EUROPEAN UNIVERSITY OF TECHNOLOGY

Technical University Sofia
Cyprus University of Technology
utt Université de Technologie Troyes
h_da hochschule darmstadt
TU Dublin
University of Cassino and Southern Lazio
Riga Technical University
Universitatea Tehnică din Cluj-Napoca
Universidad Politécnica de Cartagena

EUROPEAN UNIVERSITIES
Erasmus+

Co-funded by
the European Union

EUT+ TECH SHOWCASE DAY

Cybersecurity: Scenarios and Services for Companies

CASSINO, 2/10/2024

ORGANIZED BY

Università degli Studi di Cassino e del Lazio Meridionale – 1979 – SOL PER NOCTEM

CAMERA DI COMMERCIO
FROSINONE LATINA

AZIENDA SPECIALE
CAMERA DI COMMERCIO FR - LT
informare
internazionalizzazione formazione economia del mare

EUROPEAN
VALUES
EMPOWERING
TECHNOLOGY

EUROPEAN UNIVERSITY OF TECHNOLOGY

EUROPEAN UNIVERSITIES

Erasmus+

Co-funded by
the European Union

DARMSTADT, GERMANY

Hochschule Darmstadt

EUROPEAN VALUES
EMPOWERING TECHNOLOGY

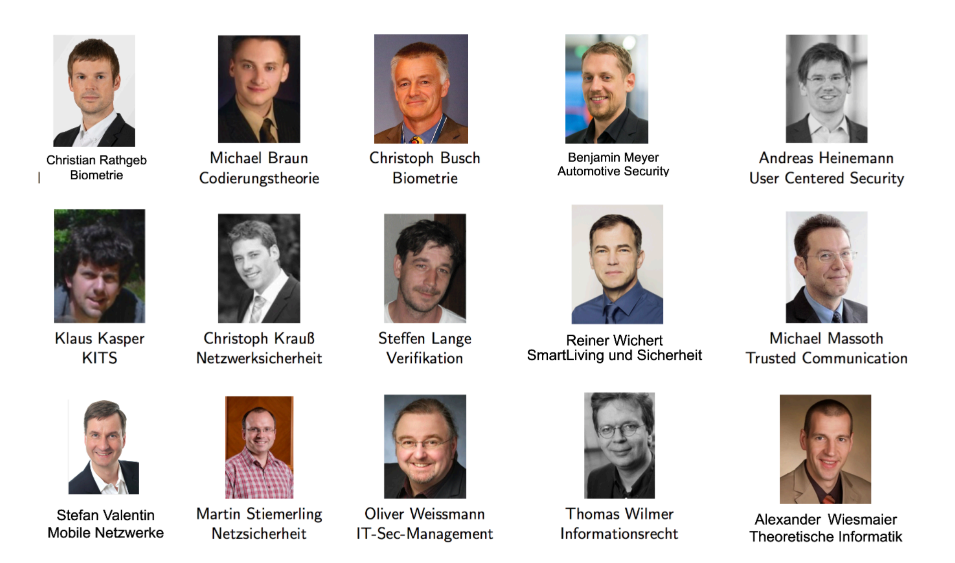
Hochschule Darmstadt

Short description

General description

- Hochschule Darmstadt (HDA) emerged as an industry needs oriented research educational institution in 1971
- Student body of about 17,000 - one of the largest and most distinguished universities of applied sciences in Germany.
- The Faculty of Computer Science has about 2,000 students. Over 40 professors and 20 lab engineers.

Main research group/people working in the Cybersecurity related fields



Research group da/sec (Busch/Rathgeb):
https://dasec.h-da.de/

Research group ACSD (Krauss/Wiesmaier)
https://fbi.h-da.de/index.php?id=1065

Research group USD (Heinemann/Lange)
https://ucs.h-da.io/

Research group Networks (Stiemerling)
https://fbi.h-da.de/personen/martin-stiemerling

Hochschule Darmstadt

Research & Tech Expertise

Main research activities

Biometrics, User Centered Security, Applied cryptography, post-quantum cryptography, design and formal security analyses of protocols, long-term security

Main technical expertise

Signal Processing, Deep Learning, Usability Testing, Automotive Security, Network Security, Embedded Systems

National and international network/partners

German Federal Office for Information Security, U.S. NIST, Federal Criminal Police, eu-LISA, Hessian Police, Idemia, HIG Global, Bundesdruckerei

Volkswagen AG, BMW, Infineon, NXP, Continental, Deutsche Telekom, Deutsche Post, MTG AG, Bosch, ZF, Denso, Allianz, Schaeffler Group

FU Berlin, TU Eindhoven, KU Leuven, NTU Singapore, TU Luxembourg, Academia Sinica Taiwan, Fraunhofer Society, Max Planck Institute, TU Darmstadt

IT-Security in Darmstadt

National Research Center for Applied Cybersecurity (ATHENE)

- 400+ scientist from 47+ countries

TECHNISCHE UNIVERSITÄT DARMSTADT

CYSEC research group at TU Darmstadt

CYSEC Cybersecurity TU Darmstadt

Fraunhofer SIT

Fraunhofer Institute for Secure Information Technology SIT

Fraunhofer IGD

Fraunhofer Institute for Computer Graphics Research IGD

h_da HOCHSCHULE DARMSTADT UNIVERSITY OF APPLIED SCIENCES

da/sec research group at Hochschule Darmstadt

da/sec BIOMETRICS AND INTERNET-SECURITY RESEARCH GROUP

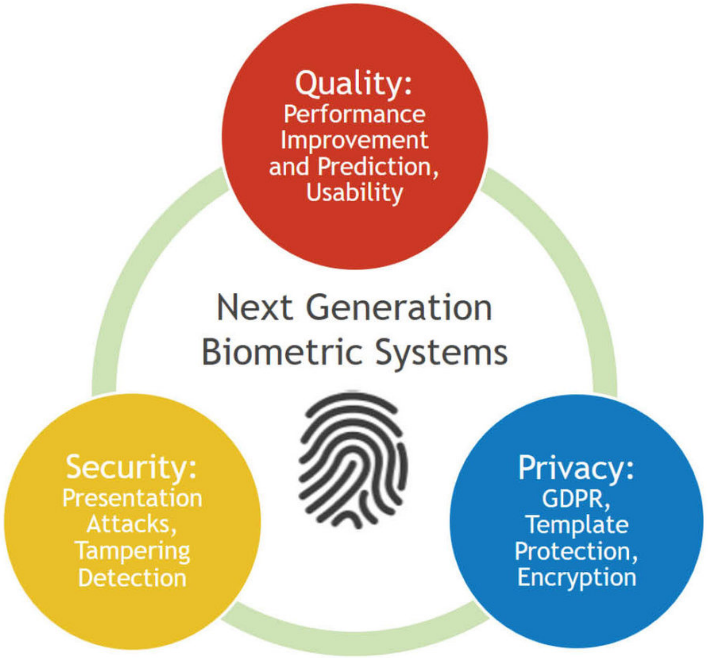
GOETHE UNIVERSITÄT FRANKFURT AM MAIN

GU Frankfurt

IT-Security in Darmstadt

National Research Center for Applied Cybersecurity (ATHENE)

- 25 scientist from Hochschule Darmstadt and Fraunhofer IGD



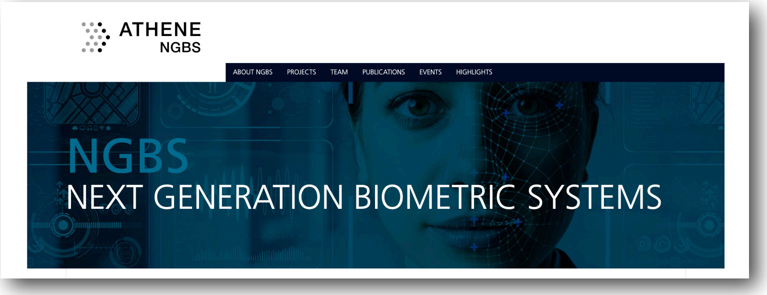
Quality:
Performance Improvement and Prediction, Usability

Next Generation Biometric Systems

Security:
Presentation Attacks, Tampering Detection

Privacy:
GDPR, Template Protection, Encryption

https://ngbs.athene-center.de/



ATHENE NGBS

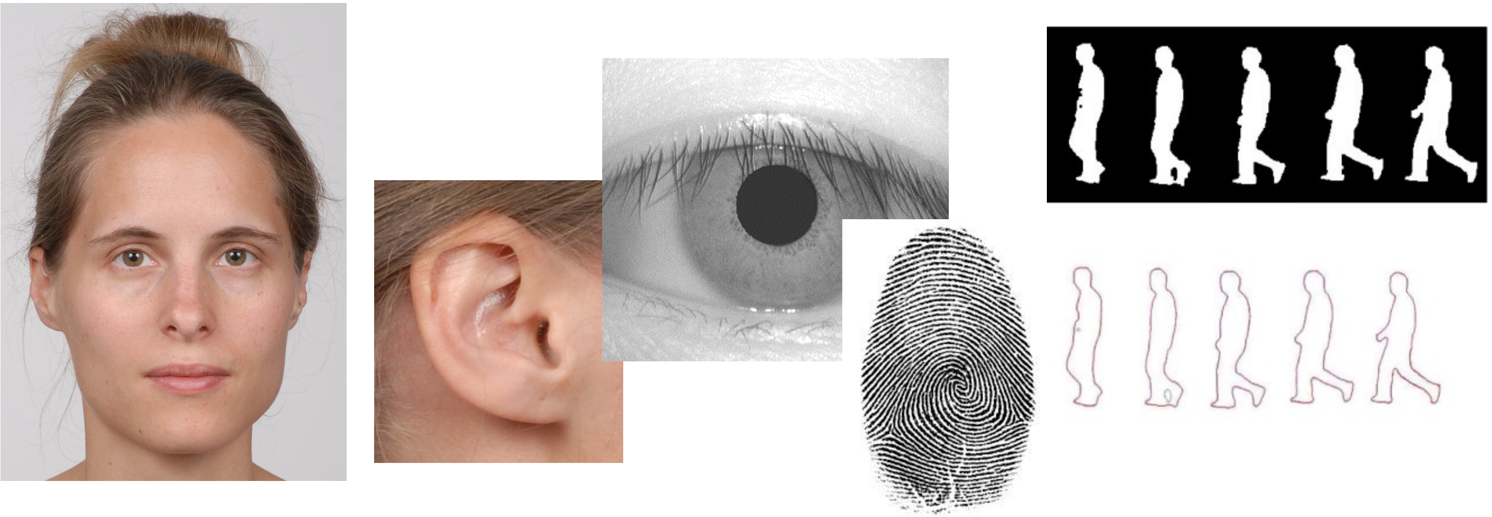
NGBS

NEXT GENERATION BIOMETRIC SYSTEMS

Research Area Biometrics

What is biometrics?

- International Organization for Standardization defines:
  - **Biometrics**:
    "*automated recognition of individuals based on their behavioural and biological characteristics* "
  - Remark: behavioural has to do with the function of the body
    biological / anatomical has to do with the structure of the body

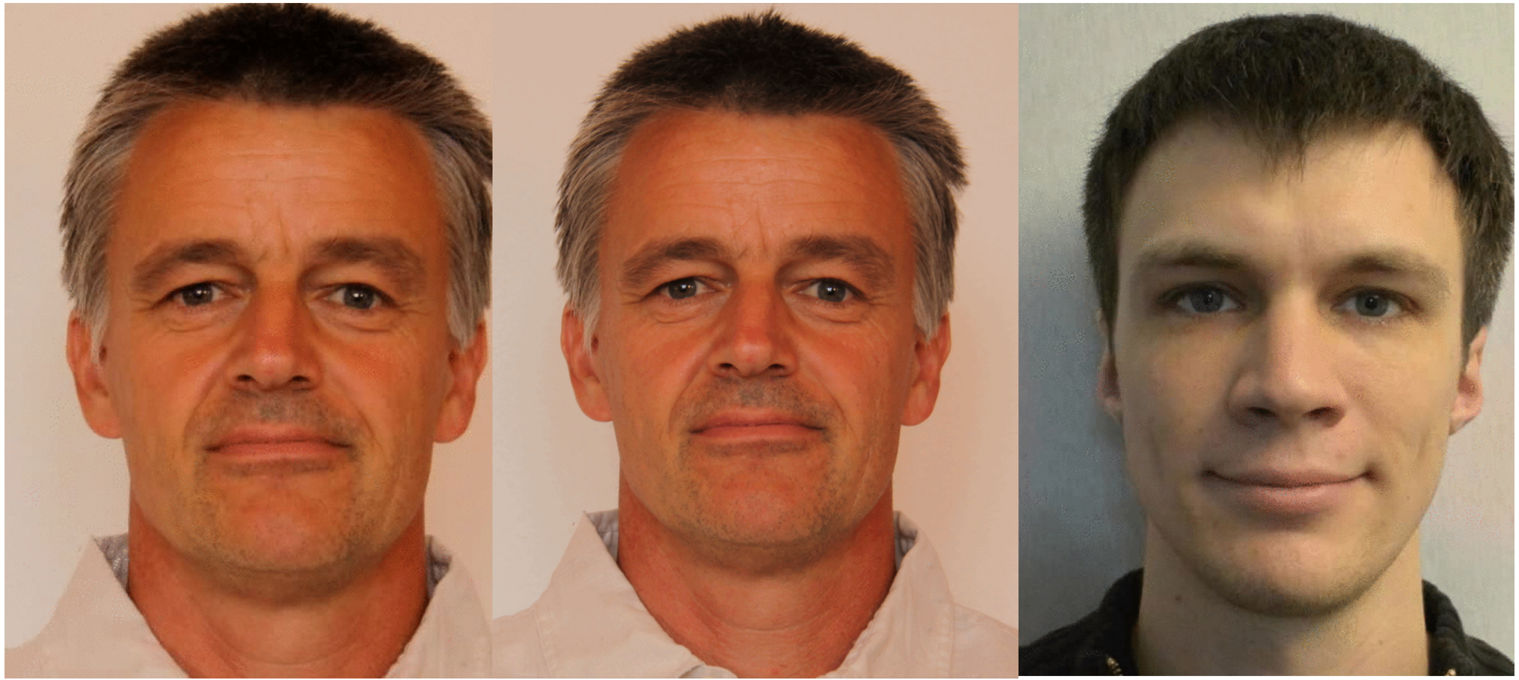


Application Oriented Research

Morphing Attack Detection

Morphing of face image can be exploit
for a passport enrolment attack

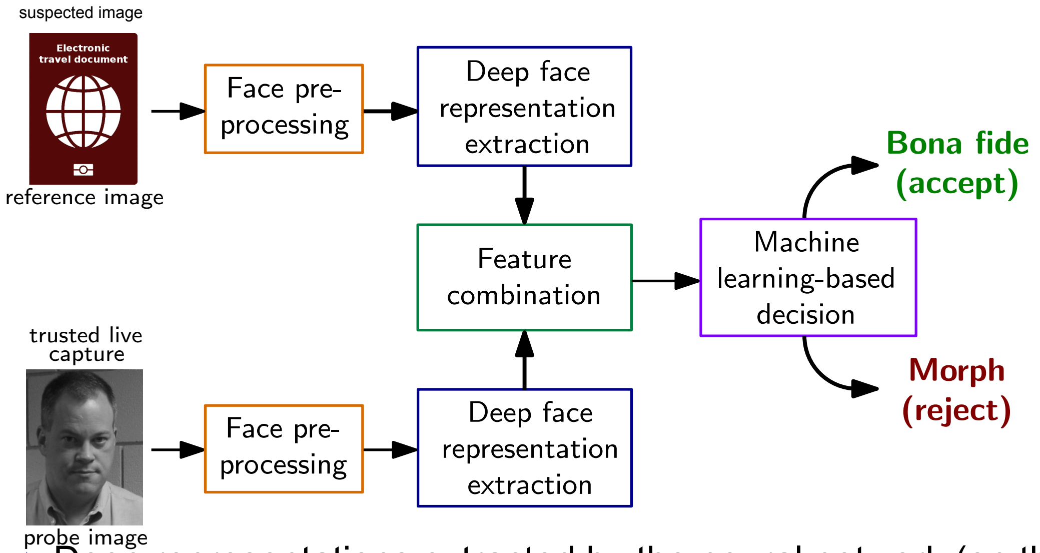
- morphing can transform one face image into the other
- and you can stop half way in the transformation



Morphing Attack Detection (MAD)

Differential method (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 / MagFace)
  - 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)

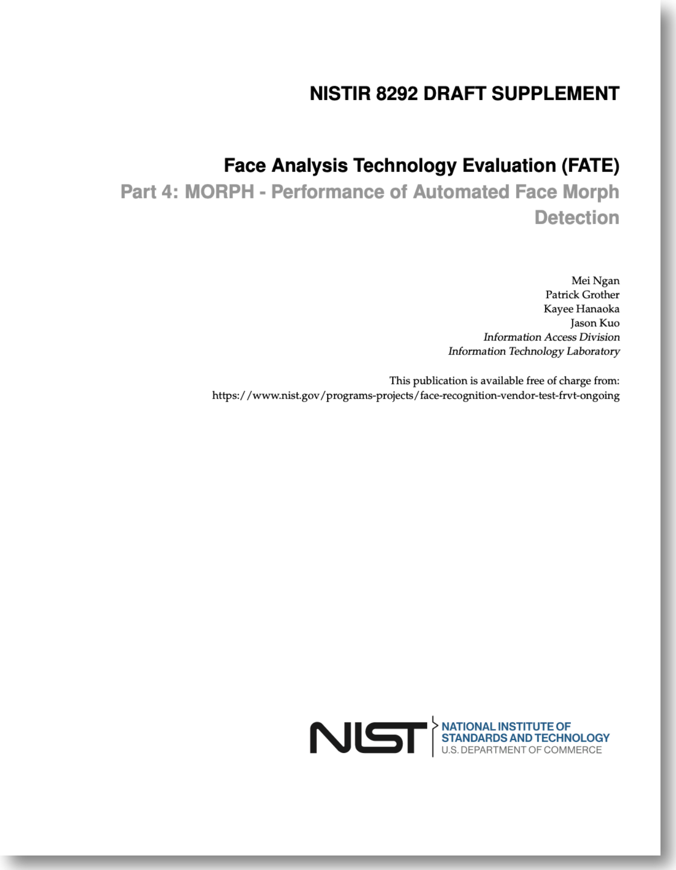
NIST-FATE-MORPH

NIST IR 8292 report presented June, 2024

FATE-MORPH since 2019

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

- Results for MAD algorithms from eleven research labs:
  - University of Bologna (UBO)
  - Norwegian University of Science and Technology (NTNU)
  - Hochschule Darmstadt (HDA)
  - West Virginia University (WVU)
  - Universidade de Coimbra (VIS)
  - Kempelen Institute of Intelligent Technologies
  - Fraunhofer (HHI)
  - Idemia (IDM)
  - secunet (SEC)
  - Neurotechnology (NET)
  - Vision Box (VIS)



NISTIR 8292 DRAFT SUPPLEMENT

Face Analysis Technology Evaluation (FATE)

Part 4: MORPH - Performance of Automated Face Morph Detection

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

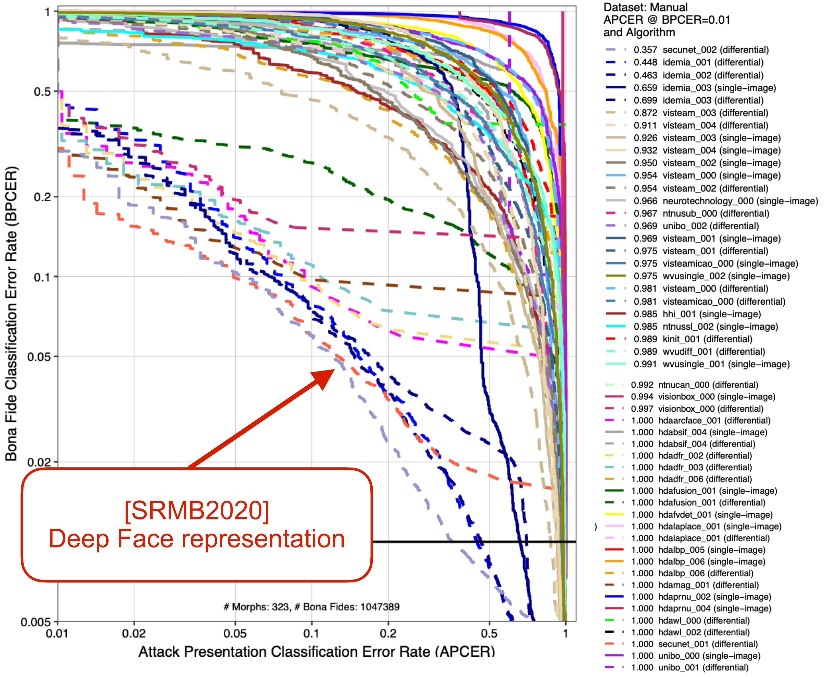
This publication is available free of charge from:
https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

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

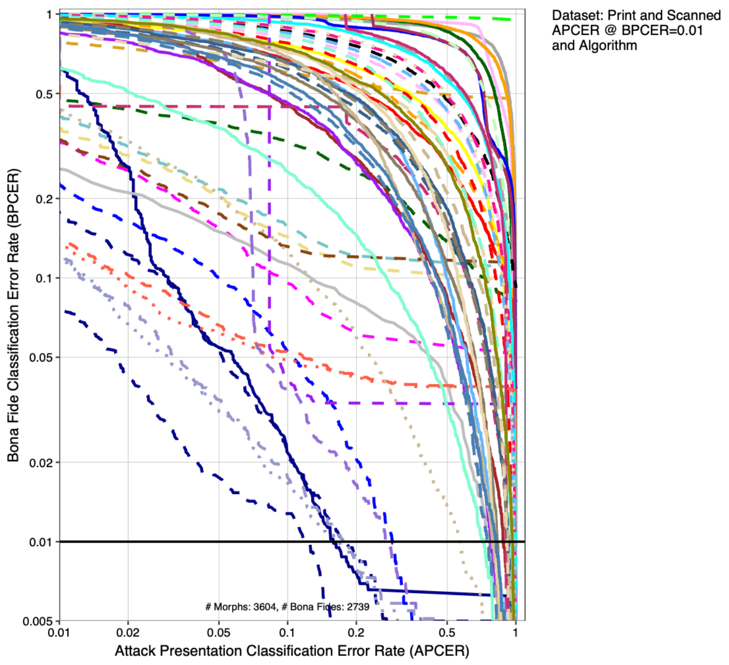
NIST-FATE-MORPH

NIST IR 8292 report presented June, 2024

- 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



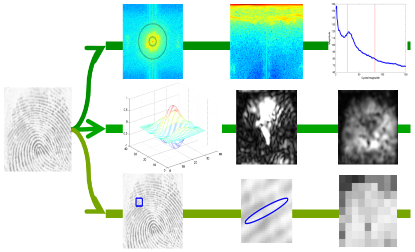
[SRMB2020]
Deep Face representation



Fingerprint Image Quality Assessment

NFIQ2.0

- Performance improvements can be achieved by improving data quality of biometric references.



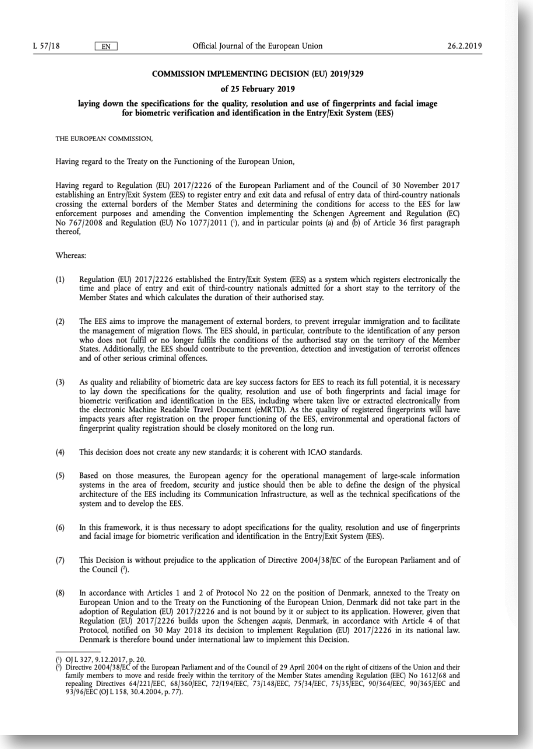
- Measure quality by filtering the signal and determine the utility of a fingerprint sample.

- Research results constitute the content of ISO/IEC 29794-4

Quality Metrics for Fingerprint Images

NFIQ2.0

- Is this (ISO/IEC 29794-4) a relevant standard?
- YES - 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.

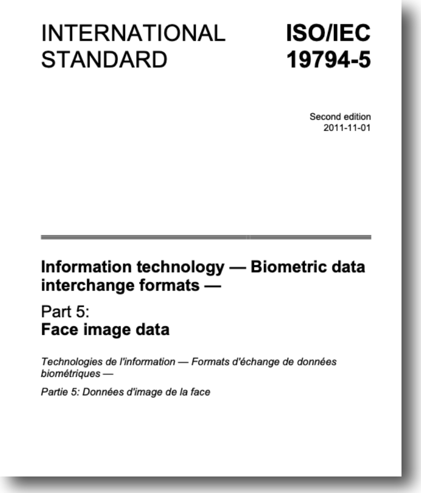
[2] Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 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).

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“*

What does that mean?



INTERNATIONAL STANDARD

ISO/IEC 19794-5

Second edition
2011-11-01

Information technology — Biometric data interchange formats —

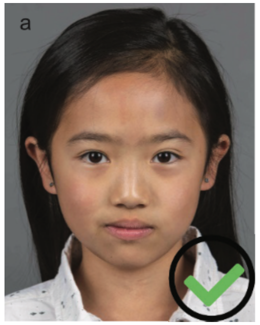
Part 5:
Face image data

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

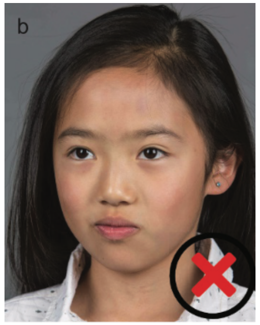
Partie 5: Données d'image de la face

Data subjects need actionable feedback

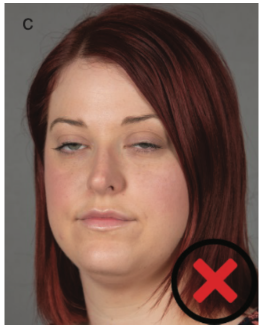
- If quality is poor, then what went wrong?



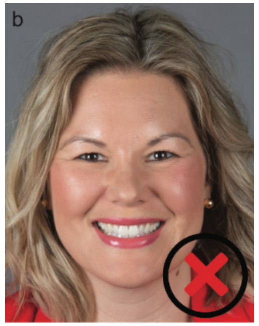
Compliant image



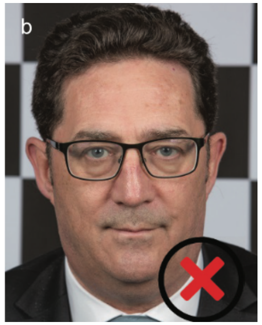
Pose



Eyes open



Mouth open



Inhomogenous background

Source: ISO/IEC 39794-5

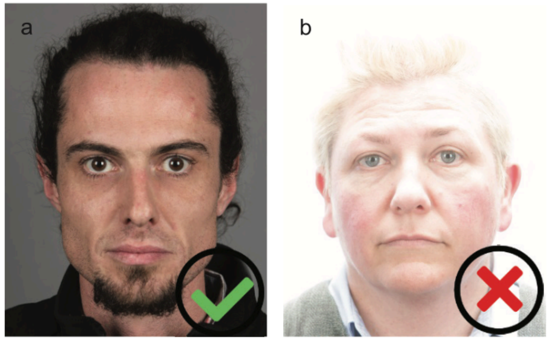
ISO/IEC 29794-5: Face Image Quality

ISO/IEC 29794-5 is aligned with both

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

Measures

- 7.2 Unified quality score
- 7.3 Capture-related quality measures
- 7.4. Subject-related quality measures



a) Compliant image b) Low contrast

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

Image Source: ISO/IEC 19794-5:2011

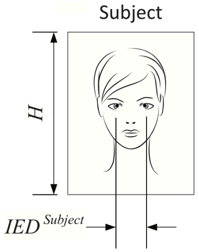
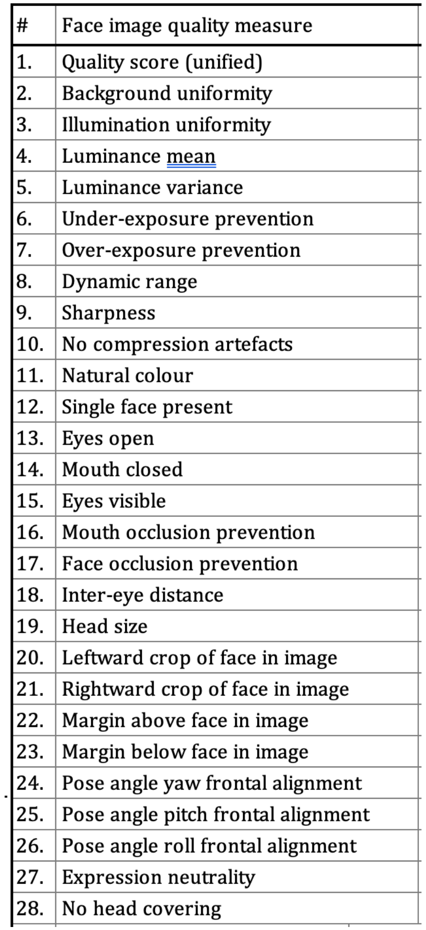


Image Source: ISO/IEC 39794-5

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

ISO/IEC IS 29794-5: Face Image Quality

ISO/IEC FDIS 29794-5 quality measures in detail



#	Face image quality measure
1.	Quality score (unified)
2.	Background uniformity
3.	Illumination uniformity
4.	Luminance mean
5.	Luminance variance
6.	Under-exposure prevention
7.	Over-exposure prevention
8.	Dynamic range
9.	Sharpness
10.	No compression artefacts
11.	Natural colour
12.	Single face present
13.	Eyes open
14.	Mouth closed
15.	Eyes visible
16.	Mouth occlusion prevention
17.	Face occlusion prevention
18.	Inter-eye distance
19.	Head size
20.	Leftward crop of face in image
21.	Rightward crop of face in image
22.	Margin above face in image
23.	Margin below face in image
24.	Pose angle yaw frontal alignment
25.	Pose angle pitch frontal alignment
26.	Pose angle roll frontal alignment
27.	Expression neutrality
28.	No head covering

Capture device related

Subject related

Hochschule Darmstadt

Projects

Description of most important projects with information like: title/funding level/partners/main topic/output/application/impact

Title:	**ATHENE NGBS**
Funding:	Total: ~ 8,9 Mio Eur / h_da ~4,8 Mio Eur
Partners:	Fraunhofer SIT, Hochschule Darmstadt, Technische Universität Darmstadt https://ngbs.athene-center.de/
Main topic:	Next Generation Biometric Systems
Output:	Robust, secure, privacy compliant and quality ensuring biometric algorithms
Application:	Biometric recognition systems
Impact:	Access control systems

Title:	**iMARS – image Manipulation Attack Resolving Solutions (H2020)**
Funding:	Total: ~6,9 Mio Eur / h_da: ~476,000 Eur
Partners:	Idemia, BKA, NTNU, others - see: https://cordis.europa.eu/project/id/883356
Main topic:	Morphing Attack Detection / Face Image Quality Assessment
Output:	Morphing Attack Detection mechanisms
Application:	Biometric Face Recognition Systems
Impact:	Robustness of Border Control

Title:	**EINSTEIN – Advancing the fight against identity fraud (H2020)**
Funding:	Total: ~5,4 Mio Eur / h_da: ~476,000 Eur
Partners:	EKEKTA, Veridos, Idemia, Fraunhofer, others - see: https://cordis.europa.eu/project/id/101121280
Main topic:	Morphing Attack Detection / Face Image Quality Assessment
Output:	Morphing Attack Detection mechanisms
Application:	Biometric Face Recognition Systems / Biometrics on the Move
Impact:	Robustness of Border Control

Hochschule Darmstadt

Projects

Description of most important projects with information like: title/funding level/partners/main topic/output/application/impact

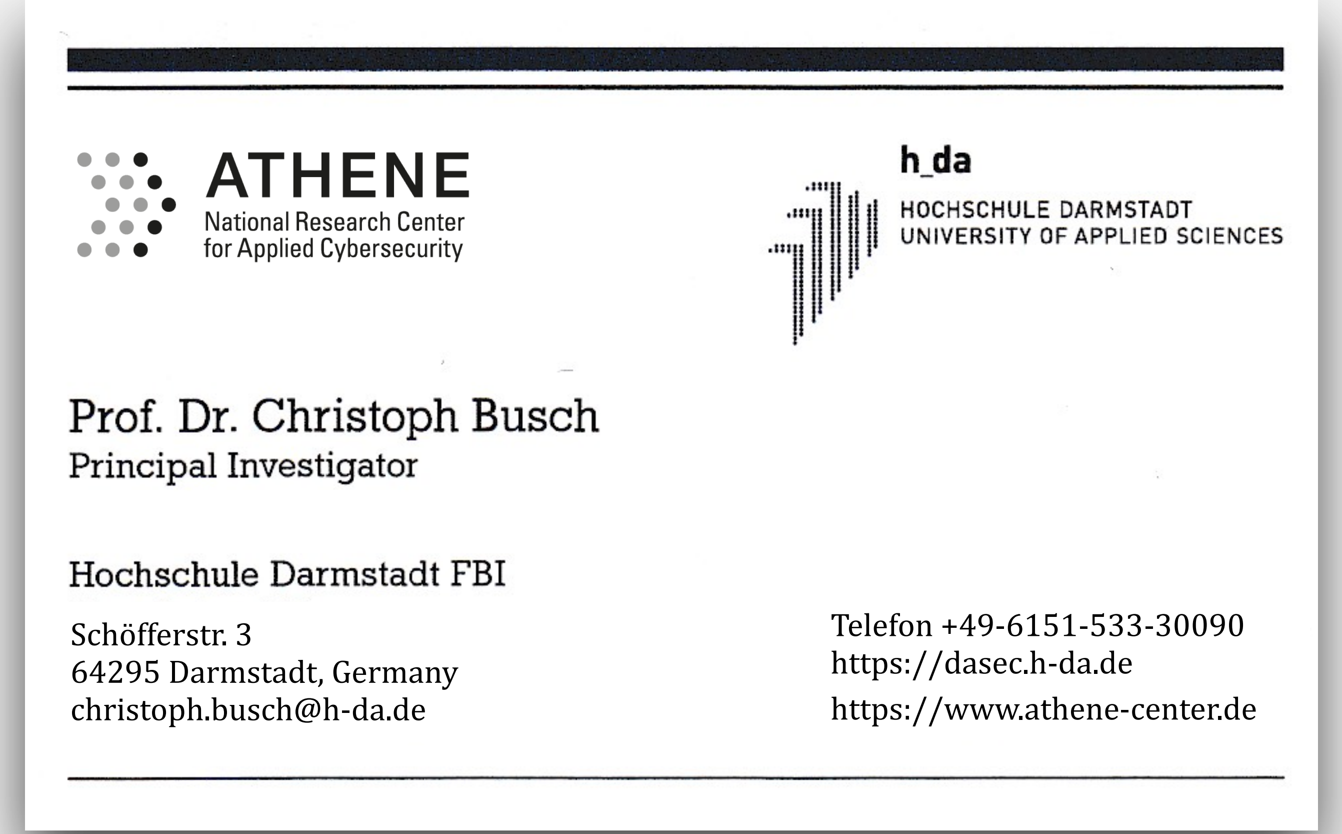
Title: **PARFAIT – Post-quantum cryptography for automotive components**
Funding: Total: ~4,43 Mio Eur / h_da: ~885,000 Eur
Partners: Infineon Technologies AG, DENSO AUTOMOTIVE Deutschland GmbH, Vitesco Technologies Germany GmbH, Fraunhofer AISEC, Freie Universität Berlin, Hochschule Darmstadt, Hochschule RheinMain, Technische Universität Darmstadt, Continental Automotive Technologies GmbH, Volkswagen AG, Max Planck Institute for Security and Privacy
Main topic: Promoting the use of post-quantum cryptography (PQC) and crypto-agility in the automotive sector
Output: Technological solutions and operational and process concepts to protect vehicles throughout their lifecycle
Application: Automotive sector
Impact: Secure future automotive components and infrastructures

Title: **QR PACE -PQC Building Blocks for eCard Applications**
Funding: Total: ~ 784,000 Eur / h_da ~509,000 Eur
Partners: Fraunhofer SIT, Hochschule Darmstadt, Technische Universität Darmstadt
Main topic: Promoting the use of post-quantum cryptography (PQC) and crypto-agility in eCard Applications
Output: Quantum-resilient password authenticated key exchange protocol
Application: Smart cards, wireless networks
Impact: Secure future eCard applications and infrastructures

Title: **HECA - Hardening of emergency vehicles to protect against cyber attacks**
Funding: Total / h_da: ~340.000€
Partners: Hessian Police Department for Technology, Hochschule Darmstadt
Main topic: Security evaluation of emergency vehicles considering special requirements of police and other first responders, development of approaches for hardening emergency vehicles against cyber attacks, practical evaluation in real police cars
Output: Security evaluation methodology, practical security analyses, hardening mechanisms for emergency vehicles
Application: Automotive Sector
Impact: Securing of current and future emergency vehicles against cyber attacks

Hochschule Darmstadt

Projects



ATHENE
National Research Center
for Applied Cybersecurity

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

Prof. Dr. Christoph Busch
Principal Investigator

Hochschule Darmstadt FBI

Schöfferstr. 3
64295 Darmstadt, Germany
christoph.busch@h-da.de

Telefon +49-6151-533-30090
https://dasec.h-da.de
https://www.athene-center.de