The iMARS Project and its Relevance to the European EES in Operation

Christoph Busch

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

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

FRONTEX ICBB 2020, December 3, 2020

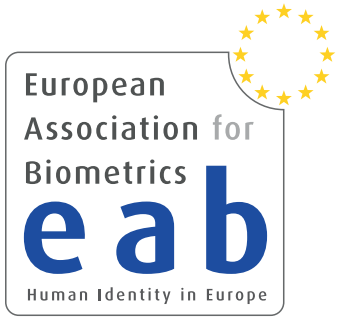
ATHENE
Steinbeis-Transferzentrum BISE – Biometrie

European Association for Biometrics
eab
Human Identity in Europe

NTNU

About my Affiliation(s)

European Association for Biometrics (EAB)



Darmstadt Research Group @Hochschule Darmstadt

ATHENE
National Research Center for Applied Cybersecurity

h_da

Steinbeis-Transferzentrum
BISE – Biometrie

Gjøvik Research Group @Norwegian University of Science and Technology

NTNU

NORWEGIAN BIOMETRICS LABORATORY

Introduction

European Association for Biometrics (EAB)

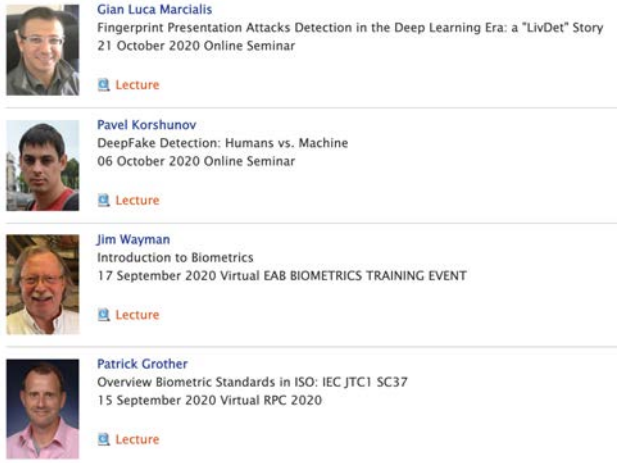
- The EAB is a non-profit, nonpartisan association
  https://eab.org/
- EAB supports all sections of the ID community across Europe, including governments, NGO's, industry, associations and special interest groups and academia.

- 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

- 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

Overview

Agenda

- Introduction
  - EAB
  - fields of initiatives
- Biometric capture process in the EES
- Presentation attack detection
- Morphing attack detection
- Face sample quality

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
  - Analog or digital biometric sample
    - subsequently scanned
  - Controlled distance and environmental conditions

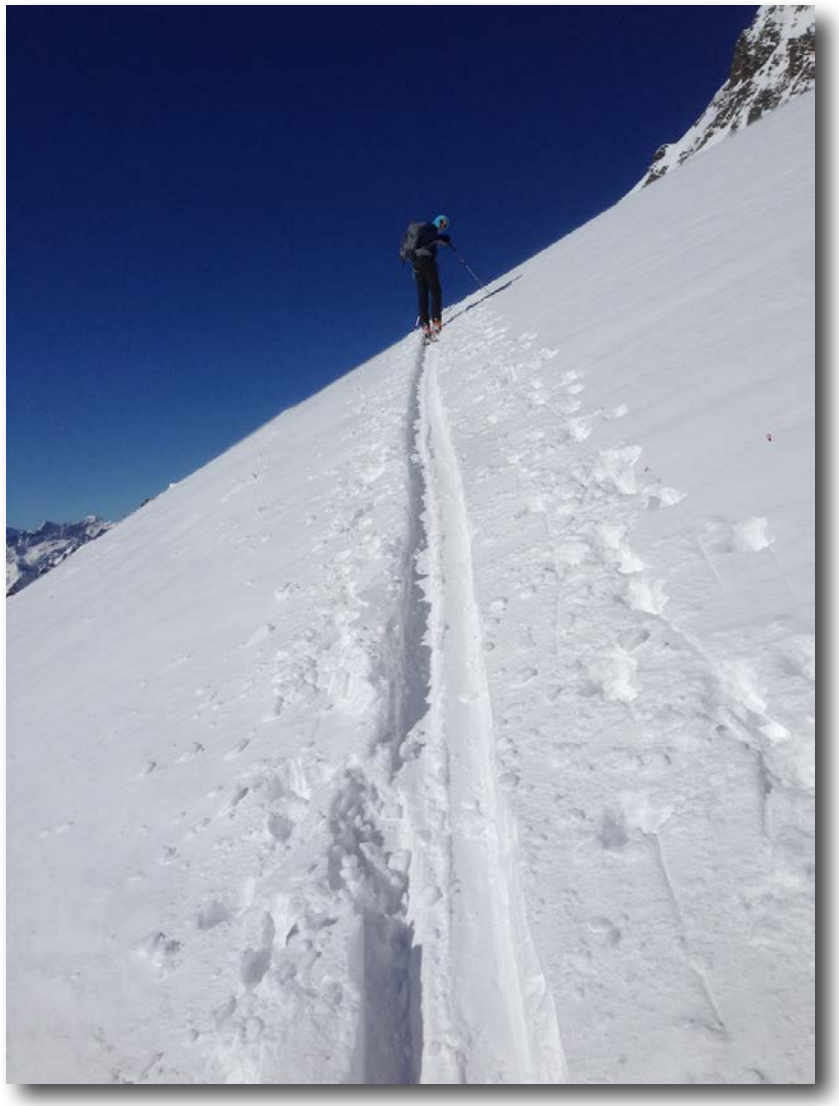
Image Source: BKA

Image Source: biometricupdate.com

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

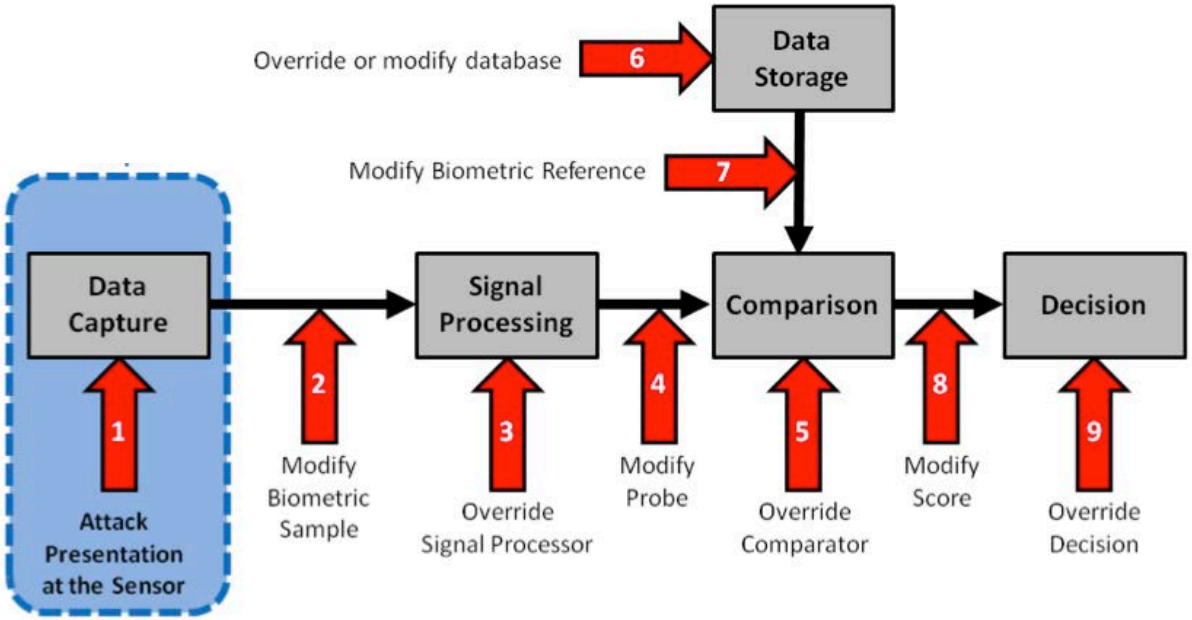
EES-kiosk enrolment systems are certainly not in the wild …
… but also **not** controlled (without attendance of a supervisor).

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

Concealer

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

- evade face detection

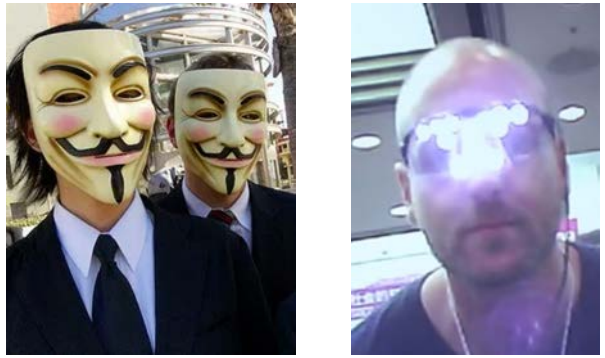


Image Source: https://www.youtube.com/watch?v=LRj8whKmN1M

Presentation Attack Detection

ISO/IEC 30107-1 - Definitions

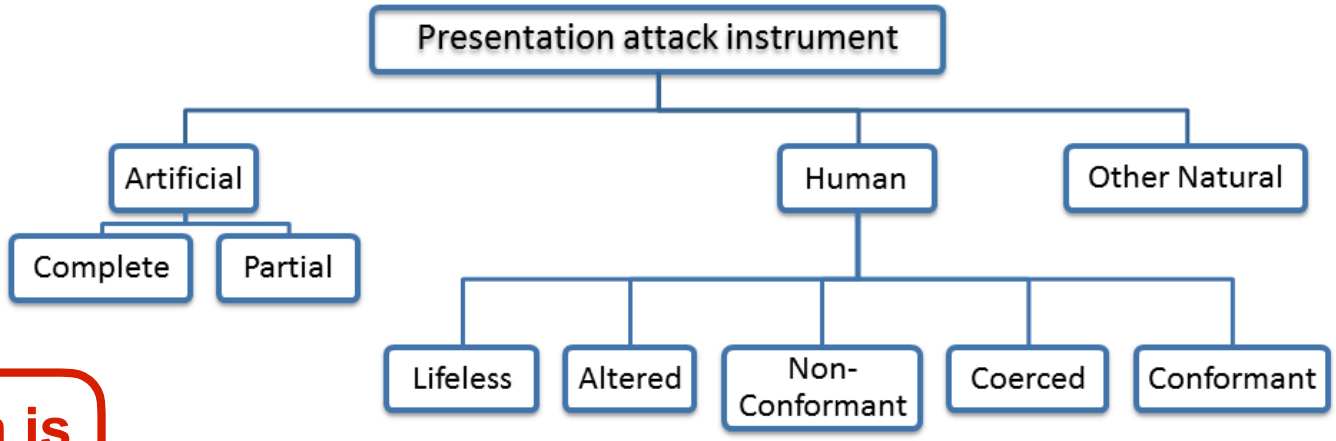
- **presentation attack instrument (PAI)**
  biometric characteristic or object used in a presentation attack
- **artefact**
  artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns

Types of presentation attacks

(General Noun)

(Adjectives describing categories)

(Qualifying adjectives)



Source: ISO/IEC 30107-1

liveness detection is NOT sufficient

Altered Fingerprint Detection - Testing

Example for fingerprint alterations

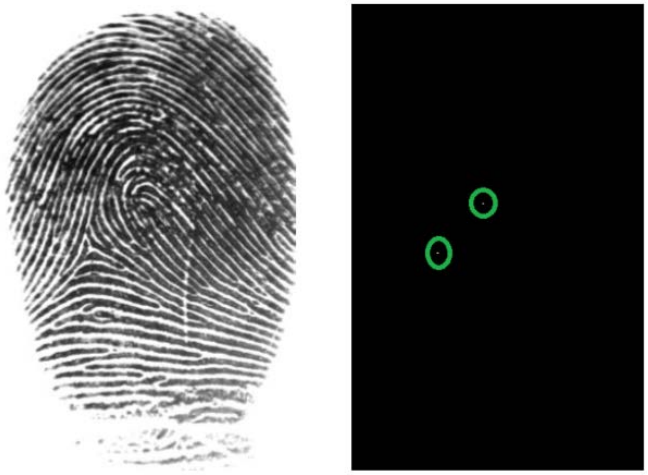
- Z-shaped alteration (Finger of Jose Izquierdo, 1995)

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

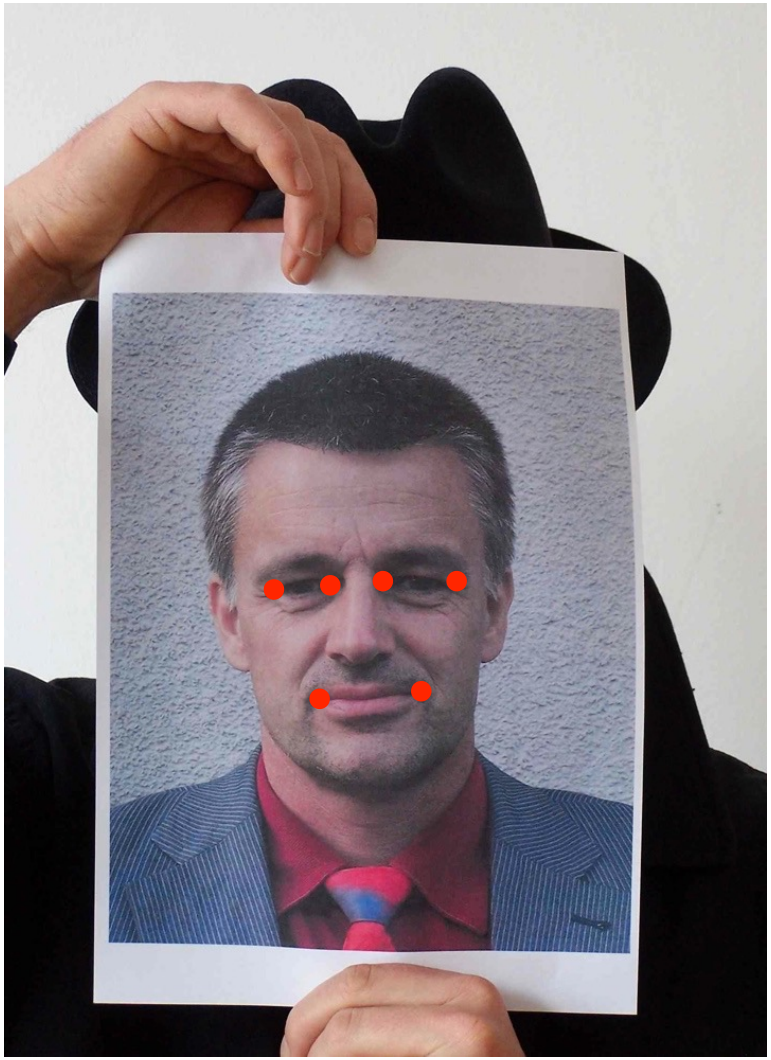
altered fingerprint

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

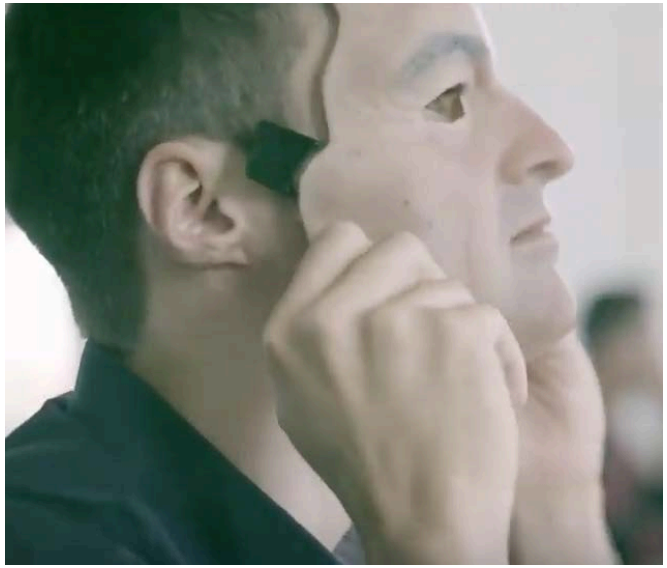


Historic - Year 2010!

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

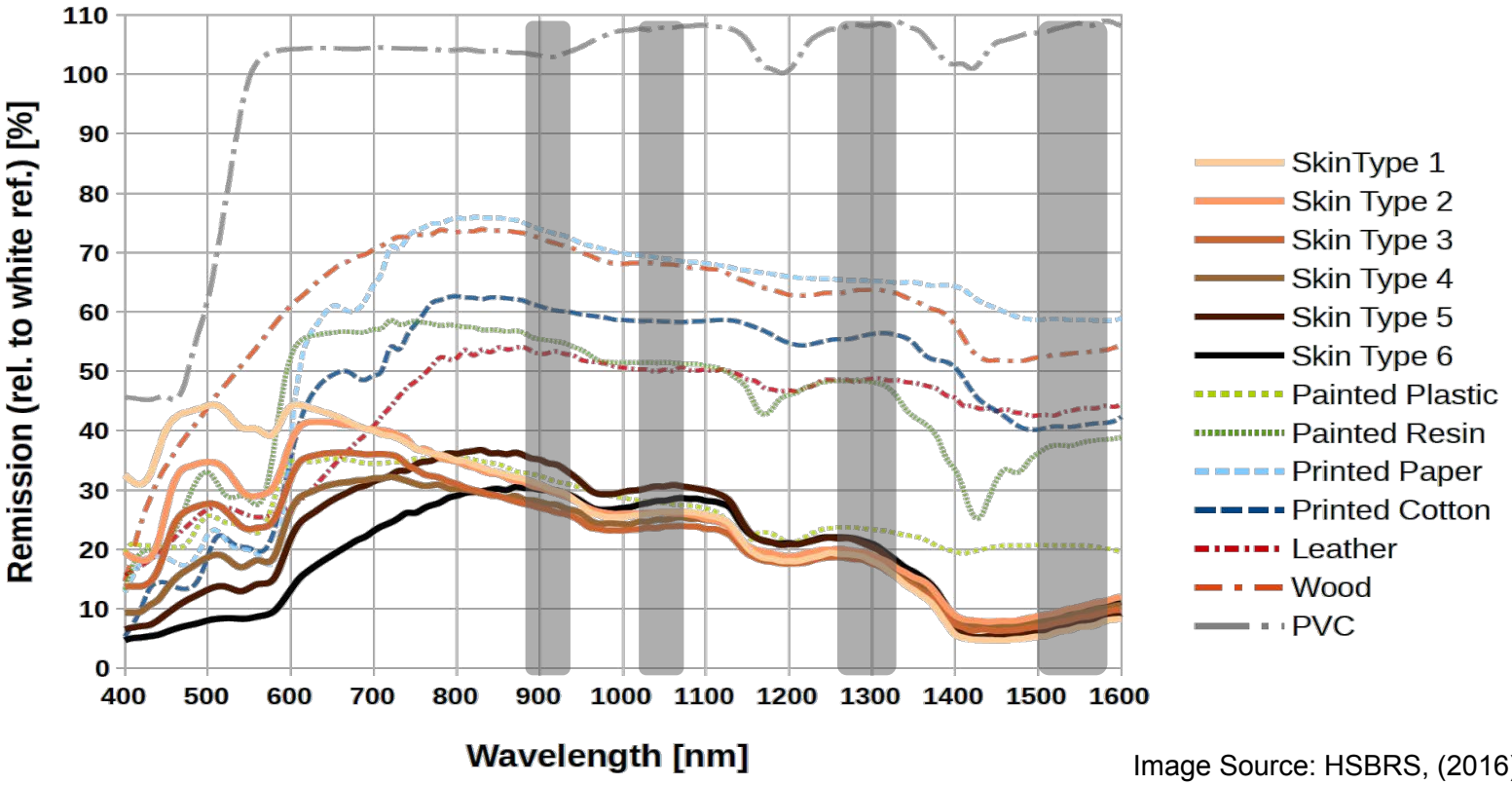


Image Source: HSBRS, (2016)

[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

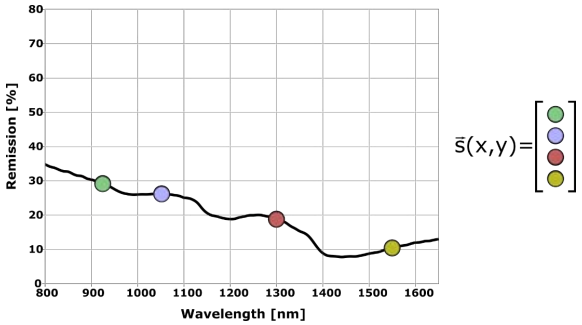


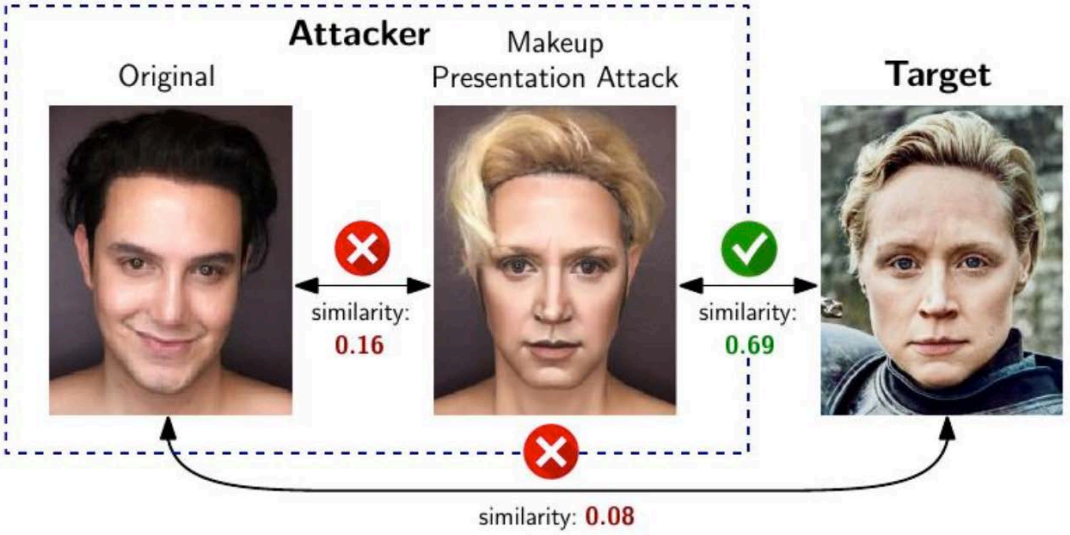
Image Source: HSBRS, (2016)

Makeup Presentation Attacks

Severe alterations

- Makeup for impersonation
- 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: "Detection of Makeup Presentation Attacks based on Deep Face Representations“, in Proceedings of 25th International Conference on Pattern Recognition (ICPR), (2020)

Face Presentation Attack Instruments

High end 3D silicone mask

Source: Impostor mask - https://www.youtube.com/watch?v=XOFYSHjXYAI

Source: Concealor mask from amazon.ca for CDN$ 244

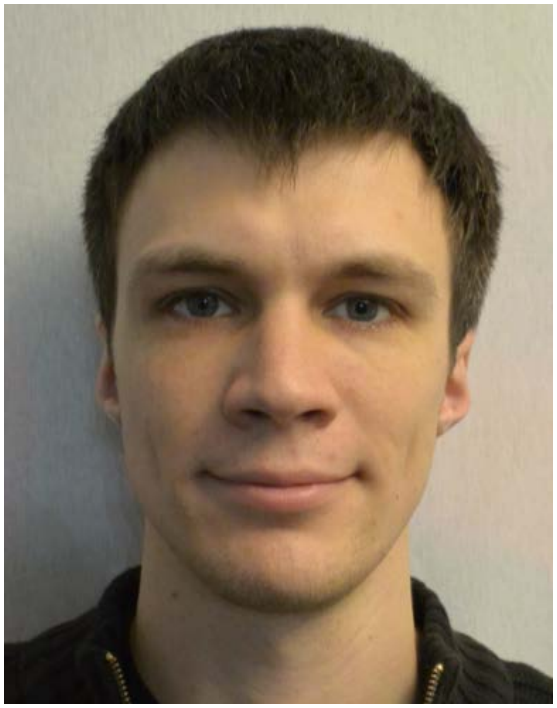
Enrolment Attacks
Face Morphing

Problem: Morphing Attacks

Enrolment attack with morphed facial images

Subject A

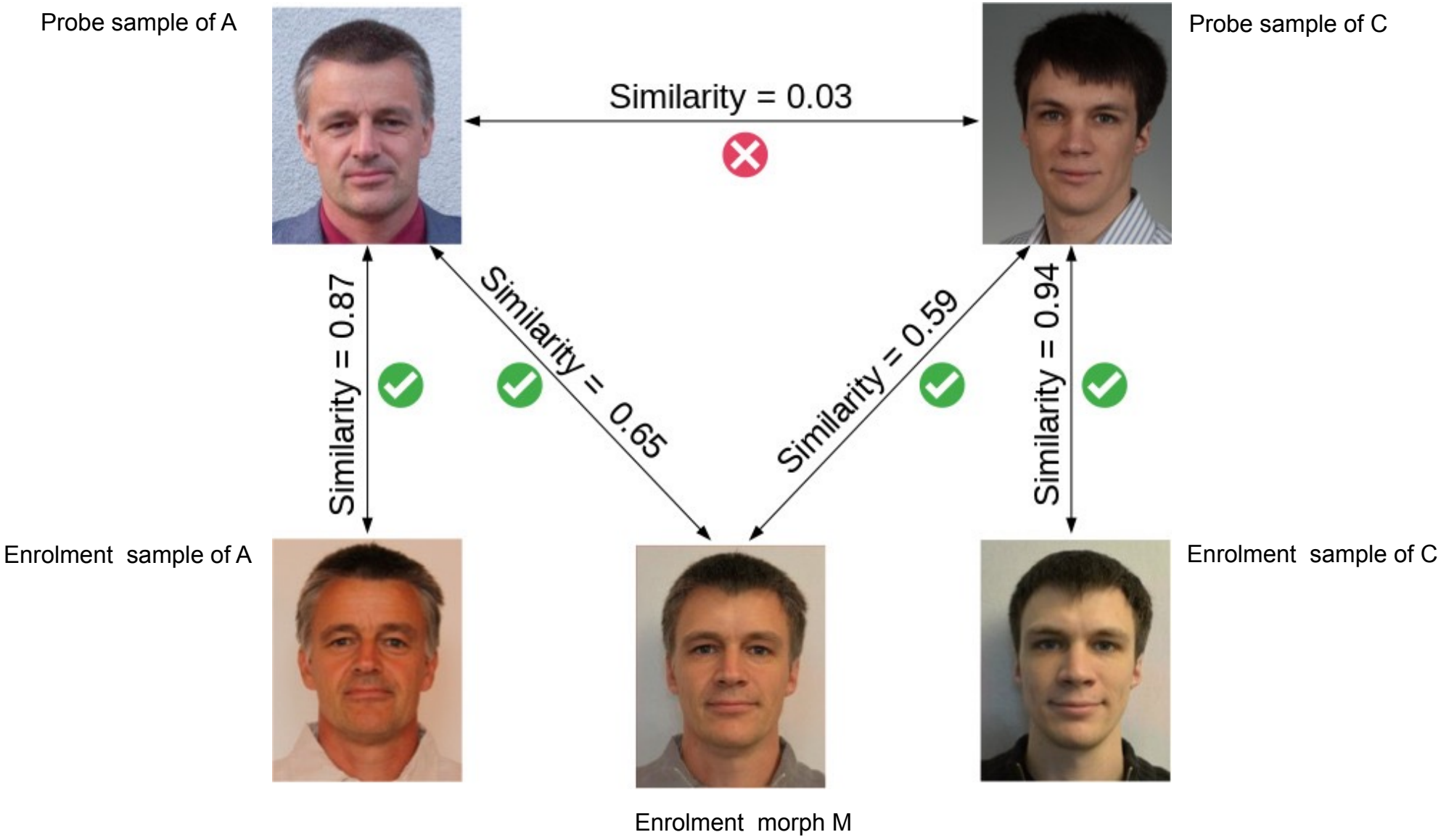
Morph = Subject A + Subject C



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

Problem: Morphing Attacks

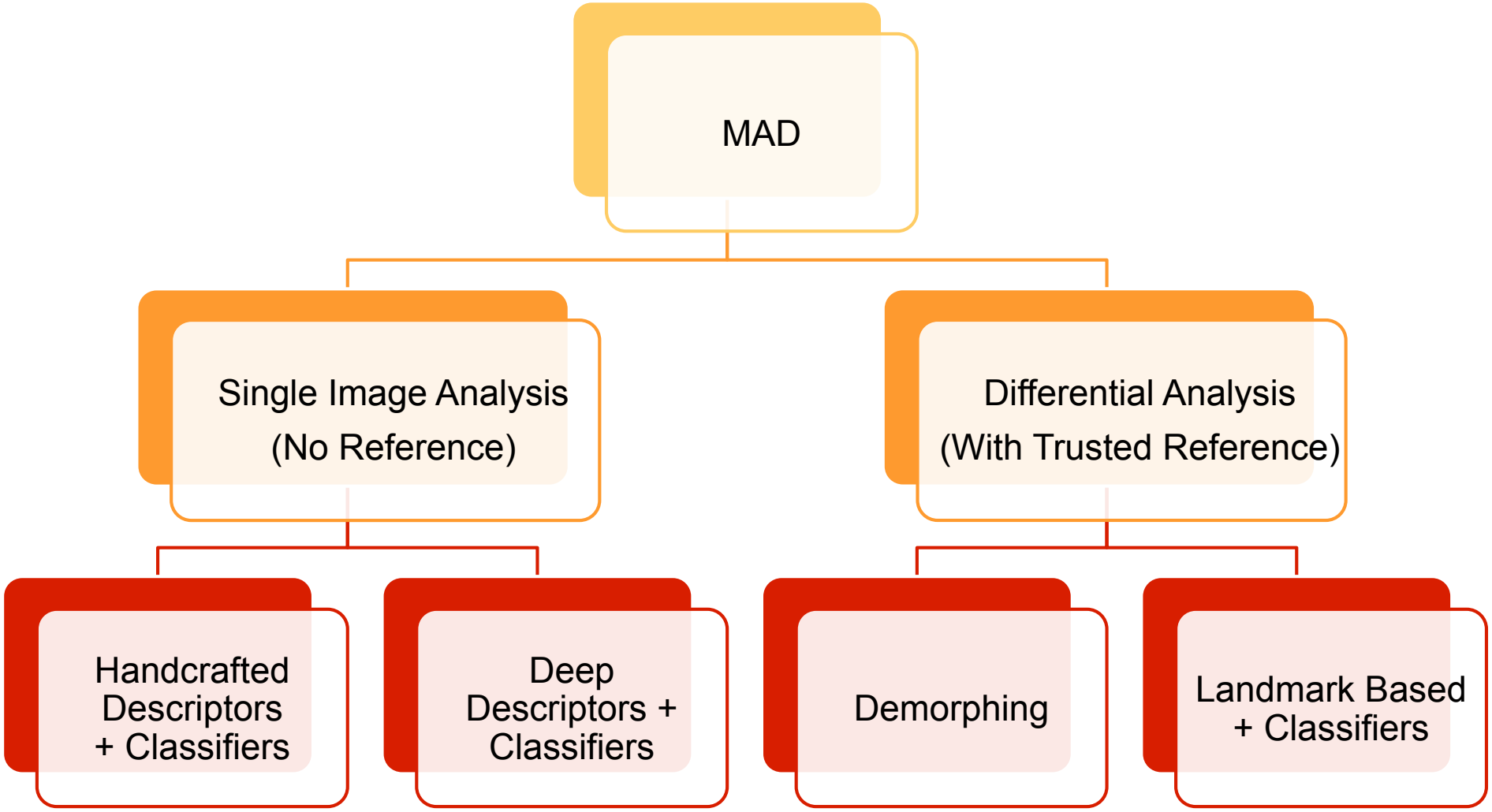
Is it a really problem ? - YES!

- 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.

Statement at the Frontex ICBB on Dec 2nd:
„*We might import the facial image from the passport of the traveller into our entry/exit control system*“

State of the Art - MAD Algorithms

Taxonomy of Morphing Attack Detection (MAD)

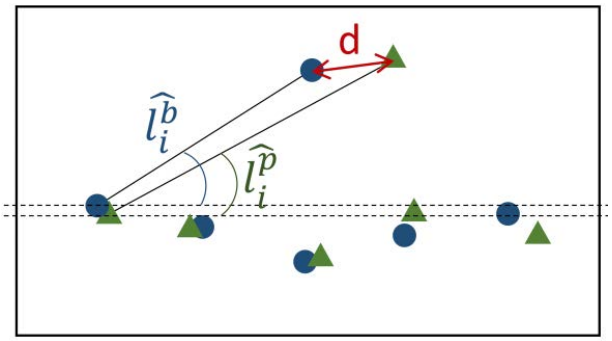


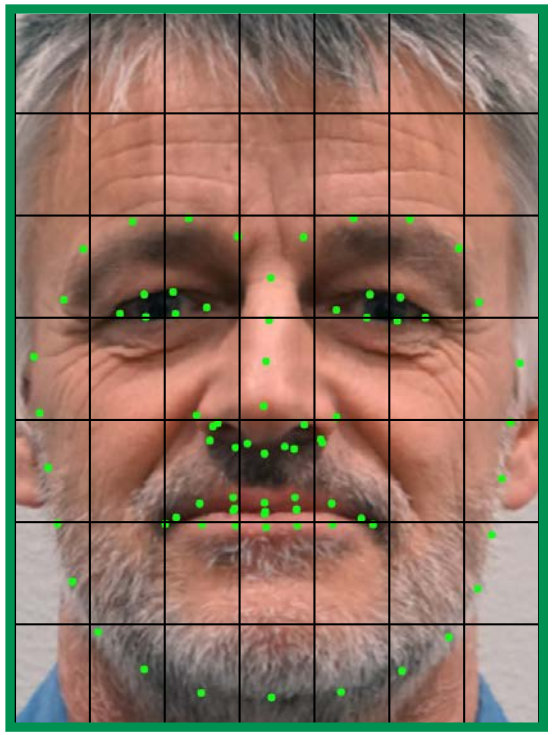
[SRMBB2019] U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, C. Busch: "Face Recognition Systems under Morphing Attacks: A Survey“, in IEEE Access, (2019)

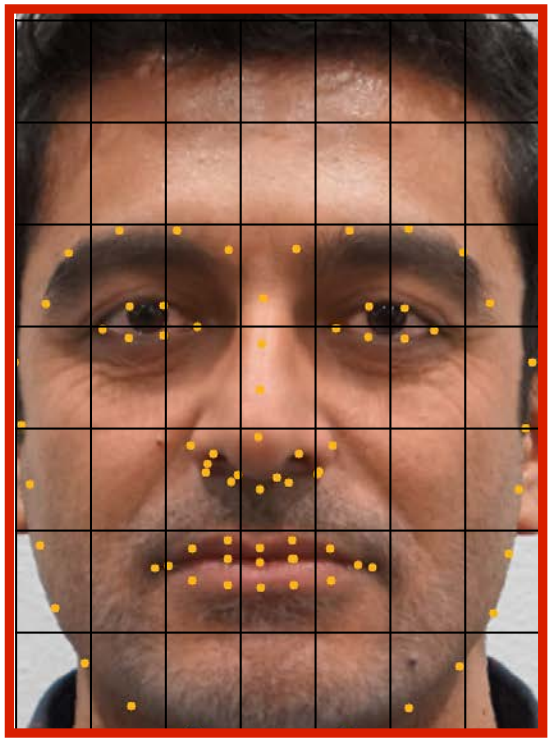
Differential Morphing Attack Detection

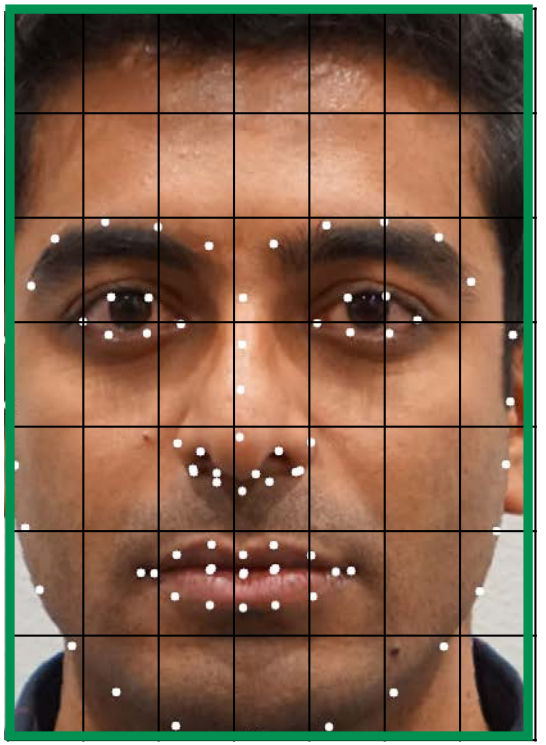
D-MAD with landmark analysis

- Angle based features
- Distance based features







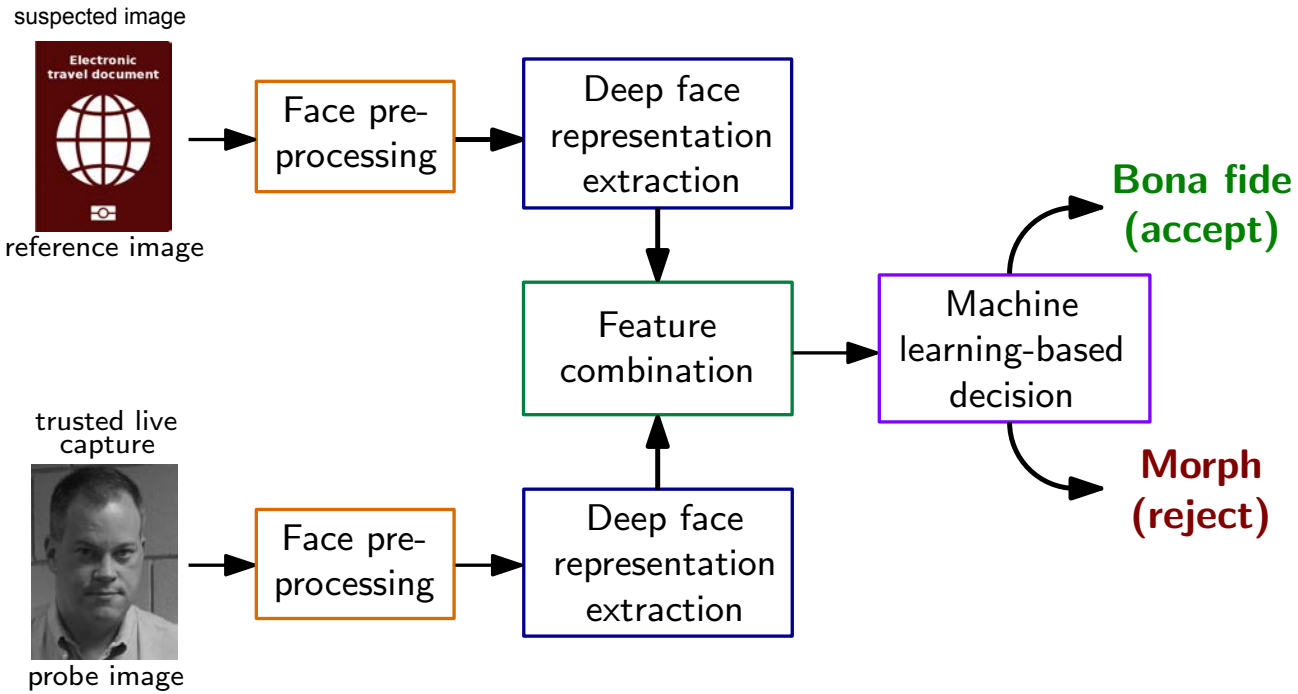


[SDGB2018] U. Scherhag, D. Budhrani, M. Gomez-Barrero, C. Busch: "Detecting Morphed Face Images Using Facial Landmarks“, in Proceedings of International Conference on Image and Signal Processing (ICISP), (2018)

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

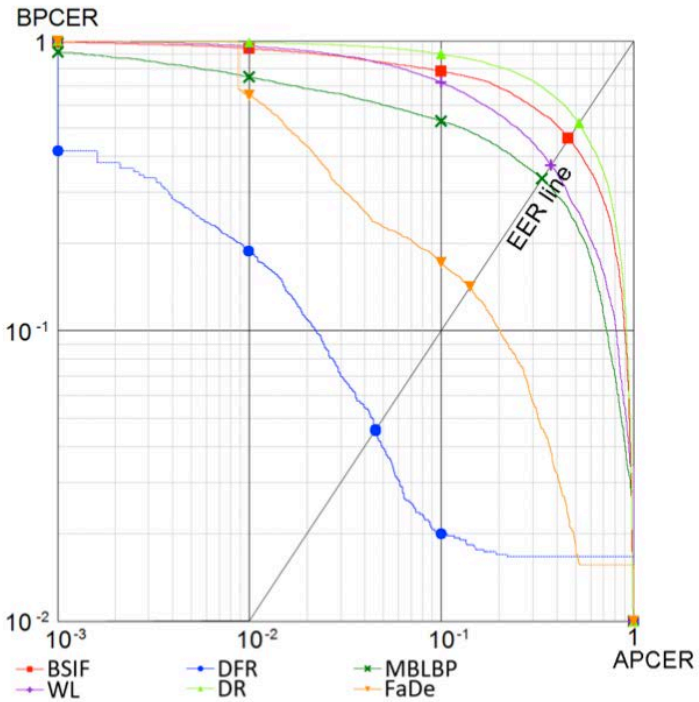
[SRMB2020] U. Scherhag, C. Rathgeb, J. Merkle, C. Busch: "Deep Face Representations for Differential Morphing Attack Detection", in IEEE Transactions on Information Forensics and Security (TIFS), (2020)

State of the Art - MAD Algorithms

Detection accuracy - focused on D-MAD

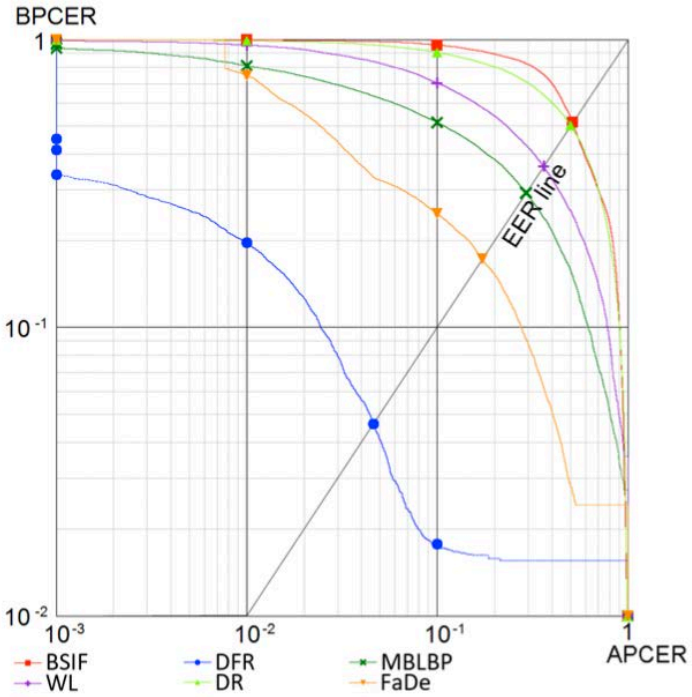
https://biolab.csr.unibo.it/FVCOnGoing/UI/Form/BenchmarkAreas/BenchmarkAreaDMAD.aspx

- Digital



SOTAMD_ D-1.0

Print and scanned



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

PAD: Standardized Testing Metrics

Definition according to ISO/IEC 30107-3

- Testing the
  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

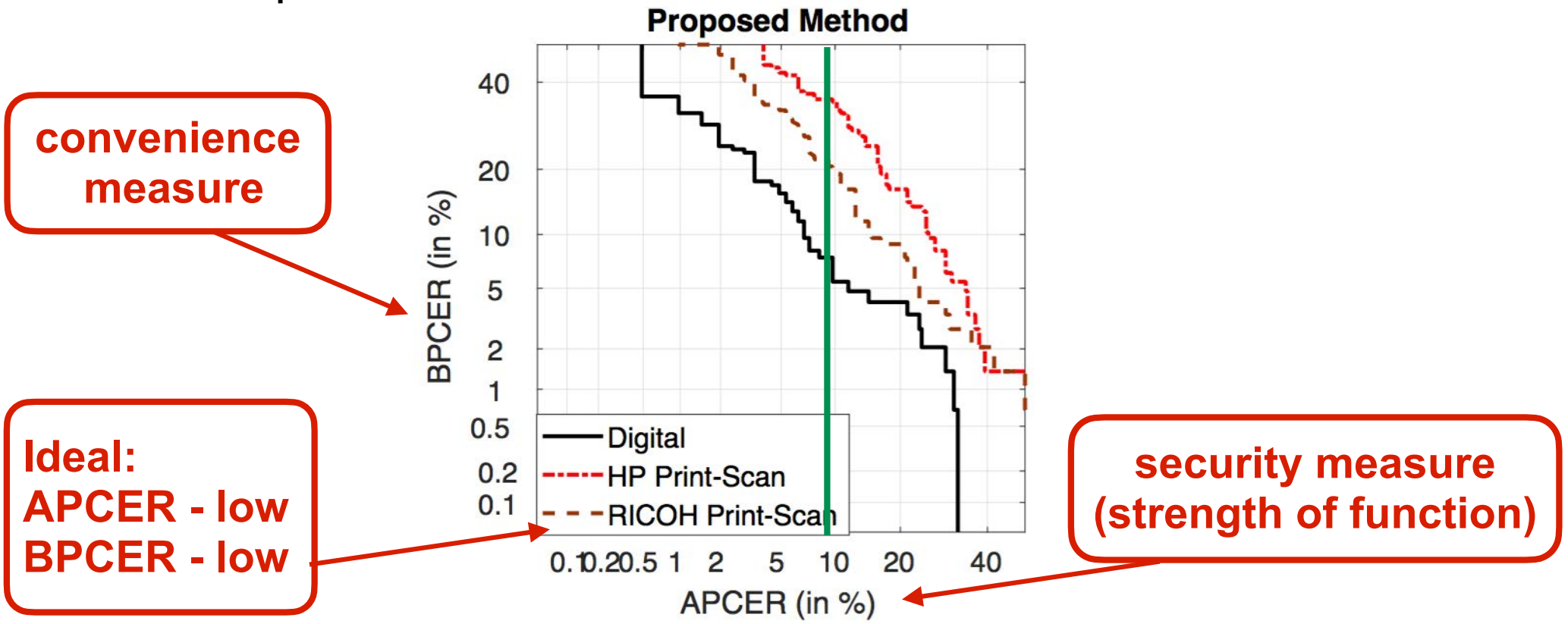
- **Bona fide presentation classification error rate (BPCER)**
  proportion of bona fide presentations incorrectly classified as attack presentations in a specific scenario

source: ISO/IEC 30107-3, “Biometric presentation attack detection - Part 3: Testing and reporting”, (2017)
https://www.iso.org/obp/ui/#iso:std:iso-iec:30107:-3:ed-1:v1:en

Standardized Testing Metrics

Definition of metrics in ISO/IEC 30107-3

- DET curve analyzing operating points for various thresholds and plot security measures versus convenience measures
- Example:



Source: R. Raghavendra, K. Raja, S. Venkatesh, C. Busch: "Transferable Deep-CNN features for detecting digital and print-scanned morphed face images", in Proceedings of 30th International Conference on Computer Vision and Pattern Recognition Workshop (CVPRW 2017), Honolulu, Hawaii, July 21-26, (2017)

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

The Consortium

24 Partners

- IDM - IDEMIA IDENTITY & SECURITY FRANCE (FR)
- DG - IDEMIA IDENTITY & SECURITY GERMANY (DE)
- COG - COGNITEC SYSTEMS GMBH (DE)
- VIS - VISION BOX (PT)
- MOB - MOBAI AS (NO)
- ART - ARTTIC (FR)
- SUR - SURYS (FR)
- NTN - NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET (NO)
- UBO - UNIVERSITA DI BOLOGNA (IT)
- HDA - HOCHSCHULE DARMSTADT (DE)
- KUL - KATHOLIEKE UNIVERSITEIT LEUVEN (BE)
- IBS - INSTITUTE OF BALTIC STUDIES (EE)
- EAB - EUROPEAN ASSOCIATION FOR BIOMETRICS
- KEM - KENTRO MELETON ASFALEIAS (EL)
- BKA - BUNDESKRIMINALAMT (DE)
- NOI - MINISTERIE VAN BINNENLANDSE ZAKEN (NL)
- INC - IMPRENSA NACIONAL (PT)
- POD - POLITIDIREKTORATET (NO)
- PBP - PORTUGUESE IMMIGRATION AND BORDERS SERVICES (PT)
- HEP - HELLENIC POLICE (EL)
- CYP - CYPRUS POLICE (CY)
- PBM - BORDER POLICE OF THE REPUBLIC OF MOLDOVA (MD)
- BFP - POLICE FEDERALE BELGE (BE)

Face Sample Quality

Factors impacting Quality

Fingerprint sample quality

- Defect caused by the source
  - Skin condition, such as moist, scares blisters etc.
- Defect caused by the capture device
  - Sampling error, low contrast
- Defect caused by the capture subject‘s behaviour
  - Improper finger placement (too low, rotated, etc)


EU-ID 2019/329: „*assess quality with NFIQ2.0“ a.k.a. ISO/IEC 29794-4*

Face sample quality

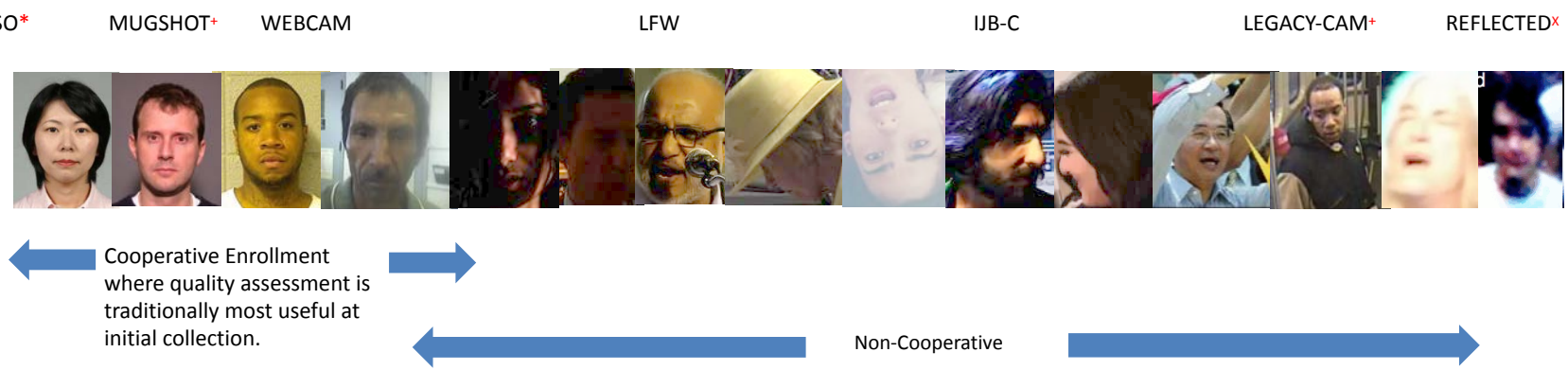
- Image capture system out of focus
- No frontal perspective


EU-ID 2019/329: „*quality shall comply with ISO/IEC 19794-5:2011“ ???*

ISO/IEC 29794-1 expectation: „*A quality algorithm should convey the predicted utility of the sample*“

Face Image Quality

Flavors of quality: good, bad, wild, ugly



Source: P. Grother, 2020

Why do we need face image quality in the first place?

Avoid poor quality data to go into your database !

Source *: http://webstore.ansi.org

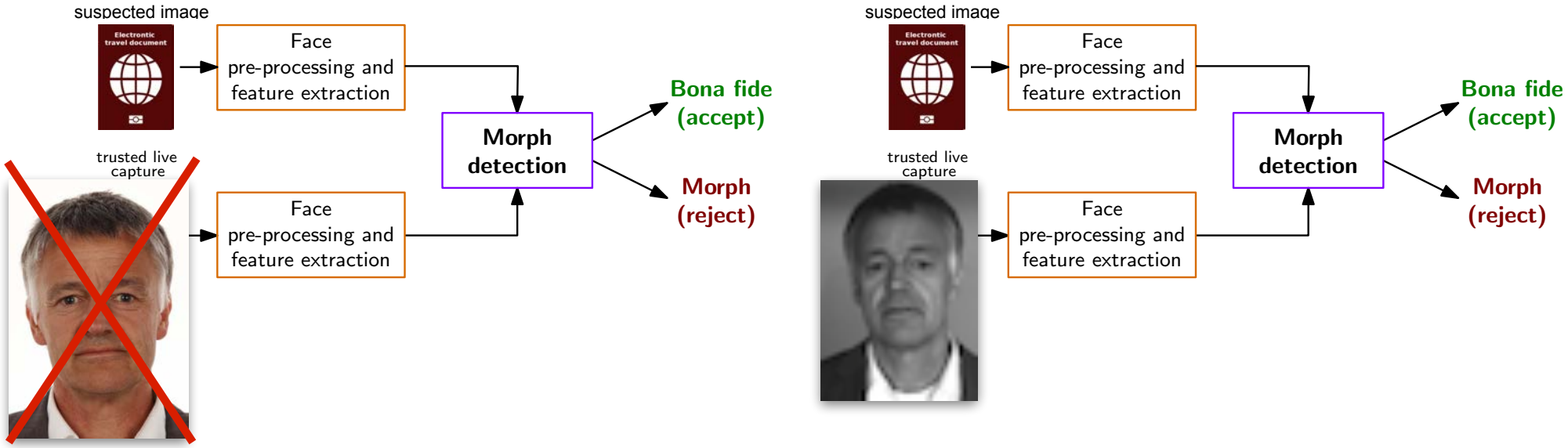
Source +: http://www.chicagonow.com/cta-tattler/2013/07/chicago-cops-use-face-recognition-software-to-nab-cta-mugger

Source X http://io9.com/hidden-faces-can-be-found-by-zooming-into-hi-res-photos-1491607189

Face Image Quality in the iMARS Project

Robust border control processes

- based on a differential morphing attack analysis, where the quality of probe image varies.
- Trusted live capture images must be in realistic degraded quality!

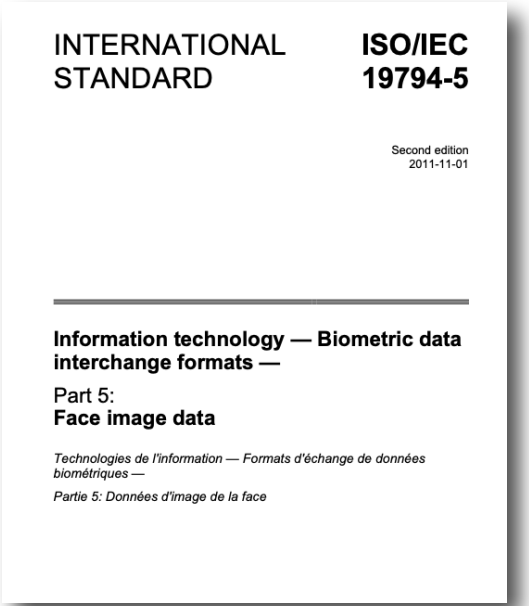


- Quality will impact explicit and implicit D-MAD algorithms

Face Image Quality in the EES

The objective in the 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

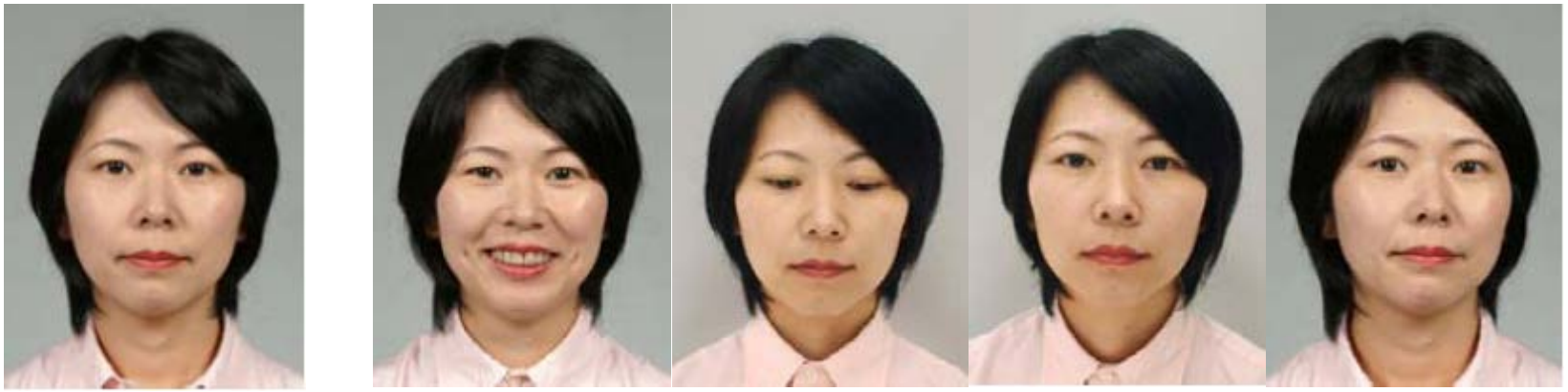
Technologies de l'information — Formats d'échange de données biométriques —

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?



ISO Standard | Expression | Gaze | Too close | Pose Angle

Source: http://webstore.ansi.org

Quality-Related Standards

Relevant standards

- ISO/IEC 29794-1: Quality Framework
  - Definitions and evaluation concepts https://www.iso.org/standard/62782.html
- ISO/IEC 29794-4: Fingerprint image quality
  - https://www.iso.org/standard/62791.html
  - NFIQ 2.1
    https://github.com/usnistgov/NFIQ2
    https://www.nist.gov/system/files/documents/2018/11/29/nfiq2_report.pdf
- ISO/IEC 29794-5: Face image quality
  - Revision of ISO/IEC 29794-5:2011
    https://www.iso.org/standard/81005.html
  - Scalar values
  - Vector values ~ Quantitative ISO/ICAO compliance checklist

Quality-Related Standards

ISO/IEC WD 29794-5 aligned with ISO/IEC 19794-5:2011 ISO/IEC 39794-5:2019

#	Image quality aspect
1	Unified quality score
2	Illumination uniformity
3	Illumination uniformity (alt)
4	Illumination under-exposure
5	Illumination over-exposure
6	Illumination over-exposure (alt)
7	Illumination modulation
8	De-focus
9	Image sharpness
10	Motion blur
11	Edge Density
12	Compression
13	Unnatural colour and colour balance
14	Eyes visible
15	Number of faces present
16	Inter-eye distance
17	Horizontal position of the face
18	Vertical position of the face
19	Background uniformity
20	Pose
21	Expression neutrality
22	Mouth closed
23	Eyes open
24	Developer-defined quality score computation

source: ISO/IEC WD 29794-5, Table 2
https://www.iso.org/standard/81005.html

Image Source: ISO/IEC 19794-5:2011

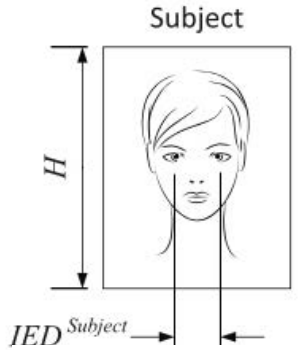


Image Source: ISO/IEC 39794-5

a) Asymmetric shadow on the left

b) Inhomogenous background

c) Body parts visible behind the head

source: ISO/IEC 39794-5:2019, Annex D
https://www.iso.org/standard/72156.html

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

More information

The Face image quality survey paper

- T. Schlett, C. Rathgeb, O. Henniger, J. Galbally, J. Fierrez, C. Busch: "Face Image Quality Assessment: A Literature Survey“, in arxiv.org, (2020) https://arxiv.org/pdf/2009.01103.pdf

Face Image Quality Assessment:
A Literature Survey

Torsten Schlett, Christian Rathgeb, Olaf Henniger, Javier Galbally, Julian Fierrez, and Christoph Busch

Abstract—The performance of face analysis and recognition systems depends on the quality of the acquired face data, which is influenced by numerous factors. Automatically assessing the quality of face data in terms of biometric utility can thus be useful to filter out low quality data. This survey provides an overview of the face quality assessment literature in the framework of face biometrics, with a focus on face recognition based on visible wavelength face images as opposed to e.g. depth or infrared quality assessment. A trend towards deep learning based methods is observed, including notable conceptual differences among the recent approaches. Besides image selection, face image quality assessment can also be used in a variety of other application scenarios, which are discussed herein. Open issues and challenges are pointed out, i.a. highlighting the importance of comparability for algorithm evaluations, and the challenge for future work to create deep learning approaches that are interpretable in addition to providing accurate utility predictions.

Index Terms—Biometrics, biometric sample quality, face quality assessment, face recognition.

I. Introduction

Face Quality Assessment (FQA) refers to the process of taking face data as input to produce some form of "quality" estimate as output, as illustrated in Figure 1. An FQA algorithm (FQAA [57]) is an automated FQA approach. FQA can consist of general Image Quality Assessment (IQA), but it is typically specialized to faces (e.g. by utilizing the position of the eyes), and thus unlikely to be applicable as general IQA.

This survey focuses on face images in the visible spectrum as input to the face processing pipeline, which represents the most common input to face recognition (FR) systems, as opposed to face images beyond the visible spectrum [58][59]. Also, only single-image input FQA approaches are considered, meaning that methods utilizing additional subject-dependent input, such as reference [60] images [61], are outside the survey's scope. Thus, unless otherwise specified, FQA(A) will refer to single-image Face image Quality Assessment Algorithms in the visible spectrum, with a Quality Score (QS [57]) output that can be represented by a single scalar value. A vector of quality values measuring different aspects such as sharpness or illumination can be generated as well. See Figure 2 for some example images that a FQAA would likely consider to be of lower quality for different reasons.

T. Schlett, C. Rathgeb and C. Busch are with the da/sec - Biometrics and Internet Security Research Group, Hochschule Darmstadt, Germany, {torsten.schlett, christian.rathgeb, christoph.busch}@h-da.de
O. Henniger is with the Fraunhofer Institute for Computer Graphics Research IGD, Darmstadt, Germany, olaf.henniger@igd.fraunhofer.de
J. Galbally is with the European Commission, Joint Research Centre, Ispra, Italy, javier.galbally@ec.europa.eu
J. Fierrez is with the Universidad Autonoma de Madrid, Madrid, Spain, julian.fierrez@uam.es

Fig. 1. Typical FQA process: A face image is preprocessed and an FQAA is applied, resulting in a scalar quality score output, based on which a decision can be made. Face image taken from [62].

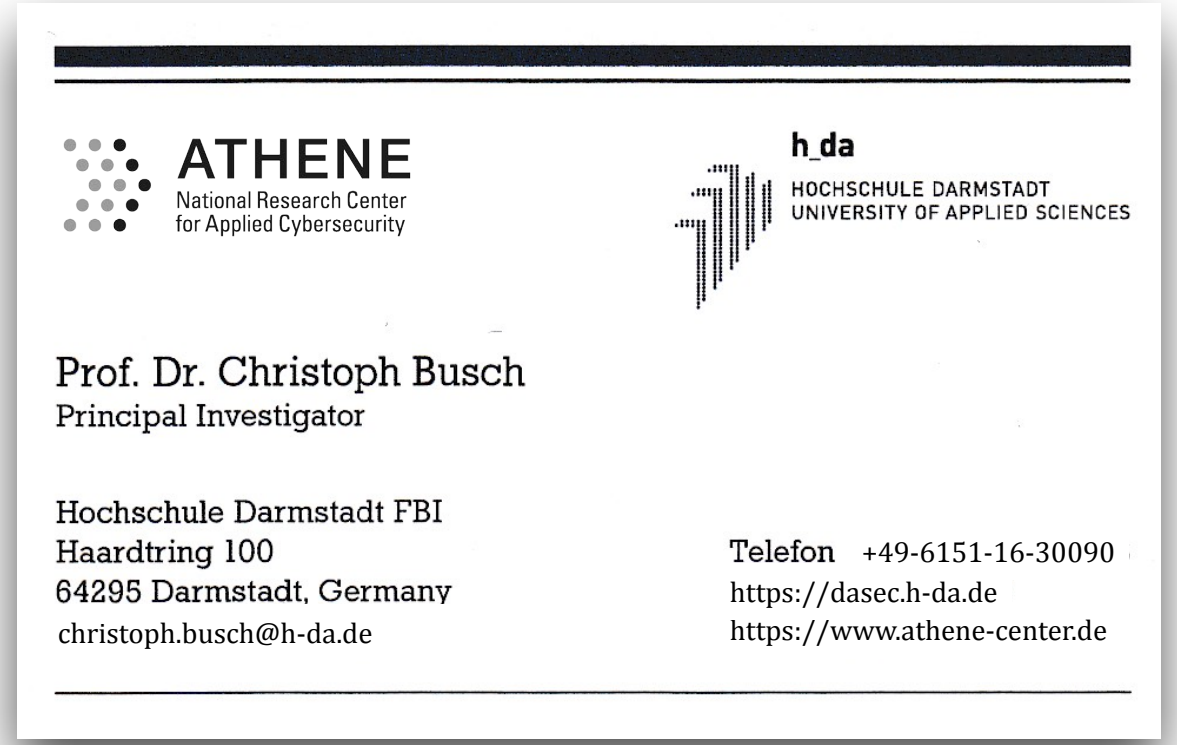
The term "quality" could refer to various definitions, with ISO/IEC 29794-1 [63] differentiating between three aspects called character, fidelity, and utility. In the context of face biometrics these can be described as follows [64].

- **Character**: Attributes associated with a biometric characteristic (e.g. the face topography or skin texture) that cannot be controlled during the biometric acquisition process (e.g. scars) [60].
- **Fidelity**: For a biometric sample [60], e.g. a face image, fidelity reflects the degree of similarity to its source biometric characteristic [63]. Thus a blurred image of a face omits detail and has low fidelity [62].
- **Utility**: The fitness of a sample to accomplish or fulfill the biometric function, which is influenced i.a. by the character and fidelity [60]. Thus, the term utility is used to indicate the value of an image to a receiving algorithm [62].

This survey considers the "utility" as the primary definition of what a quality score should convey, which is in accordance to i.a. the quality score definition of ISO/IEC 2382-37 [60] and the definition in the ongoing Face Recognition Vendor Test (FRVT) for face image quality assessment [62]. Thus, a Quality Score (QS) should be indicative of the Face Recognition (FR) performance. Note that this entails that the output of a specific FQAA may be more accurate for a specific FR system, so the FQA utility prediction effectivity ultimately depends on the combination of both. To facilitate interoperability, it is however desirable that the FQAA is predictive of recognition performance in general for a range of relevant systems, instead of being dependent on a single FR technology.

In short, under this survey's definitions, an FQAA is typically meant to output a scalar quality score to predict the FR performance from a single face input image. Being able to predict FR performance without necessarily running an FR algorithm makes FQA useful for a variety of scenarios, which are described further in subsection II-A. Note that the focus on FQA as a predictor for FR performance in the present survey

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