

Does exposure to morphed images help?



(a) D-MAD Accuracy

[GOD2022] S. Godage, F. Løvåsdal, S. Venkatesh, K. Raja, R. Raghavendra, C. Busch: “Analyzing Human Observer Ability in Morphing Attack Detection - Where Do We Stand?”, https://arxiv.org/abs/2202.12426

Super-Recognisers in MAD

What is a Super-Recogniser?

- Above-average ability to remember, recognise faces
  - Regardless of low image quality: occlusion, pose, lighting
- General SR 2%, high-ability SR estimated ≤ 1% of population [BPB2016]
- Valuable capability for criminal investigators

Are you a Super-Recogniser?

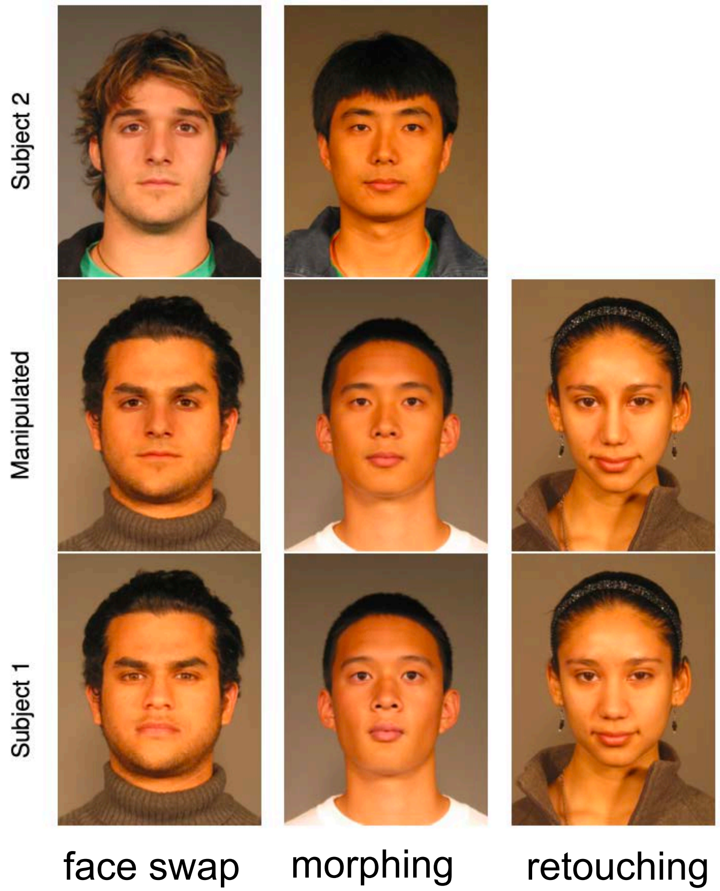
- Low probability, but it is possible
- You can take the test!
  https://www.superrecognisers.com

[BPB2016] Anna K. Bobak, Philip Pampoulov, and Sarah Bate. "Detecting Superior Face Recognition Skills in a Large Sample of Young British Adults." In: Frontiers in Psychology 7 (2016)

Super-Recognisers in MAD

Darmstadt Face Manipulation Detection Tests (DFMD)

- Designed to explore human detection performance on 3 types of digital face manipulations
- Two test procedures:
  - DFMD 1 & DFMD 2 (60 trials each)
- 787 individuals participated in the online DFMD tests
- Participants with previously evaluated face processing skills, registered super-recognizers
  - Conservative SR grouping
- Control group
- Stimulus for 15 seconds



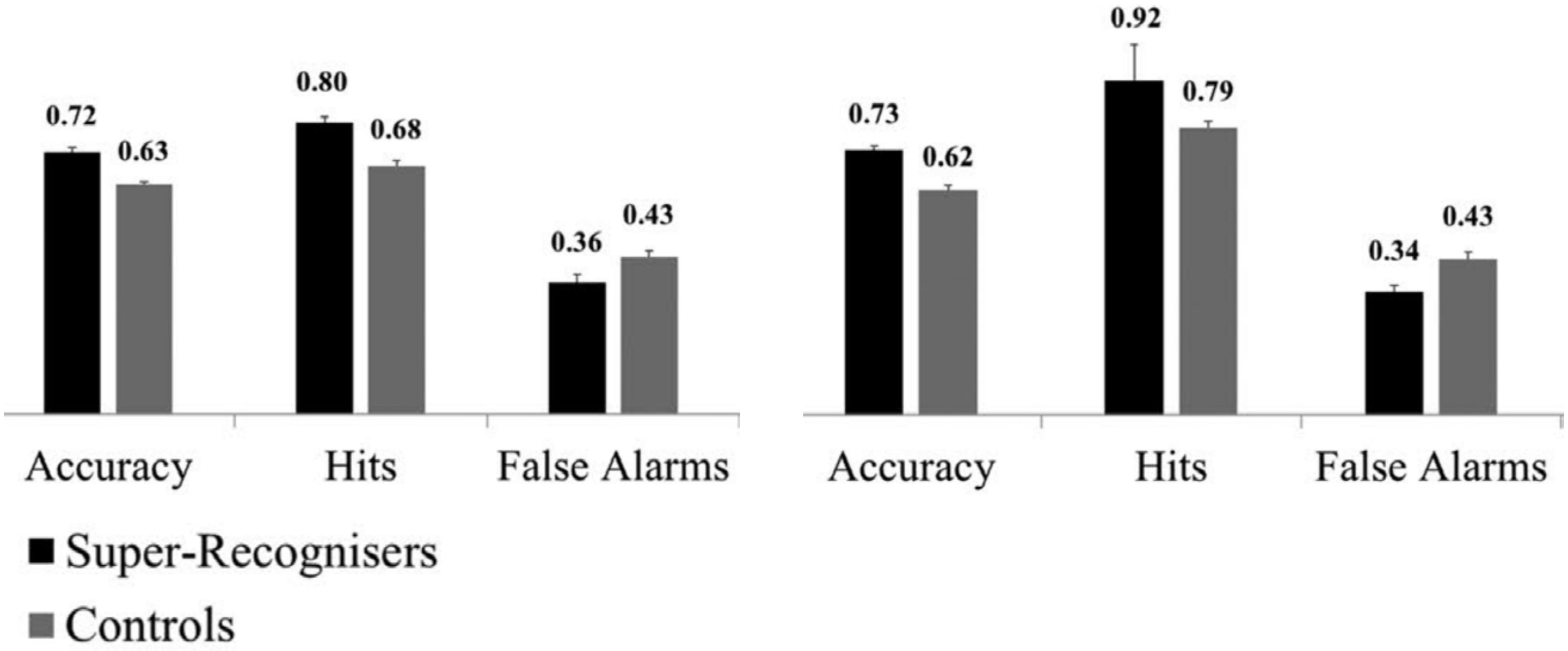
[Davis2025] J. Davis et al. “The Super-Recogniser Advantage Extends to the Detection of Digitally Manipulated Faces.” In: Applied Cognitive Psychology 39.2 (2025) https://onlinelibrary.wiley.com/doi/10.1002/acp.70053

Super-Recognisers in MAD

The Super-Recogniser advantage extends to the detection of digitally manipulated face images

DFMD1
50% manipulated images

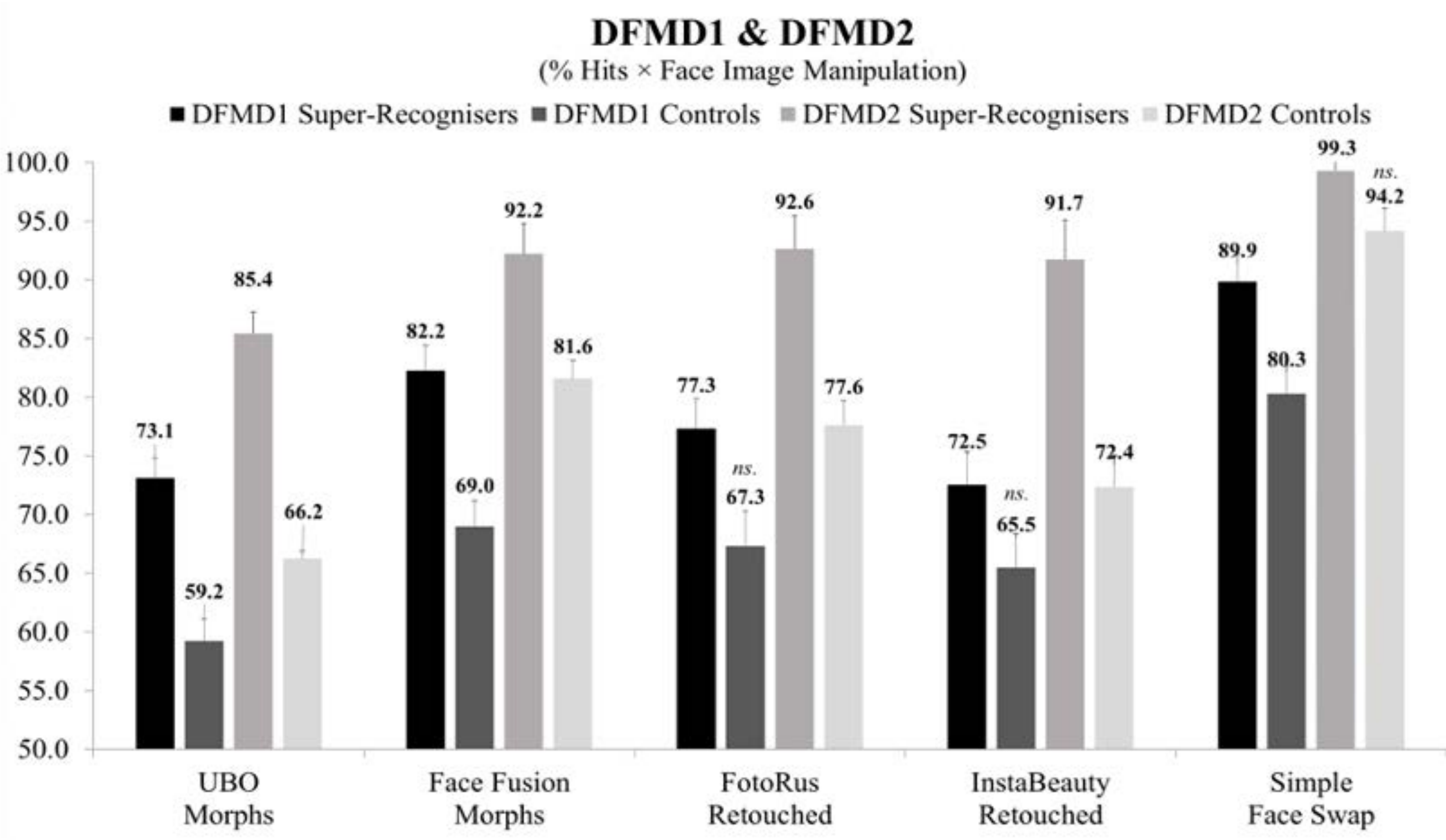
DFMD2
25% manipulated images



[Davis2025] J. Davis et al. “The Super-Recogniser Advantage Extends to the Detection of Digitally Manipulated Faces.” In: Applied Cognitive Psychology 39.2 (2025) https://onlinelibrary.wiley.com/doi/10.1002/acp.70053

Super-Recognisers in MAD

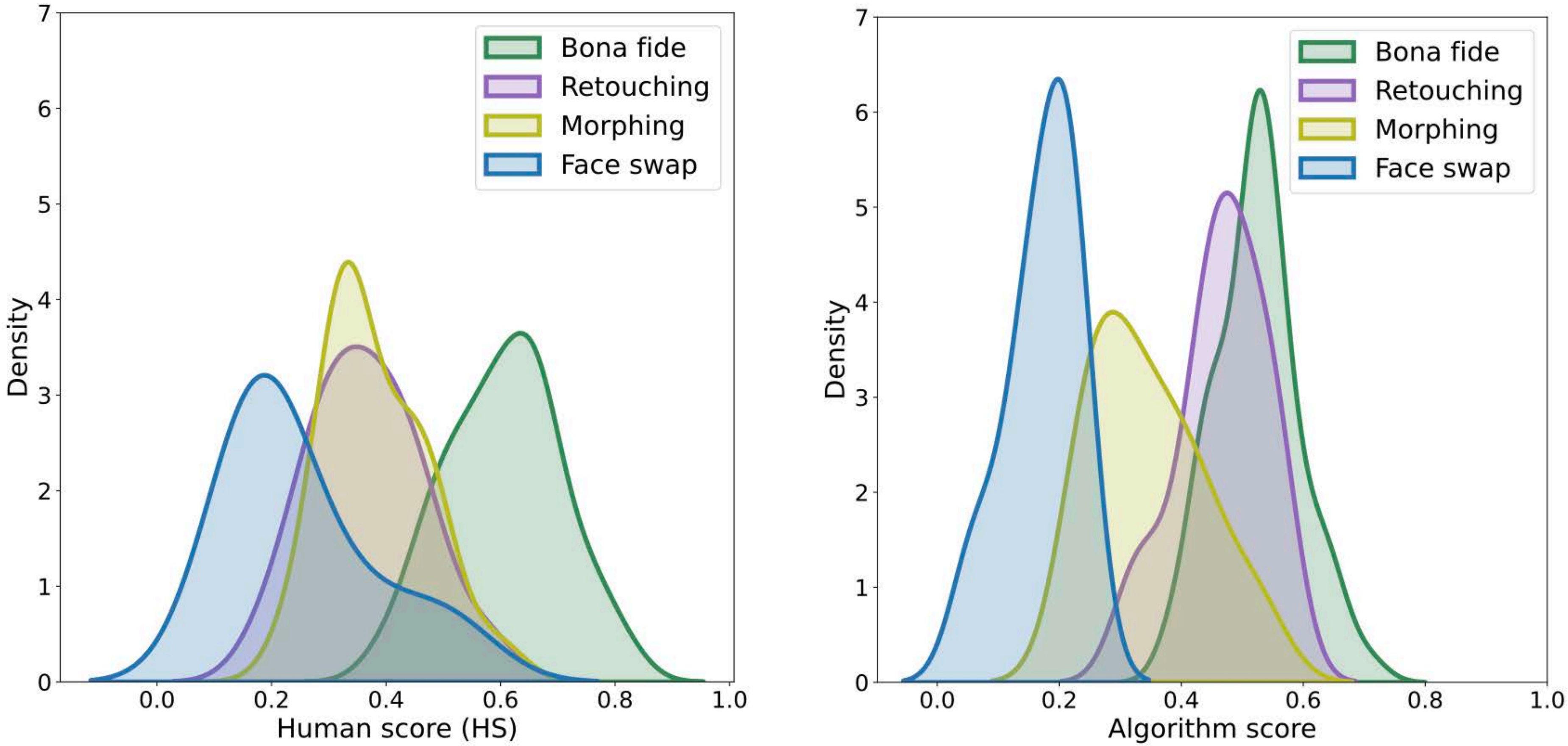
The Super-Recogniser advantage extends to the detection of morphed face images



[Davis2025] J. Davis et al. "The Super-Recogniser Advantage Extends to the Detection of Digitally Manipulated Faces." In: Applied Cognitive Psychology 39.2 (2025) https://onlinelibrary.wiley.com/doi/10.1002/acp.70053

Humans and Algorithms in MAD

Human and Algorithm Detection Scores

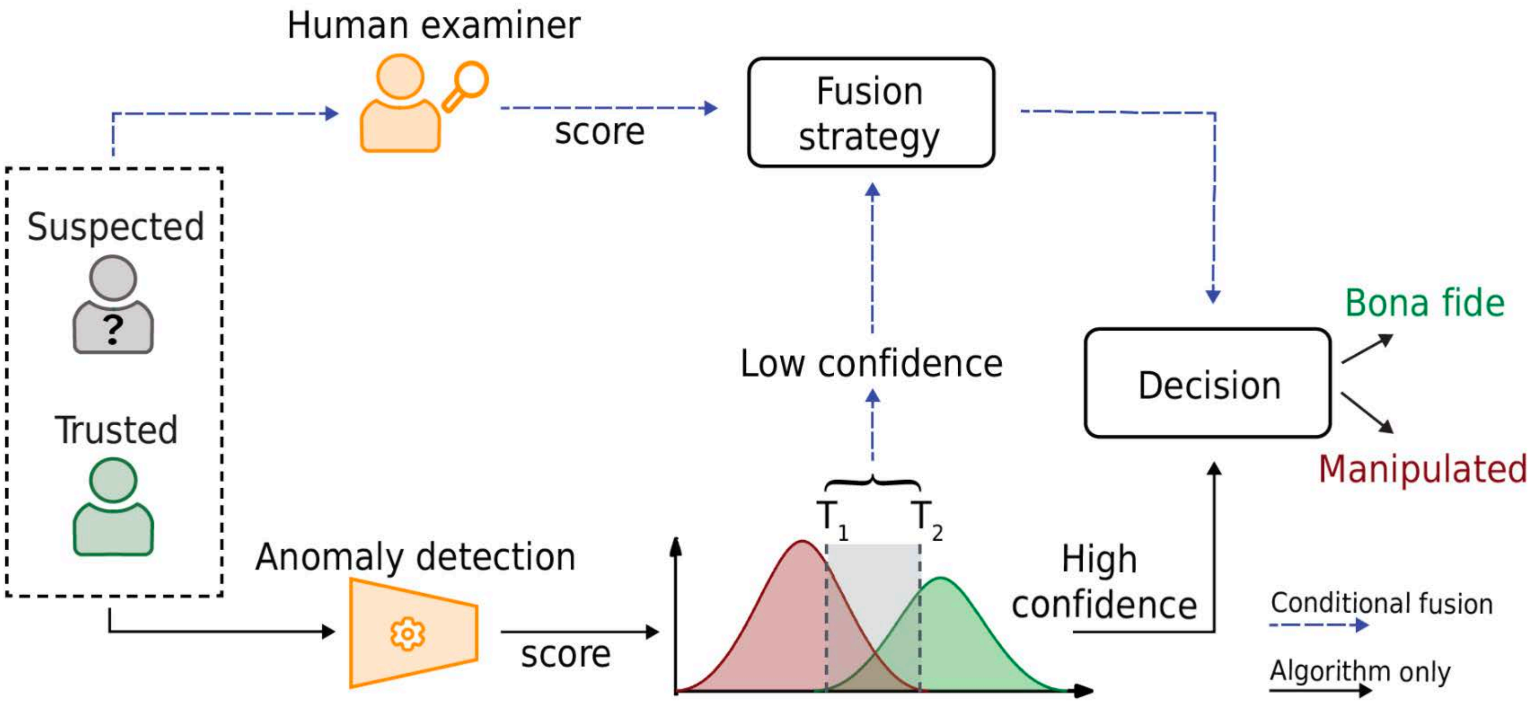


[Ibsen2024] M. Ibsen et al. “Conditional Face Image Manipulation Detection: Combining Algorithm and Human Examiner Decisions.” In: Proceedings of the Workshop on Information Hiding and Multimedia Security (IH&MMSec ’24.), (2024) https://dl.acm.org/doi/pdf/10.1145/3658664.3659649

Humans and Algorithms in MAD

Human and Algorithm Detection Scores

- Conditional fusion

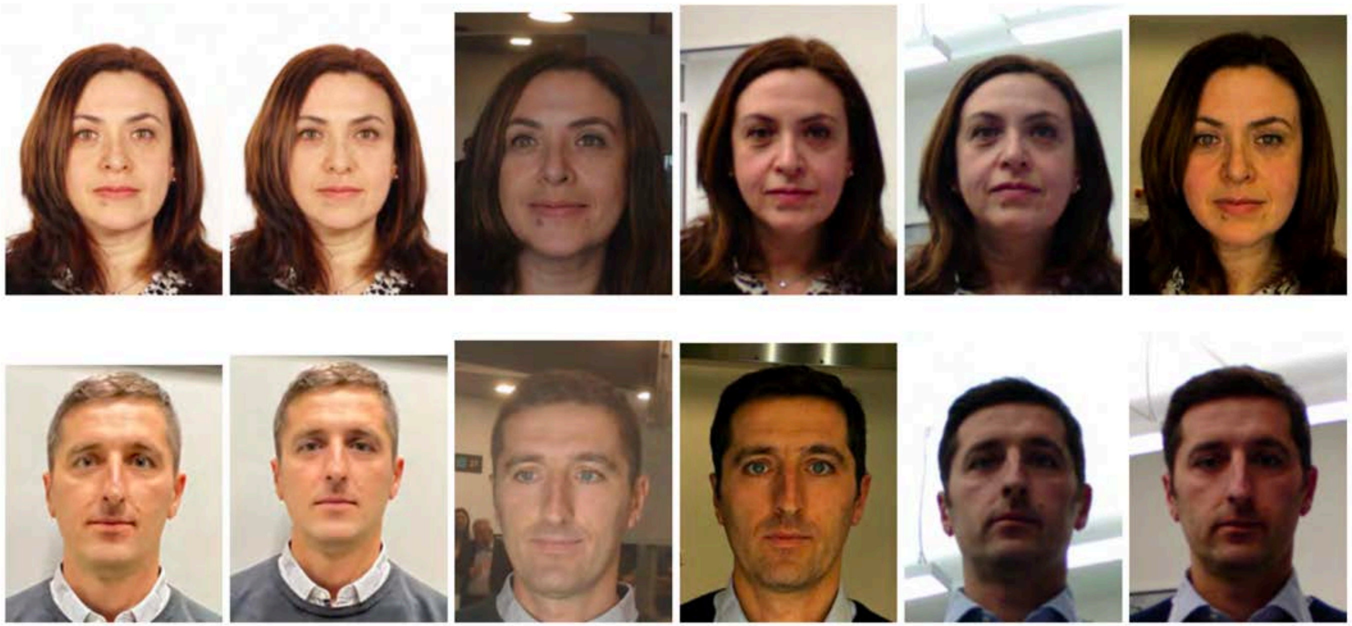


[Ibsen2024] M. Ibsen et al. “Conditional Face Image Manipulation Detection: Combining Algorithm and Human Examiner Decisions.” In: Proceedings of the Workshop on Information Hiding and Multimedia Security (IH&MMSec ’24.), (2024) https://dl.acm.org/doi/pdf/10.1145/3658664.3659649

Face Image Quality Impact on MAD

Quality of gate images

- Benchmark the impact of face image quality on morphing attack detection
- Impact measured in terms of $\Delta_{\text{D-EER}}$



(a) (b) (c) (d) (e) (f)

Figure 1. Example of images contained in the iMARS MQ database for two different subjects. For each row, bona fide, morphed and gate images are reported in the first (a), second (b) and last four (c-f) columns, respectively.

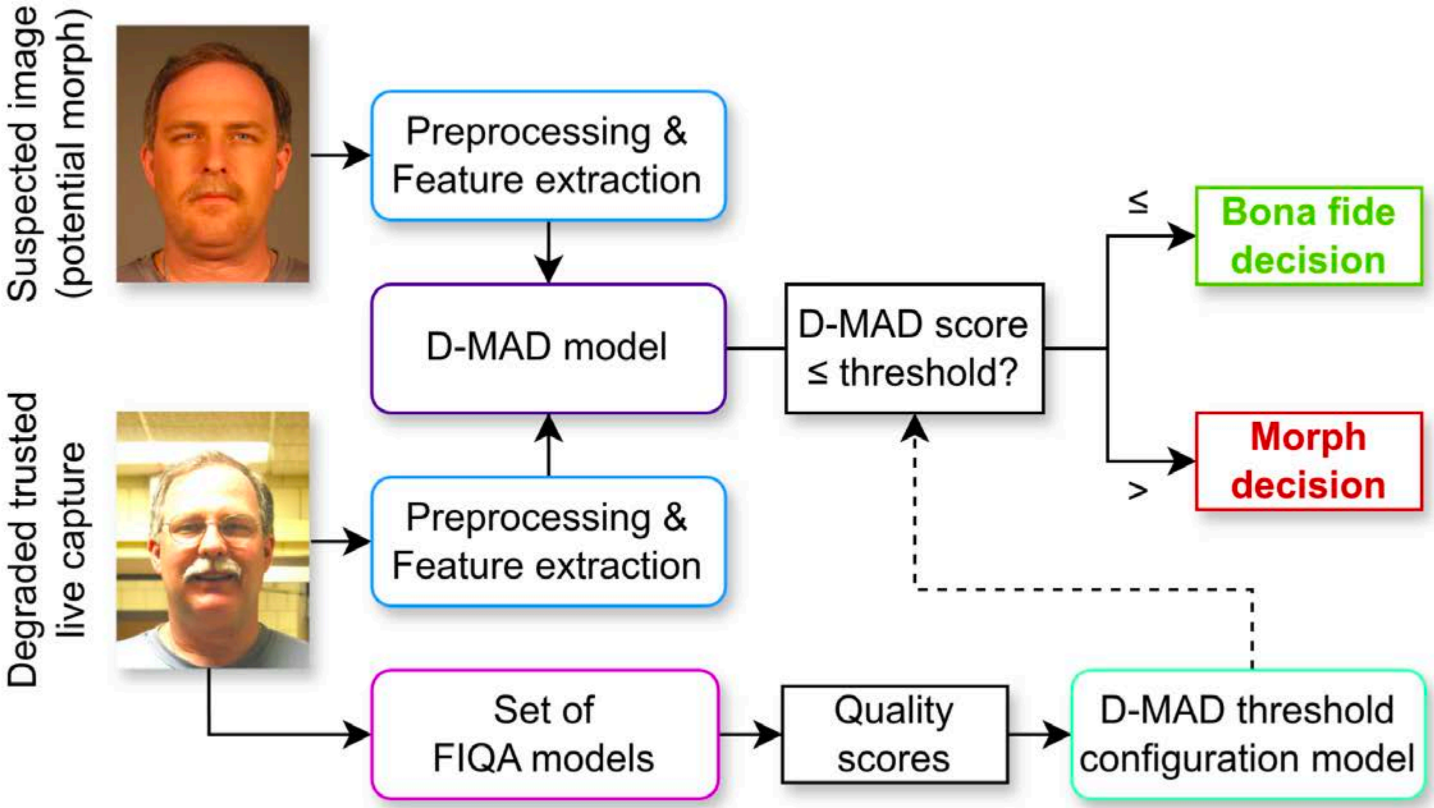
Measure	*Demorphing*
Illumination	**-12.60%**
Defocus	**-27.68%**
Pitch	**-41.11%**
Yaw	**-25.74%**

[FFLBM2024] A. Franco, M. Ferrara, C. Liu, C. Busch, D. Maltoni: "On the Impact of Face Image Quality on Morphing Attack Detection", in Proceedings of International Joint Conference on Biometrics (IJCB), Buffalo, US, September 15-18, (2024)

Face Image Quality Control on MAD

Train a model to define D-MAD thresholds

- specific to the quality of the probe image

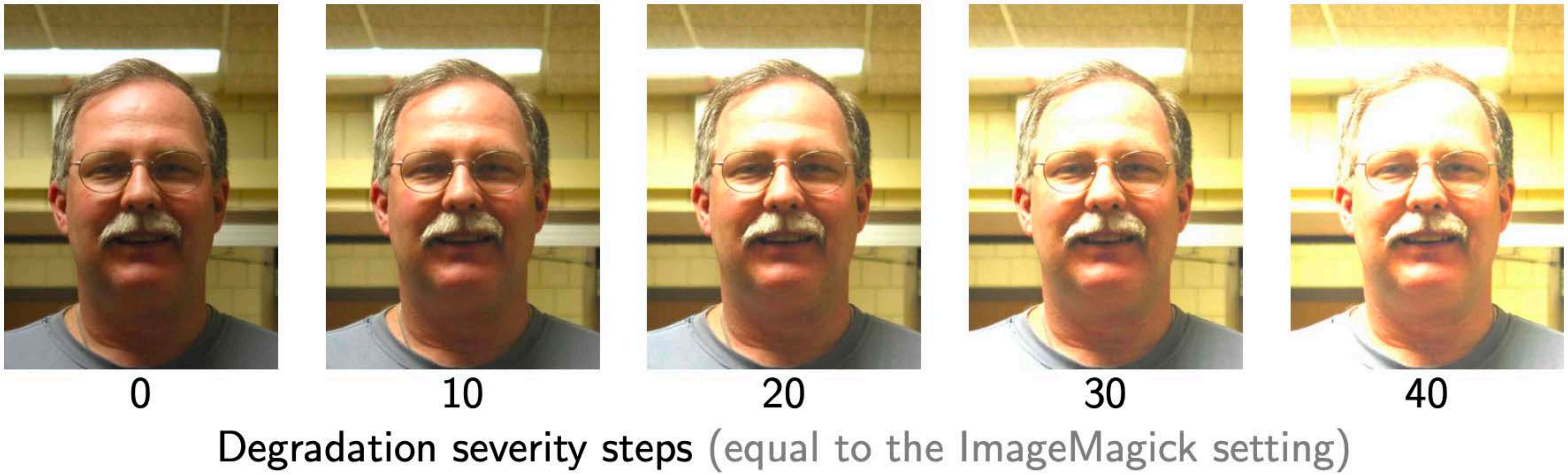


[Schlett2025] T. Schlett et al. “Impact and Mitigation of Quality Degradation for Differential Morphing Attack Detection.” In: Proceedings of the Workshop on Biometrics and Forensics (IWBF), (2025)

Face Image Quality Control on MAD

Synthetic degradation

- based on NIST FATE Quality SIDD report
- Example: Overexposure

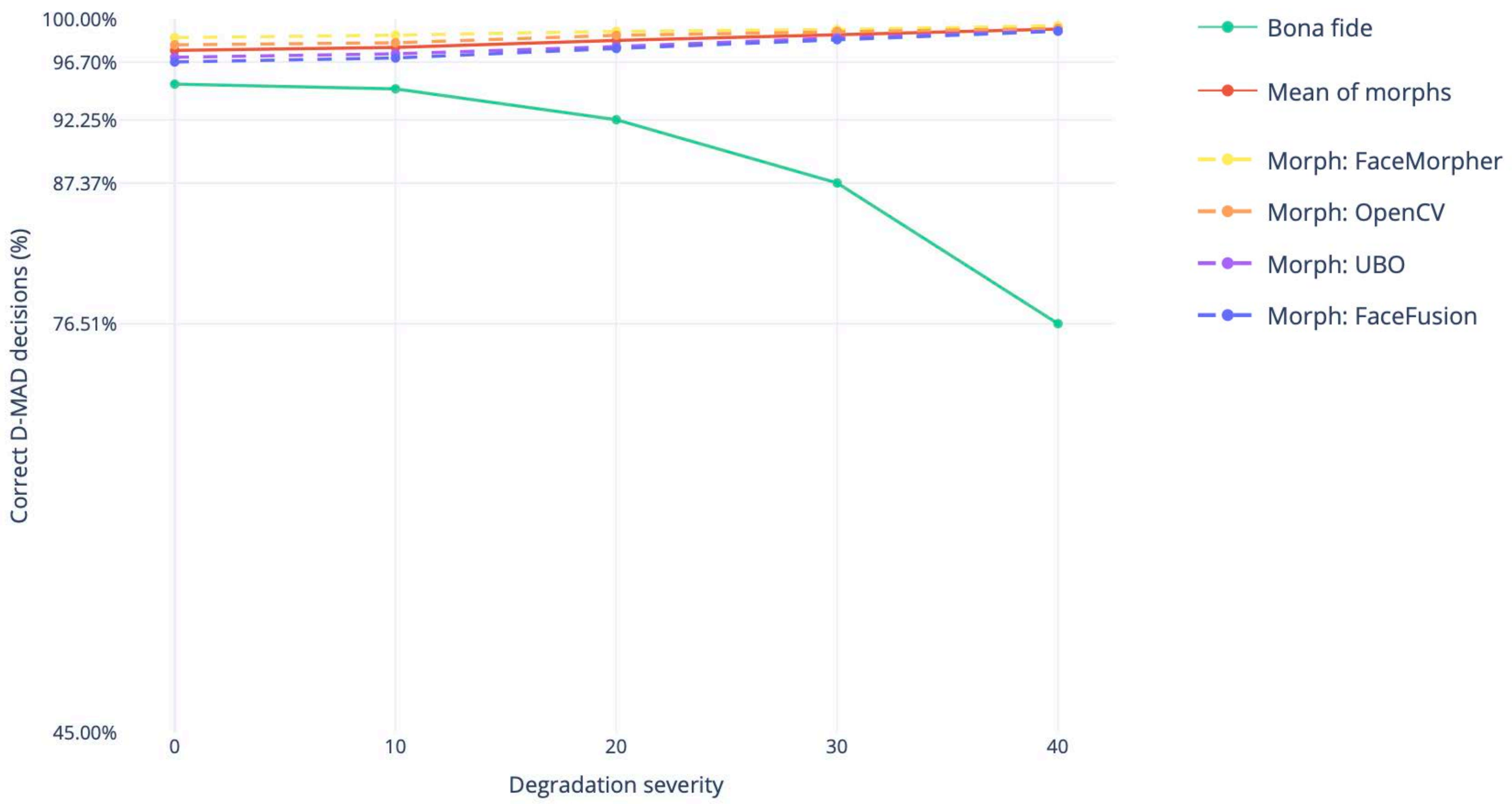


[Schlett2025] T. Schlett et al. “Impact and Mitigation of Quality Degradation for Differential Morphing Attack Detection.” In: Proceedings of the Workshop on Biometrics and Forensics (IWBF), (2025)

Face Image Quality Control on MAD

Quality impact on D-MAD decision

- Overexposure without threshold model

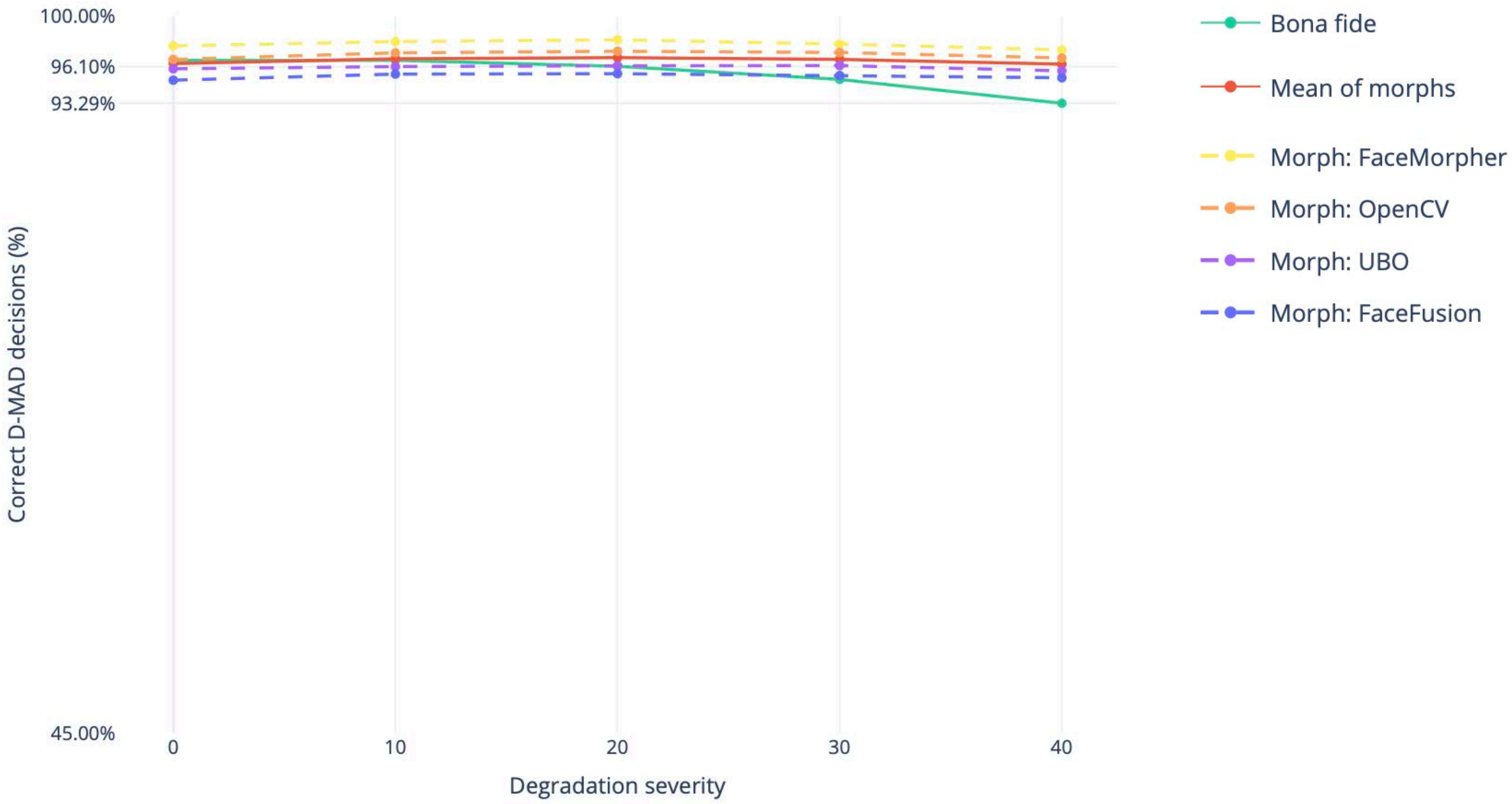


[Schlett2025] T. Schlett et al. "Impact and Mitigation of Quality Degradation for Differential Morphing Attack Detection." In: Proceedings of the Workshop on Biometrics and Forensics (IWBF), (2025)

Face Image Quality Control on MAD

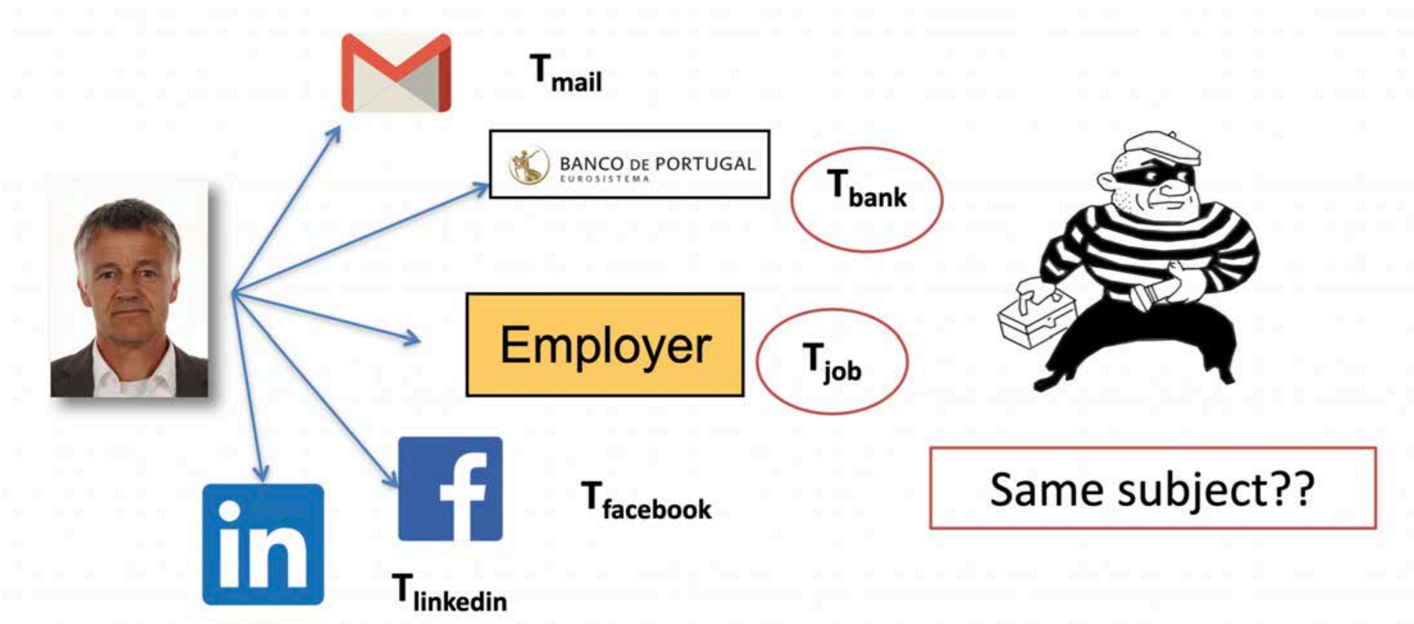
Quality impact on D-MAD decision

- Overexposure with threshold model



[Schlett2025] T. Schlett et al. “Impact and Mitigation of Quality Degradation for Differential Morphing Attack Detection.” In: Proceedings of the Workshop on Biometrics and Forensics (IWBF), (2025)

Biometric Template Protection



Why Biometric Template Protection

An incident: https://www.opm.gov/news/releases/2015/09/cyber-statement-923/

OPM.GOV ABOUT POLICY INSURANCE RETIREMENT SUITABILITY AGENCY SERVICES NEWS

OPM.gov Main > News > Latest News > News Archives > Releases > 2015 > September > Cyber Statement 9.23

Statement

FOR IMMEDIATE RELEASE
Wednesday, September 23, 2015

Contact: Office of Communications
Tel: (202) 606-2402

Statement by OPM Press Secretary Sam Schumach on Background Investigations Incident

As part of the government's ongoing work to notify individuals affected by the theft of background investigation records, the Office of Personnel Management and the Department of Defense have been analyzing impacted data to verify its quality and completeness. During that process, OPM and DoD identified archived records containing additional fingerprint data not previously analyzed. Of the 21.5 million individuals whose Social Security Numbers and other sensitive information were impacted by the breach, the subset of individuals whose fingerprints have been stolen has increased from a total of approximately 1.1 million to approximately 5.6 million. This does not increase the overall estimate of 21.5 million individuals impacted by the incident. An interagency team will continue to analyze and refine the data as it prepares to mail notification letters to impacted individuals.

Why Biometric Template Protection

Preliminary conclusion

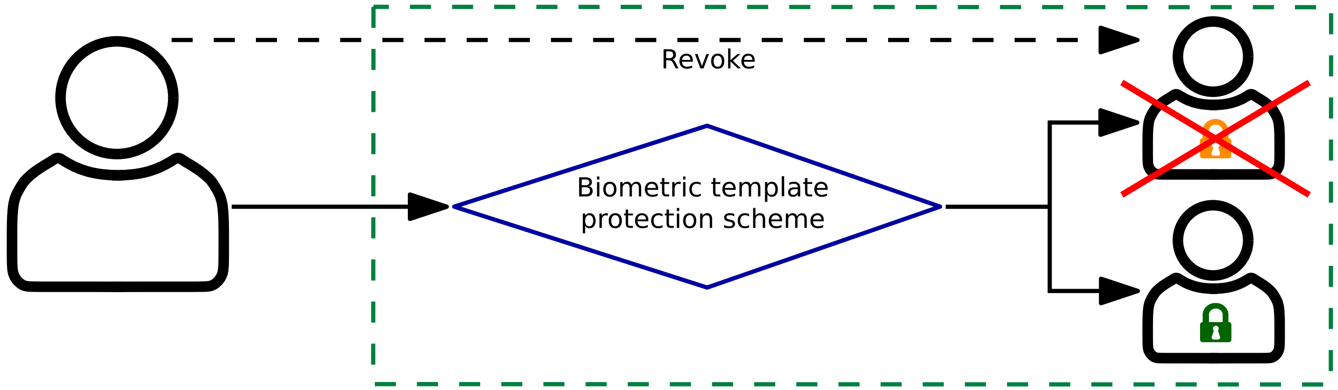
- We shall NOT store images or templates

Motivation for Template Protection

Leaking attacks against the reference data

- The face biometric characteristic as such can not be revoked
  - We have only one face ...
  - In case of being compromised, revoking and reissuing a new (different) protected biometric reference should be possible and straightforward.
  - For PW-based system you would expect renewal frequently (e.g. every 3 month)

We need renewability!



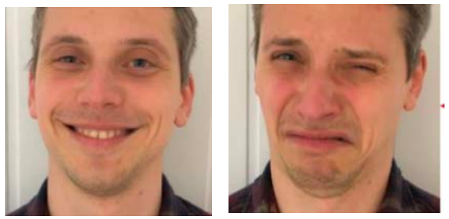
Motivation for Template Protection

Additional Information from face images

- Limited intellectual capabilities can be observed from faces
- Down syndrome (aka Trisomy 21)

Image Source: https://www.lebenshilfe-duew.de/

We can detect the mood of an individual without a biometric system.

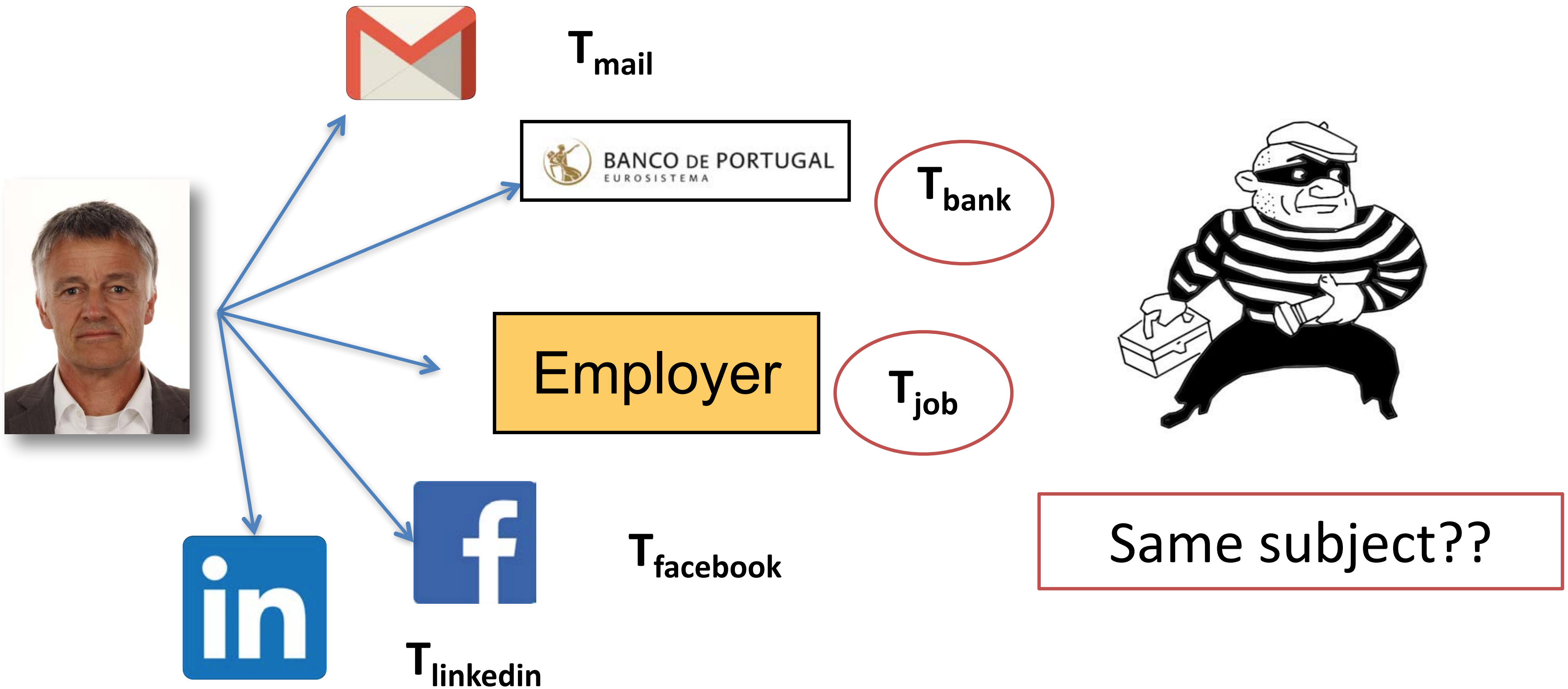


- … and we could technically keep a record of it with a sample

Motivation for Template Protection

Cross-Comparison attacks - profiling

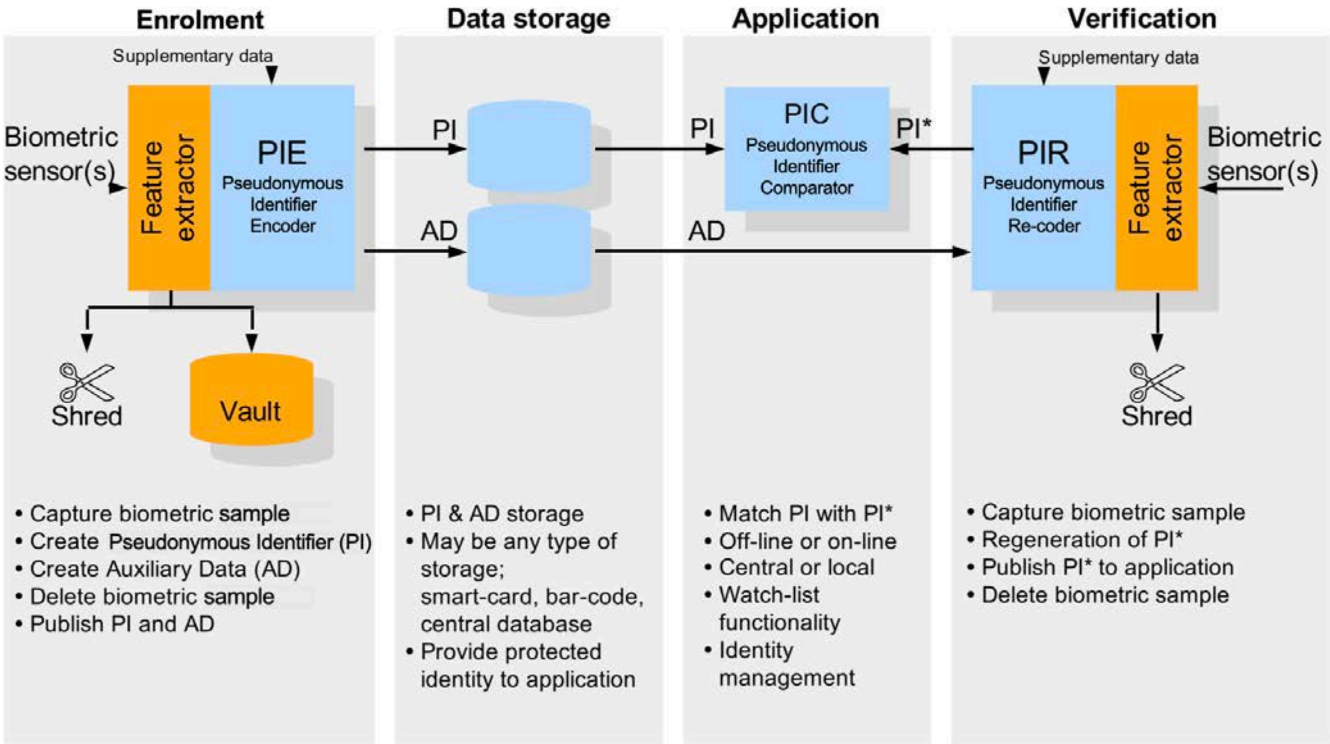
- We want to enrol with a single biometric characteristic in different applications



Biometric Template Protection (BTP)

Intention

- We transform templates to pseudonymous identifiers (PI)
- We reach renewable biometric references (RBR)

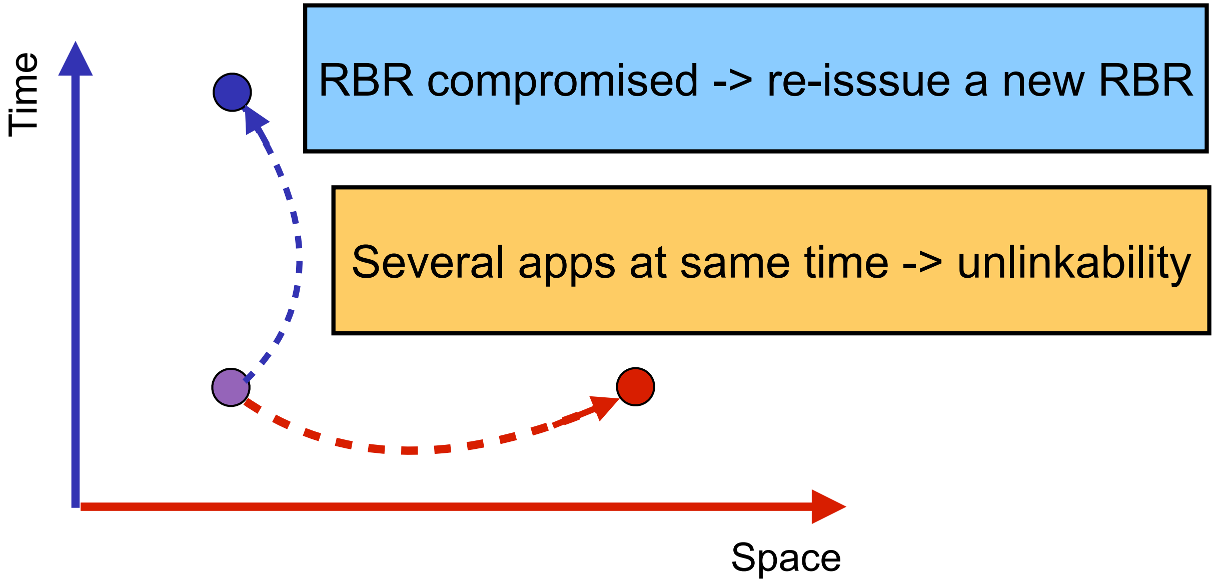


[Br2008] J. Breebaart, C. Busch, J. Grave, E. Kindt: "A Reference Architecture for Biometric Template Protection based on Pseudo Identities", in BIOSIG-2008, GI-LNI, (2008)
[ISO] International Standard: “ISO/IEC 24745:2022 Biometric information protection”, 2022

Biometric Template Protection (BTP)

Result

- Renewable biometric references (RBR) enable:
  - Secrecy: biometric references (PI) can be compared without decryption.
  - Diversification in time and space: multiple RBS can be derived from one source (i.e. face image)
  - Non-invertibility: biometric sample can not be reconstructed



[Br2008] J. Breebaart, C. Busch, J. Grave, E. Kindt: "A Reference Architecture for Biometric Template Protection based on Pseudo Identities", in BIOSIG-2008, GI-LNI, (2008)
[ISO] International Standard: "ISO/IEC 24745:2022 Biometric information protection", 2022

Biometrics in the Encrypted Domain

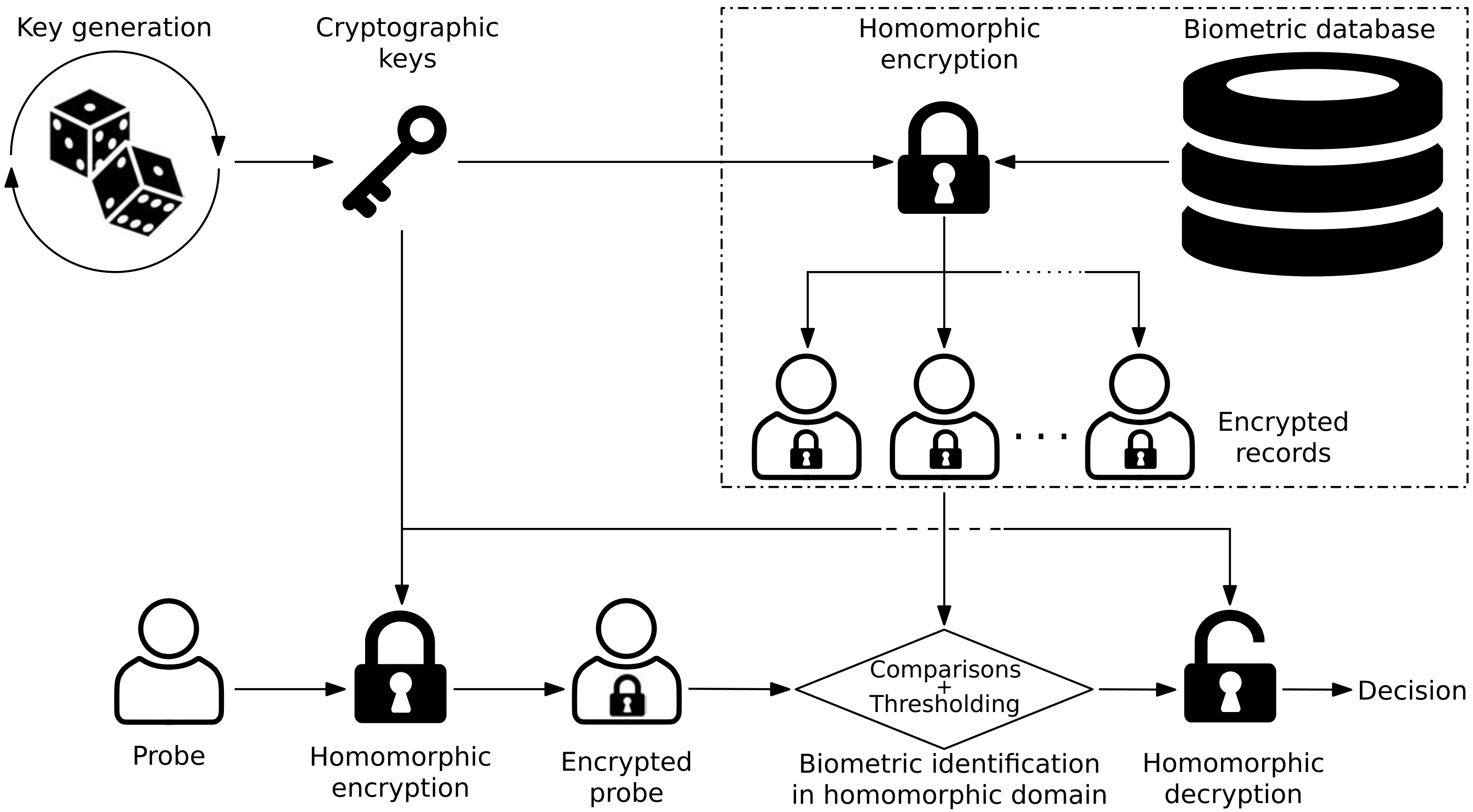
Homomorphic Encryption (HE) schemes allow for computations to be performed on ciphertexts,

- which generate encrypted results
- which decrypt to plaintexts
- that match the result of the operations carried out on the original plaintext

Biometric Template Protection

Biometrics in the Encrypted Domain

- Homomorphic Encryption (HE) schemes allow for computations to be performed on cipher-texts



Biometric Template Protection

Biometrics in the Encrypted Domain

- Partially Homomorphic Encryption (PHE) schemes
  - Are defined as allowing only a single operation type an unlimited number of times.
  - PHE schemes have been around for over 30 years supporting only either addition or multiplication.
- Somewhat Homomorphic Encryption(SHE) schemes
  - Allow multiple operation types, but only a limited number of times.
- Fully Homomorphic Encryption (FHE) schemes
  - Support an unlimited number of operations.

Biometric Template Protection

Homomorphic Encryption

- Asymmetric Cryptosystem (pk/sk)
- Post-quantum secure
- Homomorphic Properties:

$$\mathsf{Enc}_{pk}(A) + \mathsf{Enc}_{pk}(B) = \mathsf{Enc}_{pk}(A + B)$$
$$\mathsf{Enc}_{pk}(A) \cdot \mathsf{Enc}_{pk}(B) = \mathsf{Enc}_{pk}(A \cdot B)$$

[Kolb2019] J. Kolberg, et al.: "Template Protection based on Homomorphic Encryption: Computational Efficient Application to Iris-Biometric Verification and Identification ", in Proceedings of IEEE WIFS, Delft, NL, (2019)
[Dro2019] P. Drozdowski, N. Buchmann, C. Rathgeb, M. Margraf, C. Busch: "On the Application of Homomorphic Encryption to Face Identification", in Proceedings of the IEEE 18th International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, September 18-20, (2019)

Fairness of Algorithms

Image Source: https://www.flaticon.com (2020)

Demographic Factors

What is fairness?

- Dictionary:
  "*the quality of treating people equally or in a way that is right or reasonable*"
- Movie Coded Bias

Image Source: Netflix

An inherently ethical and social concept

- Influenced by cultural, historical, legal, religious, personal, and other factors
- Challenging to develop mathematical definitions,
- No single, universal notion or definition of fairness in practice
- However, everyone wants to be treated "fairly"

Reaching out towards group fairness

Demographic Effects

Current findings for facial biometric characteristics

- Most studies observed influence of demographic attributes on biometric recognition.
  - Generally, lower biometric performance was consistently observed for females and children
  - The influence of race appears to be heavily algorithm-dependent.
  - The country of algorithm development (and hence training data) may be a large factor in this context.

NIST Face Recognition Vendor Test:

- Demographics Effects Report
  - 200 algorithms tested
  - Found empirical evidence for the existence of a wide range of accuracy across demographic differences in the majority of the current face recognition algorithms that were evaluated

[Drozd2020] P. Drozdowski, C. Ratgeb, A. Dantcheva, N. Damer, C. Busch: "Demographic Bias in Biometrics: A Survey on an Emerging Challenge“, in IEEE Transactions on Technology and Society (TTS), (2020)

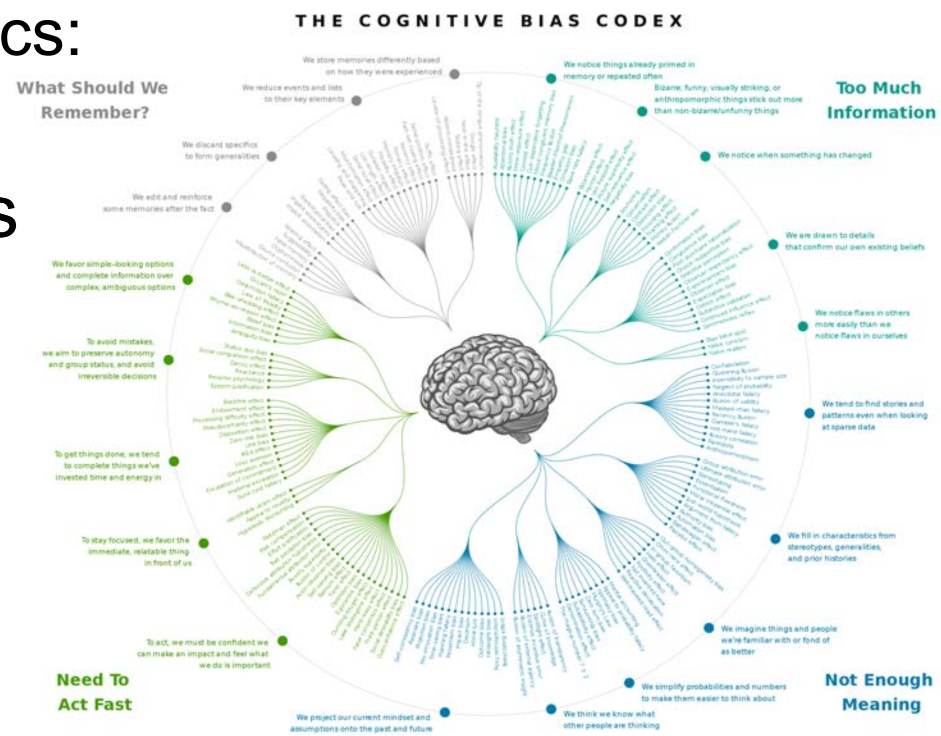
Demographic Factors

Biased machines – fair human experts?

- Cognitive biases
- Examples in the field of biometrics:
  The other race effect

Advantages and disadvantages

- Consistency over time
  (end-of-the-workday-effect)
- Experience: Pass applications
  with morphed images



Source: https://commons.wikimedia.org/wiki/File:Cognitive_bias_codex_en.svg

Hybrid systems

- Not fully automated decision systems
  but assisting algorithms (i.e conditional fusion)

Conclusion

Summary

- Presentation attacks remain a threat to non-supervised capture devices
- Face image quality assessment is accurately possible with open source algorithms
  - OFIQ provides explainable feedback to the user on why a face image is of insufficient quality
- Morphing attack detection has its limits for algorithms and human experts
- Better image quality leads to better recognition performance and better morphing attack detection accuracy
- Cross-comparison-resistant biometric template protection can prevent from profiling

Questions and Answers?

Take home information:

- Slides
- Paper
- Face image quality website:
  https://christoph-busch.de/projects-ofiq.html
- Morphing attack detection website:
  https://christoph-busch.de/projects-mad.html

ATHENE
National Research Center
for Applied Cybersecurity

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

Prof. Dr. Christoph Busch
Principal Investigator

Hochschule Darmstadt FBI

Schoefferstr. 3
64295 Darmstadt, Germany
christoph.busch@h-da.de

Telefon +49-6151-533-30090
https://dasec.h-da.de

NTNU

Prof. Dr. Christoph Busch

Norwegian University of Science and Technology
Department of Information Security and
Communication Technology
Teknologiveien 22
2802 Gjøvik, Norway
Email: christoph.busch@ntnu.no
Phone: +47-611-35-194