Biometrics and Interconnectivity

Christoph Busch

European Association for Biometrics (EAB)
https://eab.org/
copy of slides available at:
https://christoph-busch.de/about-talks-slides.html

2021-10-01

ATHENE

European Association for Biometrics eab Human Identity in Europe

NTNU

Why Biometrics? - Confirm an Identity Claim

Authentication can be achieved by:

- Something you know:
  Password, social profile

- Something you own:
  Smartphone, breeder document

- Something you are:
  Body characteristics

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

European Association for Biometrics (EAB)

Objectives of the 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.
- Structure of membership fees is inclusive
  - Free membership for Bachelor, Master and PhD students!
    https://eab.org/membership/types_of_membership.html

European Association for Biometrics (EAB)

More Information

- Our initiatives are designed to foster networking
  - Annual conference: EAB-RPC
    https://eab.org/events/program/219
  - Biometric Training Event
    https://eab.org/events/program/224
  - 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/268
  - 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/1961/EAB-research-report-2020.pdf
  - Open source repository
    https://eab.org/information/software.html

Facilitating Free Travel in the Schengen Area

Authors of EAB position paper

- appreciate the benefit of the Schengen area and the free movement of citizens in the EU
- hope that reintroduced intra-Schengen physical border controls and even closed borders will disappear
- seek technology, which is compliant with ethical principals and fundamental rights
- support demographic fairness for AI and non-AI-based systems
- anticipate that we discuss technology and steps, which will NOT require a change of the legal framework

Perspective

- fully functioning and resilient Schengen area

The full EAB position paper is available at:

https://eab.org/files/documents/2021-05-06_EABposition_Facilitating_Free_Travel_in_the_Schengen_Area.pdf

Focus of this talk:

biometrics and EXTERNAL borders

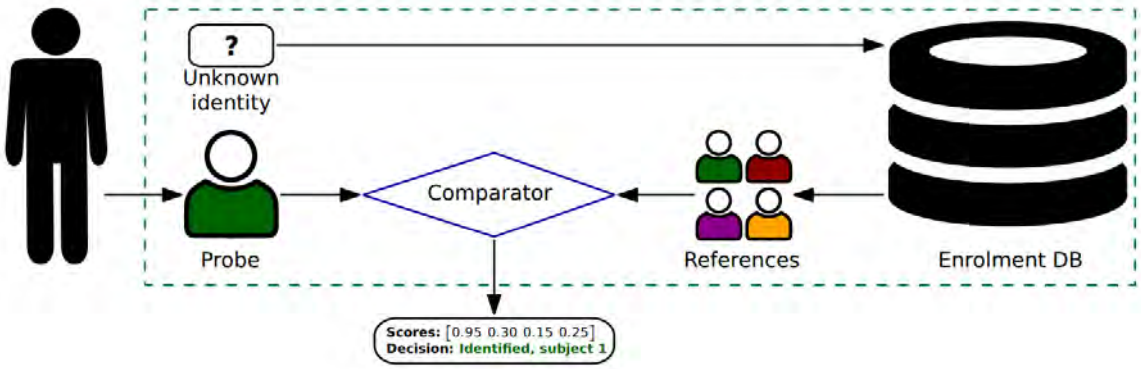
External Borders

Situation of existing technology

- modern technologies at the border (Eurodac, VIS, EES) provide promising solutions facilitating legitimate travels
  - automated border gates with biometric verification

Image source: secunet, idemia, vision-box

- biometric reference data must be accessible in personal ID document or a central database

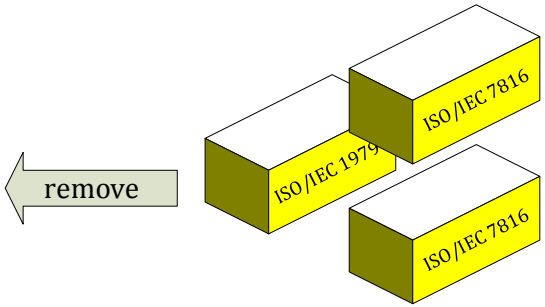


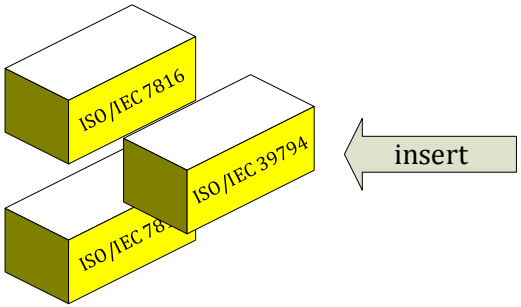
External Borders

Situation of near-term change in technology (3 years)

- modern technologies at the border (Eurodac, VIS, EES) provide promising solutions facilitating legitimate travels
  - automated border gates with biometric verification

- biometric reference data must comply with ISO/IEC 39794-1, -4 and -5 accessible in personal ID document by revision of ICAO 9303
  - passport reader equipment must be adopted by 2025-01-01





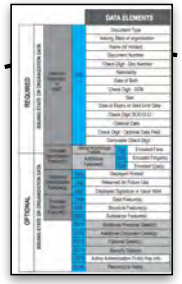
External Borders

Situation of mid-term change in technology (6 years)

- modern technologies at the border (Eurodac, VIS, EES) provide promising solutions facilitating legitimate travels
  - automated border gates with biometric verification

- biometric reference data must be accessible in personal ID document

Physical Component (PC)



Virtual Component (VC)

Physical Component (PC)

Corona Consequences

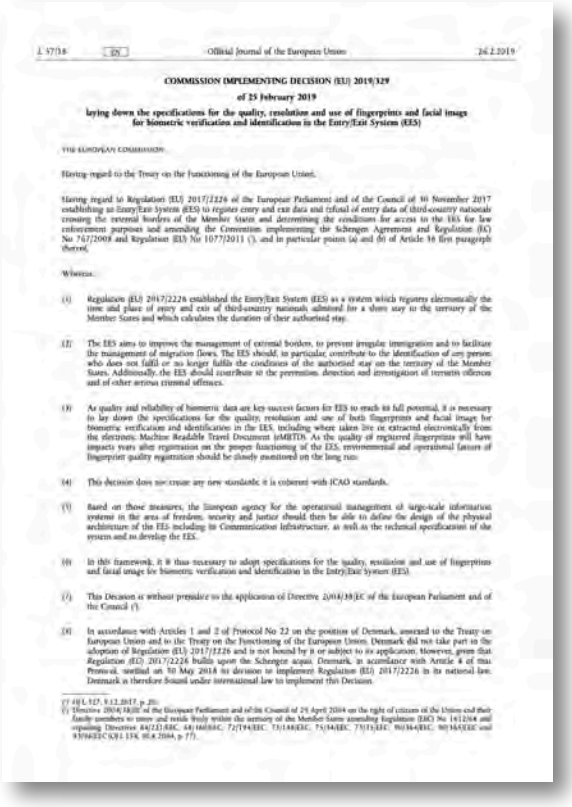
Focus on contactless biometric captures

Quality Metrics for Fingerprint Images

NFIQ2.0

- The Entry Exit System implementing decision 2019/329 defines the mandatory use:

- „*At the moment of enrolment, the version 2.0 (or newer version) of the Fingerprint Image Quality (NFIQ) metric …. shall be used for verifying that the quality of the captured fingerprint data respects the thresholds …*“



L 57/18 EN Official Journal of the European Union 26.2.2019

COMMISSION IMPLEMENTING DECISION (EU) 2019/329

of 25 February 2019

laying down the specifications for the quality, resolution and use of fingerprints and facial image for biometric verification and identification in the Entry/Exit System (EES)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes and amending the Convention implementing the Schengen Agreement and Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011 (1), and in particular points (a) and (b) of Article 36 first paragraph thereof,

Whereas:

(1) Regulation (EU) 2017/2226 established the Entry/Exit System (EES) as a system which registers electronically the time and place of entry and exit of third-country nationals admitted for a short stay to the territory of the Member States and which calculates the duration of their authorised stay.

(2) The EES aims to improve the management of external borders, to prevent irregular immigration and to facilitate the management of migration flows. The EES should, in particular, contribute to the identification of any person who does not fulfil or no longer fulfils the conditions of the authorised stay on the territory of the Member States. Additionally, the EES should contribute to the prevention, detection and investigation of terrorist offences and of other serious criminal offences.

(3) As quality and reliability of biometric data are key success factors for EES to reach its full potential, it is necessary to lay down the specifications for the quality, resolution and use of both fingerprints and facial image for biometric verification and identification in the EES, including where taken live or extracted electronically from the electronic Machine Readable Travel Document (eMRTD). As the quality of registered fingerprints will have impacts years after registration on the proper functioning of the EES, environmental and operational factors of fingerprint quality registration should be closely monitored on the long run.

(4) This decision does not create any new standards; it is coherent with ICAO standards.

(5) Based on those measures, the European agency for the operational management of large-scale information systems in the area of freedom, security and justice should then be able to define the design of the physical architecture of the EES, including its Communication Infrastructure, as well as the technical specifications of the system and to develop the EES.

(6) In this framework, it is thus necessary to adopt specifications for the quality, resolution and use of fingerprints and facial image for biometric verification and identification in the Entry/Exit System (EES).

(7) This Decision is without prejudice to the application of Directive 2004/38/EC of the European Parliament and of the Council (2).

(8) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark did not take part in the adoption of Regulation (EU) 2017/2226 and is not bound by it or subject to its application. However, given that Regulation (EU) 2017/2226 builds upon the Schengen acquis, Denmark, in accordance with Article 4 of that Protocol, notified on 30 May 2018 its decision to implement Regulation (EU) 2017/2226 in its national law. Denmark is therefore bound under international law to implement this Decision.

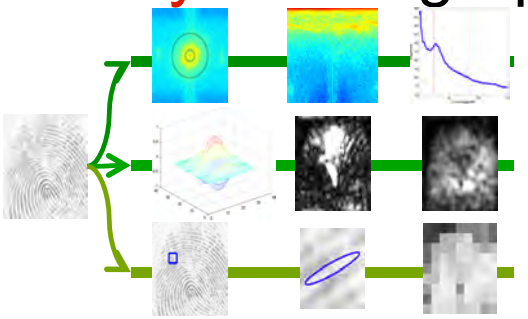
(1) OJ L 327, 9.12.2017, p. 20.

(2) Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (OJ L 158, 30.4.2004, p. 77).

Quality Metrics for Fingerprint Images

The NFIQ2.0 approach

- Measure quality by filtering the signal and determine the utility of a fingerprint sample.



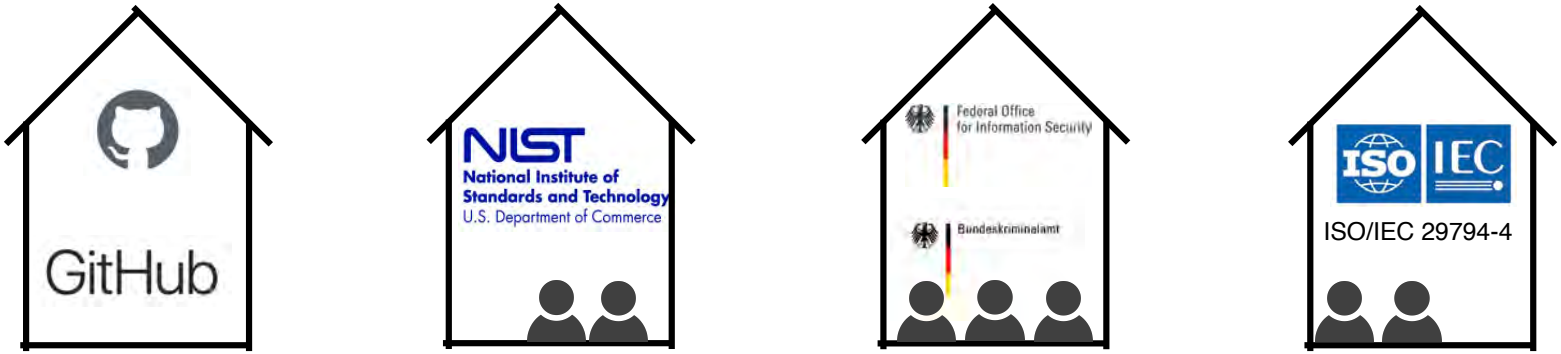
- Providing constructive feedback only possible if cause of poor quality is known.

- NFIQ2.0 constitutes the content of ISO/IEC 29794-4 https://www.iso.org/standard/62791.html

Quality Metrics for Fingerprint Images

How was NFIQ2.0 developed?

- 2010 - 2021



Maintenance | Testing | Development | Standardisation

- Status 2021
  - NFIQ2.1 in GitHub: https://github.com/usnistgov/NFIQ2
  - ISO/IEC 29794-4: https://www.iso.org/standard/62791.html
  - NFIQ IR 8382 published: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8382.pdf
  - NFIQ2.1 is for fingerprint samples from optical capture devices not for contactless !

Fingerprint Quality in Covid-19 Times

EES will need NFIQ2.1 for contactless capture devices

- Covid-19 will follow us for some more time
- contactless devices will be demanded (rather soon)
- a joint workshop on NFIQ2.1 discussed recently re-training / calibration for contactless capture devices
  - you can find presentations from the recent NFIQ 2.1 workshop at: https://eab.org/events/program/248
- a recent overview of contactless fingerprint recognition [Priesnitz2021] J. Priesnitz: „"An Overview of Touchless 2D Fingerprint Recognition", in EURASIP JIVP, (2021) https://jivp-eurasipjournals.springeropen.com/articles/10.1186/s13640-021-00548-4

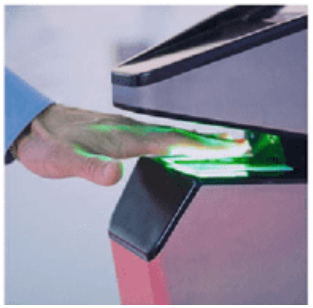


Image Source: https://www.semanticscholar.org/paper/Contactless-3D-Fingerprint-Identification-Kumar

Presentation Attack Detection

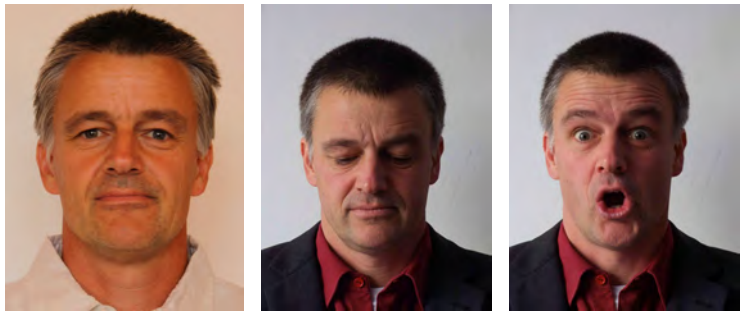
Presentation Attack Detection

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

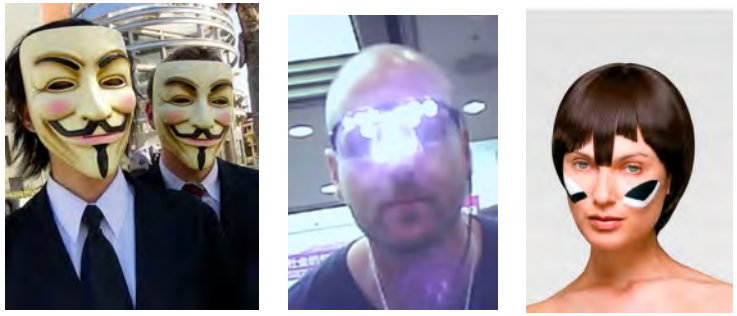


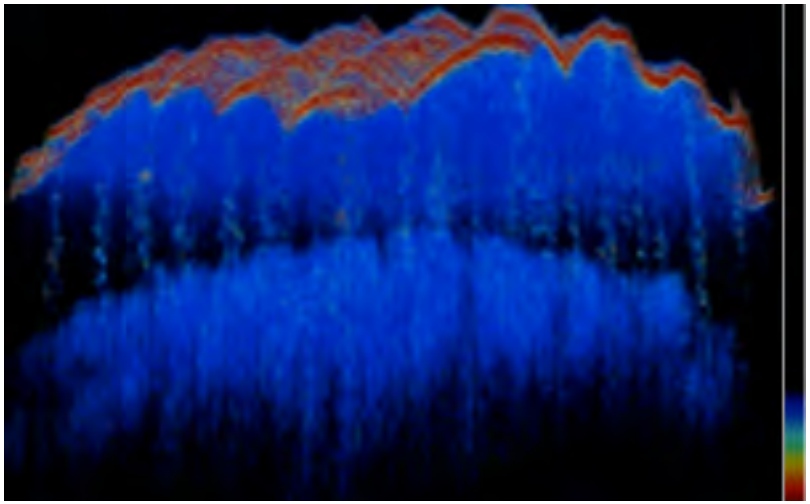
Image Source: https://www.youtube.com/watch?v=LRj8whKmN1M

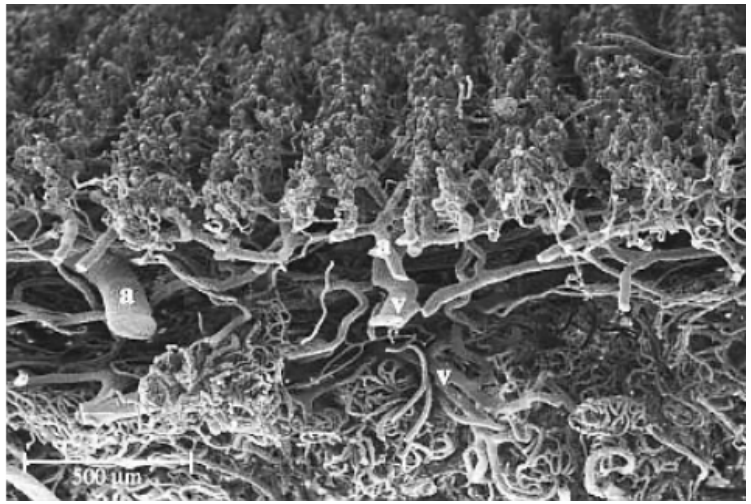
Image Source: https://cvdazzle.com

Fingerprint Capture Device Security

Countermeasures

- Observation of the live skin properties
  - Dermal-epidermal junction zone (inner fingerprint)
  - Observation of the sweat glandes and sweat ducts
- Sensors
  - Optical Coherence Tomography (OCT)

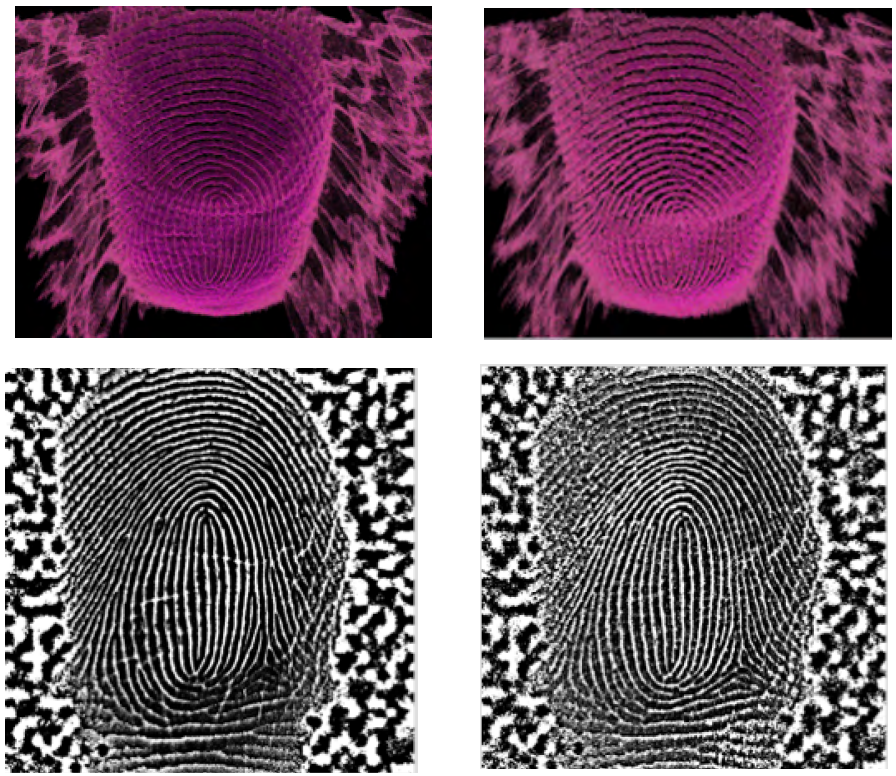




Fingerprint Capture Device Security

Comparing outer and inner fingerprint patterns

- Detection of surface and internal layer
- 2D projection

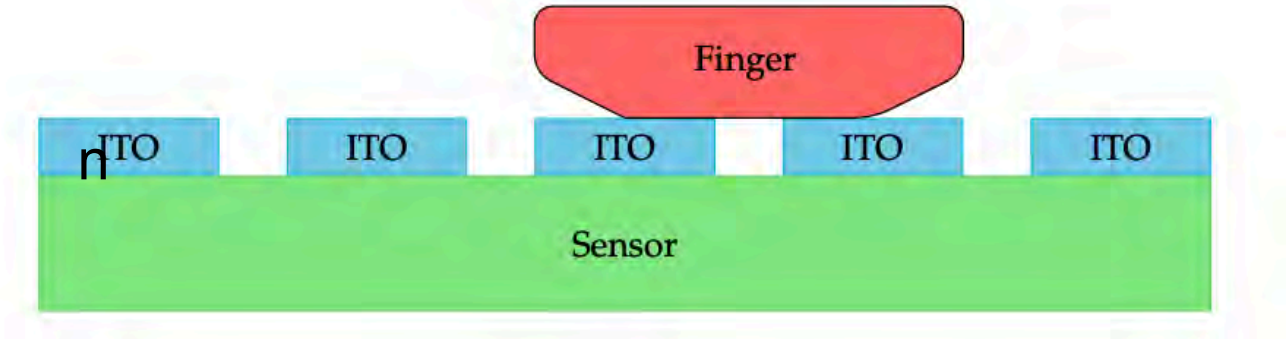


Surface Fingerprint Internal Fingerprint

Fingerprint Capture Device Security

Impedance based detection

- thin film transistor (TFT) technology
  - indium-tin-oxide (ITO) coating
- a finger connecting two conductors
  - the conductivity of human skin differs from artefacts



- Nine different frequencies in the range from 1 to 500 kHz are used for the impedance measurements.

	FQ_1	FQ_2	FQ_3	FQ_4	FQ_5	FQ_6	FQ_7	FQ_8	FQ_9
(Hz)	1000	2500	5000	10,000	25,000	50,000	100,000	250,000	500,000

[Kolberg2021] J. Kolberg, et al.: "On the Effectiveness of Impedance-based Fingerprint Presentation Attack Detection", in Sensors Journal, (2021)
https://www.mdpi.com/1424-8220/21/17/5686

Impostor Presentation Attack

3D silicone mask

http://edition.cnn.com/2010/WORLD/americas/11/04/canada.disguised.passenger

Face Capture Device - Skin Detection

Short Wave Infrared Range (SWIR) imaging

- With multiple point sensors proposed by Steiner et al.
- Skin types defined by Fitzpatrick [Fitzpatrick1988]
  - I - Always burn, never tan
  - II - Usually burn, tan less than average
  - III - Sometimes mild burn, tan about average
  - IV - Rarely burn, tan more than average
  - V - brown
  - VI - black

Image Source: HSBRS, (2016)

[Fitzpatrick1988] T. Fitzpatrick: „The validity and practicality of sun-reactive skintypes I through VI“, Archives of Dermatology, (1988)

Face Capture Device - Skin Detection

Short Wave Infrared Range (SWIR) imaging

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

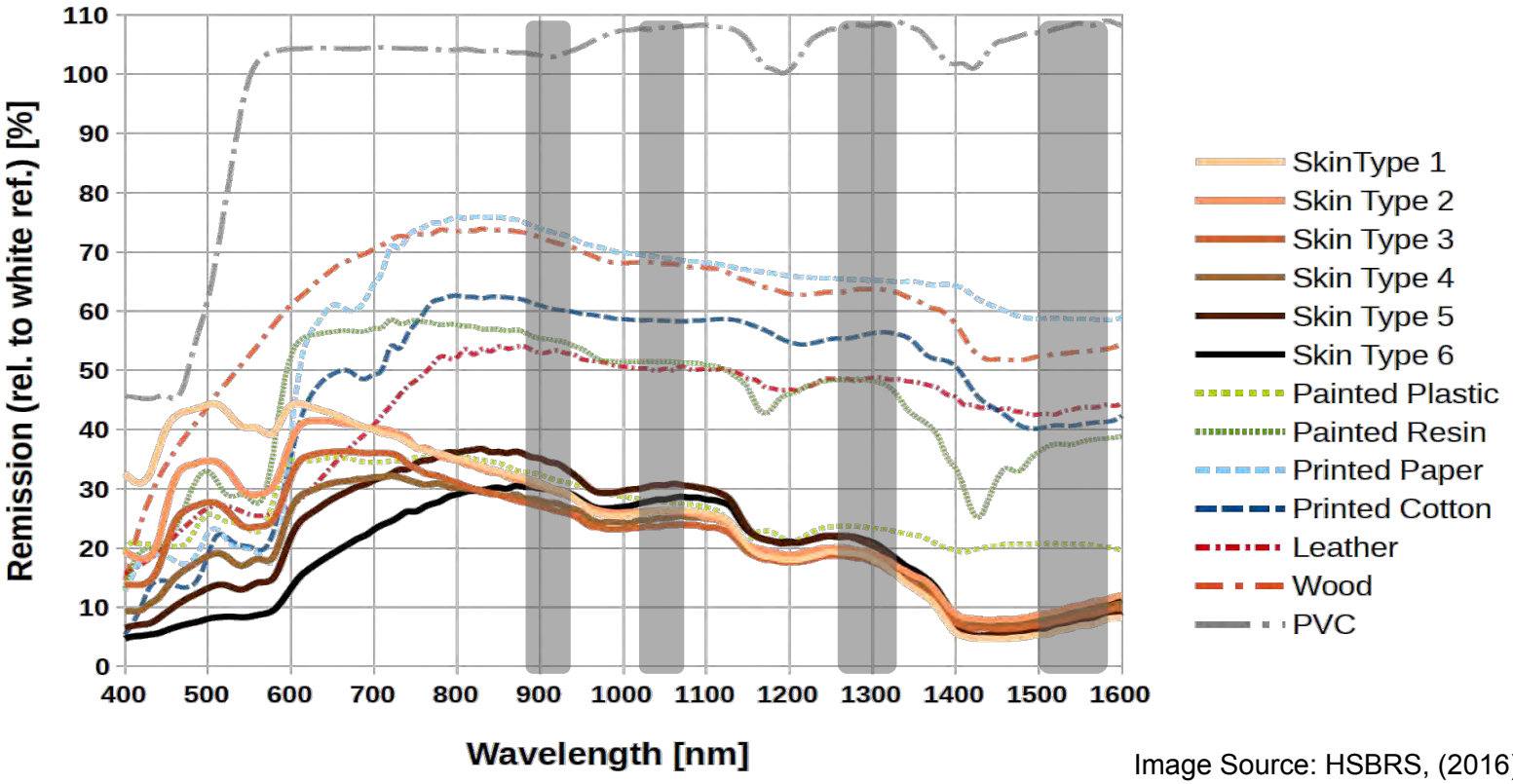


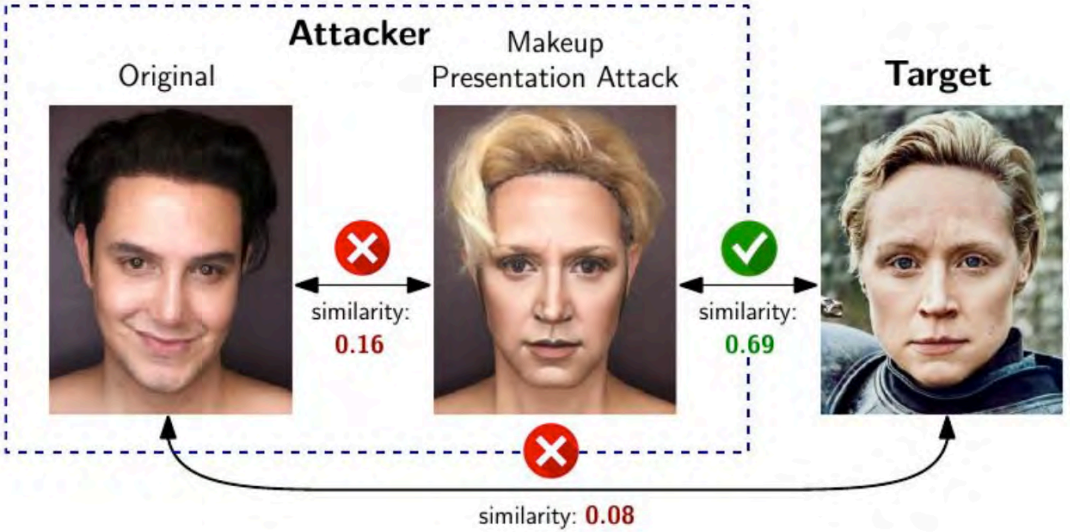
Image Source: HSBRS, (2016)

[Jacquez1955] J. Jacquez: „Spectral reflectance of human skin in the region 0.7-2.6m“,J. of Applied Physiology, (1955)

Face - Makeup Presentation Attacks

Severe alterations

- Makeup for impersonation
- Liveness detection is not sufficient
- Detection difficult since bona fide users may also apply



[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)

Morphing Attack Detection

What is Morphing?

In our real world morphing can become a threat

- with a criminal and an accomplice as actors
- take the criminal
- and the accomplice (or any other good EU citizen)
- morphing can transform one face image into the other

What is Morphing?

In our real world morphing can become a threat

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

Problem: Morphing Attacks

Morphing attack scenario

- Passport application of the accomplice A

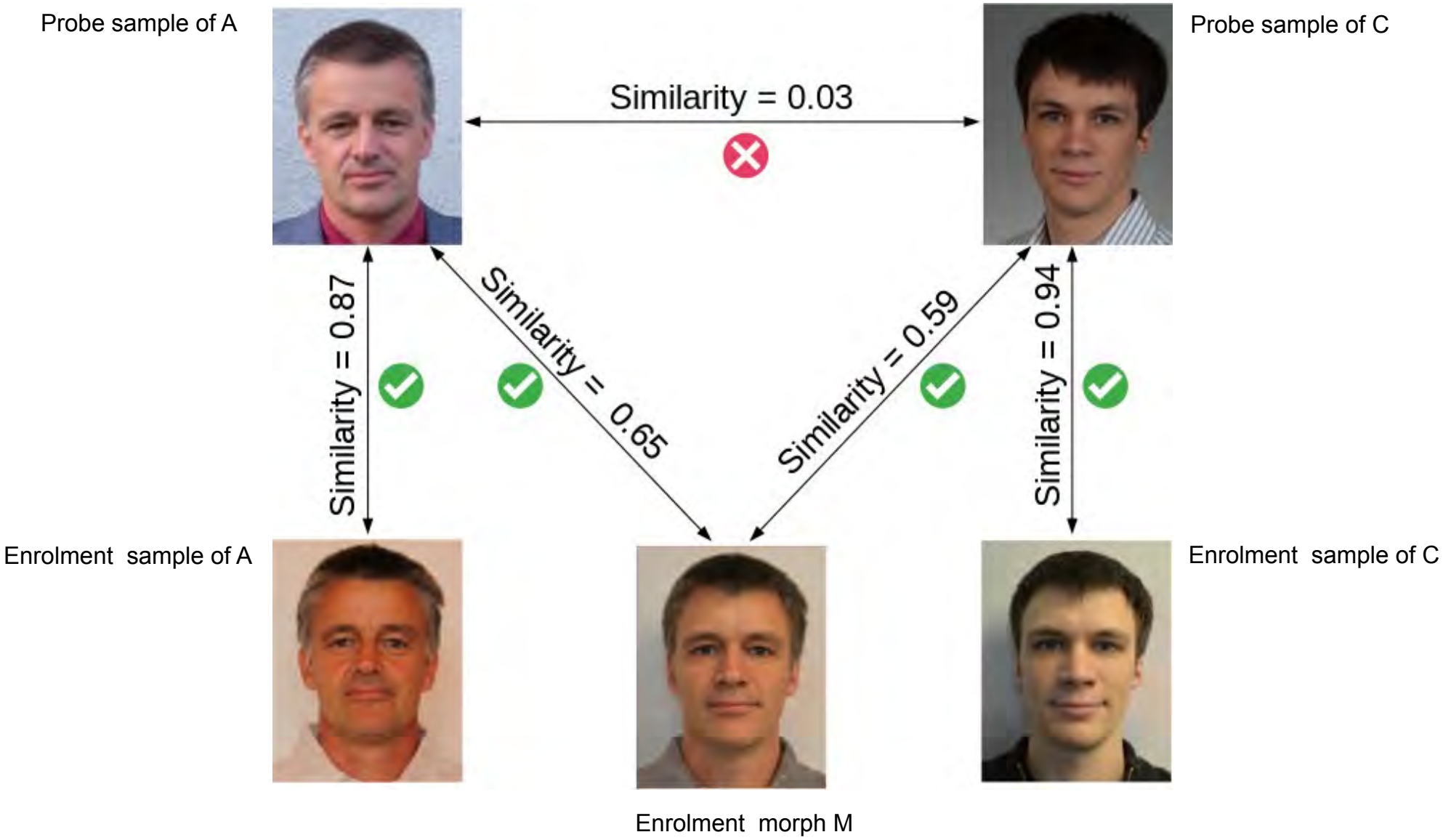
Problem: Morphing Attacks

Morphing attack scenario

- Border control

Problem: Morphing Attacks

Verification against morphed facial images



Problem: Morphing Attacks

Is it a really problem ?

Problem: Morphing Attacks

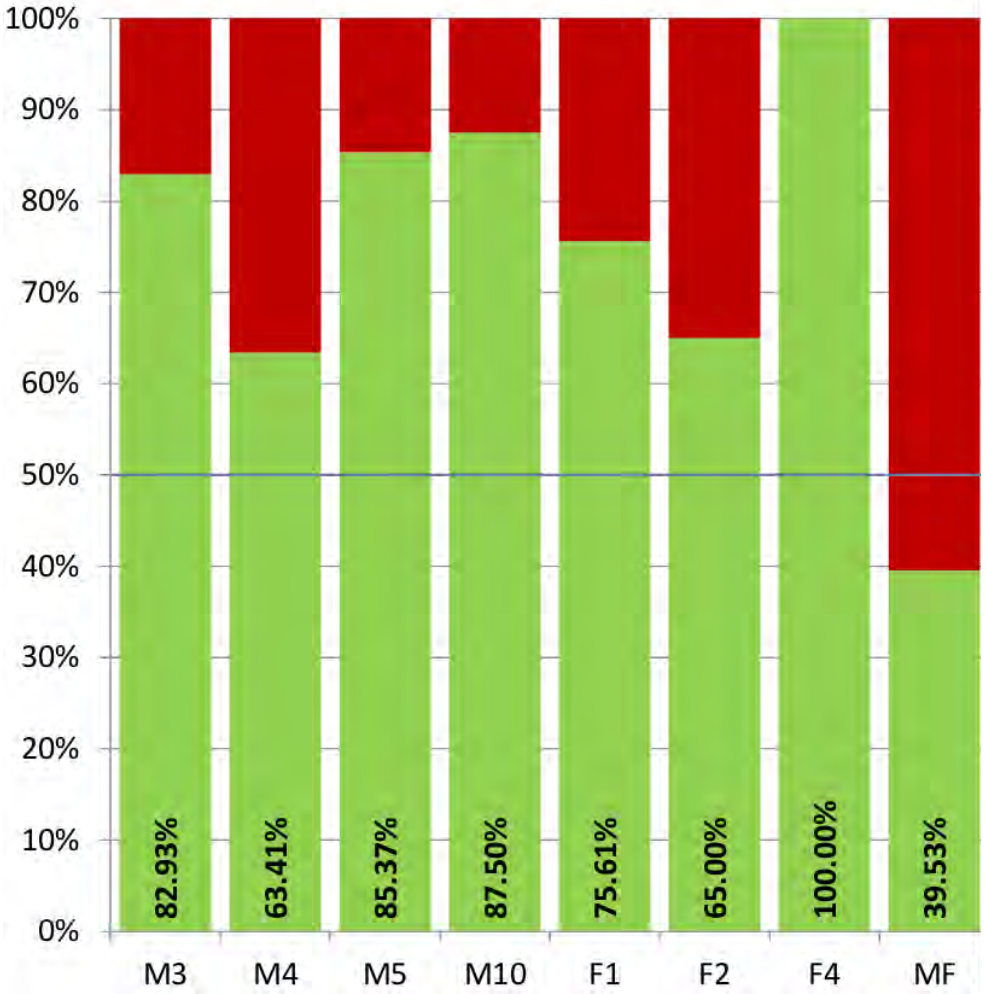
Is it a really problem ? - YES!

- 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

Scale of the Problem: Vulnerability

Human Experts Capabilities - (44 border guards)

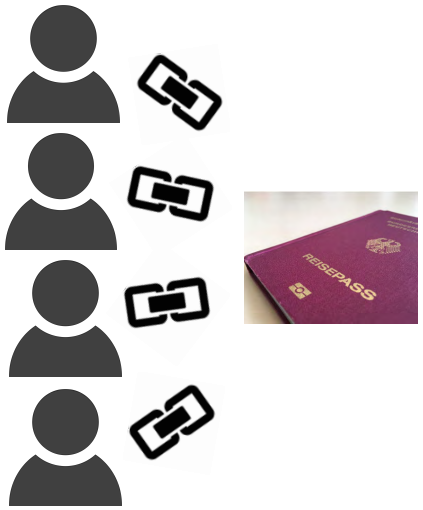


[FFM2016] M. Ferrara, A. Franco, D. Maltoni: “On the Effects of Image Alterations on Face Recognition Accuracy”, in Face Recognition Across the Imaging Spectrum, Springer Nature, (2016)

Morphing Attack - Impact

Countermeasures

- The current procedure, where a printed face photo can be provided by the citizen, poses serious security risks
  - ID-document based on printed photos are no longer providing a unique link



- Solutions
  - Photo studio should digitally sign the picture and send it to the passport application office (this is in progress for Finland)
  - Switch to live enrolment (that is the case for Norway and Sweden)
  - Software-supported detection of morphed face images at enrolment and at ID-document control

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

MAD Evaluation

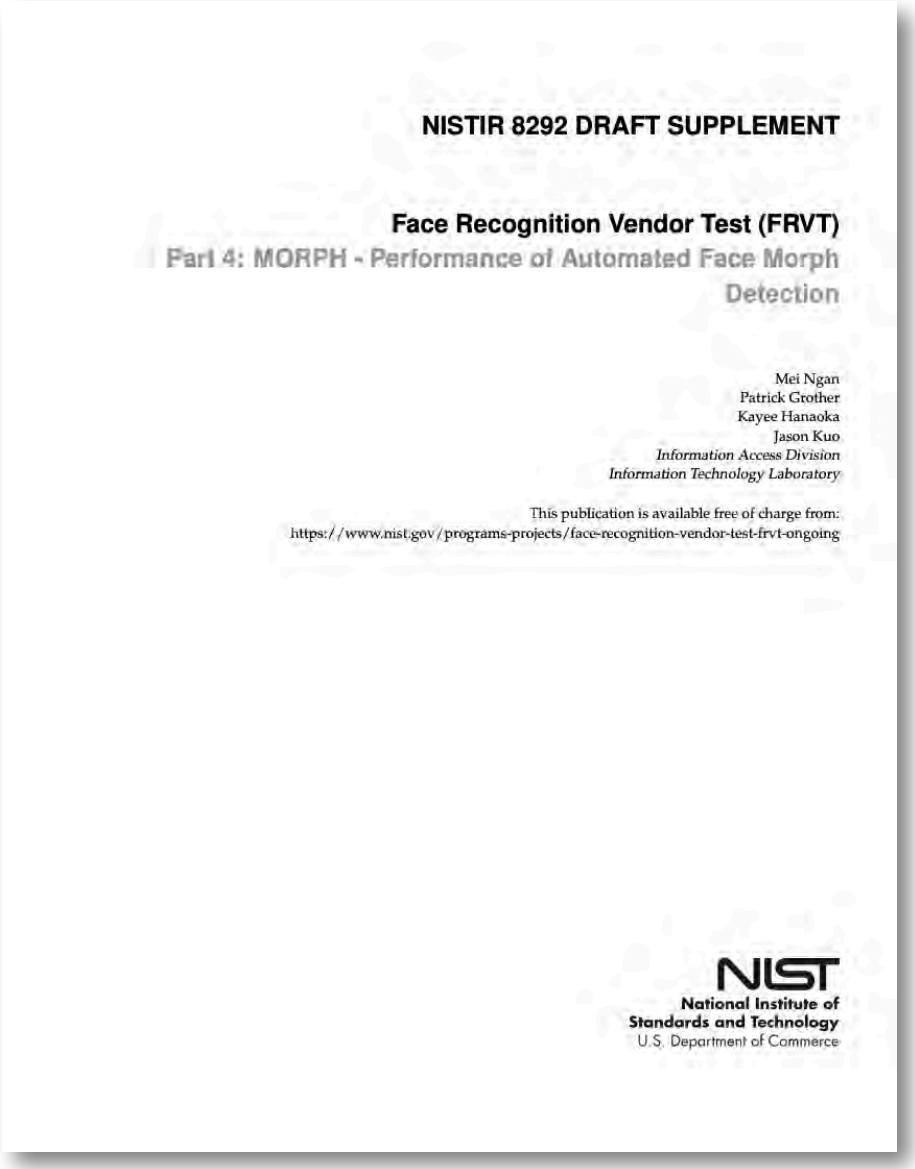
NIST-FRVT-MORPH

NIST IR 8292 report presented September, 2021

FRVT-MORPH

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

- results for MAD algorithms from four research labs:
  - Hochschule Darmstadt (HDA)
  - Norwegian University of Science and Technology (NTNU)
  - University of Bologna (UBO)
  - University of Twente (UTW)



NISTIR 8292 DRAFT SUPPLEMENT

Face Recognition Vendor Test (FRVT)
Part 4: MORPH - Performance of Automated Face Morph Detection

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

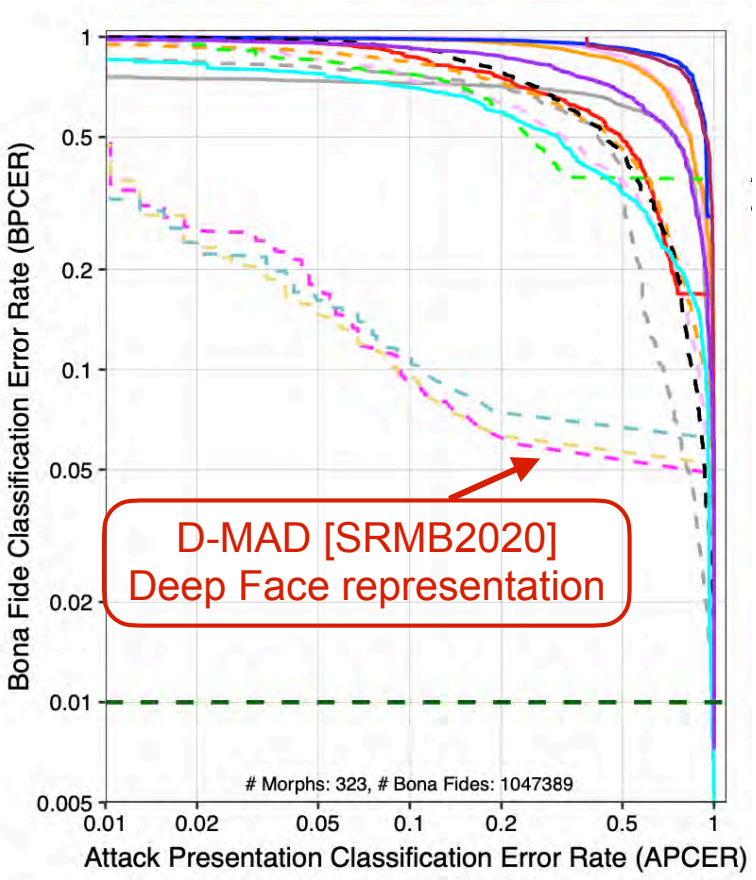
This publication is available free of charge from:
https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

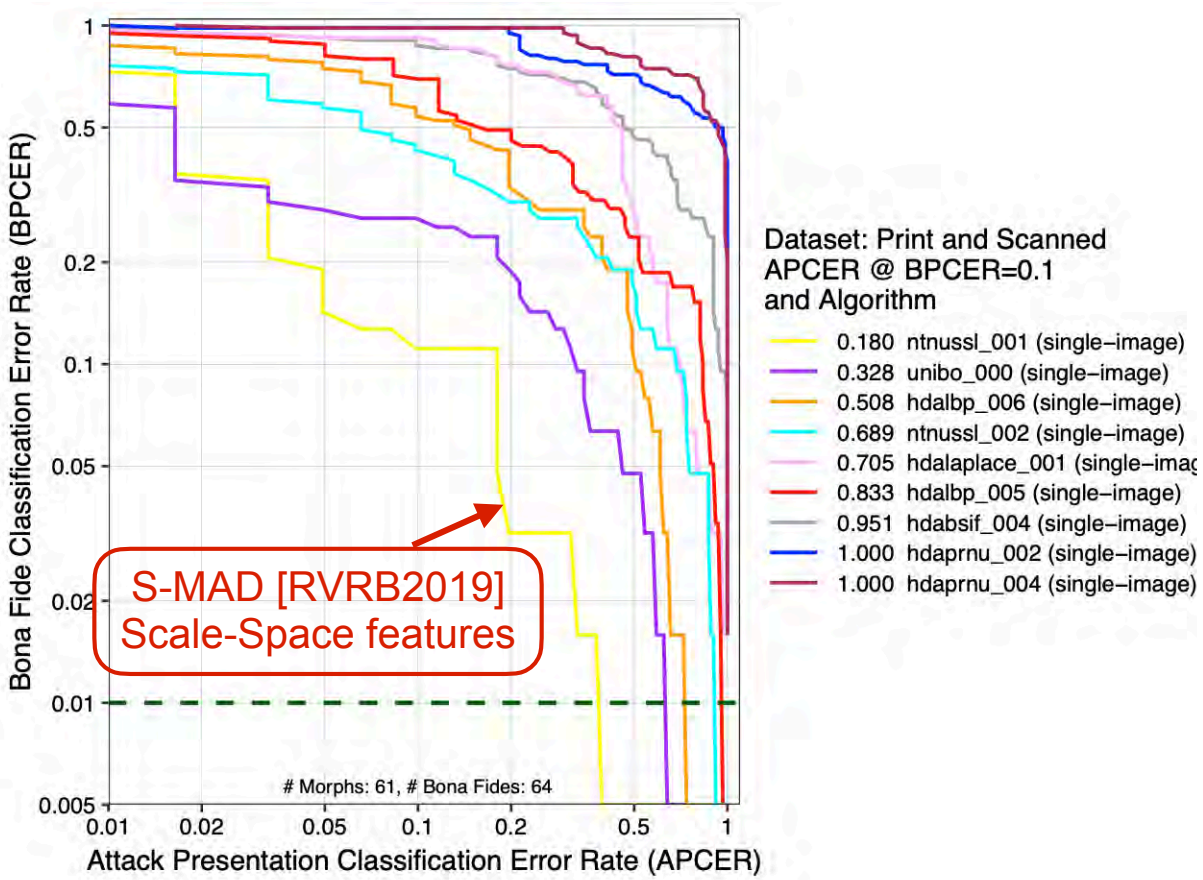
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST-FRVT-MORPH

NIST IR 8292 report presented April, 2021

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





More information

The MAD website

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

The MAD survey papers

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


IEEE Access

Face Recognition Systems Under Morphing Attacks: A Survey

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

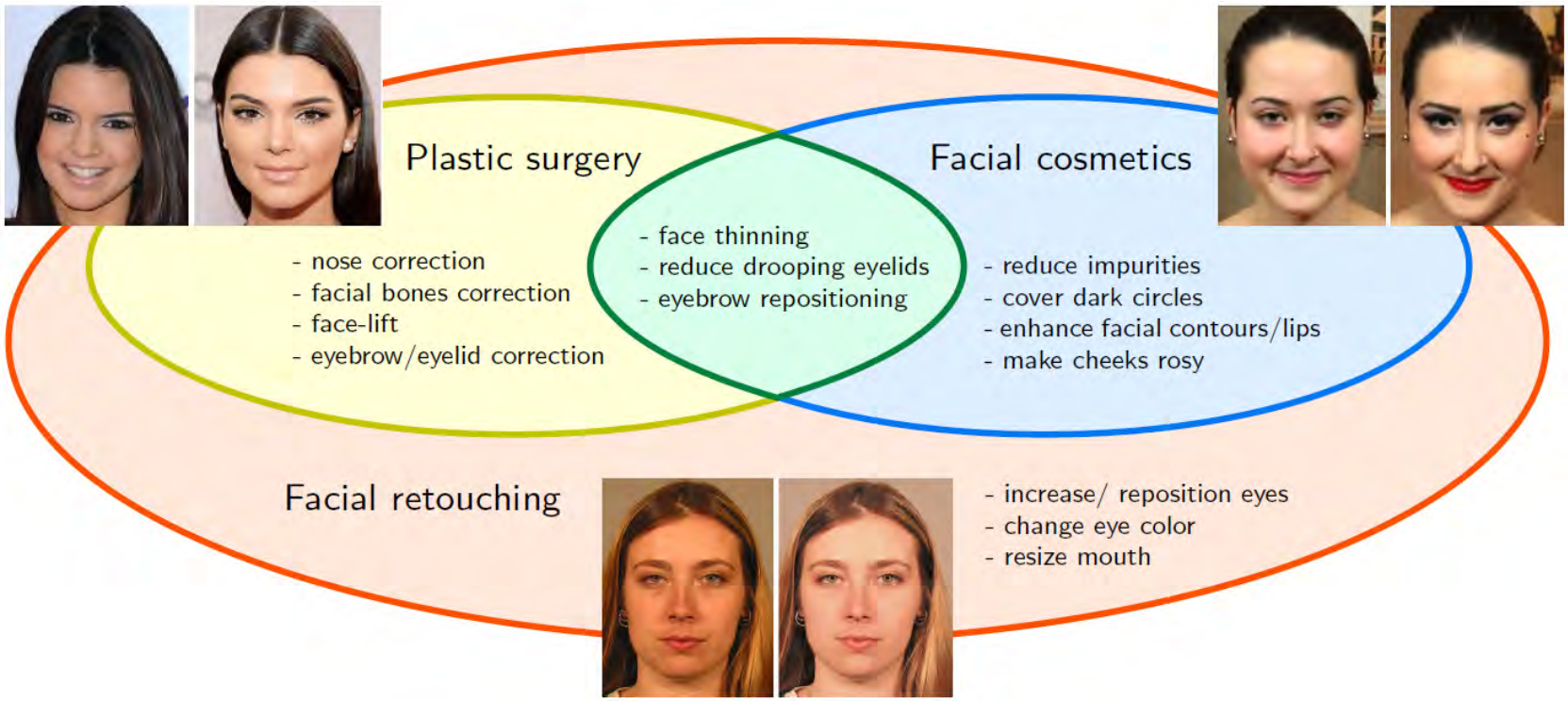

Face Morphing Attack Generation & Detection: A Comprehensive Survey

Non-Intentional Attacks - Beautification

Beautification of Facial Images

Scenario

- either the reference or the probe image has been altered



[Rathgeb2019] C. Rathgeb, A. Dantcheva, C. Busch: „Impact and Detection of Facial Beautification in Face Recognition: An Overview“, in IEEE Access, 7(1), (2019)
https://ieeexplore.ieee.org/document/8877744

Beautification of Facial Images

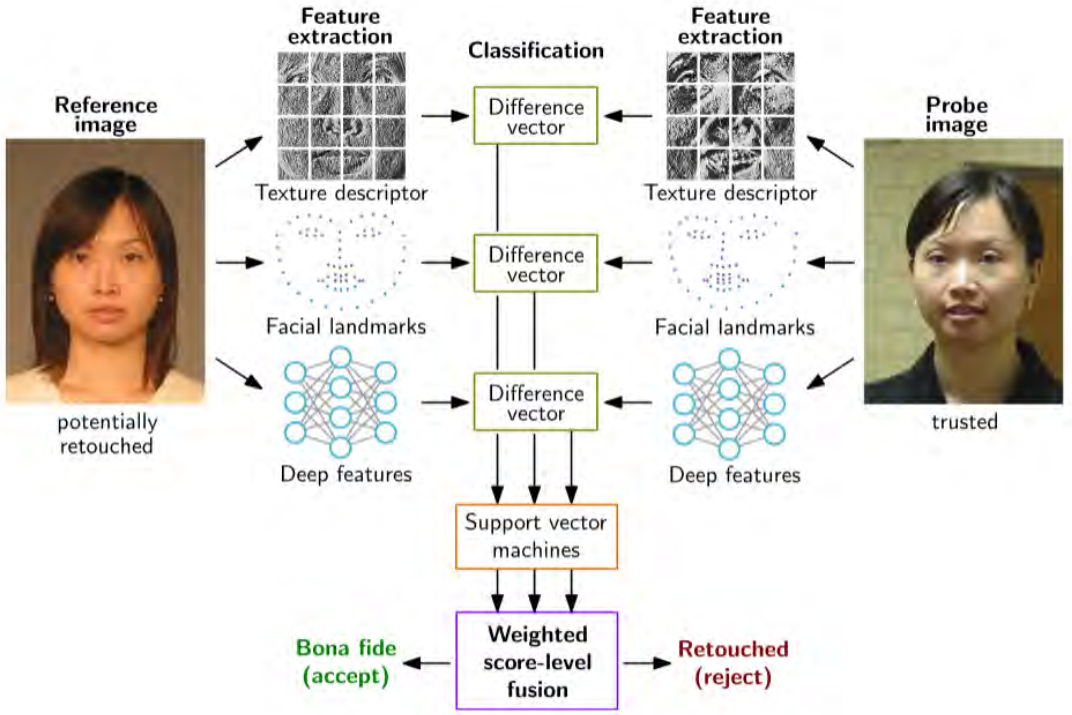
Retouching

- users may apply retouching with easy-to-use apps
- common alterations:
  - smoothing skin
  - slimming nose
  - enlarging eyes

Beautification of Facial Images

Retouching detection

- detection of retouching in differential scenario (similar to MAD)
- potential features
  - texture descriptors
  - facial landmarks
  - deep features
- results reported as D-EER
  - ~1.5% for known and
  - ~10% for unknown retouching algorithms
  - 6 apps
  - 9000 retouched facial images



[Rathgeb2020] C. Rathgeb, C. Satnoianu, N. Haryanto, K.Bernardo, C. Busch: „Differential Detection of Facial Retouching: A Multi-Biometric Approach“, in IEEE Access, (2020)
https://ieeexplore.ieee.org/document/9109348

Further Challenges

Quality Metrics for Facial Images

Standard ISO/IEC 29794-5 to be aligned with both

- ISO/IEC 19794-5:2011
- ISO/IEC 39794-5:2019

Definitions

- 6.2 Unified quality score
  FaceQnet (JRC)
- 6.3 Capture-related
  quality elements
- 6.4. Subject-related
  quality elements

a) Compliant image **b) Low contrast**

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

images with +8 degrees (left) and -8 degrees (right) rotation in roll

Image Source: ISO/IEC 19794-5:2011

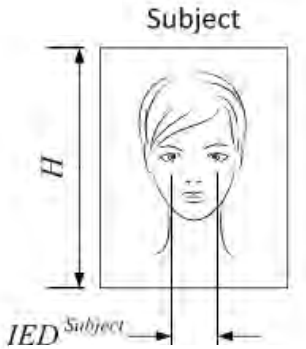


Image Source: ISO/IEC 39794-5

Quality Metrics for Facial Images

ISO/IEC 3rd WD 29794-5 to be aligned with both

- ISO/IEC 19794-5:2011
- ISO/IEC 39794-5:2019

Table 2 - Conformance requirements by activity

#	Image quality aspect	Collection of reference samples for ID credentials	Collection of probe for instantaneous verification	Enrolment for other enrolment, delayed verification, probe later used as enrolment
1	Unified quality score	6.2	6.2	6.2
2	Illumination uniformity	6.3	6.3 optional	6.3 optional
3	Illumination mean	6.3.3.2	6.3.3.2 optional	6.3.3.2 optional
4	Illumination variance	6.3.3.3	6.3.3.3 optional	6.3.3.3 optional
5	Illumination skewness	6.3.3.4	6.3.3.4 optional	6.3.3.4 optional
6	Illumination kurtsosis	6.3.3.5	6.3.3.5 optional	6.3.3.5 optional
7	Illumination under-exposure	6.3.3	6.3.3 optional	6.3.3 optional
8	Illumination over-exposure	6.3.5	6.3.5 optional	6.3.5 optional
9	Dynamic Range	6.3.6	6.3.6 optional	6.3.6 optional
10	De-focus	6.3.7	6.3.7 optional	6.3.7 optional
11	Image sharpness	6.3.8	6.3.8 optional	6.3.8 optional
12	Motion blur	6.3.9	6.3.9 optional	6.3.9 optional
13	Edge Density	6.3.10	6.3.10 optional	6.3.10 optional
14	Compression	6.3.11		
15	Unnatural colour and colour balance	6.3.12	6.3.12 optional	6.3.12 optional
16	Eyes visible	6.4	6.4 optional	6.4
17	~~Number of faces present~~		mandatory	Even more mandatory
18	Inter-eye distance	6.4.3	6.4.3	6.4.3
19	Horizontal position of the face	6.4.4	6.4.4	6.4.4
20	Vertical position of the face	6.4.5	6.4.5	6.4.5
21	Background uniformity	6.4.6		
22	Pose	6.4.7	6.4.7 optional	6.4.7
23	Expression neutrality	6.4.8	6.4.8 optional	6.4.8 optional
24	Mouth closed	6.4.9	6.4.9 optional	6.4.9
25	Eyes open	6.4.10	6.4.10 optional	6.4.10 optional
26	Developer-defined quality score computation	8 and Annex A	8 and Annex A	8 and Annex A

source: ISO/IEC 3rdWD 29794-5, Table 2
https://www.iso.org/standard/81005.html

a) Compliant image **b) Low contrast**

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

images with +8 degrees (left) and -8 degrees (right) rotation in roll

Image Source: ISO/IEC 19794-5:2011

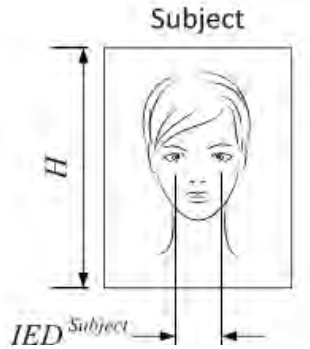


Image Source: ISO/IEC 39794-5

Quality Metrics for Facial Images

How to develop face quality metrics? - Standardisation

- 2021 - 2024

Patrick Grother
Mei Ngan

Christoph Busch
Patrick Grother

- NIST FRVT Quality Assessment
  https://pages.nist.gov/frvt/html/frvt_quality.html
- workshop on face quality assessment
  https://eab.org/events/program/261

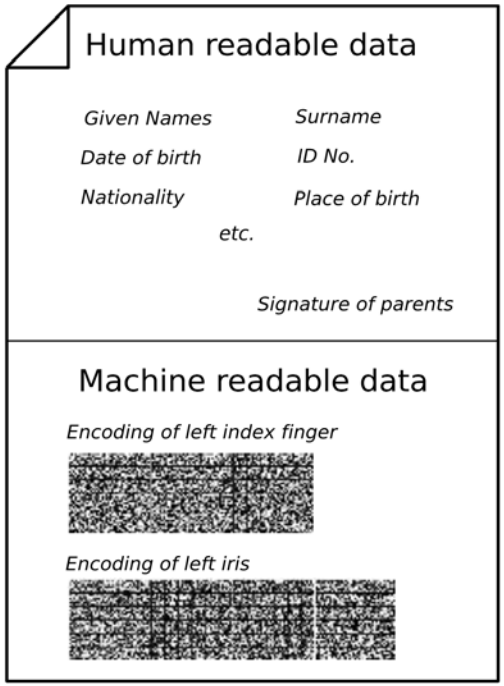
Save the date:
November 16th to18th

- Join the SC37 WG3 work!
  https://www.iso.org/members.html

External Borders - Need

Standardised birth certificates (long term benefit)

- definition of an ISO/IEC standard for birth certificates
  - and the registration of such certificates by a global institution (i.e., United Nations)
  - biometric link to a persistent biometric characteristic which does not change over the live time of a human



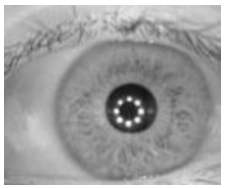


Image source: FIDELITY, FVC04, CASIAv3

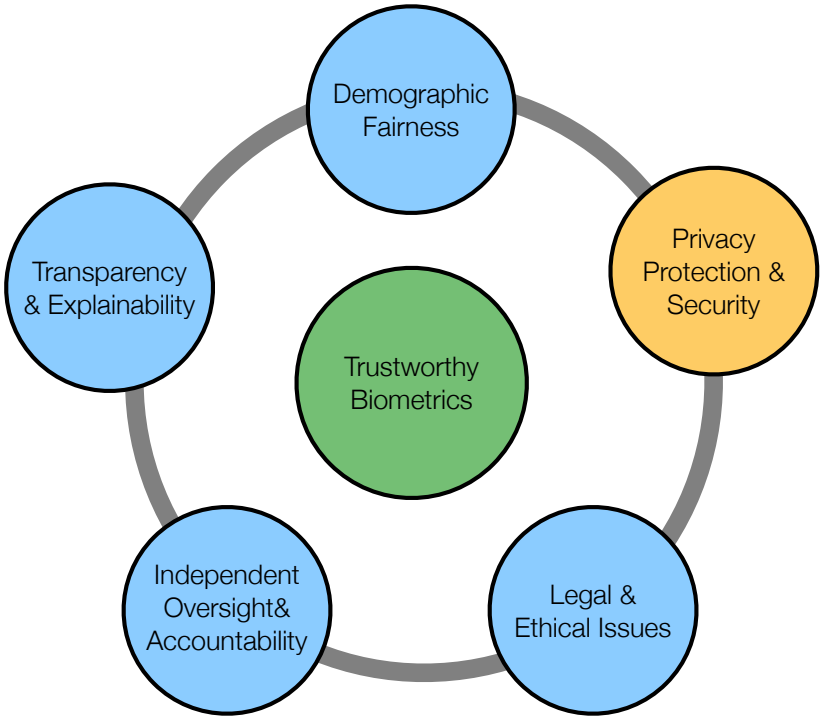
Trustworthy Biometrics

Acceptance of technology

- technology itself often considered as threat

Increase trust in technology can be achieved by

- security and privacy by design
- public consultations and information campaigns
- and other factors …



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