Manipulierte Ausweisdokumente - wie gefälschte Lichtbilder erkannt werden können

Christoph Busch

copy of slides available at:
https://christoph-busch.de/about-talks-slides.html
more information at:
https://christoph-busch.de/projects-mad.html

Ringvorlesung Cybersicherheit (HMdIS)
November 10, 2022

da/sec
BIOMETRICS AND INTERNET-SECURITY
RESEARCH GROUP

ATHENE

NORWEGIAN BIOMETRICS LABORATORY

NTNU

Overview

Agenda

- Introduction on Biometrics
- Morphing Problem description
- Morphing Attack Detection (MAD) - Scenarios and Methods
- Automated Face Morphing Attack Detection
- Human examiners at Face Morphing Attack Detection
- Conclusion

Identity Authentication in General

Identity authentication can be achieved by:

- Something you know:
  Password, PIN, other secret
- Something you own:
  SmartCard, USB-token, key
- Something you are
  Body characteristics

Something you know or own
you may loose, forget or forward to someone else,
with biometrics this is more difficult.

Biometric Face Recognition

Automated Border Control (ABC) gates

- supervised control

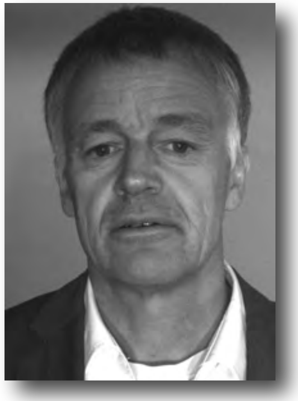
Project goals:

- Self-Service to increase throughput
- Biometric verification

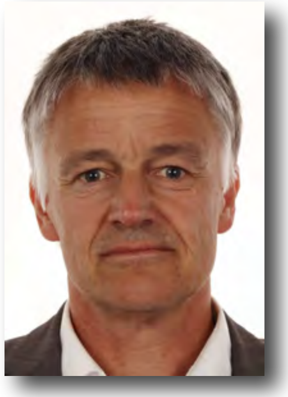
Biometric probe

Biometric reference

Source: Bundespolizei



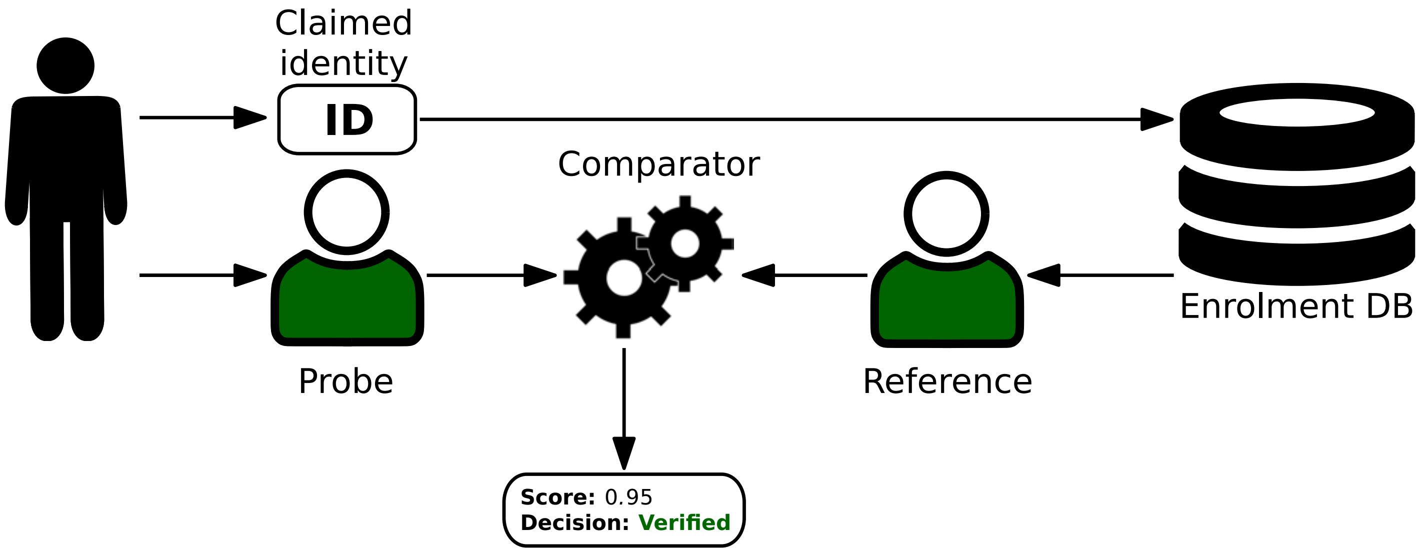
$\overset{?}{=}$



Verification - Identification

Verification

- 1:1
- validate a biometric claim

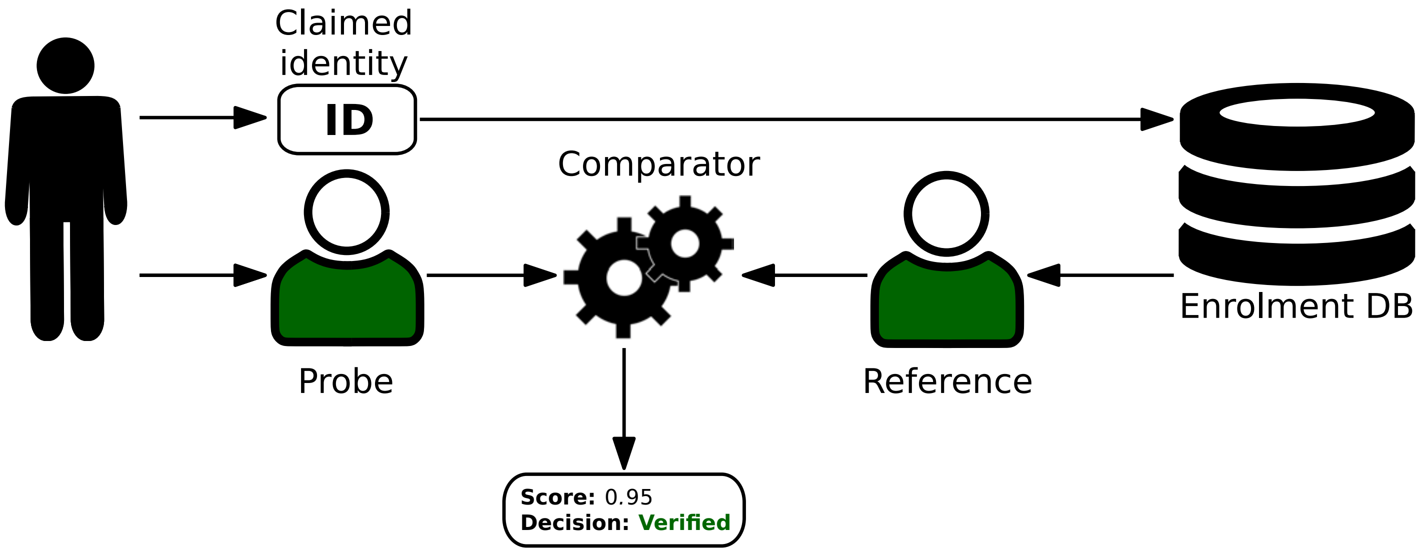


Score: 0.95
Decision: Verified

Verification - Identification

Verification

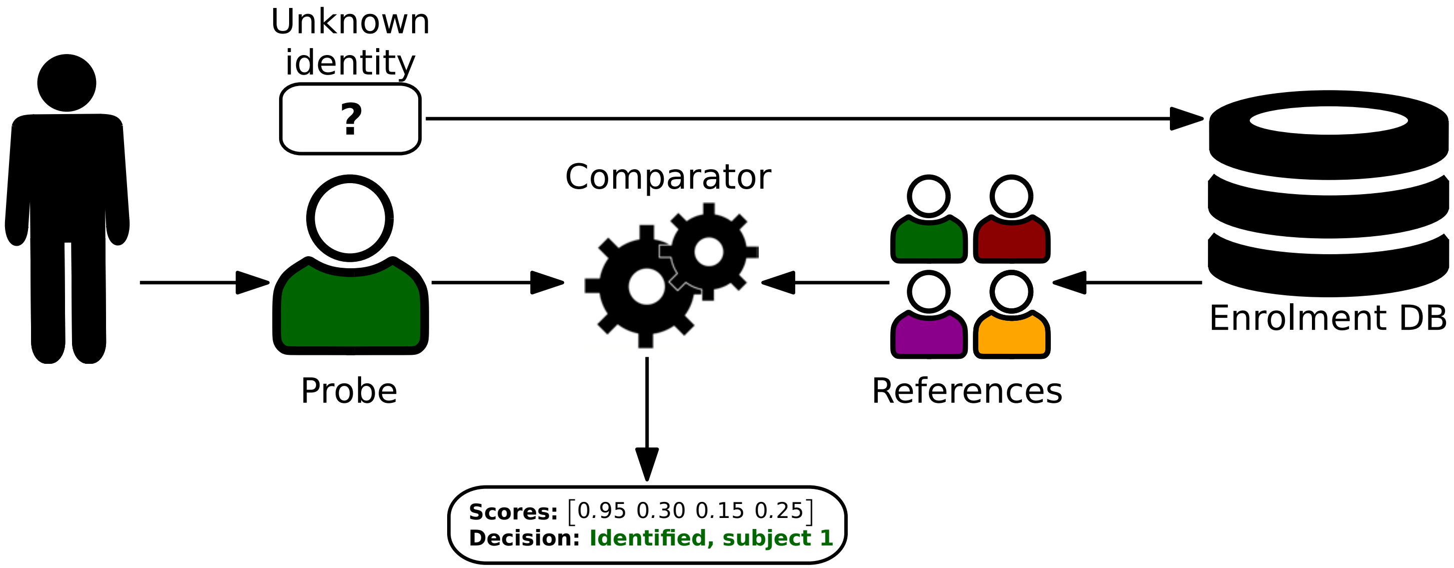
- 1:1
- validate a biometric claim



Score: 0.95
Decision: Verified

Identification

- 1:n search



Scores: $[0.95\ 0.30\ 0.15\ 0.25]$
Decision: Identified, subject 1

Border Security depends on Passport Security

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 Passport Security

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

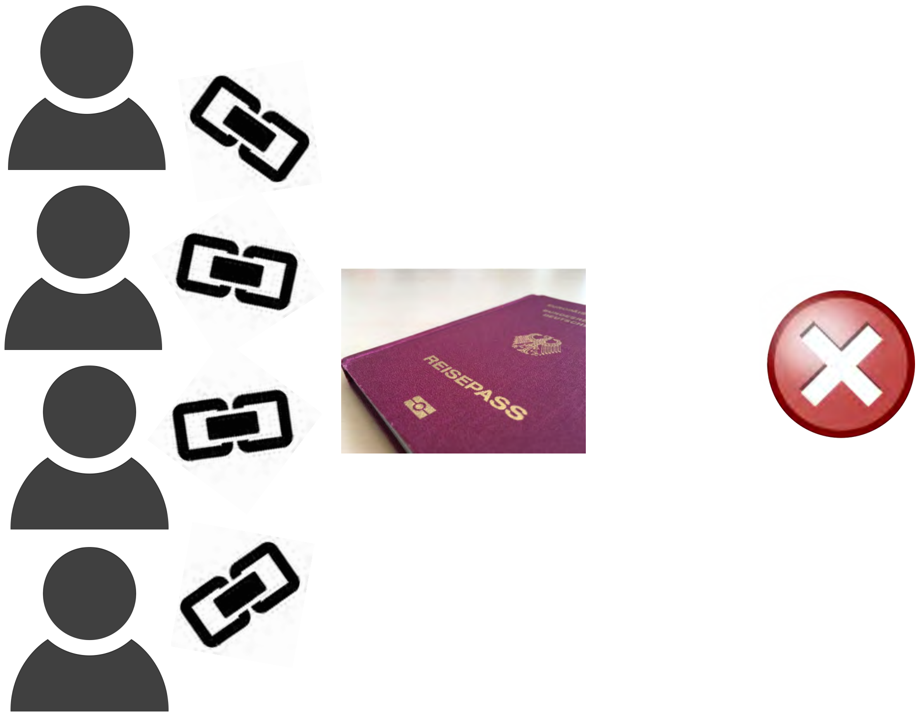


image source: https://pixabay.com/de/vectors/tick-sternchen-kreuz-rot-gr%C3%BCn-40678/

What is Morphing?

What is Morphing?

Do you remember the story

- if you kiss a frog …

What is Morphing?

Do you remember the story

- if you kiss a frog …
- … the frog will turn into a prince

Source: www.promipool.de

What is Morphing?

Or with minor modification of the story:

- if you kiss a frog …
- … the frog will turn into a princess

What is Morphing?

Or with minor modification of the story:

- if you kiss a frog …
- … the frog will turn into a princess
- Morphing can make this dream possible (even without the kiss)
  - with the frog and the princess as actors

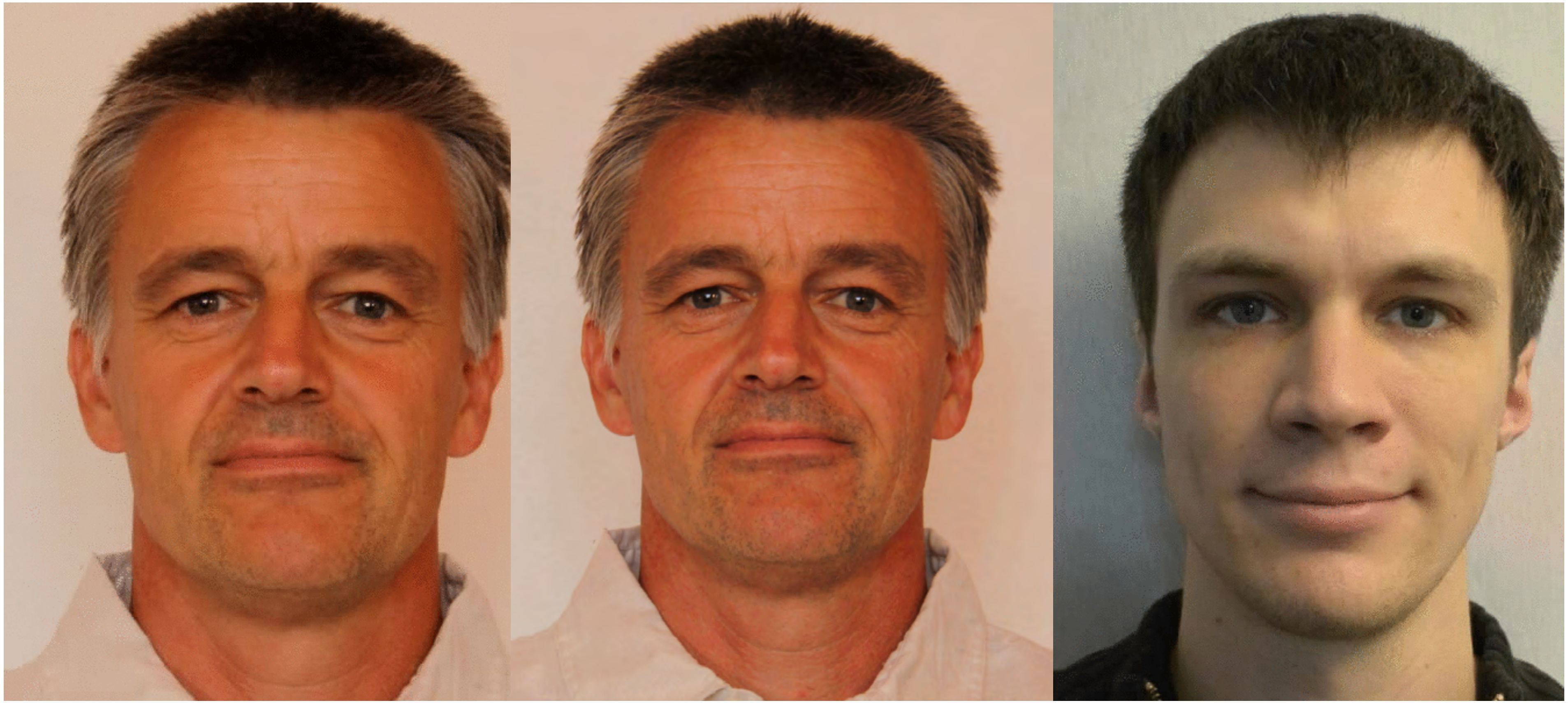
Image source: https://www.myposter.de/motive/frosch-bild
acting in this talk

Therese Johaug acting as princess in this talk

What is Morphing?

In our real world morphing can become a threat

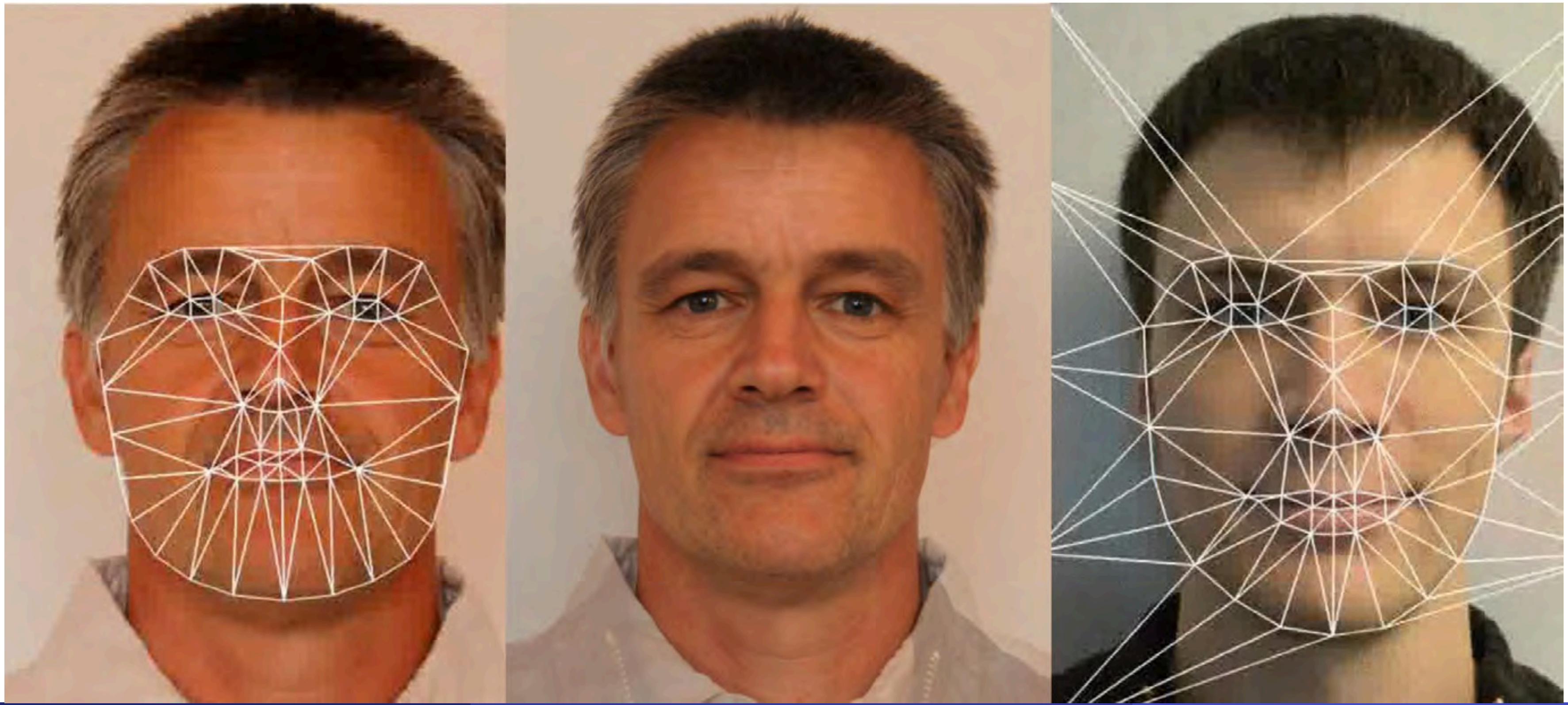
- with a criminal and an accomplice as actors
- take the criminal
- and the accomplice
- morphing can transform one face image into the other



What is Morphing?

In our real world morphing can become a threat

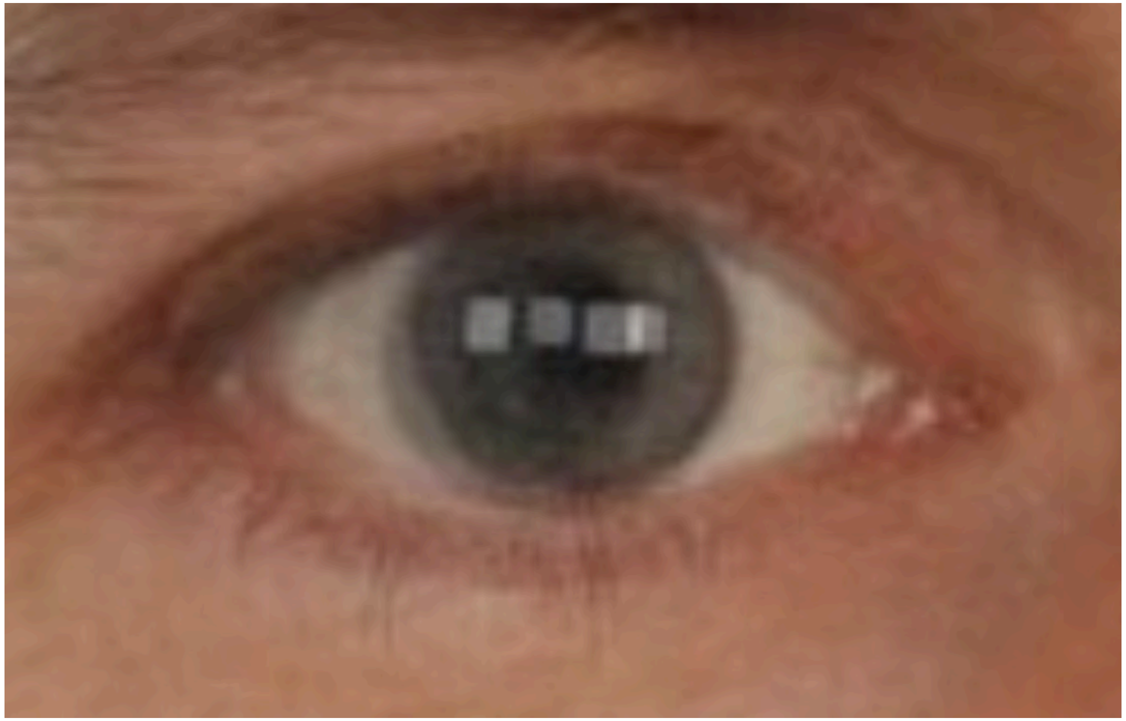
- with a criminal and an accomplice as actors
- take the criminal
- and the accomplice
- morphing can transform one face image into the other
- and you can stop half way in the transformation



A good Morph …

… is not as simple as you think

- Alignment at inner and outer eyecorner landmarks, will cause artifacts (e.g. iris shadows)



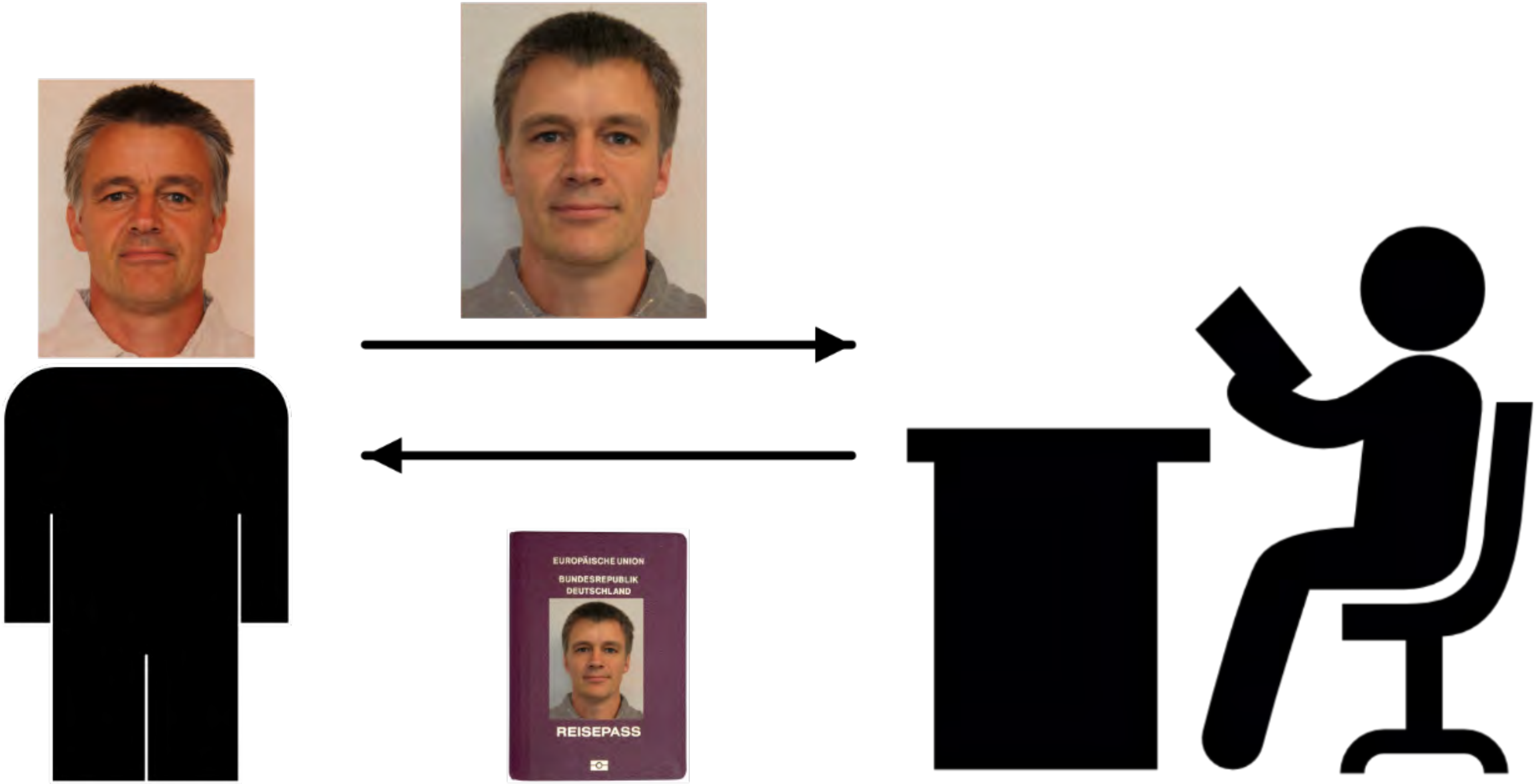
- A good morph requires automated and manual post-processing

Problem Description

Problem: Morphing Attacks

Morphing attack scenario

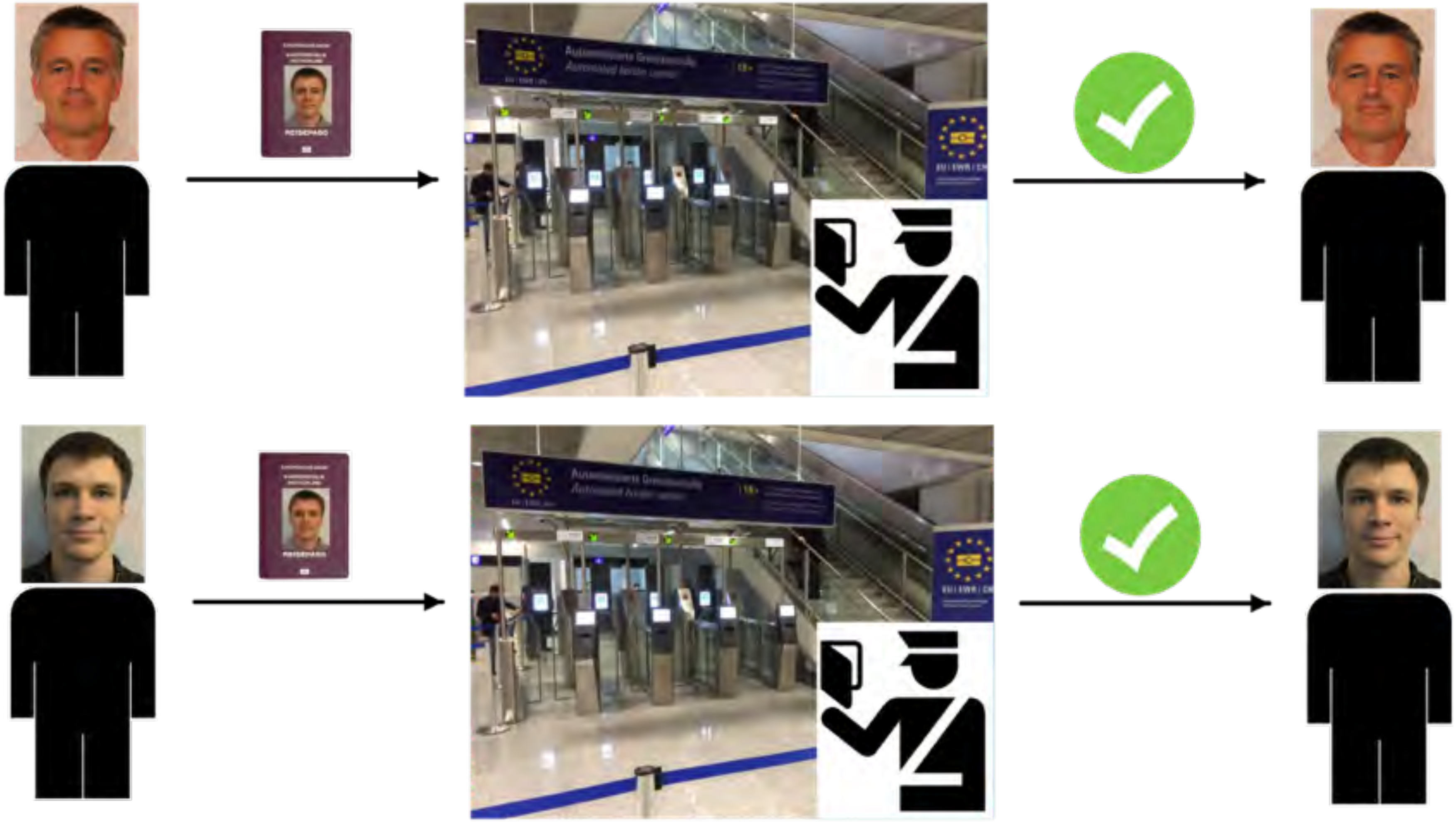
- Passport application of the accomplice A



Problem: Morphing Attacks

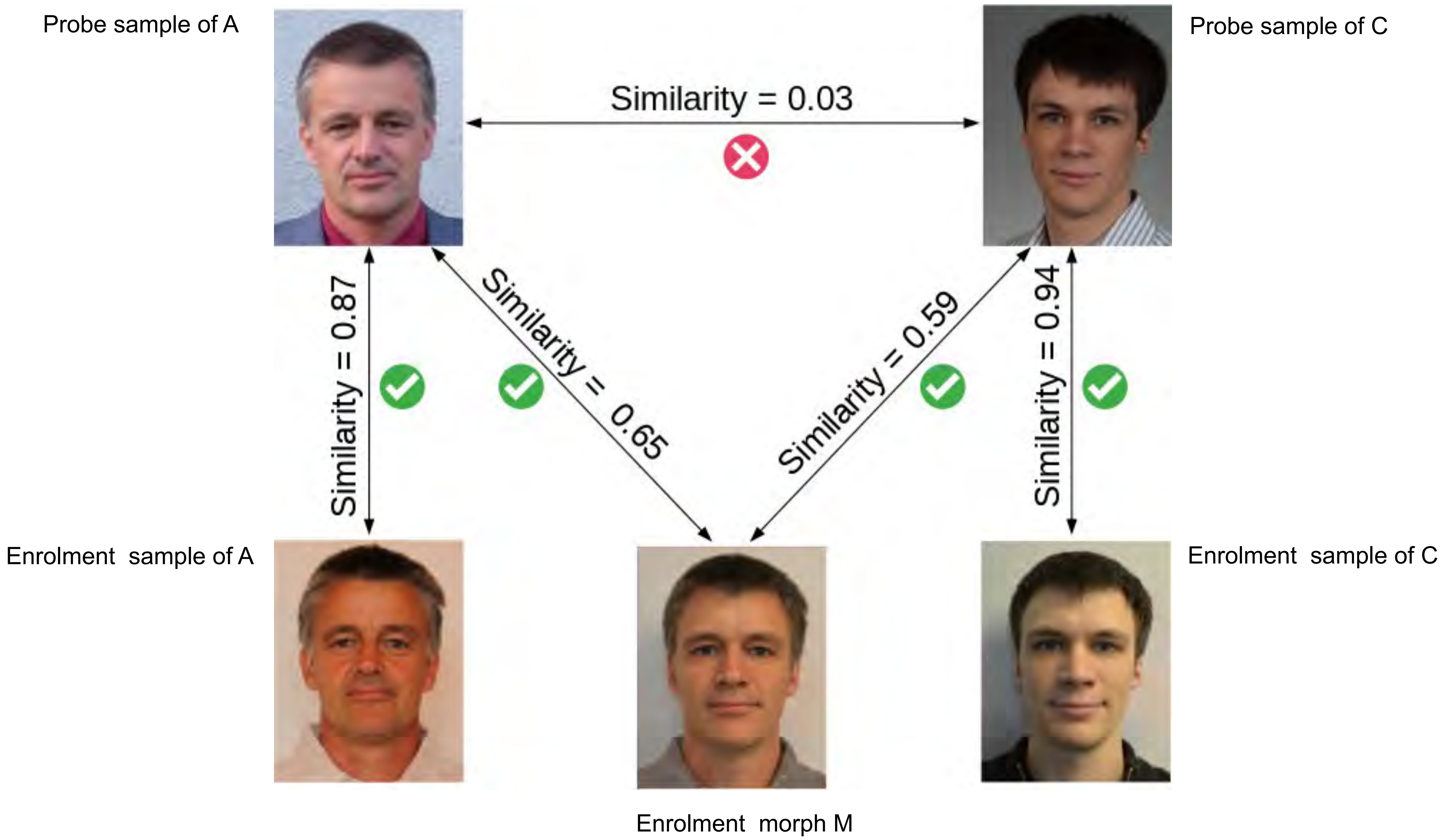
Morphing attack scenario

- Border control



Problem: Morphing Attacks

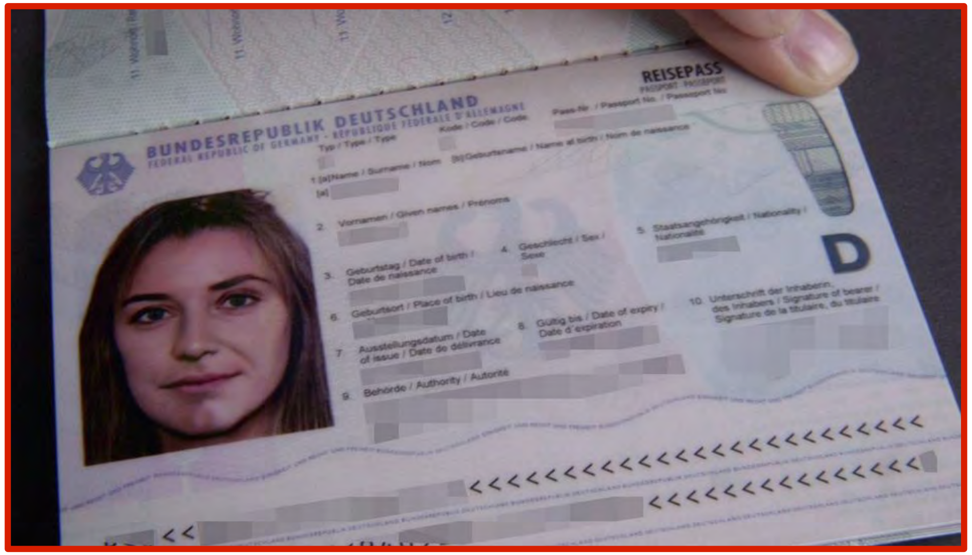
Verification against morphed facial images



Problem: Morphing Attacks

Is it a really problem ? - YES!

- In September 2018 German activists
  - used a morphed images of Federica Mogherini (High representative of the European Union for Foreign Affairs and Security Policy) and a member of their group
  - and received an authentic German passport.



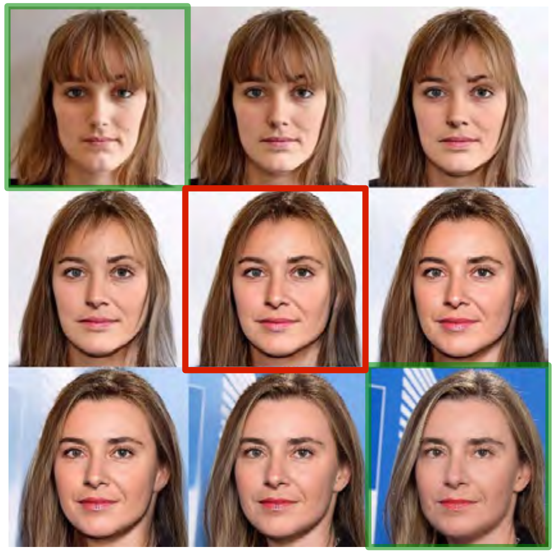


Image source: https://www.spiegel.de/netzwelt/netzpolitik/biometrie-im-reisepass-peng-kollektiv-schmuggelt-fotomontage-in-ausweis-a-1229418.html

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

Problem: Morphing Attacks

Proposed solutions to the Morphing Attack Problem:

- 1.) Photo studio should digitally sign the picture taken by Photo Studio and send it to the passport application office
  - this is in progress for Finland
- 2.) Switch to live enrolment
  - that is the case for Norway and Sweden
- 3.) Software-supported detection of morphed face images

Regarding 2.) EU Regulation 2019/1157:

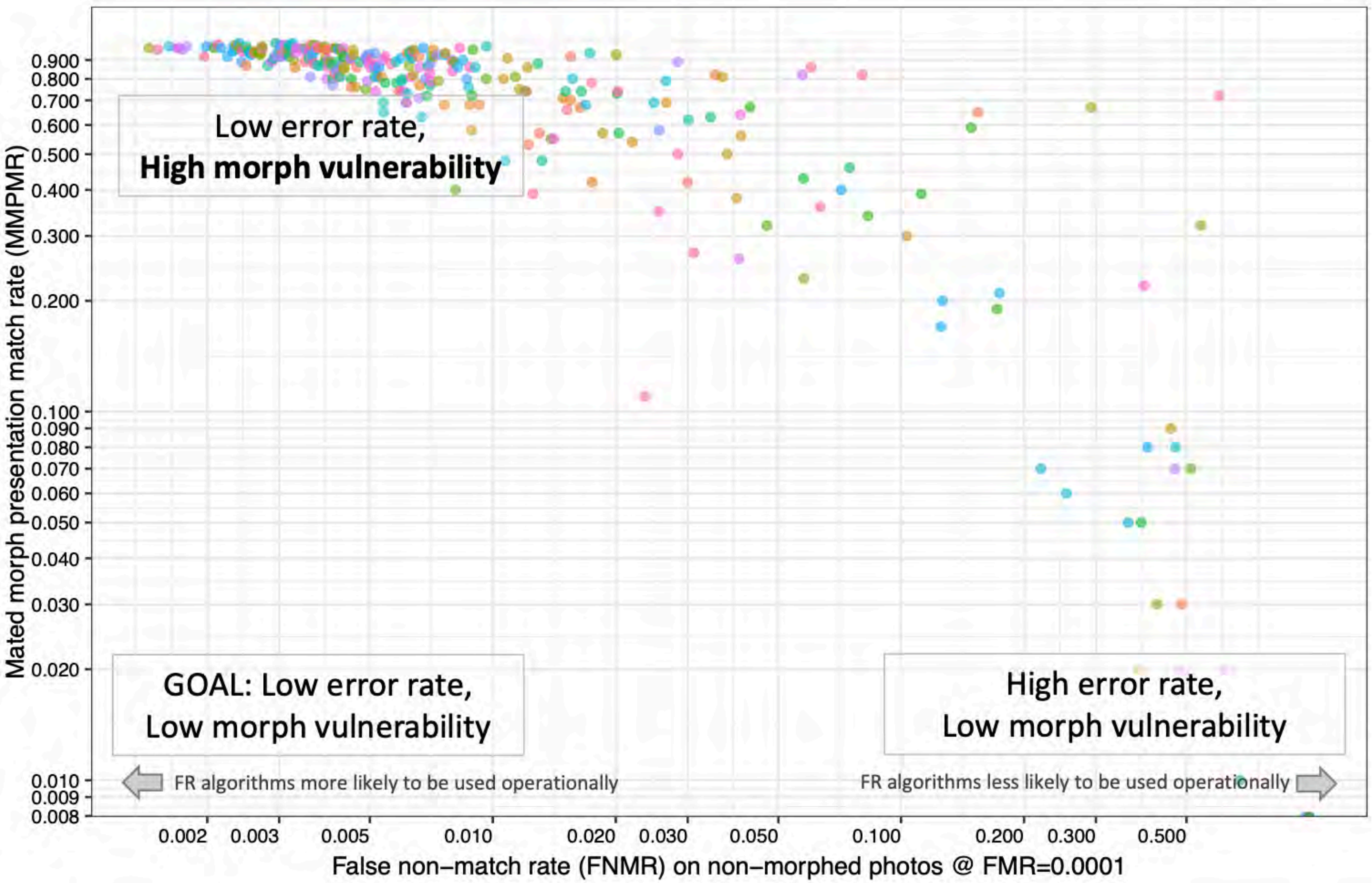
- on strengthening the security of identity cards in recital 32 states: *"... To this end, Member States could consider collecting biometric identifiers, particularly the facial image, by means of live enrolment by the national authorities issuing identity cards."*

What is the vulnerability of FRS?

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!

☹

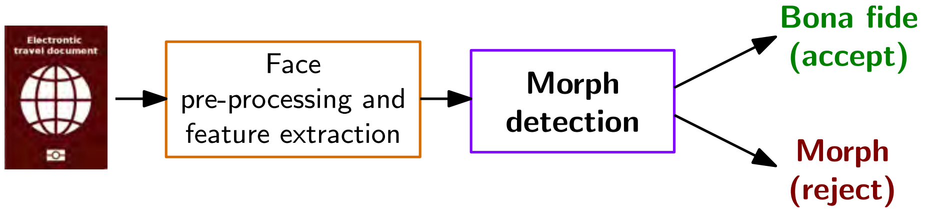
Morphing Attack Detection (MAD)

Scenarios and Methods

Morphing Attack Detection Scenarios

Real world scenarios

- Single image morphing attack detection (S-MAD)
  - One single *suspected* facial image is analysed (e.g. in the passport application)

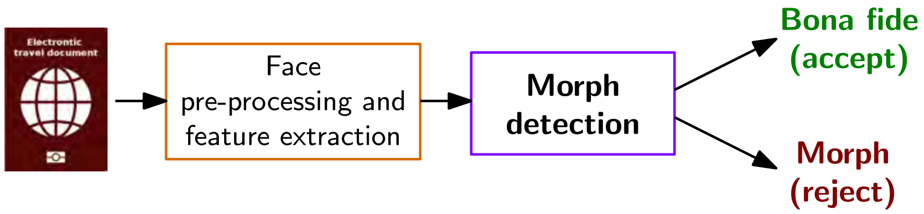

Electronic travel document
Face pre-processing and feature extraction
Morph detection
Bona fide (accept)
Morph (reject)

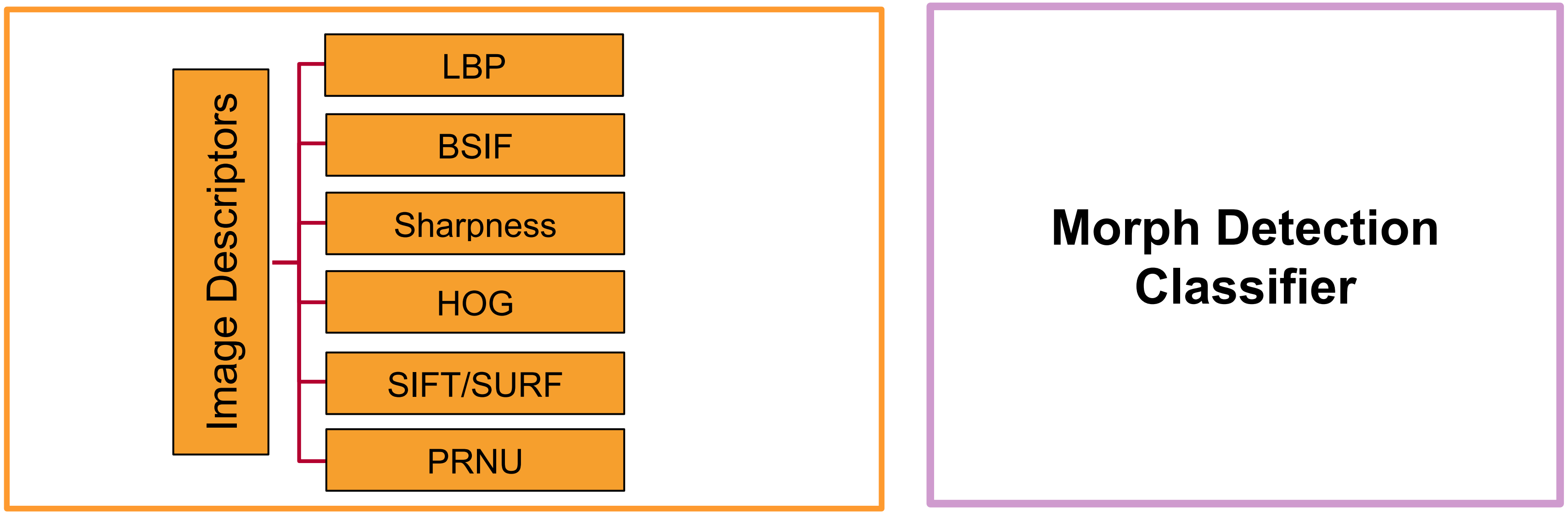
[SRB2018a] U. Scherhag, C. Rathgeb, C. Busch: "Towards Detection of Morphed Face Images in electronic Travel Documents“, in Proceedings of the 13th IAPR International Workshop on Document Analysis Systems (DAS), April 24-27, (2018)

Face Pre-processing and Feature Extraction

Morphing Attack Detection (S-MAD) with texture analysis

- Image descriptors as hand-crafted features


Electrontic travel document
Face pre-processing and feature extraction
Morph detection
Bona fide (accept)
Morph (reject)

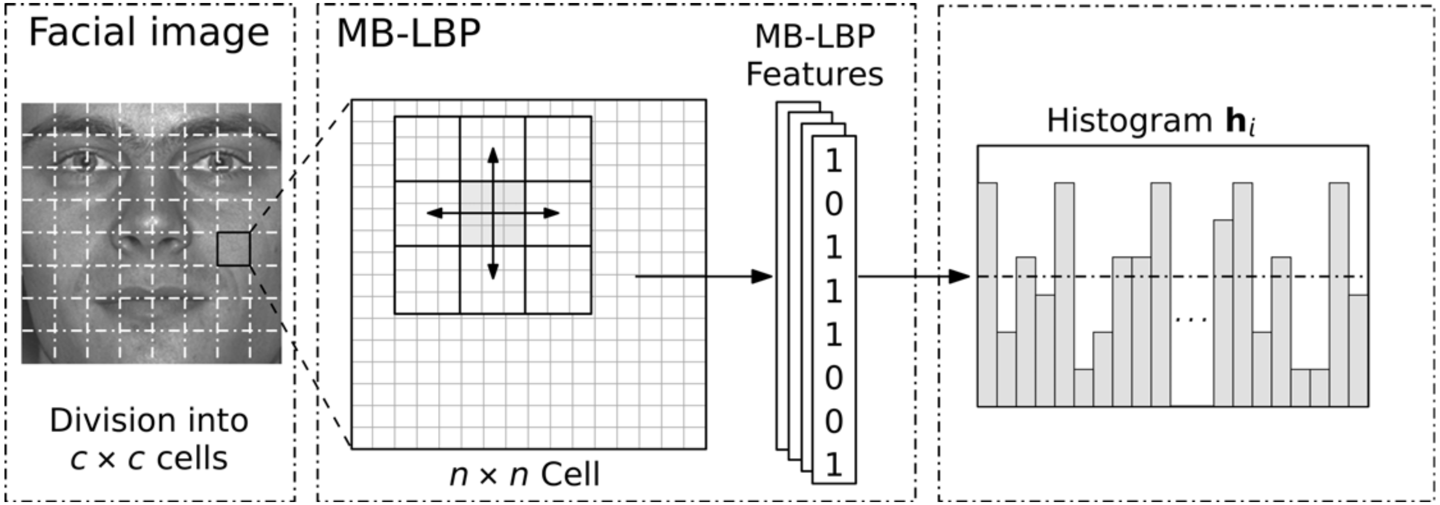


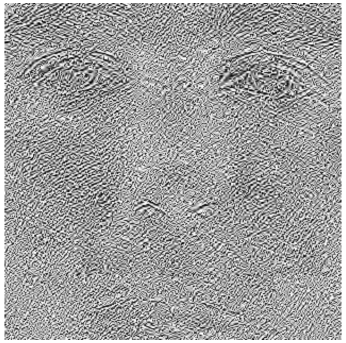
[SRB2018b] U. Scherhag, C. Rathgeb, C. Busch: „Detection of Morphed Faces from Single Images: a Multi-Algorithm Fusion Approach“, in Proceedings if of the 2nd International Conference on Biometric Engineering and Applications (ICBEA), Amsterdam, The Netherlands, May 16-18, (2018)

Face Pre-processing and Feature Extraction

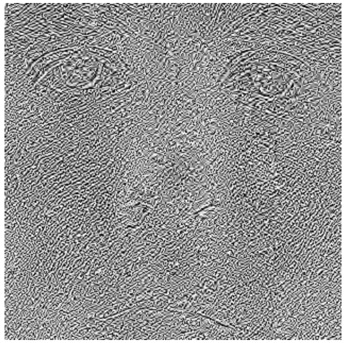
S-MAD with image descriptor

- Local Binary Pattern (LBP)





Morph

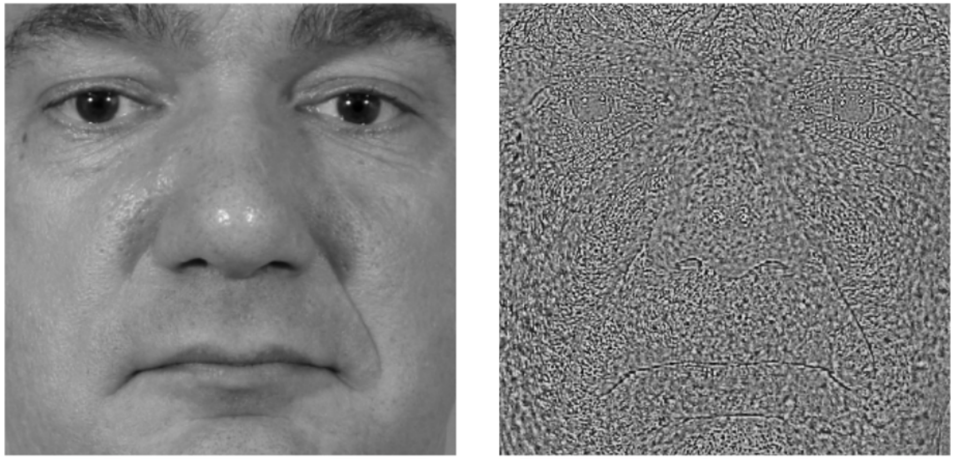


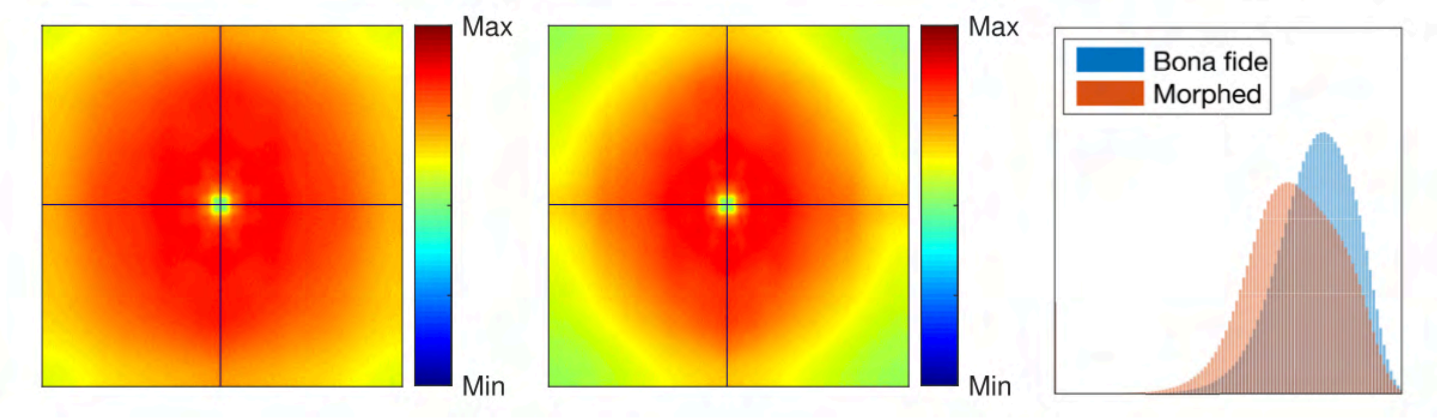
Bona Fide

Face Pre-processing and Feature Extraction

S-MAD with image descriptor / forensic approach

- Photo Response Non-Uniformity (PRNU)





Bona Fide

Morph

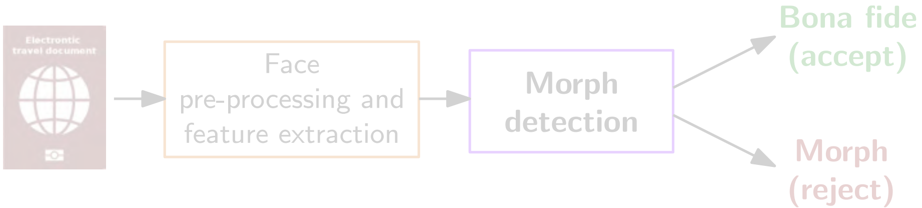
Histograms

[SDRBU2019] U. Scherhag, L. Debiasi, C. Rathgeb, C. Busch and A. Uhl: "Detection of Face Morphing Attacks based on PRNU Analysis“, in IEEE TBIOM, (2019)

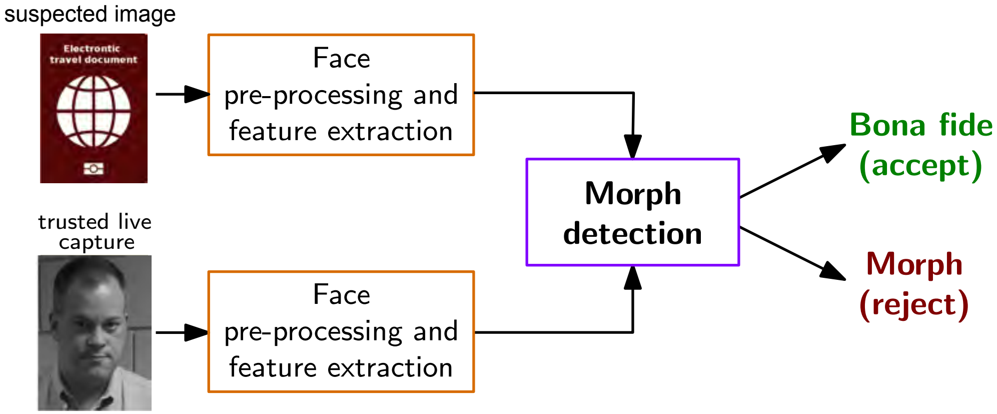
Morphing Attack Detection Scenarios

Real world scenarios

- Single image morphing attack detection (S-MAD)
  - One single *suspected* facial image is analysed (e.g. in the passport application)


Electronic travel document
Face pre-processing and feature extraction
Morph detection
Bona fide (accept)
Morph (reject)

- Differential morphing attack detection (D-MAD)
  - A pair of images is analysed - and one is a trusted Bona Fide image
  - Biometric verification (e.g. at the border)

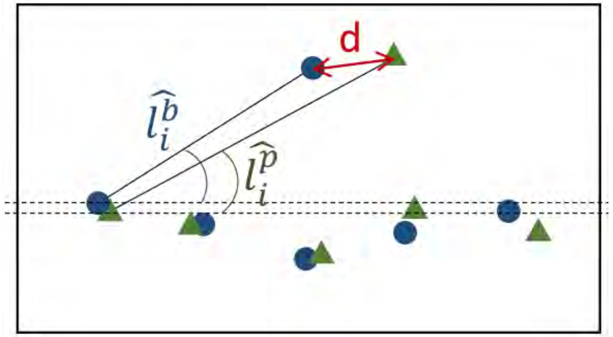

suspected image
Electronic travel document
trusted live capture
Face pre-processing and feature extraction
Face pre-processing and feature extraction
Morph detection
Bona fide (accept)
Morph (reject)

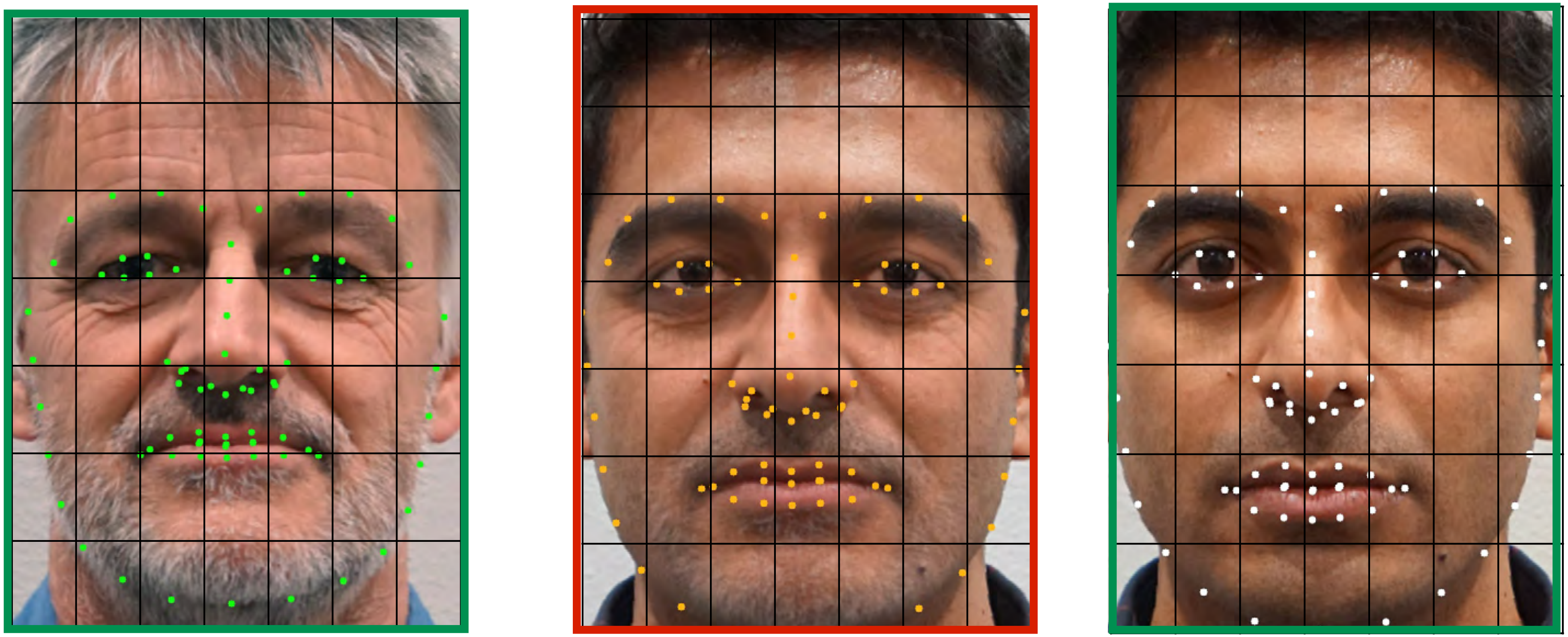
[SRB2018a] U. Scherhag, C. Rathgeb, C. Busch: "Towards Detection of Morphed Face Images in electronic Travel Documents“, in Proceedings of the 13th IAPR International Workshop on Document Analysis Systems (DAS), April 24-27, (2018)

Differential Morphing Attack Detection

D-MAD with landmark analysis

- Angle based features
- Distance based features



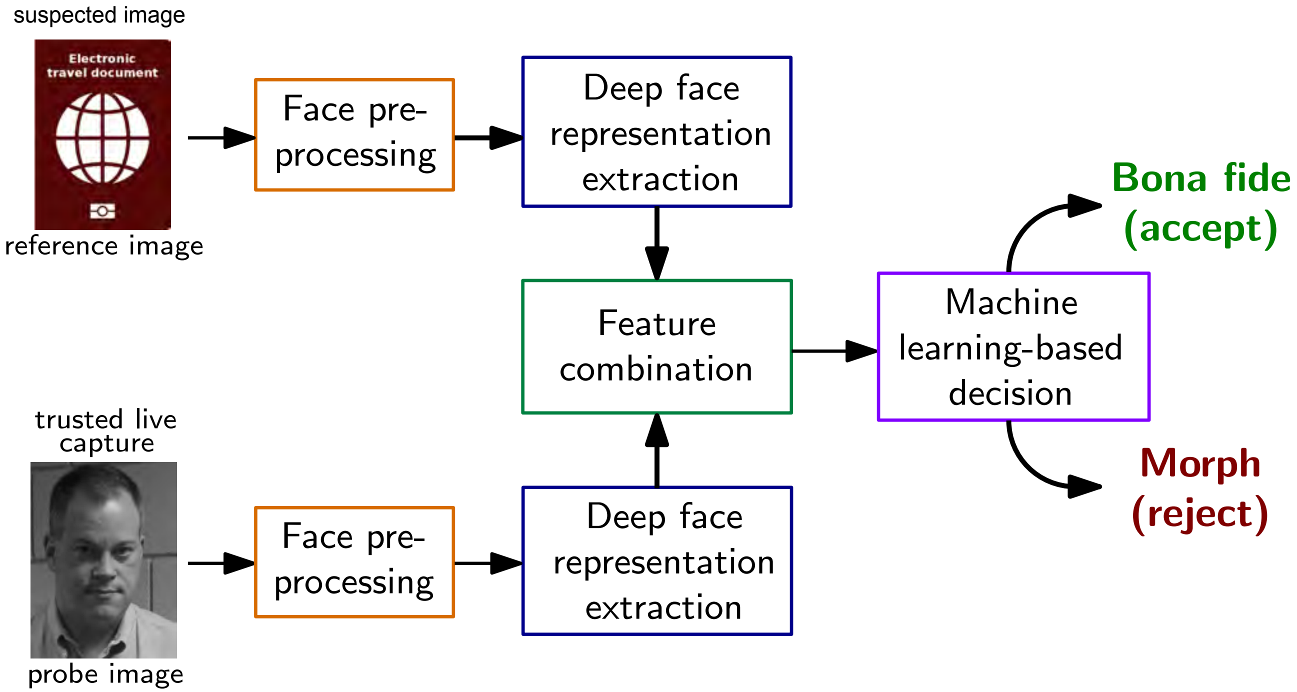


[SDGB2018] U. Scherhag, D. Budhrani, M. Gomez-Barrero, C. Busch: "Detecting Morphed Face Images Using Facial Landmarks“, in Proceedings of International Conference on Image and Signal Processing (ICISP), (2018)

Differential Morphing Attack Detection

D-MAD with deep learning

- Deep Face representations of Deep CNNs



suspected image

reference image

trusted live capture

probe image

Face pre-processing

Face pre-processing

Deep face representation extraction

Deep face representation extraction

Feature combination

Machine learning-based decision

Bona fide (accept)

Morph (reject)

  - 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

NIST FRVT MORPH

NIST IR 8292 report presented September, 2022

FRVT MORPH

https://pages.nist.gov/frvt/html/frvt_morph.html

- results for MAD algorithms from six research labs:
  - University of Bologna (UBO)
  - Norwegian University of Science and Technology (NTNU)
  - Hochschule Darmstadt (HDA)
  - West Virginia University (WVU)
  - Universidade de Coimbra (VIS)
  - secunet (SEC)

NISTIR 8292 DRAFT SUPPLEMENT

Face Recognition Vendor Test (FRVT)

Part 4: MORPH - Performance of Automated Face Morph Detection

Mei Ngan
Patrick Grother
Kayee Hanaoka
Jason Kuo
Information Access Division
Information Technology Laboratory

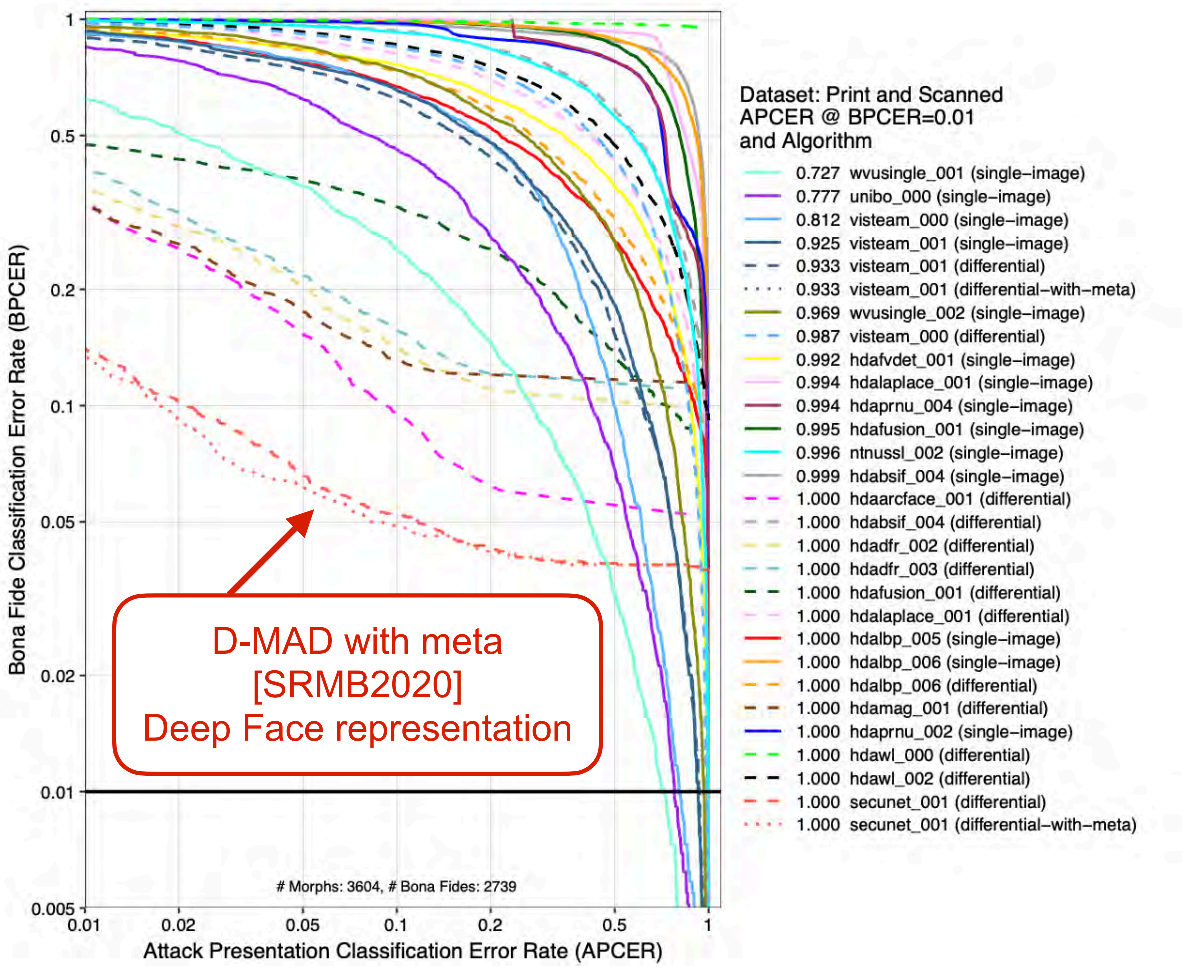
This publication is available free of charge from:
https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST FRVT MORPH

NIST IR 8292 report presented September, 2022

- Performance of Automated Face Morph Detection
  https://pages.nist.gov/frvt/reports/morph/frvt_morph_report.pdf
  - results for print and scanned morphs

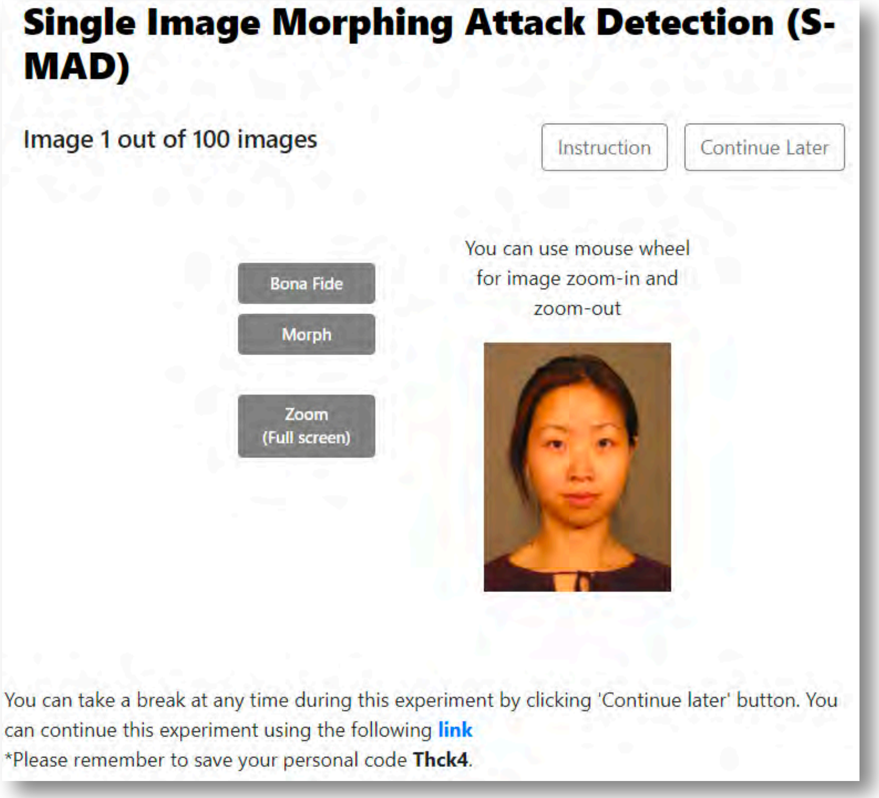


D-MAD with meta
[SRMB2020]
Deep Face representation

Human Experts in MAD

Border guards, case handlers, document examiners, ID experts

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



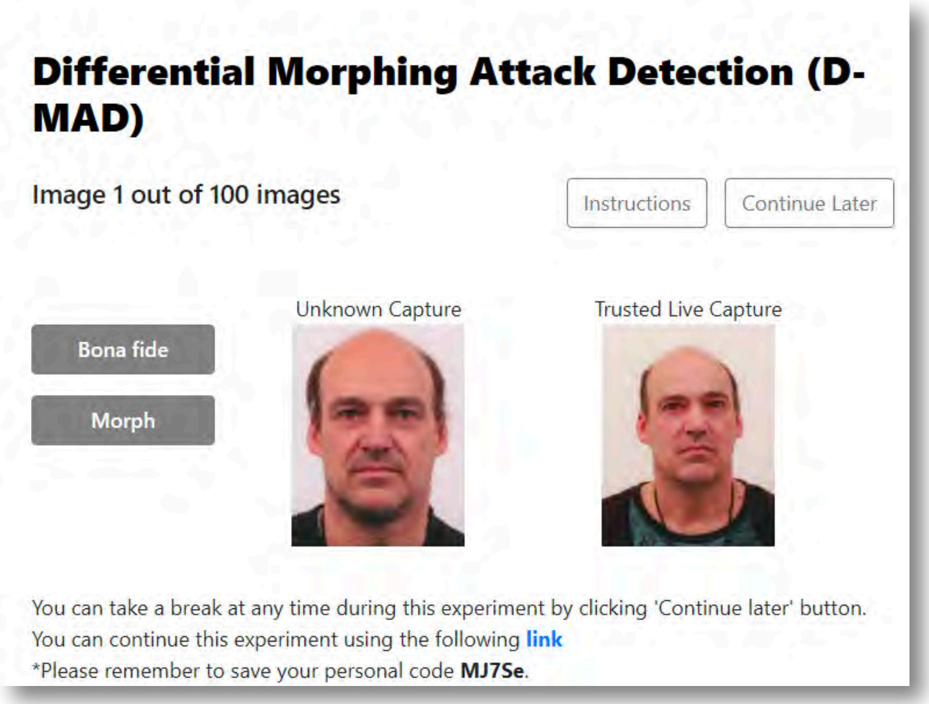
Single Image Morphing Attack Detection (S-MAD)

Image 1 out of 100 images

You can use mouse wheel for image zoom-in and zoom-out

You can take a break at any time during this experiment by clicking 'Continue later' button. You can continue this experiment using the following link

*Please remember to save your personal code **Thck4**.



Differential Morphing Attack Detection (D-MAD)

Image 1 out of 100 images

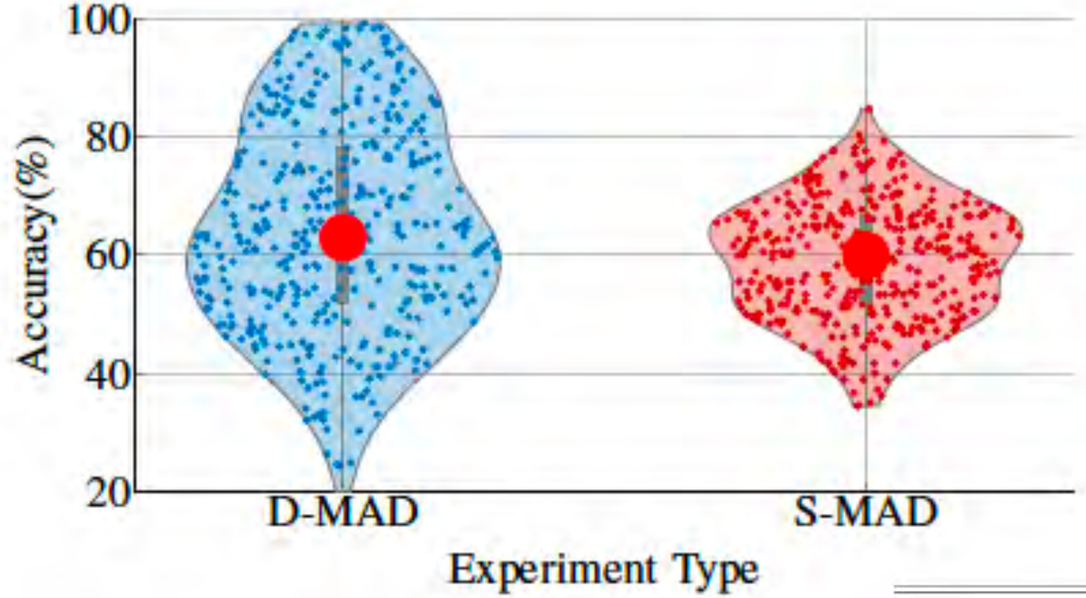
You can take a break at any time during this experiment by clicking 'Continue later' button. You can continue this experiment using the following link

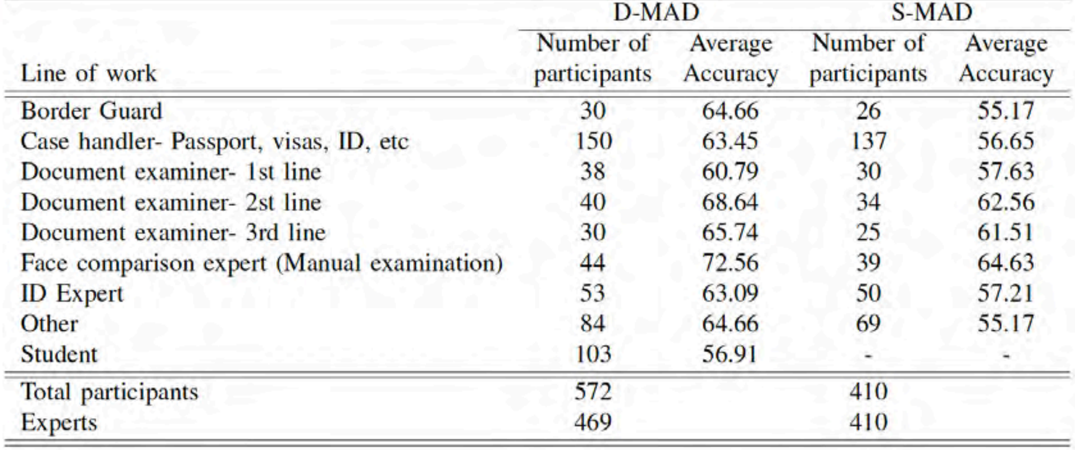
*Please remember to save your personal code **MJ7Se**.

[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



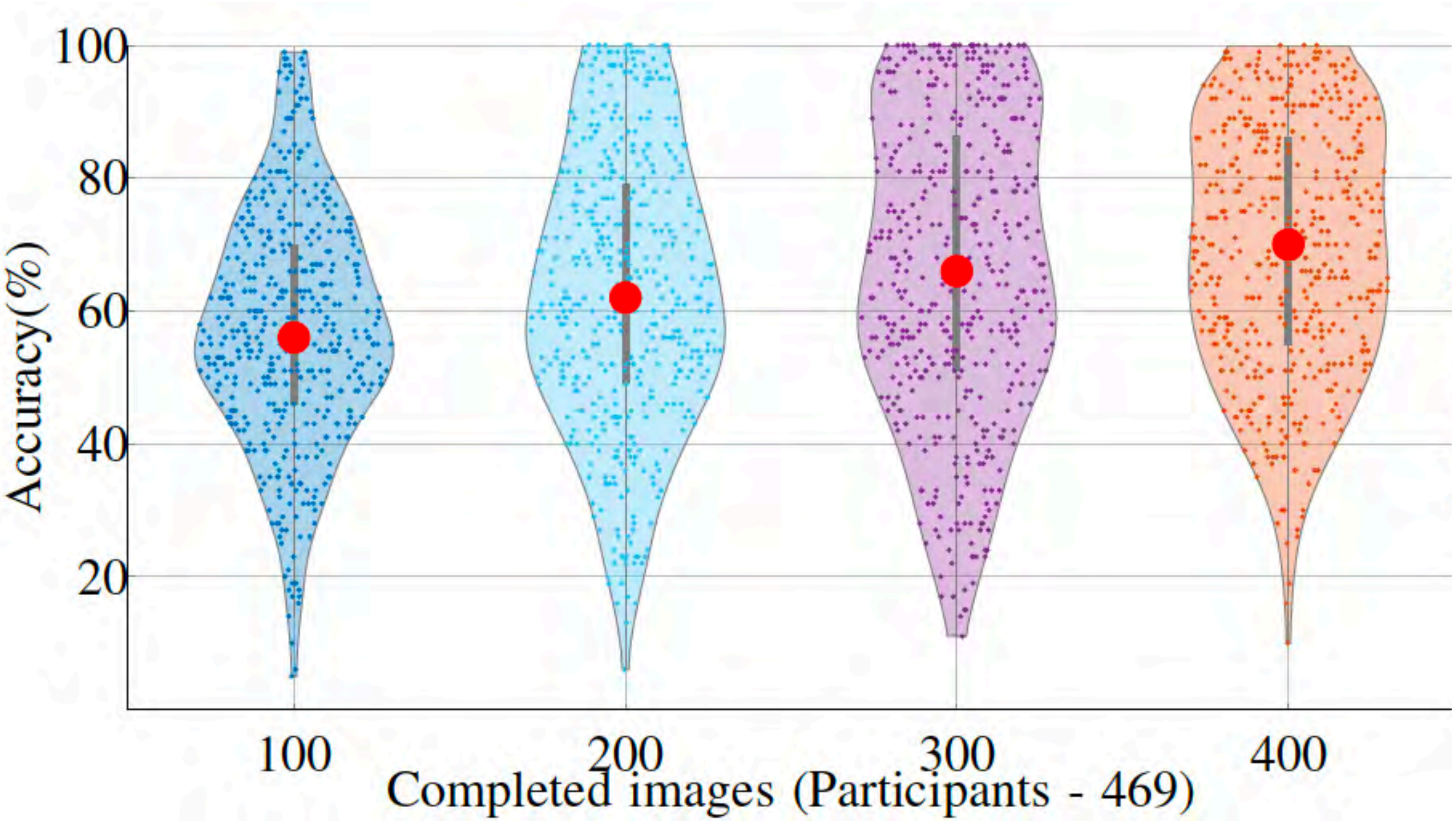


	D-MAD		S-MAD	
Line of work	Number of participants	Average Accuracy	Number of participants	Average Accuracy
Border Guard	30	64.66	26	55.17
Case handler- Passport, visas, ID, etc	150	63.45	137	56.65
Document examiner- 1st line	38	60.79	30	57.63
Document examiner- 2st line	40	68.64	34	62.56
Document examiner- 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

Conclusion

We are facing a situation, where

- Passports with morphs are already in circulation
  - 1000+ reported cases
  - Switch to live enrolment is a good decision,
    but does not solve the problem - at least for the upcoming 10 years
- Passports with morphed face images
  will have a major impact on border security
  - introduction of EU’s entry/exit system
- In combination with passport brokers a dramatic problem
  - the darknet offers numerous opportunities …

- Summary: MAD is the hardest challenge that I have seen
  in my 25 research years on biometrics

More information

The MAD website

https://www.christoph-busch.de/projects-mad.html

The MAD survey papers

- U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, C. Busch: "Face Recognition Systems under Morphing Attacks: A Survey“, in IEEE Access, (2019) https://ieeexplore.ieee.org/document/8642312

IEEE Access

Face Recognition Systems Under Morphing Attacks: A Survey

ULRICH SCHERHAG, CHRISTIAN RATHGEB, JOHANNES MERKLE, RALPH BREITHAUPT, AND CHRISTOPH BUSCH

- S. Venkatesh, R. Raghavendra, K. Raja, C. Busch: "Face Morphing Attack Generation & Detection: A Comprehensive Survey", in IEEE Transactions on Technology and Society (TTS), (2021) https://ieeexplore.ieee.org/document/9380153

Transactions on Technology and Society

Face Morphing Attack Generation & Detection: A Comprehensive Survey

Sushma Venkatesh Raghavendra Ramachandra Kiran Raja Christoph Busch
Norwegian University of Science and Technology (NTNU), Norway
E-mail: {sushma.venkatesh;raghavendra.ramachandra;kiran.raja;christoph.busch} @ntnu.no

More information on MAD

The 2021 NBL - EAB workshop

https://eab.org/events/program/229

- Luuk Spreeuwers (University of Twente) - recorded talk
  - Morphing Attacks on Face Recognition Systems
- David Robertson (University of Strathclyde) - recorded talk
  - Psychological Experiments on Morphed Faces
- Kiran Raja (NTNU) - recorded talk
  - Morphing Attack Detection Approaches
- Matteo Ferrara (University of Bologna) - recorded talk
  - Bologna Online Evaluation Platform
- Frøy Løvåsdal (Norwegian Police) - recorded talk
  - Morphing Attack Detection Capabilities of Human Examiners
- Mei Ngan (NIST) - recorded talk
  - Face Morphing Detection Evaluation
- Naser Damer (Fraunhofer IGD) - recorded talk
  - Generating Morphs with Generative Adversarial Networks
- Christian Rathgeb (Hochschule Darmstadt) - recorded talk
  - Detection of Face Beautification Manipulations
- Uwe Seidel (BKA)
  - Research Needs for Morphing Attack Detection

More Information on MAD

National Institute of Standards and Technology (NIST)

- Will host the virtual
  3rd International Face Performance Conference (IFPC)
- November 15 - 17, 2022.
- The registration is open and free.
- The first draft agenda is posted at:
  https://www.nist.gov/news-events/events/2022/11/international-face-performance-conference-ifpc-2022
- The presentations:
  - Matjaž Torkar (Ministry of the Interior Police, Slovenia)
    - Morphing Cases in Slovenia
  - Matteo Ferrara (University of Bologna)
    - Morphing Attack Potential (MAP)
  - Nasser Nasrabadi (West Virginia University)
    - Face Morph Generation and Attack Detection
  - Kiran Raja (Norwegian University of Science and Technology)
    - Overview on Morph Attack Detection Development
  - Frøy Løvåsdal (National Police Directorate, Norway)
    - Morphing Attack Detection - Analysing Human Observer Ability

Thanks

I would like to thank my colleagues working on this topic:

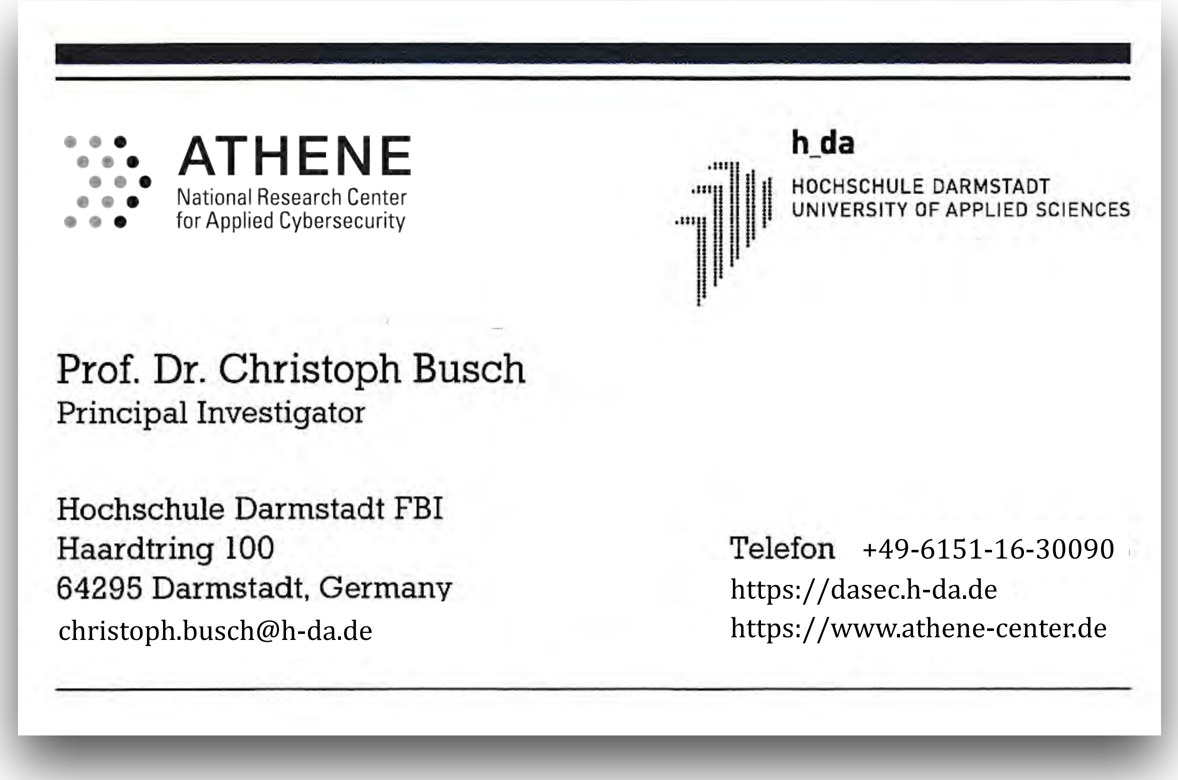
- In the NBL - HDA research group:
  - Kiran Raja, Raghu Ramachandra, Loic Bergeron, Sankini Godage, Guoqiang Li, Jag Mohan Singh, Sushma Venkatesh, Haoyu Zhang
  - Ulrich Scherhag, Christian Rathgeb, Daniel Fischer, Siri Lorenz, Robert Nichols Sergey Isadskiy, Marta Gomez-Barrero, Juan Tapia, Mathias Ibsen

- In the FACETRUST-Project:
  - Ralph Breithaupt, Johannes Merkle

- In the SOTAMD-Project and iMARS-Project:
  - Dinusha Frings, Fons Knopjes, Uwe Seidel, Frøy Løvåsdal
  - Davide Maltoni, Matteo Ferrara, Analisa Franco
  - Raymond Veldhuis, Luuk Spreeuwers,

- In the NIST-FRVT-MORPH-Project:
  - Mei Ngan, Patrick Grother, Kayee Hanaoka, Jason Kuo

Contact



ATHENE
National Research Center
for Applied Cybersecurity

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

Prof. Dr. Christoph Busch
Principal Investigator

Hochschule Darmstadt FBI
Haardtring 100
64295 Darmstadt, Germany
christoph.busch@h-da.de

Telefon +49-6151-16-30090
https://dasec.h-da.de
https://www.athene-center.de