Standards and Challenges for Large Scale Systems

Christoph Busch

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

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

eu-LISA roundtable, November 3, 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)

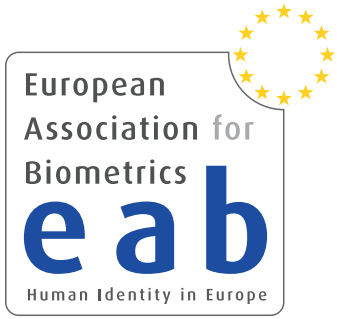
Gjøvik Research Group
@Norwegian University of Science and Technology

NTNU

NORWEGIAN BIOMETRICS LABORATORY

About my Affiliation(s)

European Association for Biometrics (EAB)



Darmstadt Research Group @Hochschule Darmstadt

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

Overview

Agenda

- Introduction
  - EAB
  - fields of initiatives
- Presentation attack detection
- Face sample quality
- Relevant standards

Introduction

European Association for Biometrics (EAB)

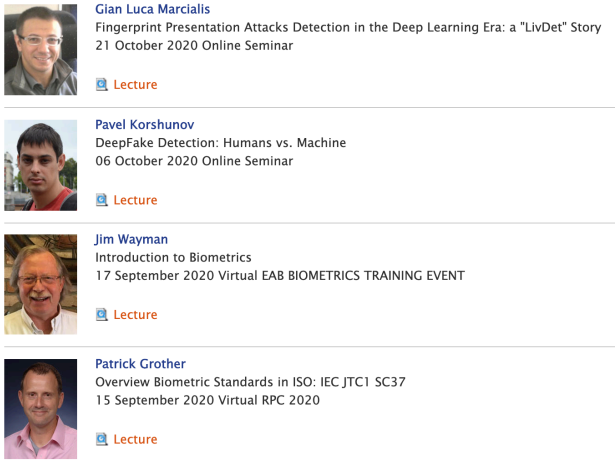
- The EAB is a non-profit, nonpartisan association
  https://eab.org/
- EAB supports all sections of the ID community across Europe, including governments, NGO's, industry, associations and special interest groups and academia.

- 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

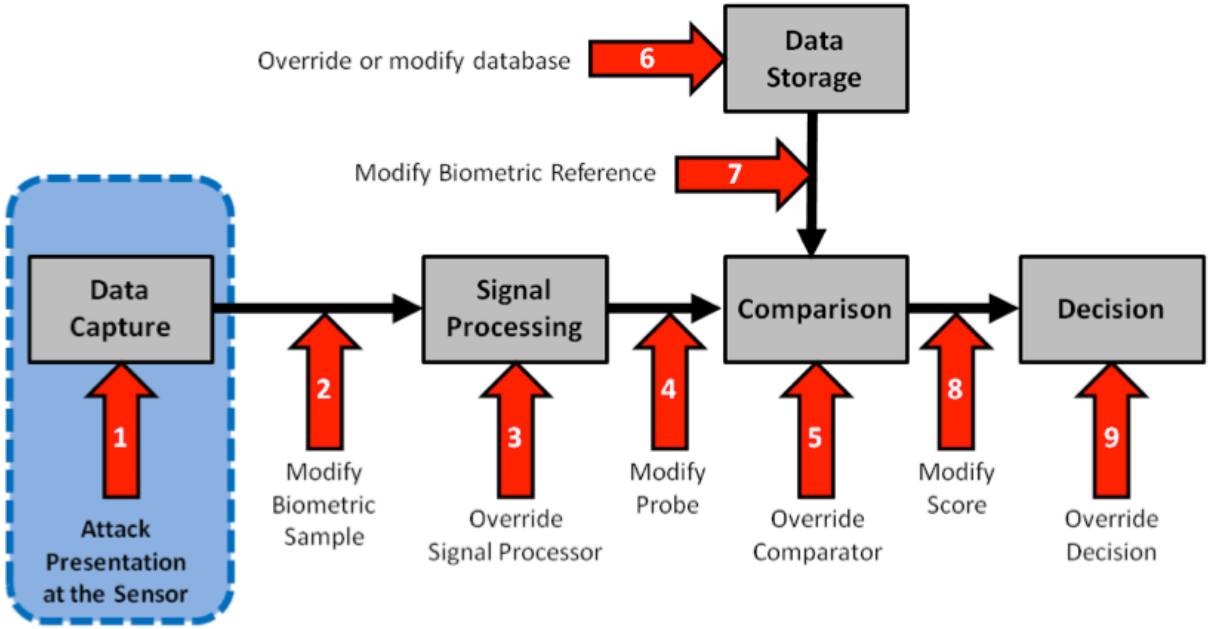
European Association for Biometrics (EAB)

- 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

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 Situation (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

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

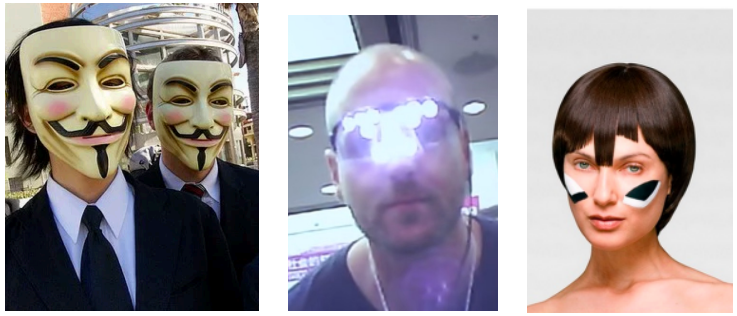


Image Source: https://www.youtube.com/watch?v=LRj8whKmN1M

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

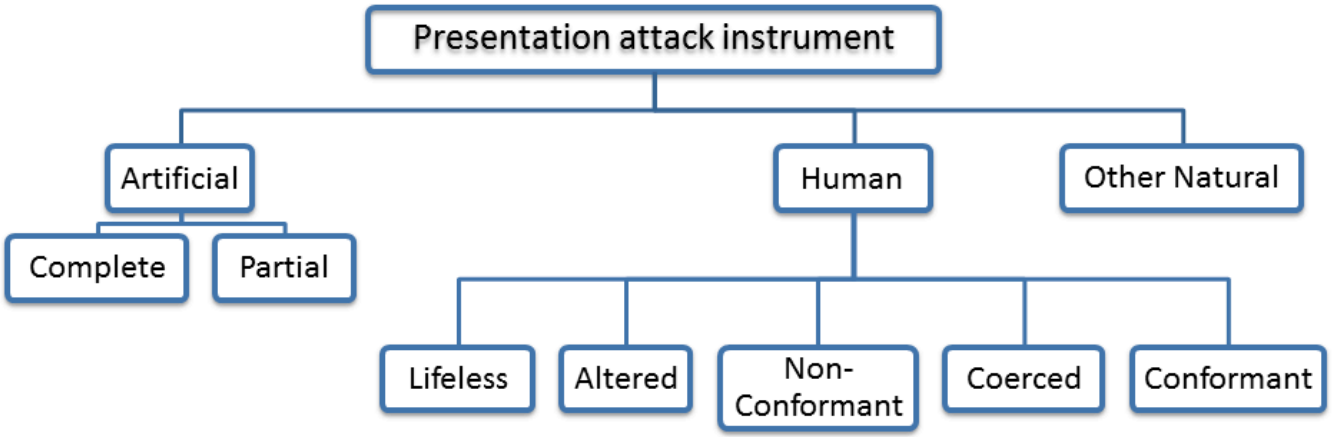
- **presentation attack instrument (PAI)**
  biometric characteristic or object used in a presentation attack
- **artefact**
  artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns

Types of presentation attacks

(General Noun)

(Adjectives describing categories)

(Qualifying adjectives)

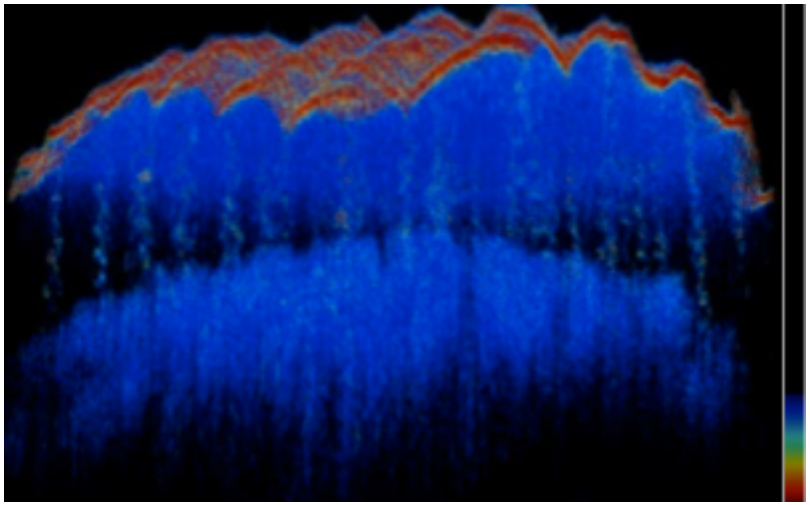


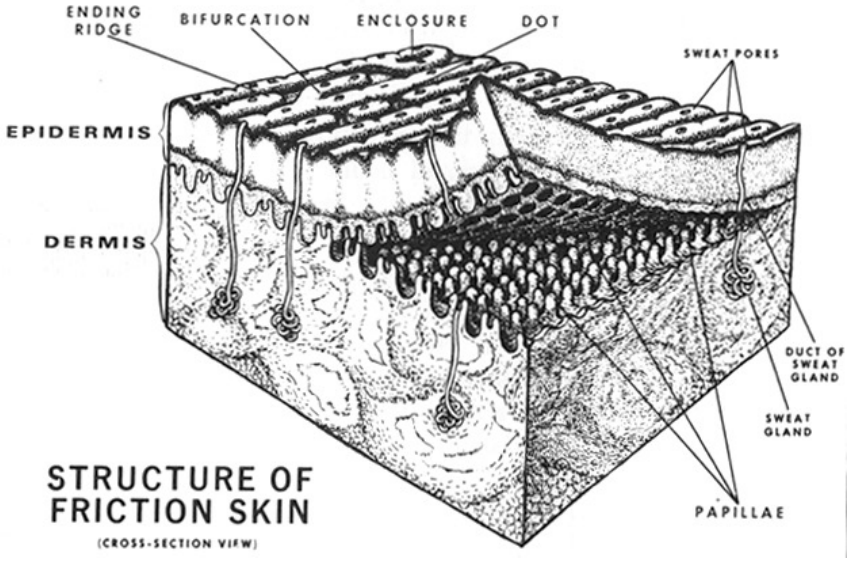
Source: ISO/IEC 30107-1

Fingerprint Capture Device Security

Countermeasures

- Observation of the live skin properties
- Observation of the sweat glandes
- Sensor technology
  - Optical Coherence Tomography (OCT)

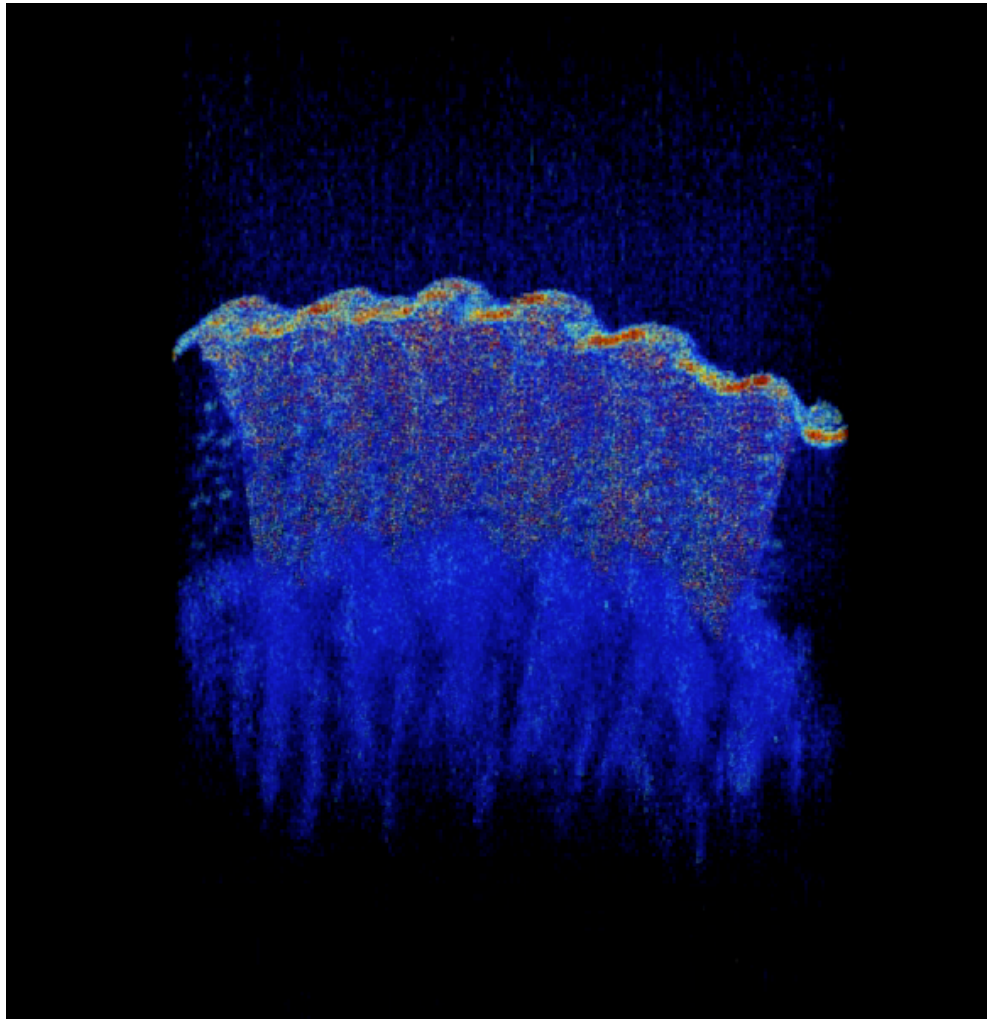




Fingerprint Capture Device Security

OCT Capture Device

- Cooperation with the German BSI
- Prototype for a high-end fingerprint sensor
- Requirements
  - Capture area: 20x20x6 mm
  - up to 3000 dpi
- Visualization of sweat glands

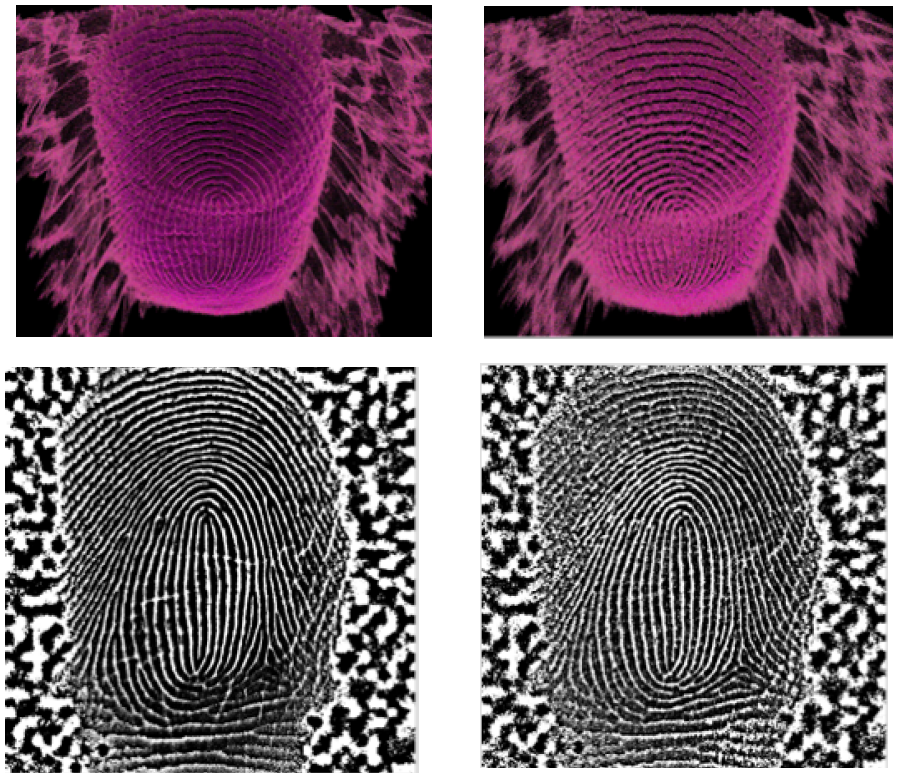


Source: C. Sousedik, NTNU, 2016

Fingerprint Capture Device Security

OCT - PAD

- Comparing outer and inner fingerprint patterns
- Detection of surface and internal layer
- 2D projection of the segmented layers

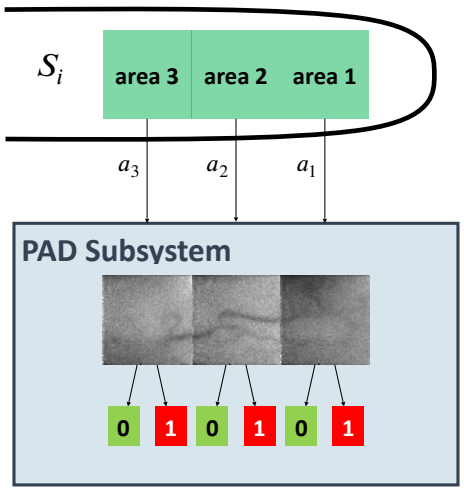


Surface Fingerprint Internal Fingerprint

Fingerprint Capture Device Security

Laser Speckle Contrast Imaging

- LSCI is a technology for imaging and monitoring blood flow in biomedical applications
- Based on the laser speckle effect:
  - Laser light illuminates a sufficiently rough surface and is scattered
  - Interference produces a granular pattern of dark and bright spots causing the speckle pattern
- Blood flow, causes fluctuations in the speckle pattern [Sen2013]



[Vaz2016] P. G. Vaz et al. „Laser Speckle Imaging to Monitor Microvascular Blood Flow: A Review“, IEEE Reviews in Biomedical Engineering, vol. 9, pp. 106-120, (2016)

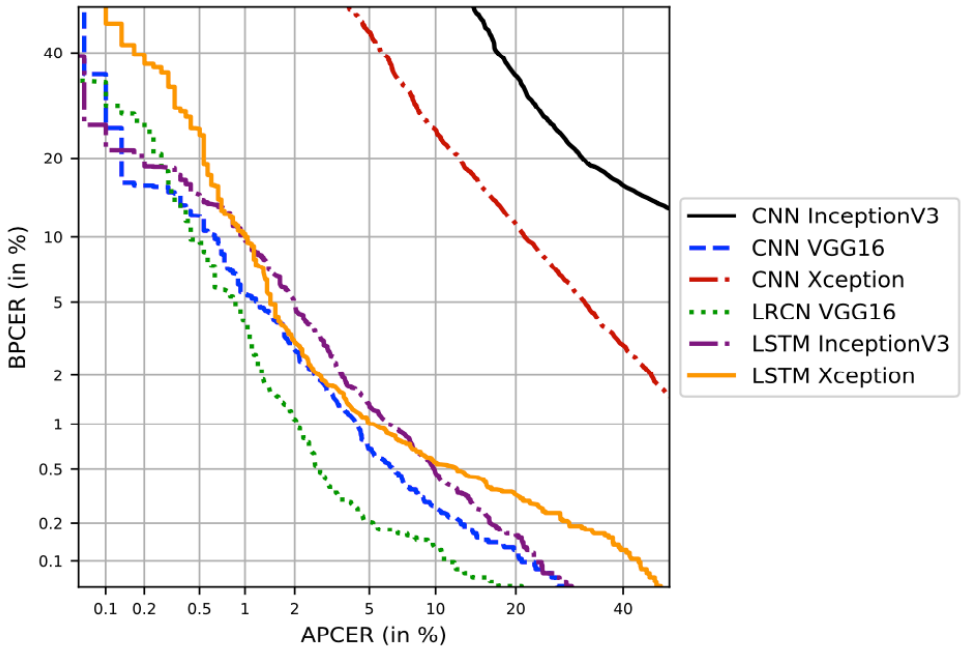
[Sen2013] J. Senarathna et al. "Laser Speckle Contrast Imaging: Theory, instrumentation and applications," IEEE Reviews in Biomedical Engineering, vol. 6, pp. 99-110, (2013)

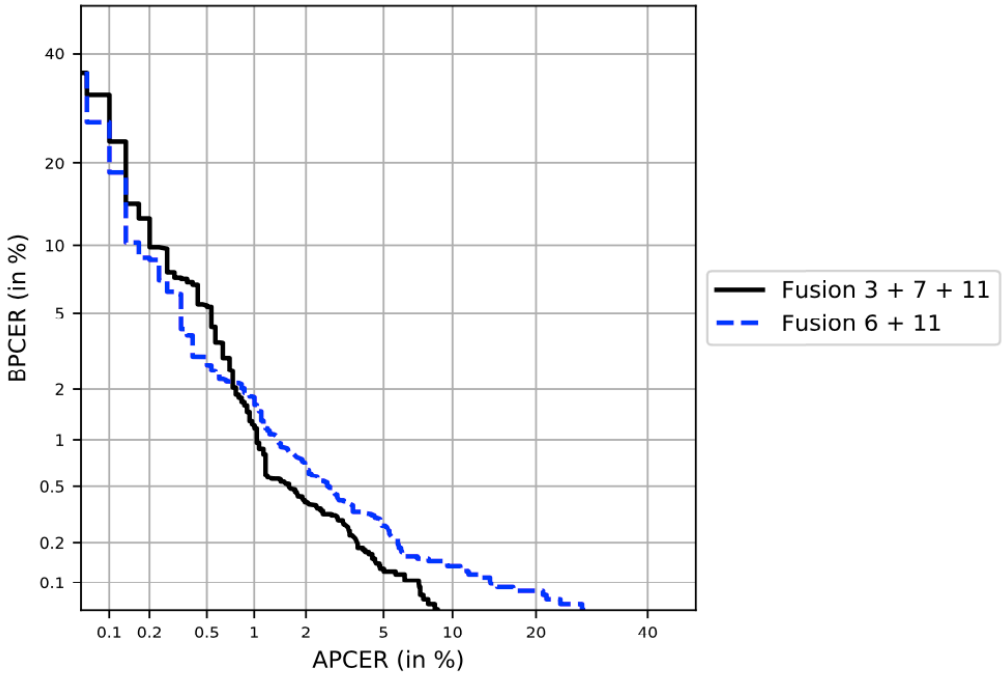
[Kolb2020] J. Kolberg, A. Vasile, M. Gomez-Barrero, C. Busch: "Analysing the Performance of LSTMs and CNNs on 1310 nm Laser Data for Fingerprint Presentation Attack Detection“, in Proceedings of International Joint Conference on Biometrics (IJCB 2020), Houston, US, September 28 – October 1, (2020)

Fingerprint Capture Device Security

LSCI - PAD

- Recent results based on IARPA ODIN
  - 1310 nm laser illumination
  - short video (100 frames)
  - CNN and long short-term memory (LSTM) networks





[Kolb2020] J. Kolberg, A. Vasile, M. Gomez-Barrero, C. Busch: "Analysing the Performance of LSTMs and CNNs on 1310 nm Laser Data for Fingerprint Presentation Attack Detection“, in Proceedings of International Joint Conference on Biometrics (IJCB 2020), Houston, US, September 28 – October 1, (2020)

Altered Fingerprint Detection - Testing

Example for fingerprint alterations

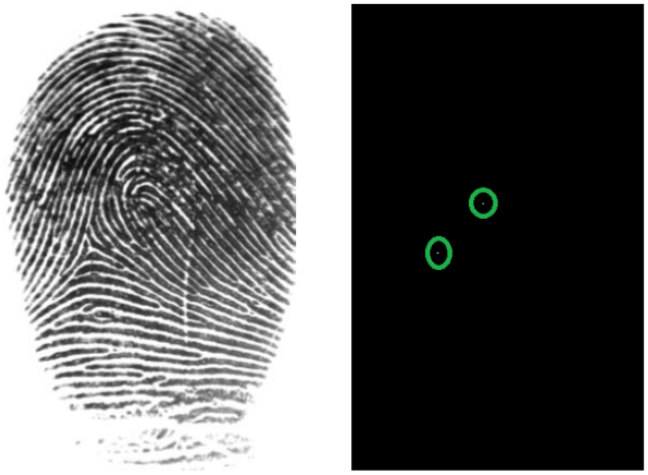
- Z-shaped alteration (Finger of Jose Izquierdo, 1995)

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

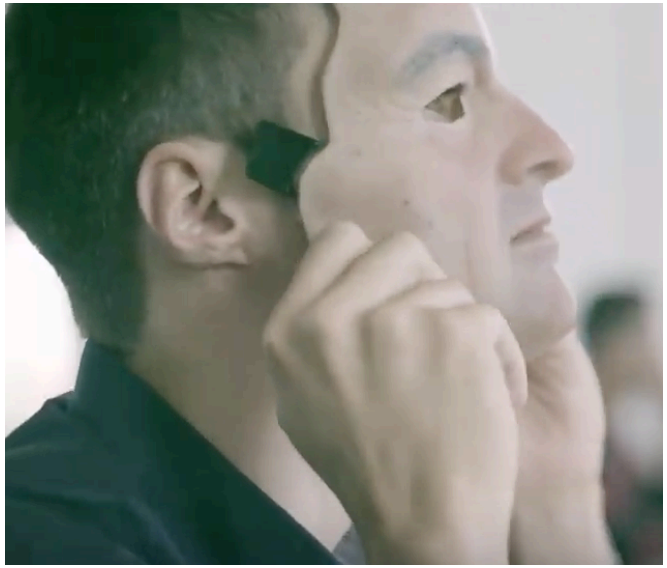
[Ellingsg2014] J. Ellingsgaard, C. Sousedik, and C. Busch, “Detecting fingerprint alterations by orientation field and minutiae orientation analysis,” in Proc. IWBF, Valletta, Malta, (2014)

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

Impostor Presentation Attack

3D silicone mask

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



Skin Detection

Short Wave Infrared Range (SWIR) imaging

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

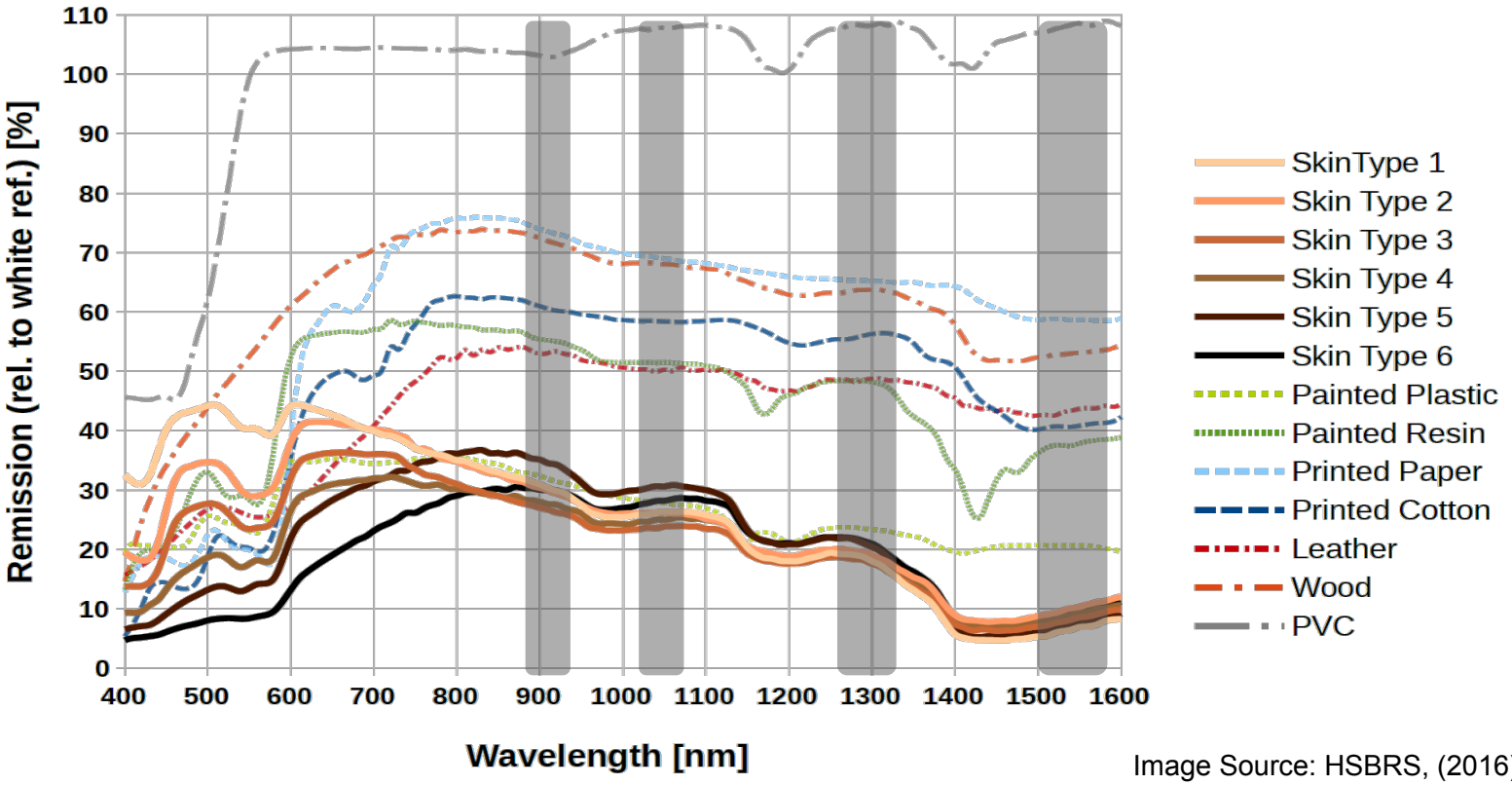


Image Source: HSBRS, (2016)

[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

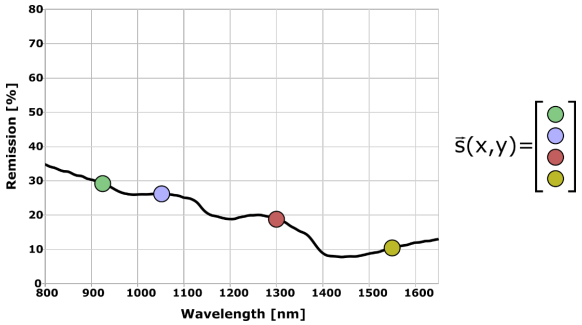


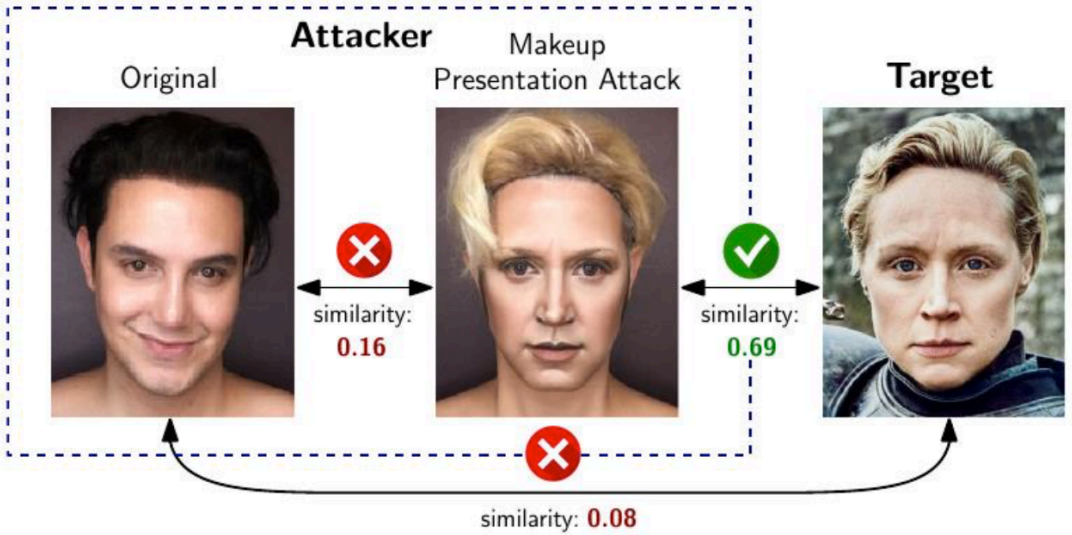
Image Source: HSBRS, (2016)

Makeup Presentation Attacks

Severe alterations

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

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

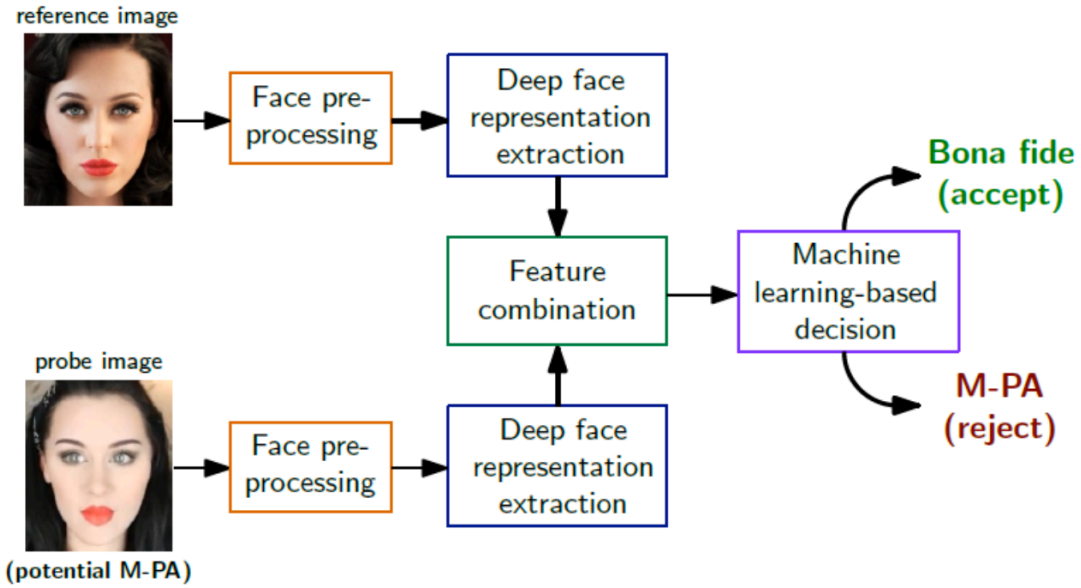


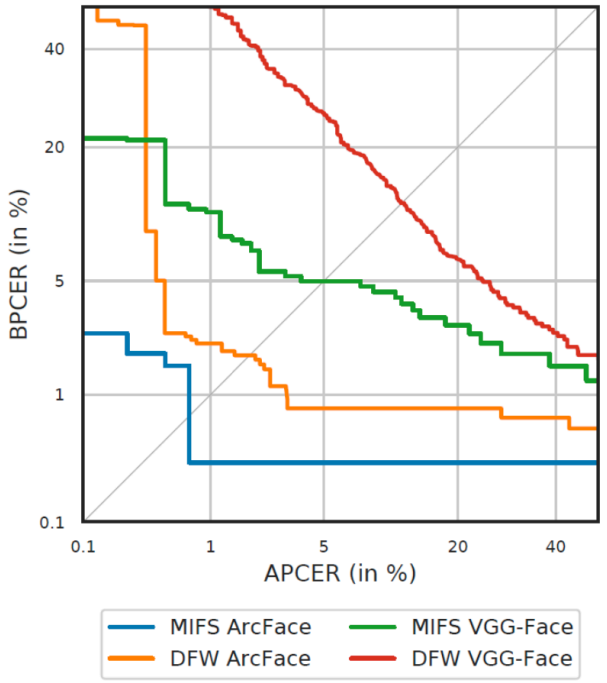
[Rathg2020] C. Rathgeb, P. Drozdowski, D. Fischer, C. Busch: "Vulnerability Assessment and Detection of Makeup Presentation Attacks“, in Proceedings of 8th International Workshop on Biometrics and Forensics (IWBF 2020), Porto, PT, April 29 - 30, (2020)

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)

Concealer Presentation Attack

Face disguise for privacy protection

Concealer Presentation Attack

Face disguise for organized crime (June 2012)

- http://www.dailymail.co.uk/news/article-2153346/Black-armed-robber-disguised-white-man-using-latex-mask.html

The man in the latex mask: BLACK serial armed robber disguised himself as a WHITE man to rob betting shops

- **Henley Stephenson wore the disguise during a 12-year campaign of hold-ups at betting shops and other stores across London**
- **He was part of a three-man gang jailed for a total of 28 years**
- **CCTV footage showed him firing a semi-automatic pistol into the ceiling during a raid on a betting shop**
- **The mask was bought from the same London shop which supplied masks used in the £40m Graff Diamonds heist**

By ROB PREECE and REBECCA CAMBER FOR THE DAILY MAIL

PUBLISHED: 17:22 GMT, 1 June 2012 | **UPDATED:** 16:21 GMT, 2 June 2012

Most masked robbers opt for a balaclava to hide their identity.

Not this one. Henley Stephenson, 41, eluded police for more than ten years thanks to an extraordinarily lifelike latex mask, which turned him into a white skinhead.

Officers discovered that their man was in fact black when they finally caught up with Stephenson after a string of armed raids dating back to 1999.

Enrolment Attacks
Face Morphing

Problem: Morphing Attacks

Enrolment attack with morphed facial images

Subject A

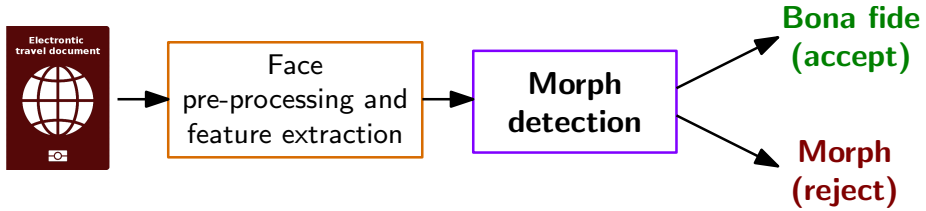
Morph = Subject A + Subject C

Subject C

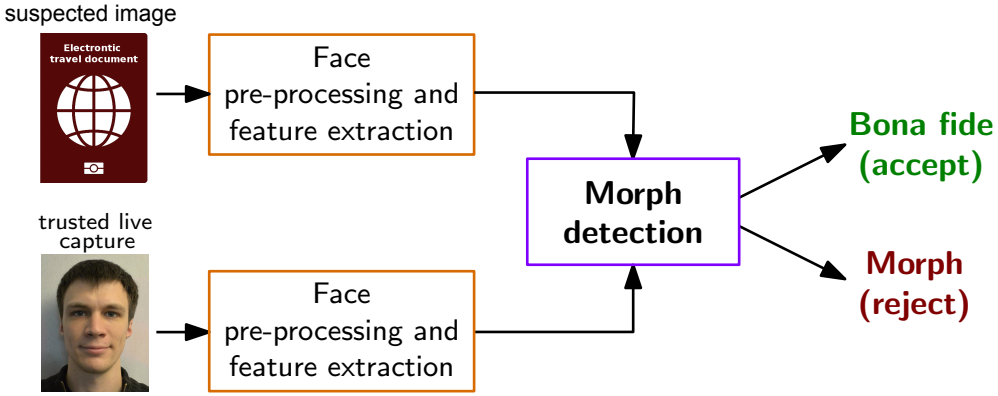
Morphing Attack Detection Scenarios

Real world scenarios

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



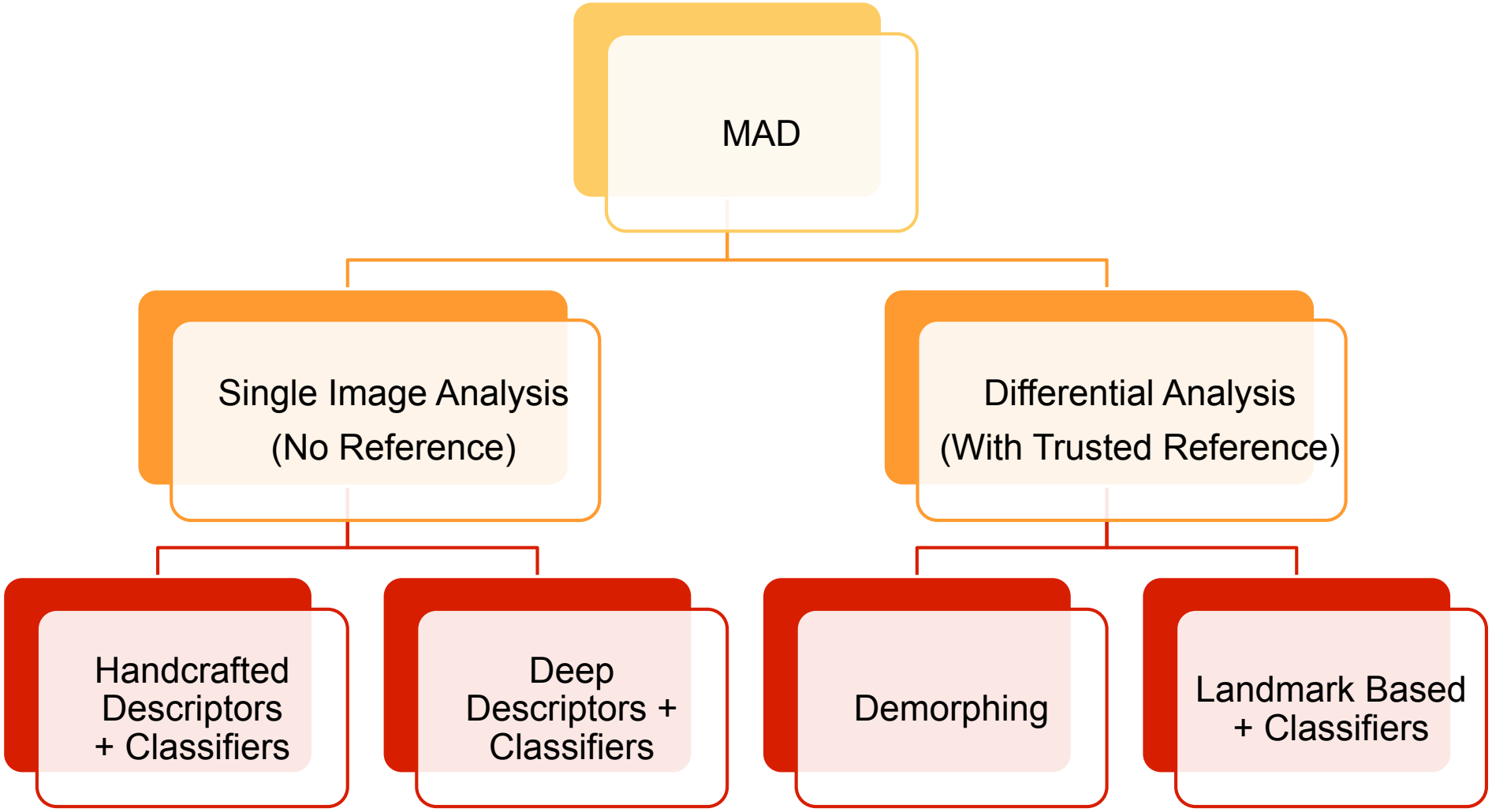
- Differential morphing attack detection (D-MAD)
  - A pair of images is analysed - and one is a trusted Bona Fide image
  - Biometric verification (e.g. at the border)



[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)



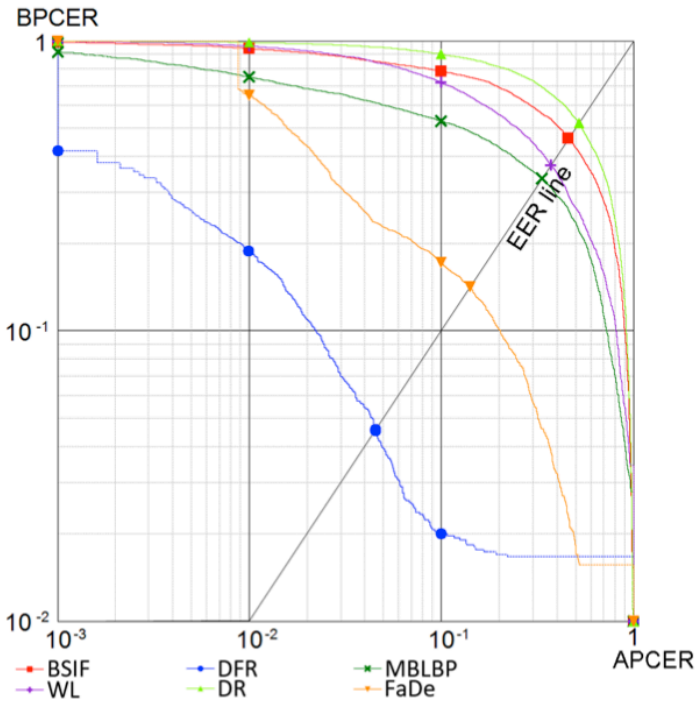
[SRMBB2019] U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, C. Busch: "Face Recognition Systems under Morphing Attacks: A Survey“, in IEEE Access, (2019)

State of the Art - MAD Algorithms

Detection accuracy - focused on D-MAD

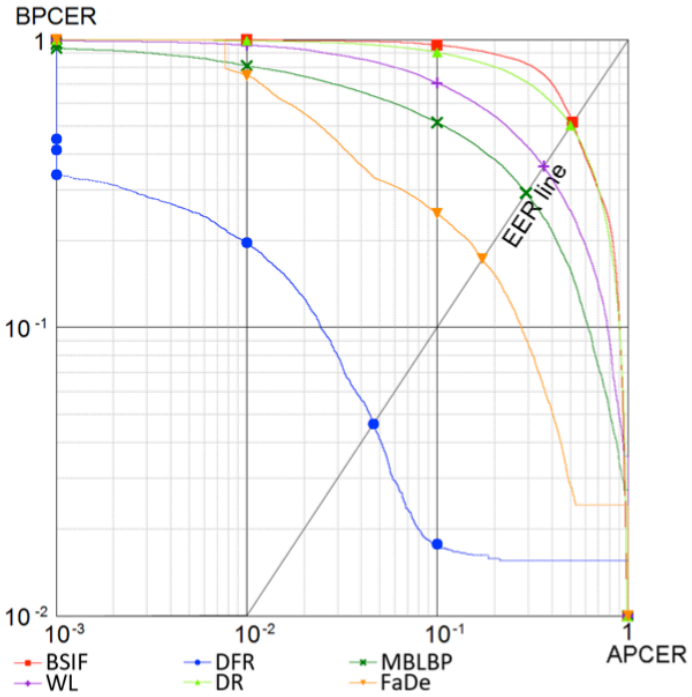
https://biolab.csr.unibo.it/FVCOnGoing/UI/Form/BenchmarkAreas/BenchmarkAreaDMAD.aspx

- 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

Face Sample Quality

Factors impacting Quality

Face sample quality

- Image capture system out of focus
- No frontal perspective

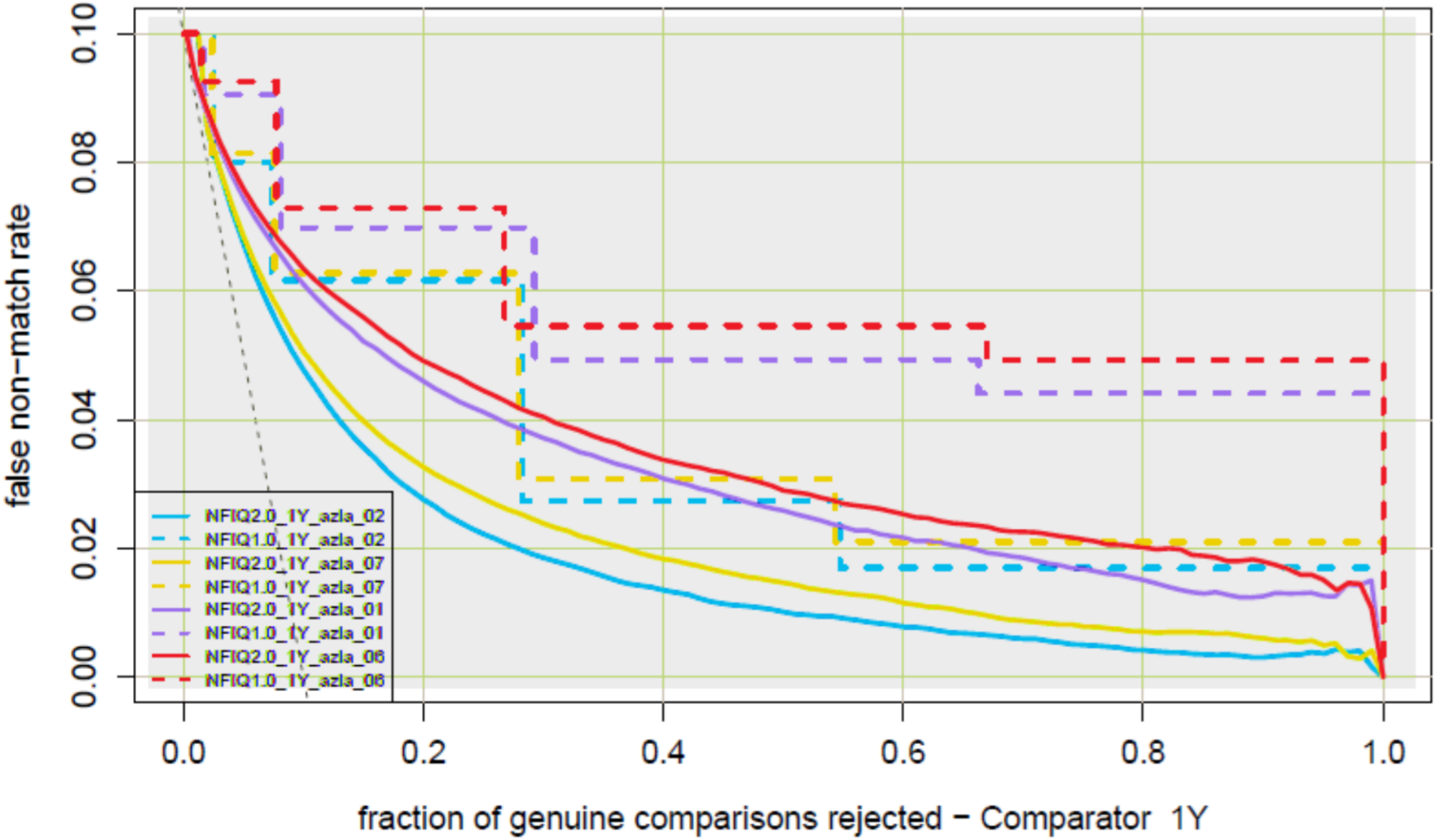
Fingerprint sample Quality

- Defect caused by the source
  - Skin condition such as moist, oily, dry and so on
  - Scars, wrinkles, blisters, eczema, dirt
- Defect caused by the capture device
  - Sampling error, low contrast
- Defect caused by the capture subject‘s behaviour
  - Elastic deformation
  - Improper finger placement (too low, rotated, etc)

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

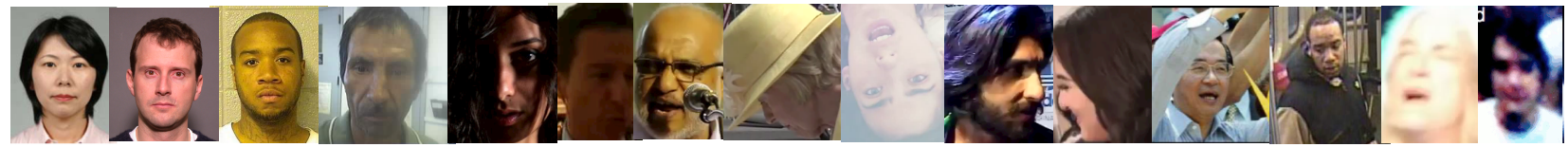
NFIQ2.0: Finger Image Quality

Evaluation - Error versus reject curve



Face Image Quality

Flavors of quality: good, bad, wild, ugly



Cooperative Enrollment where quality assessment is traditionally most useful at initial collection.

Non-Cooperative

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

Testing of the Entry-Exit-System

- Real data in large numbers is not (yet) accessible
- StyleGAN can generate unlimited number of images
- Is the quality of synthetic data as good as real data?

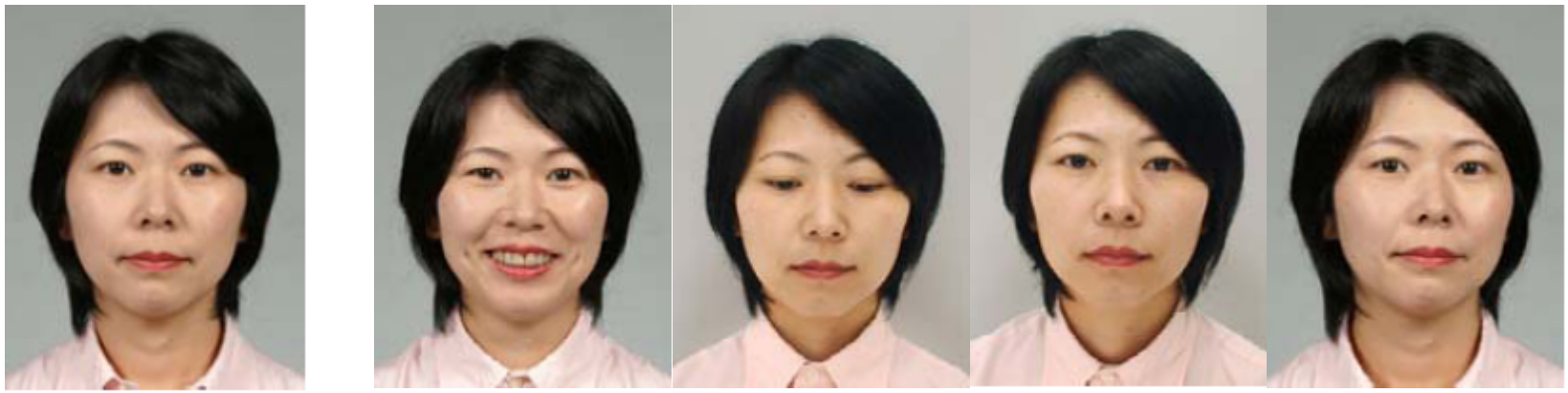
- eu-LISA study with
  - HDA-Steinbeis-Darmstadt
  - NTNU-Mobai-Gjøvik
  - PLUS-Salzburg

https://christoph-busch.de/projects-euLISA.html

Face Image Quality

Actionable feedback

- If quality is poor, then what went wrong?



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

Source: http://webstore.ansi.org

Face Image Quality

The literature shows numerous approaches [Schlett2020]

- Non-DeepLearning based face quality assessment
- Standard focused face quality assessment
- Video frame face quality assessment
- DeepLearning based face quality assessment

For more on Face Image Quality see
the keynote by Javier Galbally on November 4th

[Schlett2020] 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

Standards

Quality-Related Standards

Relevant standards

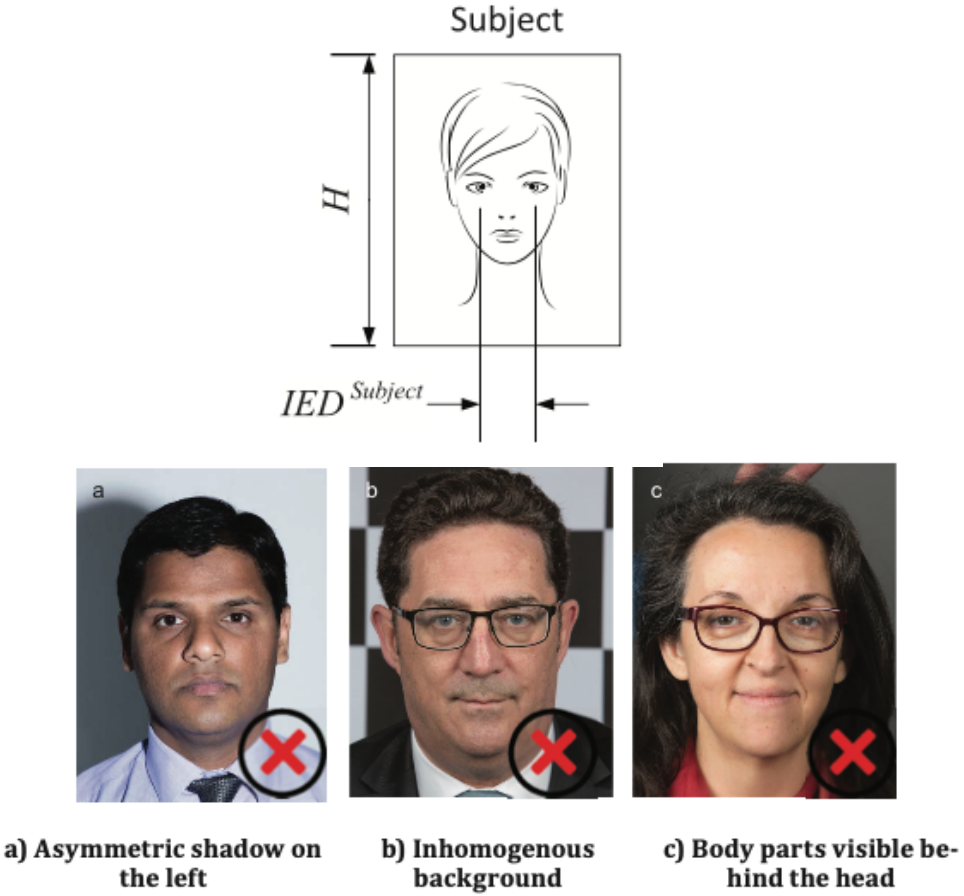
- ISO/IEC 29794-1: Quality Framework
  - Definitions and evaluation concepts https://www.iso.org/standard/62782.html
- ISO/IEC 29794-4: Fingerprint image quality
  - NFIQ 2.1
    https://github.com/usnistgov/NFIQ2
    https://www.nist.gov/system/files/documents/2018/11/29/nfiq2_report.pdf
- ISO/IEC 29794-5: Face image quality
  - Revision of ISO/IEC 29794-5:2011
    http://www.paddymondo.net/ISO_IEC_29794_5.pdf
  - Scalar values
  - Vector values ~ Quantitative ISO/ICAO compliance checklist
- ISO/IEC 24358: Face-aware capture device
  http://www.paddymondo.net/ISO_IEC_24358.pdf
  - Face detector
  - Face pose estimator
  - Background face detection removal

Quality-Related Standards

ISO/IEC WD 29794-5 aligned with ISO/IEC 39794-5

#	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
http://www.paddymondo.net/ISO_IEC_29794_5.pdf



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

ICAO 9303 Logical Data Structure

Data stored on the chip (LDS)

- DG1: Information printed on the data page
- DG2: Facial image of the holder (mandatory)

- DG3: Fingerprint image of left and right index finger

- DG4: Iris image

....

- DG15: Active Authentication Public Key Info
- DG16: Persons to notify

Document Security Object

- Hash values of DGs

					DATA ELEMENTS
REQUIRED	ISSUING STATE OR ORGANIZATION DATA	Detail(s) Recorded in MRZ	DG1		Document Type
					Issuing State or organization
					Name (of Holder)
					Document Number
					Check Digit - Doc Number
					Nationality
					Date of Birth
					Check Digit - DOB
					Sex
					Data of Expiry or Valid Until Date
					Check Digit DOE/VUD
					Optional Data
					Check Digit - Optional Data Field
					Composite Check Digit
		Encoded Identification Feature(s)	Global Interchange Feature	DG2	Encoded Face
			Additional Feature(s)	DG3	Encoded Finger(s)
				DG4	Encoded Eye(s)
OPTIONAL	ISSUING STATE OR ORGANIZATION DATA	Displayed Identification Feature(s)	DG5		Displayed Portrait
			DG6		Reserved for Future Use
			DG7		Displayed Signature or Usual Mark
		Encoded Security Feature(s)	DG8		Data Feature(s)
			DG9		Structure Feature(s)
			DG10		Substance Feature(s)
			DG11		Additional Personal Detail(s)
			DG12		Additional Document Detail(s)
			DG13		Optional Detail(s)
			DG14		Security Options
			DG15		Active Authentication Public Key Info
			DG16		Person(s) to Notify

Source: ICAO 9303 Part 10, 2015

ICAO 9303 Logical Data Structure

Data to be stored in the ICAO 9303 LDS

- Alpha-numeric data: 5 Kbyte
- Facial image: ISO/IEC 19794-5:2005
  - 12 Kbyte (JPEG, JPEG2000)
- Fingerprint images: ISO/IEC 19794-4:2005
  - 2* 10 Kbyte (JPEG, JPEG2000, WSQ)

- Facial image: ISO/IEC 39794-5:2019
  https://www.iso.org/standard/72155.html
- Fingerprint images: ISO/IEC 39794-4:2019
  https://www.iso.org/standard/72156.html
  - ICAO will adopt its 9303 specification in 2020 and refer to ISO/IEC 39794 and its Parts 1, 4 and 5 by December 2020.
  - Passport reader equipment must be able to handle ISO/IEC 39794 data by 2025-01-01 (5 years preparation period).
  - Between 2025 and 2030, passport issuers can use the old version or the new version of standards (5 years transition period).

New in 2020

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

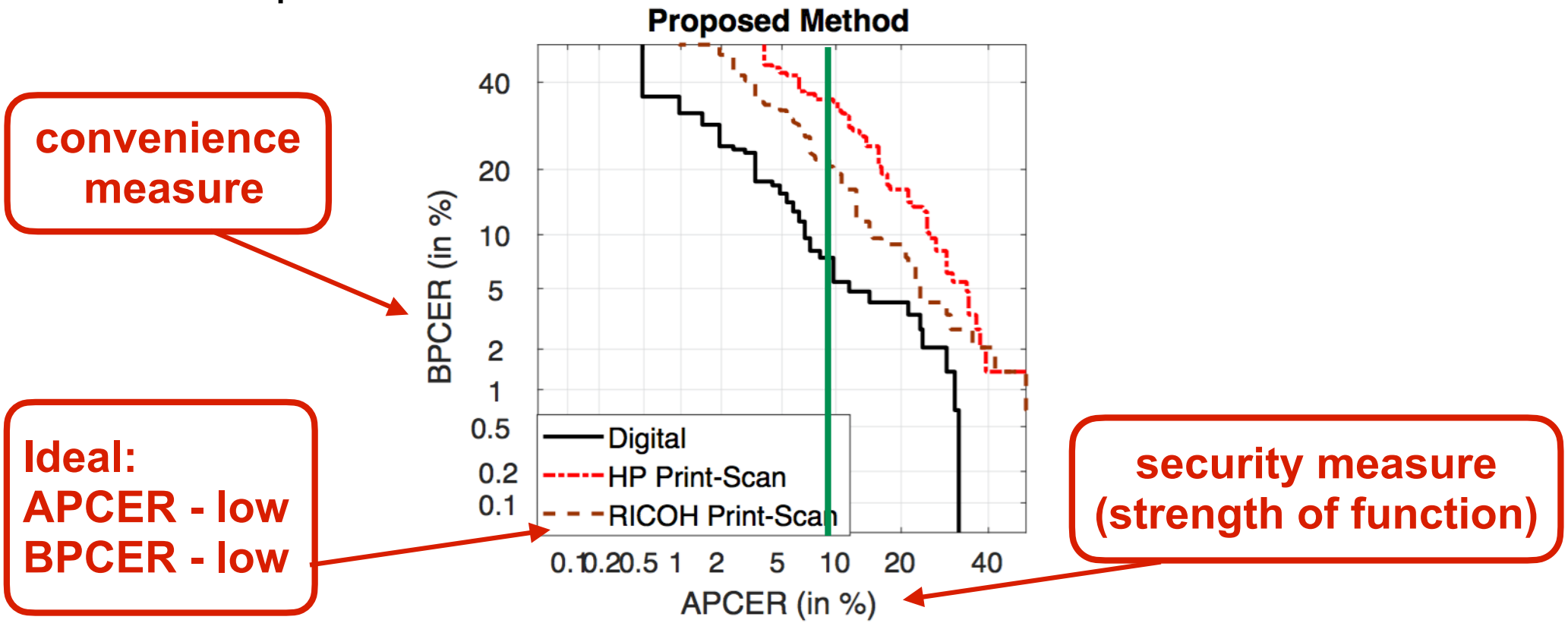
- **Bona fide presentation classification error rate (BPCER)**
  proportion of bona fide presentations incorrectly classified as attack presentations in a specific scenario

source: [ISO/IEC 30107-3] SO/IEC 30107-3, “Biometric presentation attack detection - Part 3: Testing and reporting”, (2017)
https://www.iso.org/standard/67381.html

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)

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-3

- Testing the vulnerability of the biometric system:
- **Impostor attack presentation match rate (IAPMR)**
  in a full-system evaluation of a verification system,
  the proportion of impostor attack presentations
  using the same presentation attack instrument species
  in which the target reference is matched

Source: ISO/IEC 30107-3

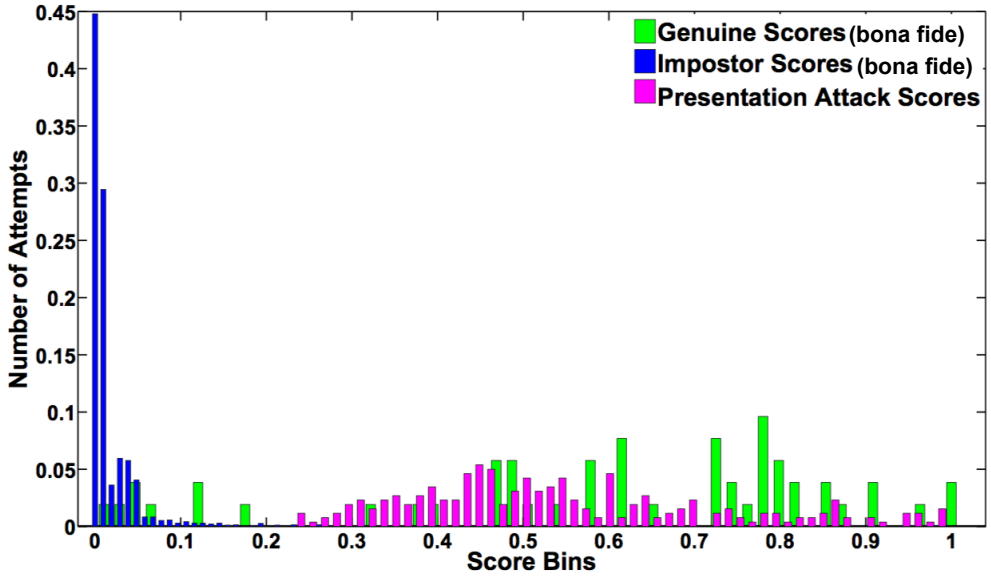


Image Source: K. Raja, R. Raghavendra, C. Busch: "Video Presentation Attack Detection in Visible Spectrum Iris Recognition Using Magnified Phase Information", in IEEE TIFS, June 2015

- Revision project ISO/IEC 30107-3: http://www.paddymondo.net/ISO_IEC_30107_3.pdf

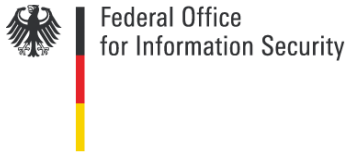
Thanks

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

Received January 11, 2019, accepted January 31, 2019, date of publication February 14, 2019; date of current version March 4, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2899367

Face Recognition Systems Under Morphing Attacks: A Survey

ULRICH SCHERHAG[1], CHRISTIAN RATHGEB[1,2], JOHANNES MERKLE[2], RALPH BREITHAUPT[3], AND CHRISTOPH BUSCH[1]

[1]da/sec–Biometrics and Internet Security Research Group, Hochschule Darmstadt, 64295 Darmstadt, Germany
[2]secunet Security Networks AG, 45138 Essen, Germany
[3]Federal Office of Information Security (BSI), 53133 Bonn, Germany

Corresponding author: Ulrich Scherhag (ulrich.scherhag@h-da.de)

This work was supported in part by the German Federal Ministry of Education and Research (BMBF), in part by the Hessen State Ministry for Higher Education, Research and the Arts (HMWK), Center for Research in Security and Privacy, and in part by the Federal Office of Information Security (BSI) through the FACETRUST Project.

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

Automated face recognition [1], [2] represents a long-standing field of research in which a major break-though has been achieved by the introduction of deep neural networks [3], [4]. Due to the high generalization capabilities of deep neural networks specifically and recognition systems in general, the performance of operational face recognition systems in unconstrained environments, e.g., regarding illumination, poses, image quality or cameras, improved significantly. Resulting performance improvements paved the way for deployments of face recognition technologies in diverse application scenarios, ranging from video-based surveillance and mobile device access control to Automated Border Control (ABC). However, recently researchers found that the generalizability of (deep) face recognition systems increases their vulnerability against attacks, e.g., spoofing attacks (also referred to as presentation attacks) [5]. An additional attack vector enabled by the high generalization capabilities is a specific attack against face recognition systems based on morphed face images, as introduced by Ferrara *et al.* [6].

The associate editor coordinating the review of this manuscript and approving it for publication was Zahid Akhtar.

A. FACE MORPHING ATTACK

Image morphing has been an active area of image processing research since the 80s [7], [8] with a wide variety of application scenarios, most notably in the film industry. Morphing techniques can be used to create artificial biometric samples, which resemble the biometric information of two (or more) individuals in image and feature domain. An example of a *morphed* face image as the result of two non-morphed, i.e., *bona fide* [9], face images, is depicted in Fig. 1. The created morphed face image will be successfully verified against probe samples of both contributing subjects by state-of-the-art face recognition systems. This means, if a morphed face image is stored as reference in the database of a face recognition system, both contributing subjects can be successfully verified against this manipulated reference. Thus, morphed face images pose a severe threat to face recognition systems, as the fundamental principal of biometrics, the unique link between the sample and its corresponding subject, is violated.

In many countries, the face image used for the ePassport issuance process is provided by the applicant in either analog or digital form. In a face morphing attack scenario,

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 Center, 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].

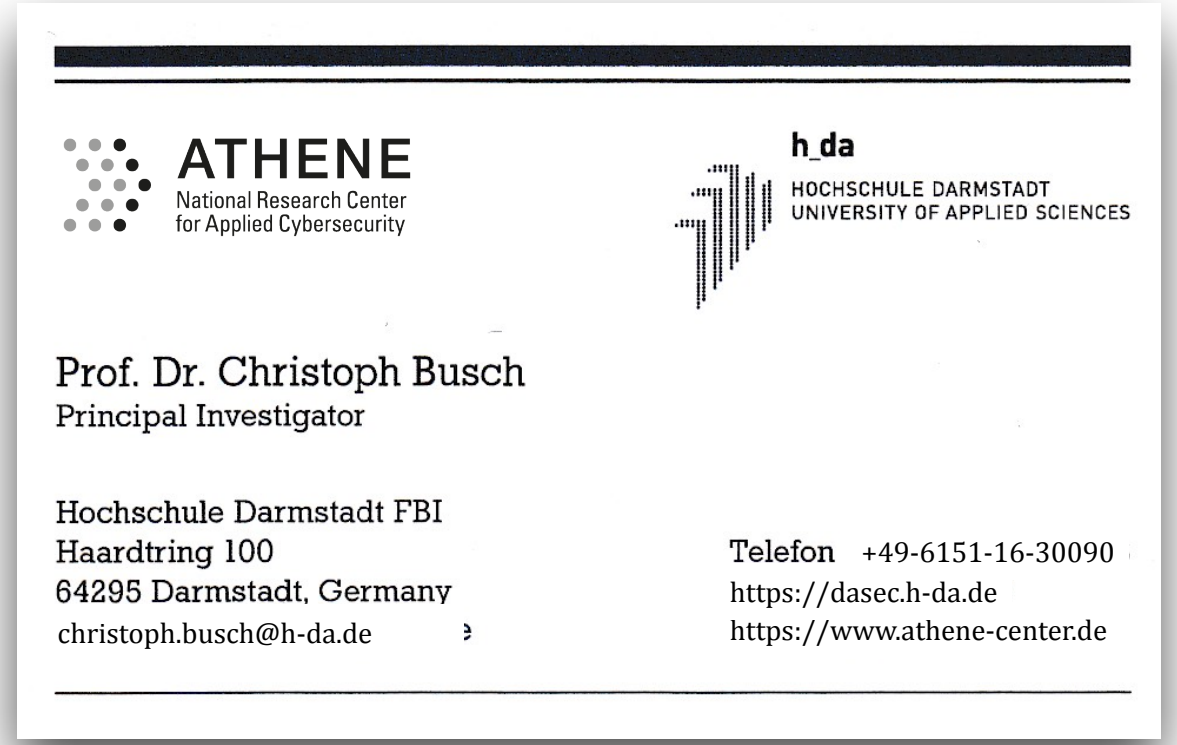
The term "quality" could refer to various definitions, with ISO/IEC 29794-1 [63] differentiating between three aspects called character, fidelity, and utility. In the context of face biometrics these can be described as follows [64]:

- **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

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