Update on latest PAD & Morphing Developments

Christoph Busch

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

latest news at:
https://twitter.com/busch_christoph

secunet EES workshop, December 1, 2020

ATHENE
Steinbeis-Transferzentrum BISE – Biometrie

European Association for Biometrics
eab
Human Identity in Europe

NTNU

About my Affiliation(s)

Darmstadt Research Group
@Hochschule Darmstadt

ATHENE
National Research Center
for Applied Cybersecurity

h_da

Steinbeis-Transferzentrum
BISE – Biometrie

About my Affiliation(s)

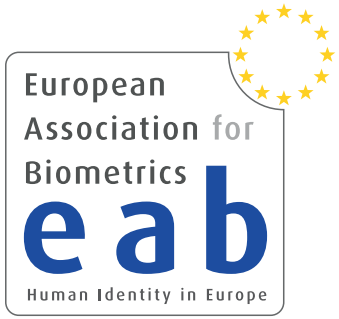
Gjøvik Research Group
@Norwegian University of Science and Technology

NTNU

NORWEGIAN BIOMETRICS LABORATORY

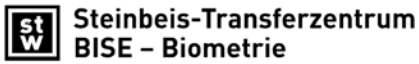
About my Affiliation(s)

European Association for Biometrics (EAB)



Darmstadt Research Group @Hochschule Darmstadt

h_da



Gjøvik Research Group @Norwegian University of Science and Technology

Introduction

European Association for Biometrics (EAB)

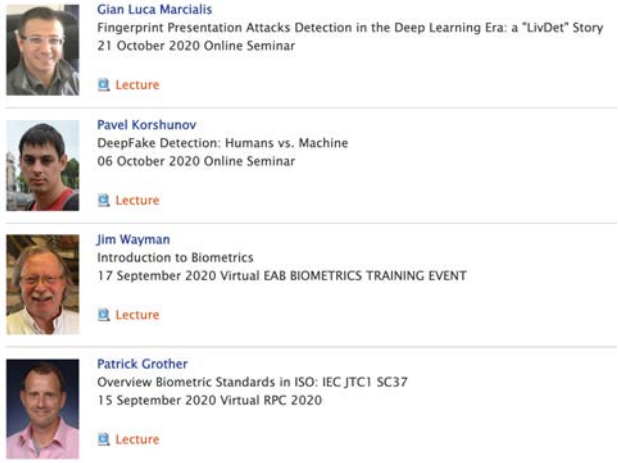
- The EAB is a non-profit, nonpartisan association
  https://eab.org/
- EAB supports all sections of the ID community across Europe, including governments, NGO's, industry, associations and special interest groups and academia.

- Our role is to promote the responsible use and adoption of modern digital identity systems that enhance people's lives and drive economic growth.

Introduction

European Association for Biometrics (EAB)

- Our initiatives are designed to foster networking
  - Annual conference: EAB-RPC
    https://eab.org/events/program/195
  - Biometric Training Event
    https://eab.org/events/program/208
  - Workshops on relevant topics (e.g. Presentation Attack Detection, Morphing Attack Detection, Sample Quality, Bias in Biometric Systems)
    https://eab.org/events/
  - Online Seminar every second week
    https://eab.org/events/program/227
  - Recorded keynote talks
    https://eab.org/events/lectures.html
  - Monthly newsletter
    https://eab.org/news/newsletter.html
  - Annual academic graduation report
    https://eab.org/upload/documents/1799/EAB-research-report-2019.pdf
  - Open source repository
    https://eab.org/information/software.html



Introduction

European Association for Biometrics (EAB)

- Key stakeholders of EAB are „standardisation enthusiasts“ in ISO/IEC JTC1 SC37
- Key stakeholder of EAB are core members of European research projects on pressing operational problems and vulnerabilities of large scale systems like VIS and EES
  - Presentation Attack Detection
  - Morphing Attack Detection
  - Sample Quality
- Project examples are
  - TReSPAsS ETN on secure and privacy preserving biometrics https://www.trespass-etn.eu/
  - iMARS on morphing attack detection https://cordis.europa.eu/project/id/883356

Introduction

Definition of a biometric capture device

- **biometric capture device:**
  - *device that collects a signal from a biometric characteristic and converts it to a captured biometric sample*

  - Note 1 to entry: A signal can be generated by the biometric characteristic or generated elsewhere and affected by the biometric characteristic, for example, face illuminated by incident light.
  - Note 2 to entry: A biometric capture device can be any piece of hardware (and supporting software and firmware).
  - Note 3 to entry: A biometric capture device may comprise components such as an illumination source, one or more biometric sensors, etc.

  https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-2:v1:en:term:3.4.1

Introduction

The capture environment may change

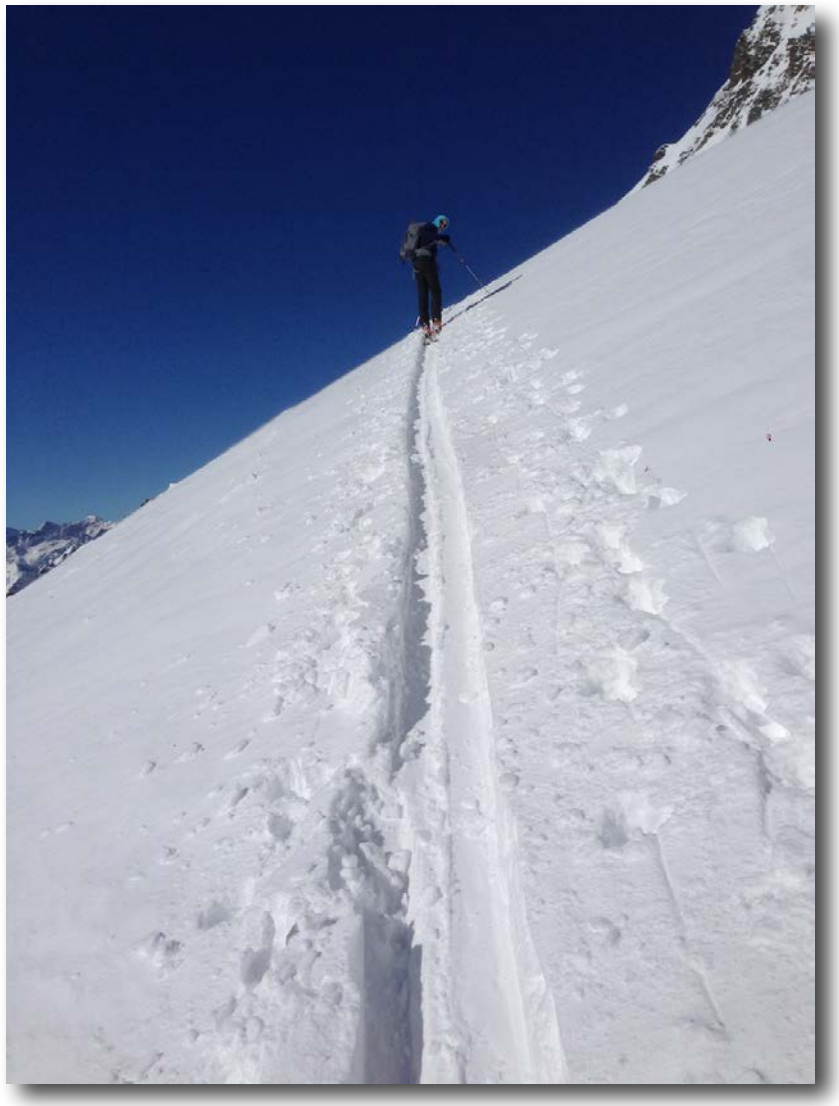
- Fingerprint capture process
- Acquisition under controlled conditions
  - Data subject - police officer
  - Controlled distance
  - analog representation

Image Source: BKA

Introduction

The capture environment may change

- Face capture process
- Acquisition in the wild:
  - Data subject with uncontrolled pose, occlusions (head cover, sun glasses)
  - Unknown distance subject to the capture device
  - Low resolution images
    - 90 pixel inter eye distance?



Introduction

The EES self-service kiosk

- Is that capture in the wild?
- Is that controlled conditions?

Image Source: secunet

Image Source: Thales Gemalto

Image Source: Idemia

Image Source: Vision-Box

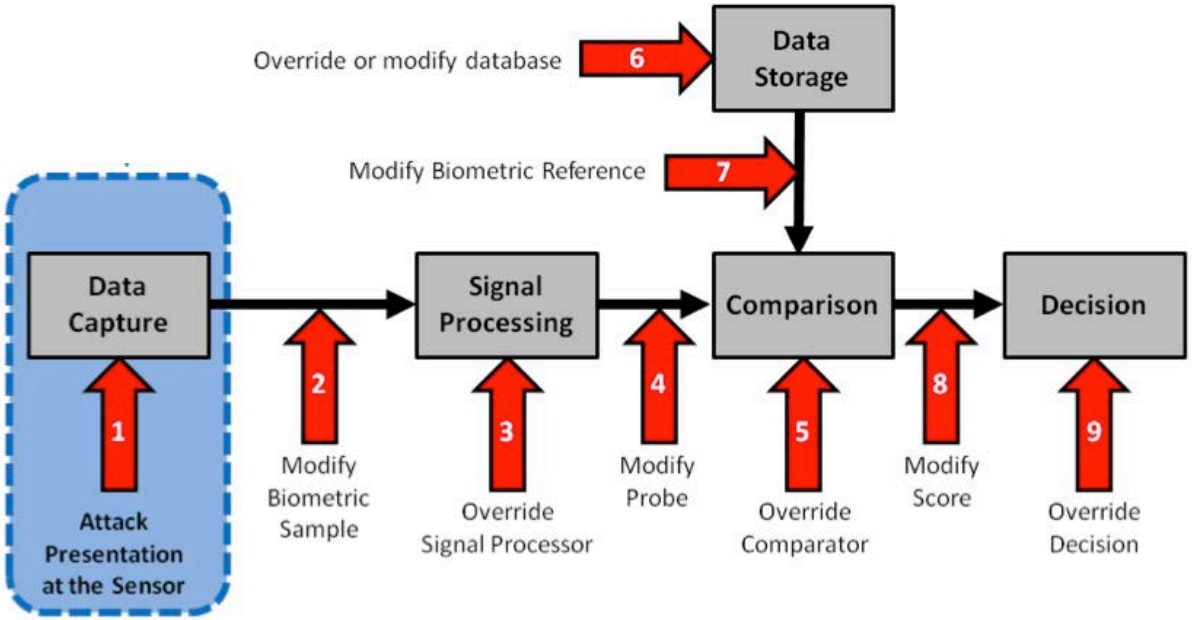
EES-kiosk enrolment systems are not in the wild,
but also **not** controlled (without attendance of a supervisor).

Thus we must look at the vulnerabilities of biometric systems!

Vulnerabilities of Biometric Systems

Three main points for a targeted attack

- Capture device (1): Camera, fingerprint sensor
  - Countered by presentation attack detection
- Data transmission (2): Network
  - Attacks on data transmission channel countered by cryptographic protocols
  - Enrolment attacks (i.e. face morphing attacks) need to be countered
- Data storage (6): Database
  - Countered by biometric template protection



Source: ISO/IEC 30107-1:2016

Presentation Attack Detection
in non-supervised Data Capture Situations (e.g. Kiosks)

Security of Fingerprint Sensors

Attack without support of an enrolled individual

- Recording of an analog fingerprint from flat surface material
  - z.B. glass, CD-cover, etc. with iron powder and tape
- Scanning and post processing:
  - Correction of scanning errors
  - Closing of ridge lines (as needed)
  - Image inversion
- Print on transparent slide
- Photochemical production of a circuit board

Historic - Year 2000 !

[Zwie2000] A. Zwiesele, A. Munde, C. Busch, H. Daum: "Comparative Study of Biometric Identification Systems"
In: 34th Annual 2000 IEEE International Carnahan Conference on Security Technology, Ottawa, pp. 60-63, (2000)

Presentation Attack Detection

Impostor

- impersonation attack
  - positive access 1:1 (two factor application)
  - positive access 1:N (single factor application)
- finding a look-a-like
- making appearance similar to the reference
- artefact presentation

Image Source: http://upshout.net/game-of-thrones-make-up

Concealer

- evasion from recognition
  - negative 1:N identification (watchlist application)
- depart from standard pose

- evade face detection

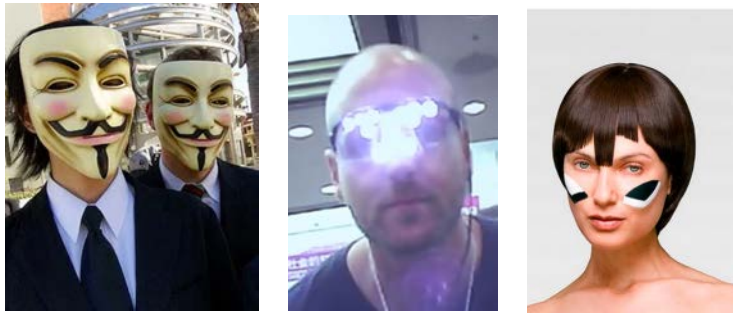


Image Source: https://www.youtube.com/watch?v=LRj8whKmN1M

Image Source: https://cvdazzle.com

Presentation Attack Detection

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 determination of a presentation attack

Definitions in ISO/IEC 2382-37: Vocabulary

http://www.christoph-busch.de/standards.html

- **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

Presentation Attack Detection

ISO/IEC 30107-1 - Definitions

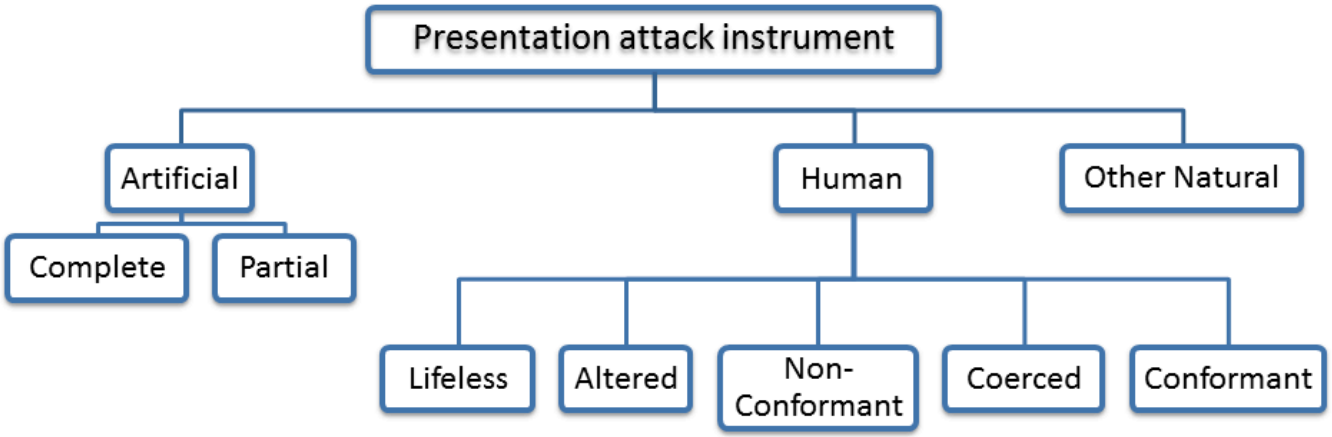
- **presentation attack instrument (PAI)**
  biometric characteristic or object used in a presentation attack
- **artefact**
  artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns

Types of presentation attacks

(General Noun)

(Adjectives describing categories)

(Qualifying adjectives)



Source: ISO/IEC 30107-1

Altered Fingerprint Detection - Testing

Example for fingerprint alterations

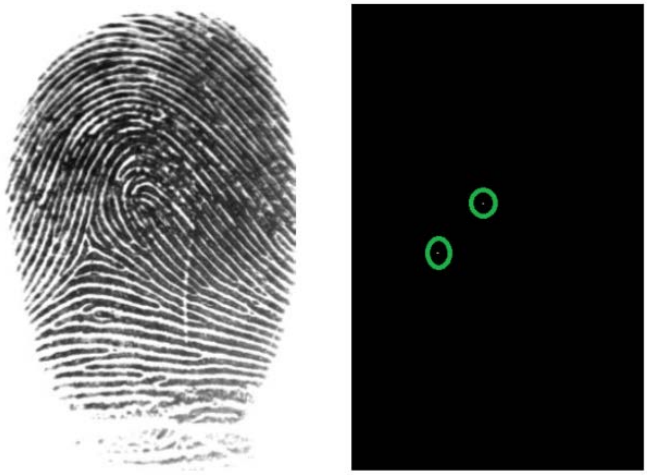
- Z-shaped alteration (Finger of Jose Izquierdo, 1995)

Image Source: S. Yoon, J. Feng, and A. Jain, “Altered fingerprints: Analysis and detection,”
IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 34, no. 3, pp. 451–464, Mar. 2012

Altered Fingerprint Detection - Algorithms

Singular Point Density Analysis

- using the Poincare´ index to detect noisy friction ridge areas



BonaFide fingerprint

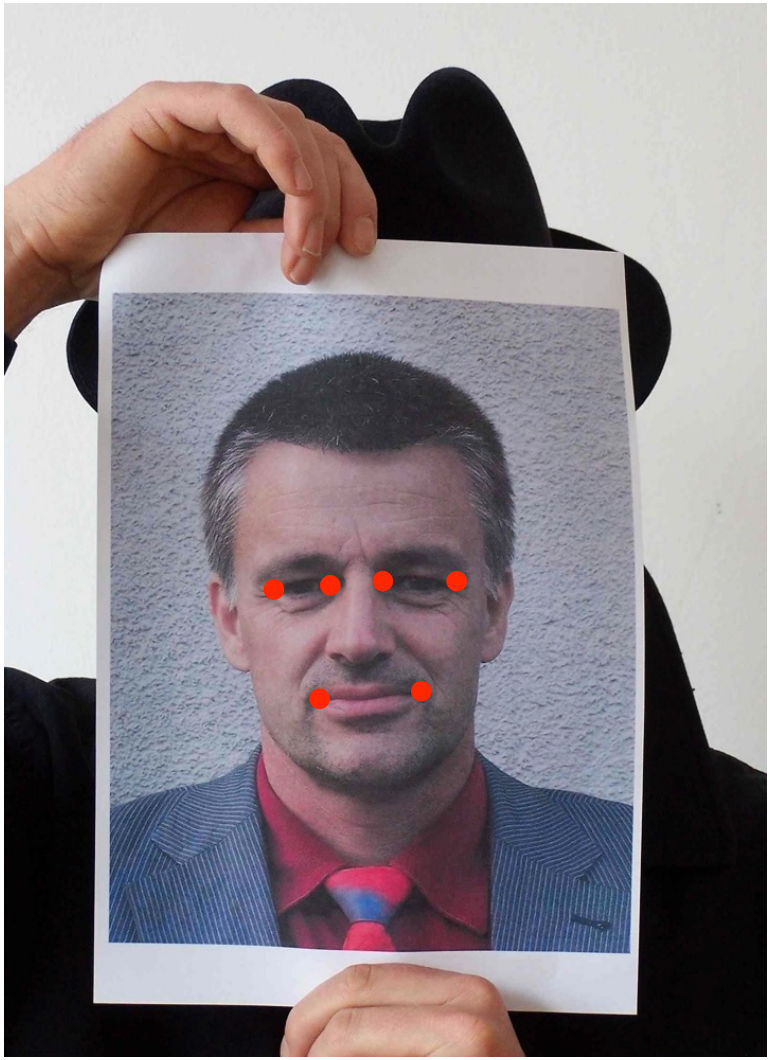
altered fingerprint

Poincare´ index response

[Ellingsg2014] J. Ellingsgaard, C. Sousedik, and C. Busch, “Detecting fingerprint alterations by orientation field and minutiae orientation analysis,” in Proc. IWBF, Valletta, Malta, (2014)

[Ellingsg2017] J. Ellingsgaard, C. Busch: "Altered Fingerprint Detection", in Handbook of Biometrics for Forensic Science, Springer, February, (2017)

Face Presentation Attacks

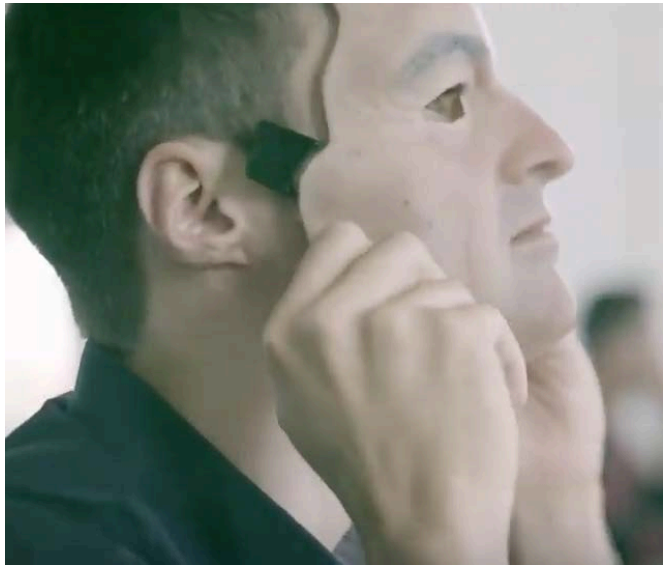


Historic - Year 2010!

Impostor Presentation Attack

3D silicone mask

- Targeted attack with 3D silicone custom mask
- Cost more than 3000 USD



Skin Detection with Dedicated Sensor

Short Wave Infrared Range (SWIR) imaging

- Analysis of spectral remission properties
- Remission spectrum above 1200 nm independent of melanin, but strongly impacted by water

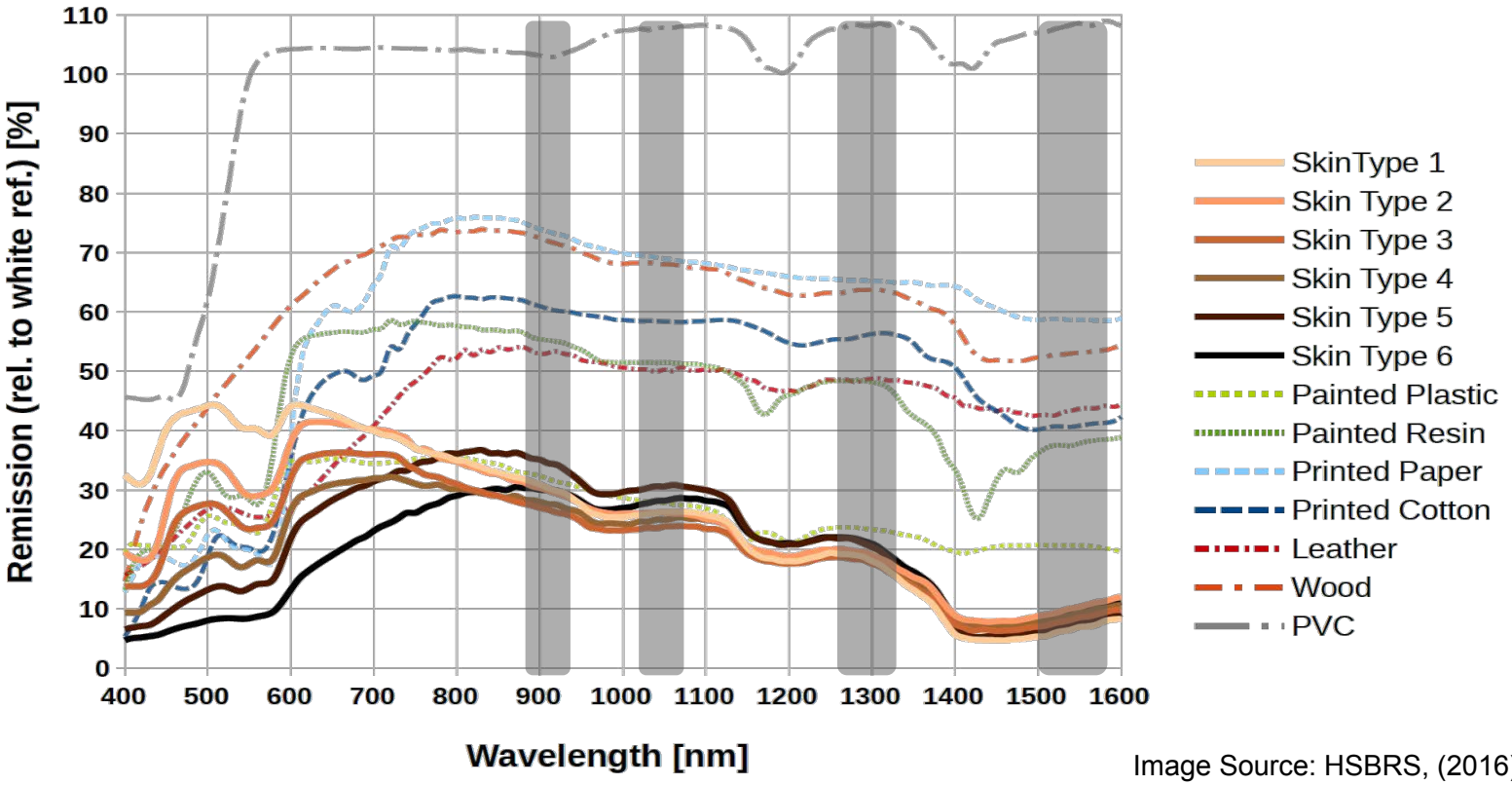


Image Source: HSBRS, (2016)

[Steiner2016] H. Steiner, A. Kolb, N. Jung: „Reliable Face Anti-Spoofing Using Multispectral SWIR Imaging“, in Proceedings ICB, (2016)

Skin Detection

Short Wave Infrared Range (SWIR) imaging

- Computing a signature from four spectral bands
  - Transform spectral remission to normalized differences
  - False color images based on three channel differences

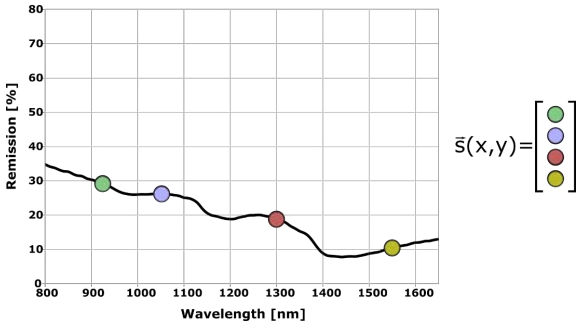


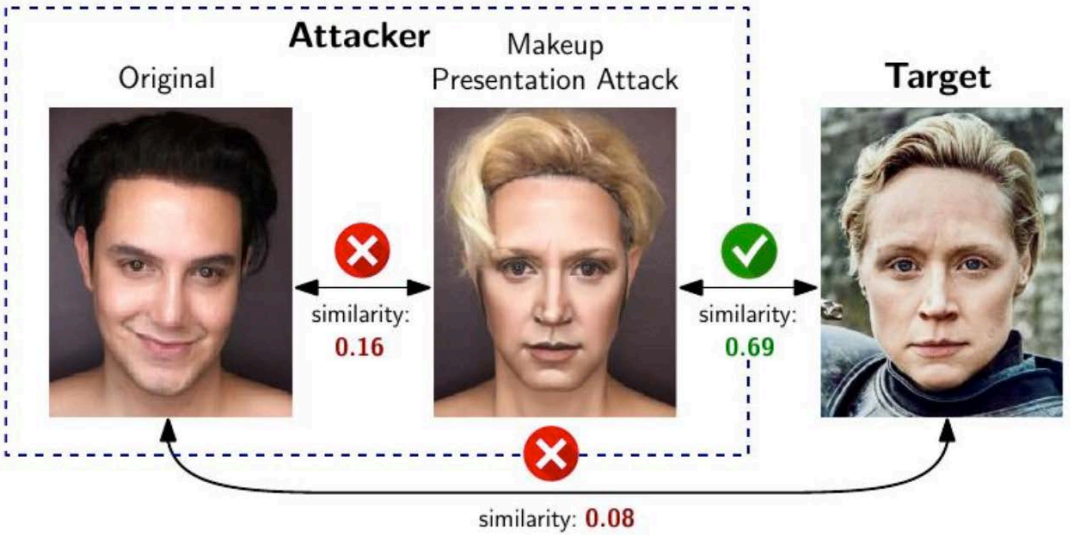
Image Source: HSBRS, (2016)

Makeup Presentation Attacks

Severe alterations

- Makeup for impersonation
- Detection difficult since bona fide users may also apply makeup

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

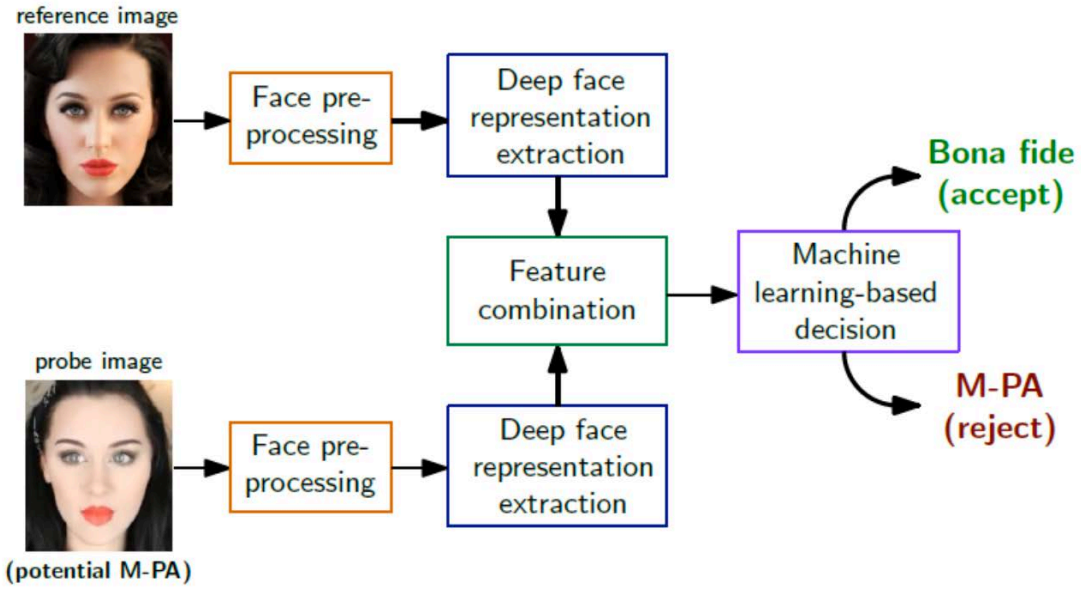


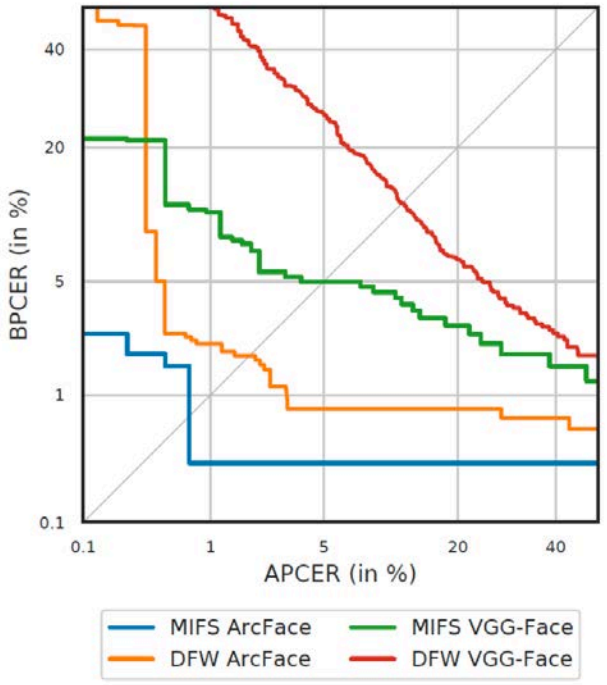
[Rathg2020] C. Rathgeb, P. Drozdowski, D. Fischer, C. Busch: "Vulnerability Assessment and Detection of Makeup Presentation Attacks“, in Proceedings of 8th International Workshop on Biometrics and Forensics (IWBF 2020), Porto, PT, April 29 - 30, (2020)

Makeup Presentation Attack Detection

Detecting alterations in a differential detection scenario

- Employ deep face representations (ArcFace)
- Classification with SVM
- Missing training data
  - Creation of semi-synthetic database

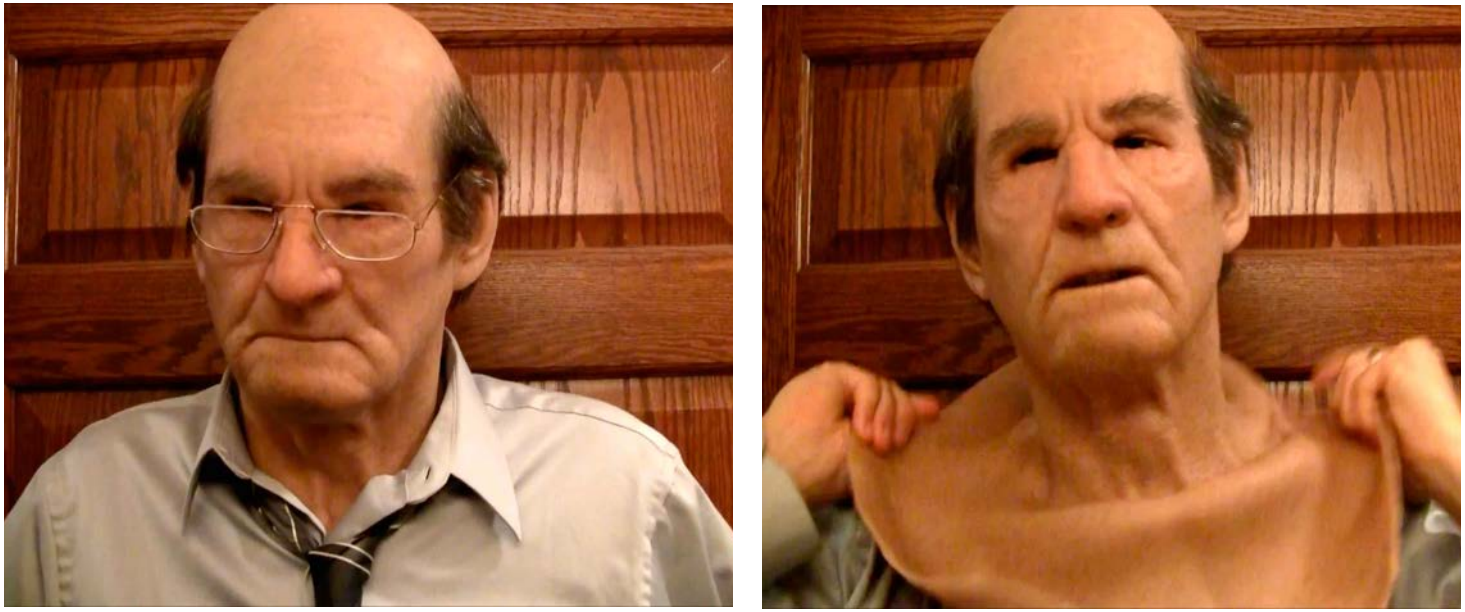




[RDB2020] C. Rathgeb, P. Drozdowski, C. Busch: "Detection of Makeup Presentation Attacks based on Deep Face Representations“, in Proceedings of 25th International Conference on Pattern Recognition (ICPR), (2020)

Impostor Presentation Attack

High end 3D silicone mask



Source: https://www.youtube.com/watch?v=2yuXTZGbJ38

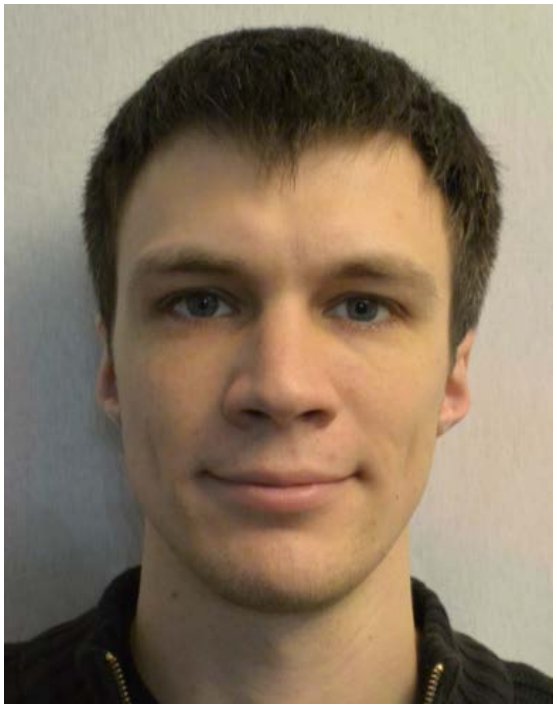
Enrolment Attacks
Face Morphing

Problem: Morphing Attacks

Enrolment attack with morphed facial images

Subject A

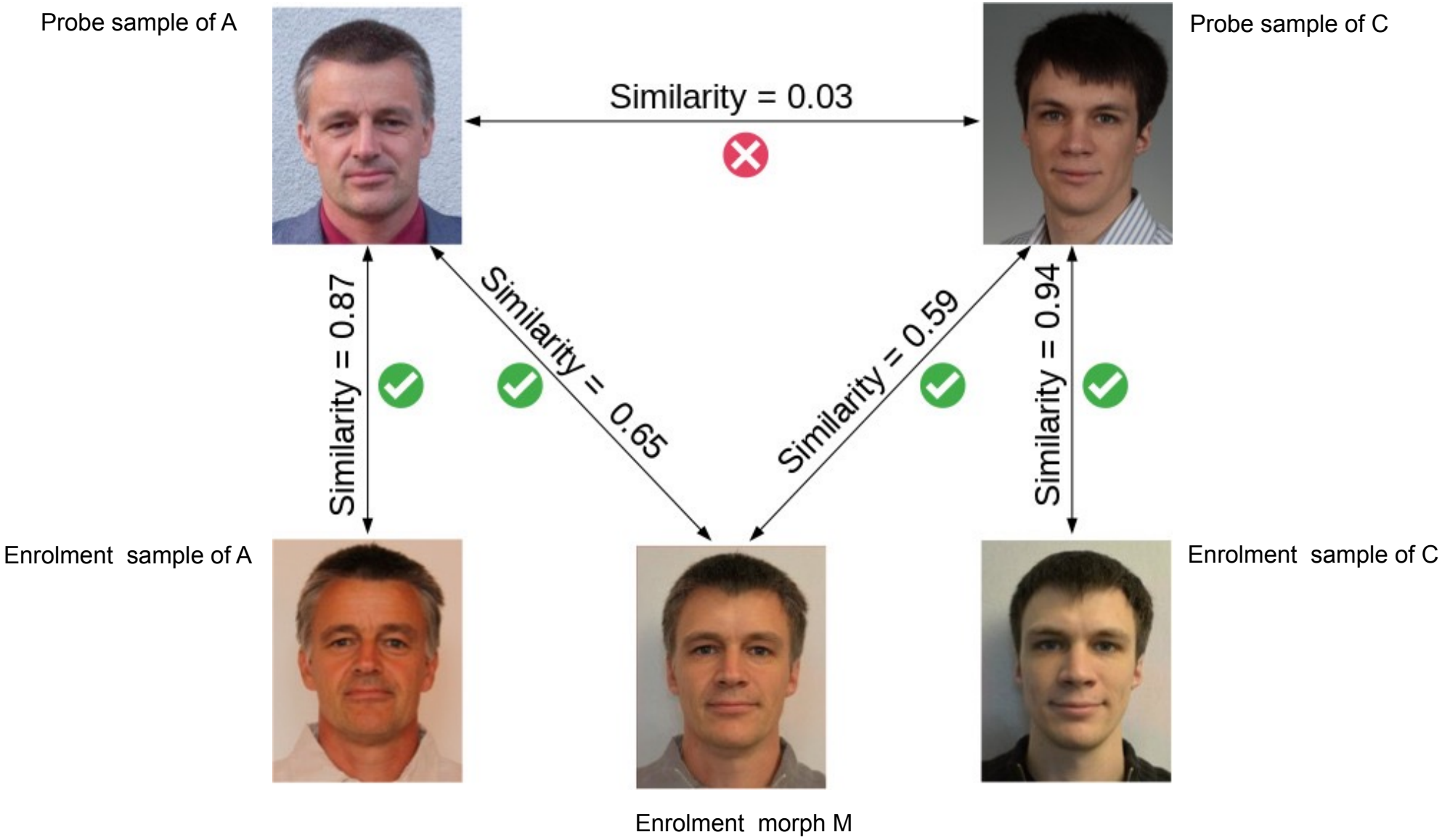
Morph = Subject A + Subject C



Subject C

Problem: Morphing Attacks

Verification against morphed facial images



Problem: Morphing Attacks

Is it a really problem ? - YES!

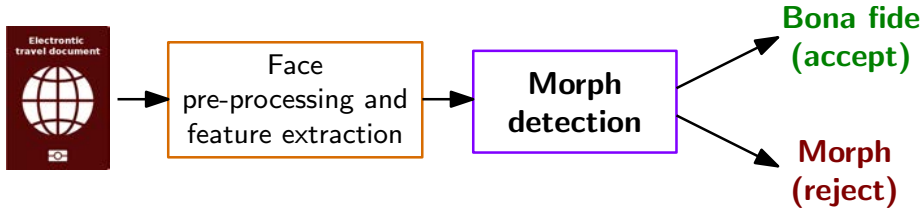
- In September 2018 German activists
  - used a morphed images of Federica Mogherini (High representative of the European Union for Foreign Affairs and Security Policy) and a member of their group
  - and received an authentic German passport.

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

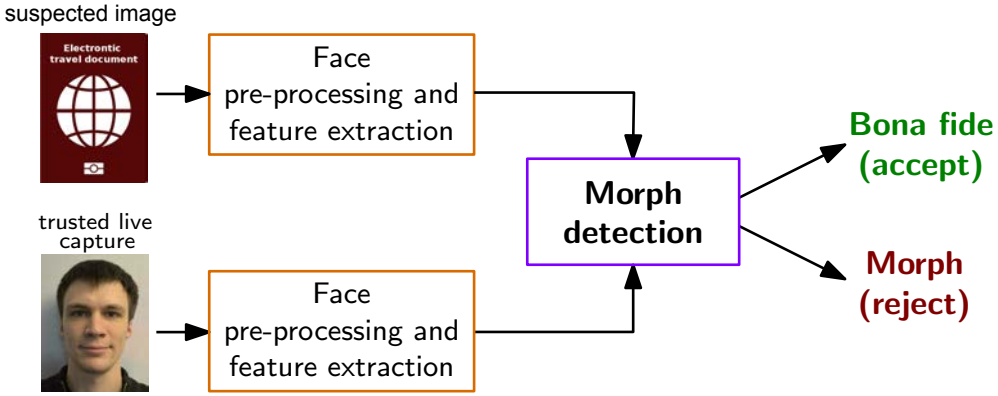
Morphing Attack Detection Scenarios

Real world scenarios

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



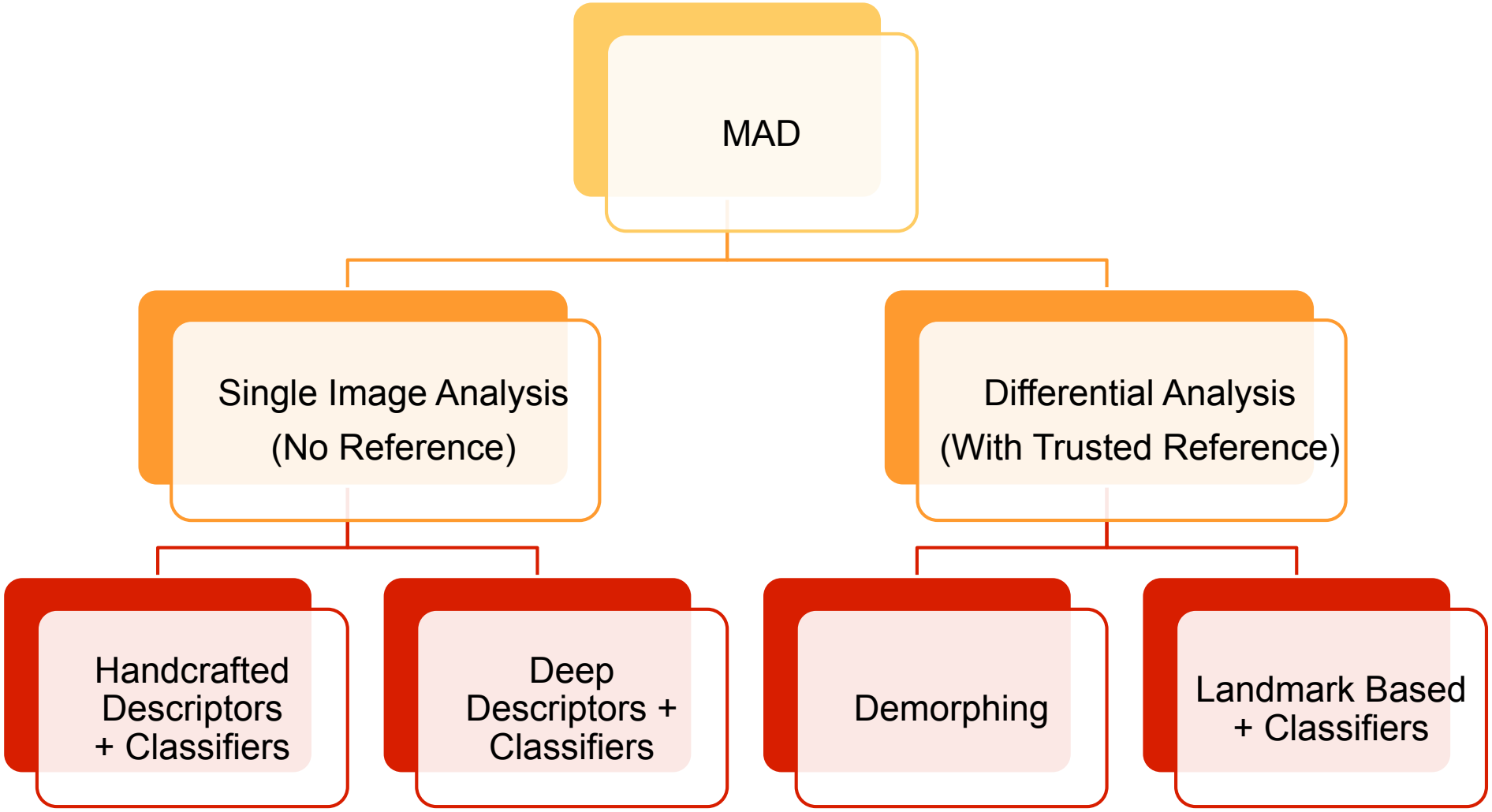
- Differential morphing attack detection (D-MAD)
  - A pair of images is analysed - and one is a trusted Bona Fide image
  - Biometric verification (e.g. at the border)



[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)

State of the Art - MAD Algorithms

Taxonomy of Morphing Attack Detection (MAD)

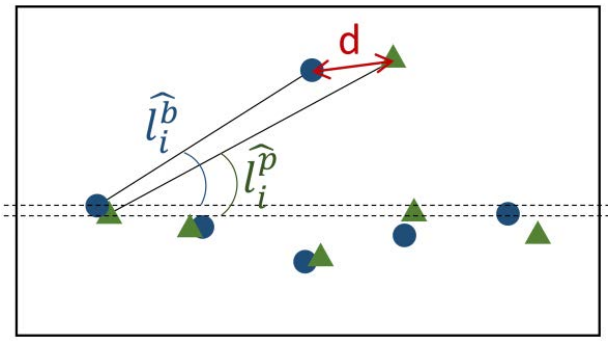


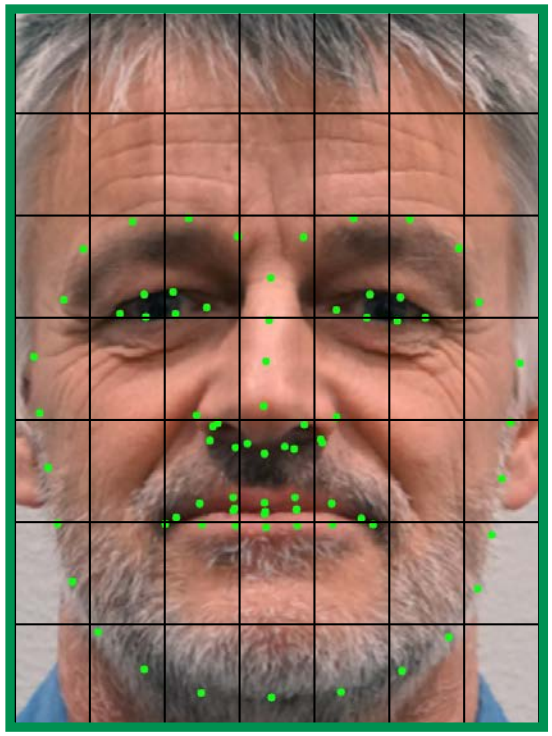
[SRMBB2019] U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, C. Busch: "Face Recognition Systems under Morphing Attacks: A Survey“, in IEEE Access, (2019)

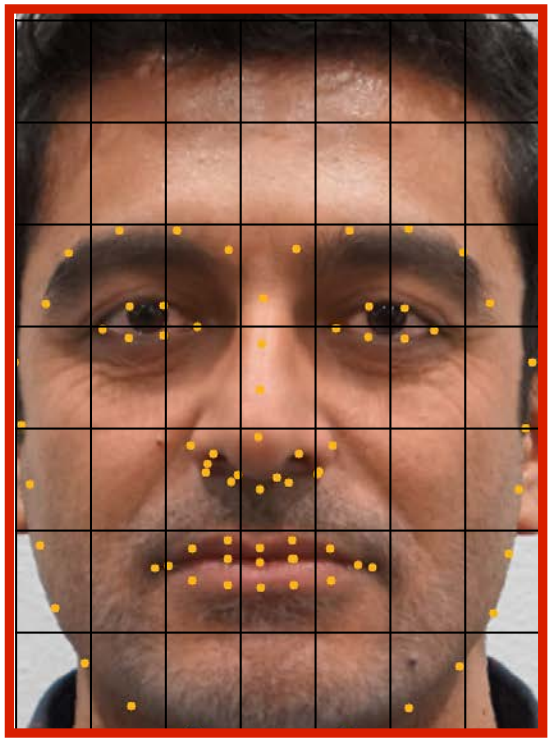
Differential Morphing Attack Detection

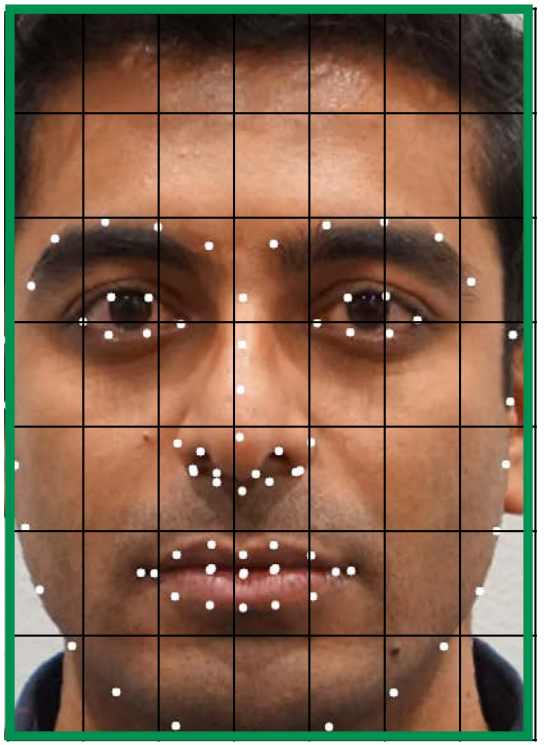
D-MAD with landmark analysis

- Angle based features
- Distance based features







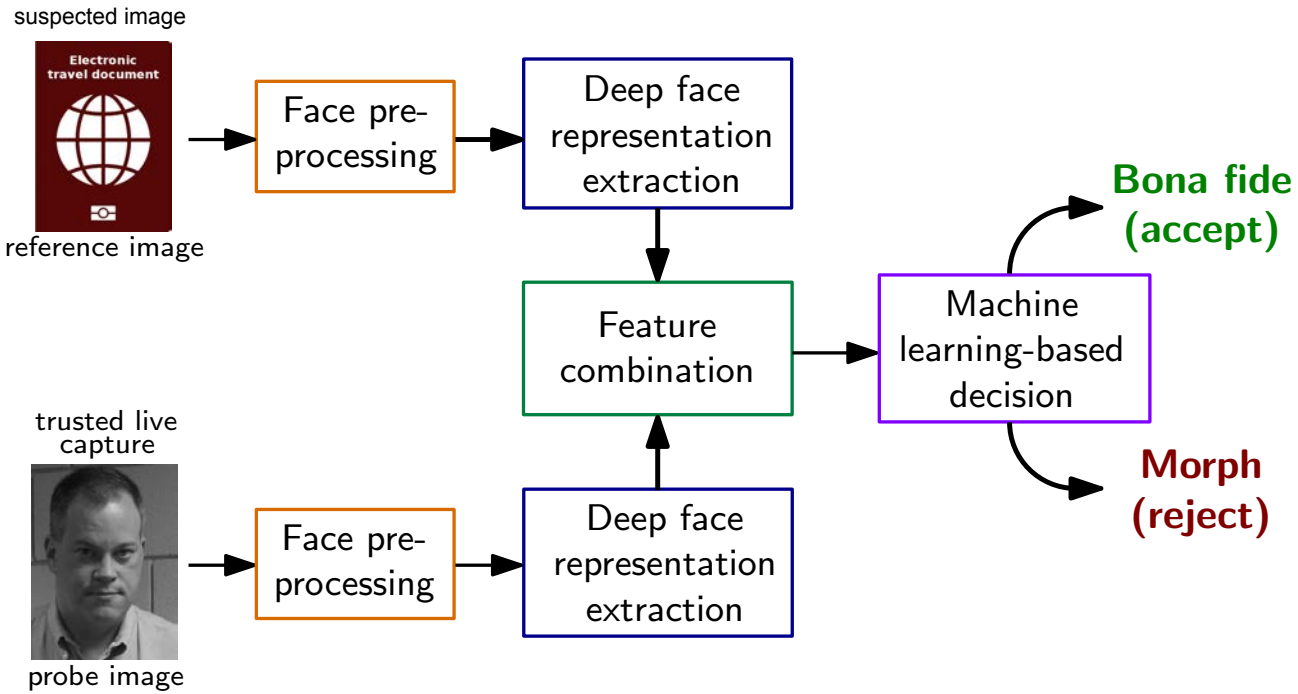


[SDGB2018] U. Scherhag, D. Budhrani, M. Gomez-Barrero, C. Busch: "Detecting Morphed Face Images Using Facial Landmarks“, in Proceedings of International Conference on Image and Signal Processing (ICISP), (2018)

Differential Morphing Attack Detection

D-MAD with deep learning

- Deep Face representations of Deep CNNs



- Deep representations extracted by the neural network (on the lowest layer)
- Feature space with small dimension: 512 (for ArcFace and FaceNet)
- 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)

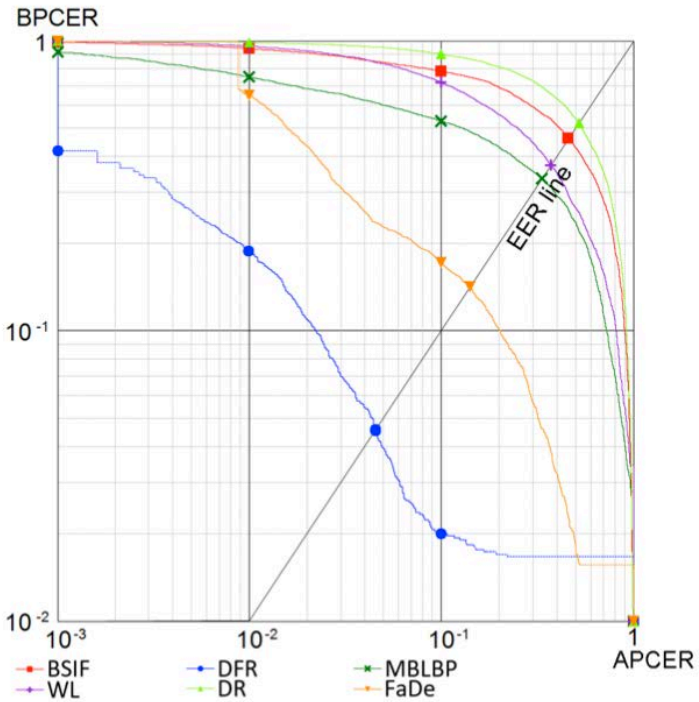
State of the Art - MAD Algorithms

Detection accuracy - focused on D-MAD

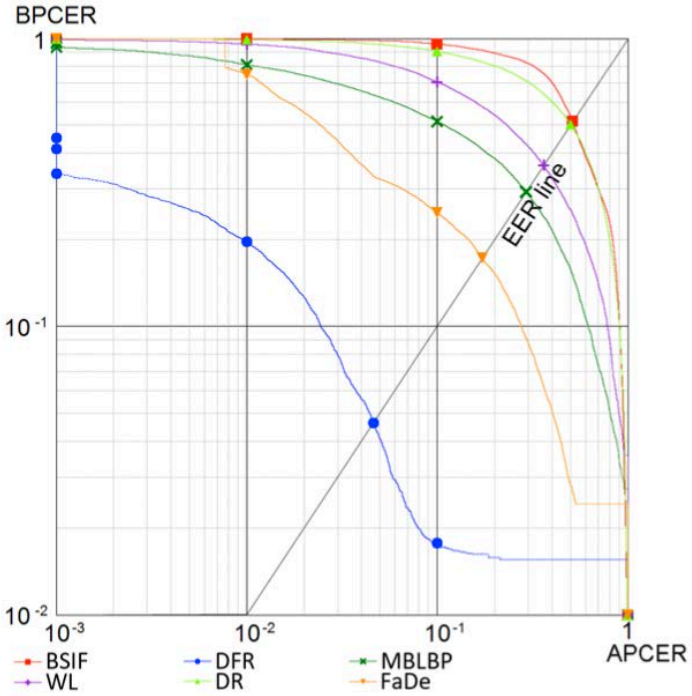
https://biolab.csr.unibo.it/FVCOnGoing/UI/Form/BenchmarkAreas/BenchmarkAreaDMAD.aspx

- Digital

Print and scanned



SOTAMD_ D-1.0



D-MAD-SOTAMD P&S-1.0.

[Raja2020] K. Raja, M. Ferrara, A. Franco, L. Spreeuwers, I. Batskos, F. Wit, M. Gomez-Barrero, U. Scherhag, D. Fischer, S. Venkatesh, J. Singh, G. Li, L. Bergeron, S. Isadskiy, R. Raghavendra, C. Rathgeb, D. Frings, U. Seidel, F. Knopjes, R. Veldhuis, D. Maltoni, C. Busch: "Morphing Attack Detection - Database, Evaluation Platform and Benchmarking", in IEEE Transactions on Information Forensics and Security (TIFS), (2020)
https://arxiv.org/abs/2006.06458

The Key Figures

iMARS project

- Start date: 1 September 2020
- End date: 31 August 2024
- H2020-SU-SEC-2019
- Grant agreement ID: 883356
- Programme(s):
  - H2020-EU.3.7.3. - Strengthen security through border management
  - H2020-EU.3.7.8. - Support the Union's external security policies including through conflict prevention and peace-building
- Topic: SU-BES02-2018-2019-2020 - Technologies to enhance border and external security
- Overall budget: € 6 988 521,25
- Website: https://cordis.europa.eu/project/id/883356
- Twitter: https://twitter.com/iMARS_h2020

Thanks

I would like to thank the sponsors of this work:

- NGBS-Project funded by ATHENE
- SWAN-Project funded by RCN
- FACETRUST-Project funded by BSI
- SOTAMD-Project funded by the European Union's Internal Security Fund
- iMARS-Project has received funding from the European Union's H2020 research and innovation programme under grant agreement No 883356
  - The content of this presentation represents the views of the author only and is his sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
- Evaluation and improvement of eu-LISA synthetic biometric datasets

More information

The MAD website

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

The MAD survey paper

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

IEEE Access

Face Recognition Systems Under Morphing Attacks: A Survey

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

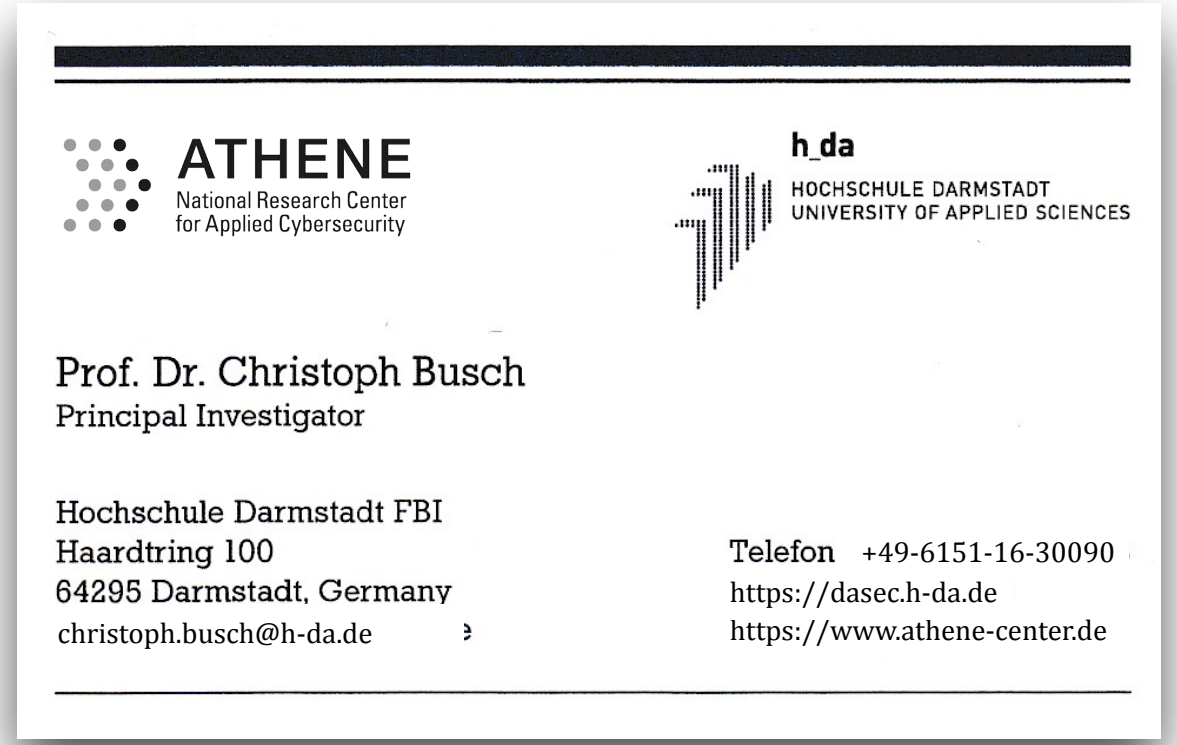
ABSTRACT Recently, researchers found that the intended generalizability of (deep) face recognition systems increases their vulnerability against attacks. In particular, the attacks based on morphed face images pose a severe security risk to face recognition systems. In the last few years, the topic of (face) image morphing and automated morphing attack detection has sparked the interest of several research laboratories working in the field of biometrics and many different approaches have been published. In this paper, a conceptual categorization and metrics for an evaluation of such methods are presented, followed by a comprehensive survey of relevant publications. In addition, technical considerations and tradeoffs of the surveyed methods are discussed along with open issues and challenges in the field.

INDEX TERMS Biometrics, face morphing attack, face recognition, image morphing, morphing attack detection.

I. INTRODUCTION

A. FACE MORPHING ATTACK

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

Contact

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