Face Morphing Attack Detection in the iMARS Project

Christoph Busch

copy of slides available at:
https://christoph-busch.de/about-talks-slides.html
more information at:
https://christoph-busch.de/projects-mad.html
latest news at:
https://twitter.com/busch_christoph

NIST-IFPC, October 28, 2020

European Association for Biometrics
eab
Human Identity in Europe

ATHENE

NTNU

Passports and Identity Cards of European Union Citizens

Standardised Travel Documents

Passports

- Regulation 2252/2004
  - face image
  - two fingerprint images

Identity Cards of European Union Citizens

- Regulation 2019/1157
  https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R1157
  - face image
  - two fingerprint images

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

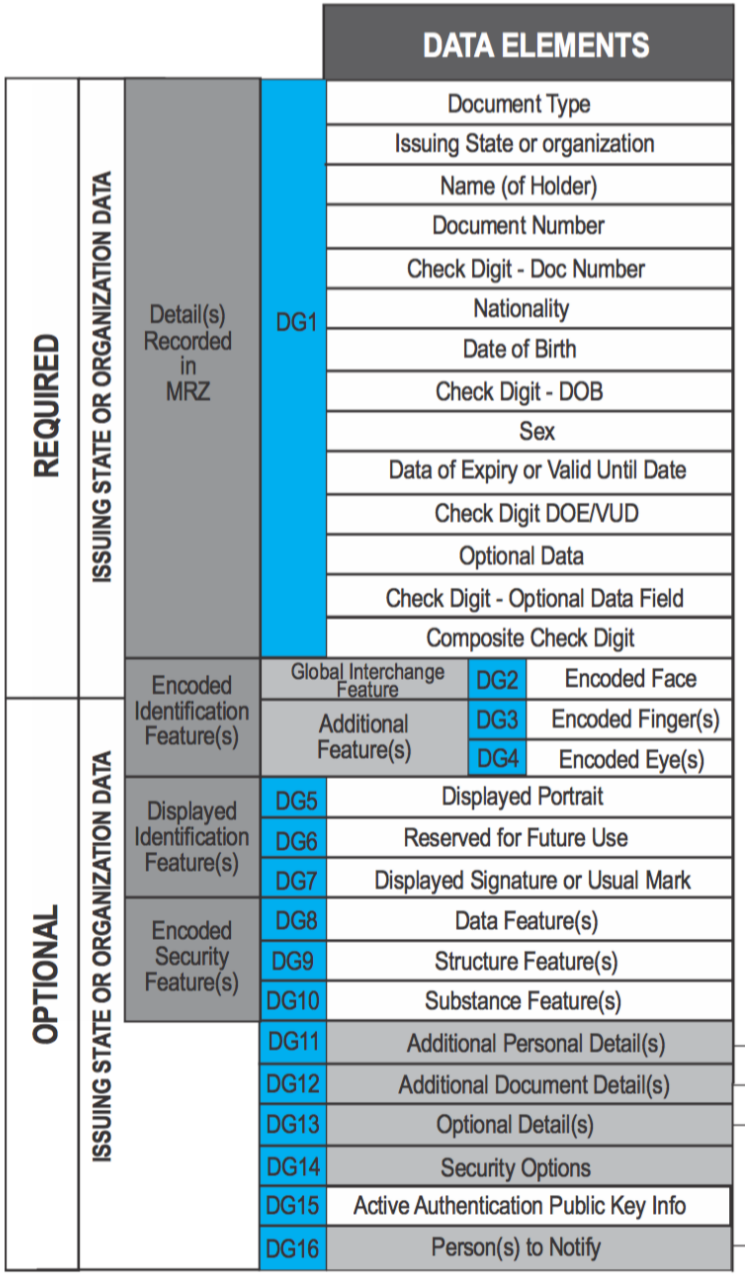
- DG4: Iris image

....

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

Document Security Object

- Hash values of DGs



Source: ICAO 9303 Part 10, 2015

ICAO 9303 Logical Data Structure

Data to be stored in the RFID-Chip

- 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

Is the Principle valid on the left Side?

Principle of equality - in our society

- One individual - one passport

Principle of unique link of ICAO

- One individual - one passport

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

Is the Principle valid on the left Side?

Principle of equality - in our society

- One individual - one passport

Principle of unique link of ICAO

- One individual - one passport
- ICAO 9303 part 2, 2006:
  *„**Additional security measures:** inclusion of a machine verifiable biometric feature linking the document to its legitimate holder“*

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

Is the Principle valid on the left Side?

Principle of unique link of ICAO

- One individual - one passport

We don’t want this principle of unique link to be broken

- Multiple individuals - one passport

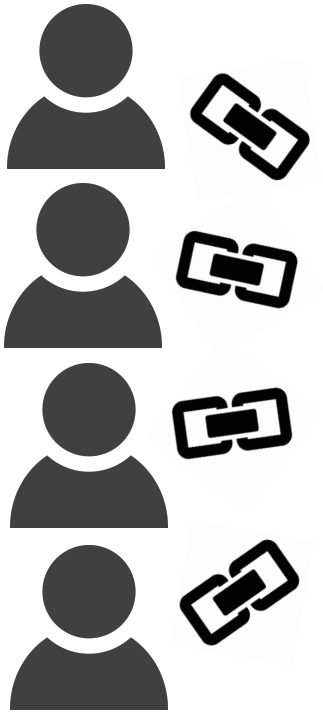


image source: https://pixabay.com/de/vectors/tick-sternchen-kreuz-rot-gr%C3%BCn-40678/

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.

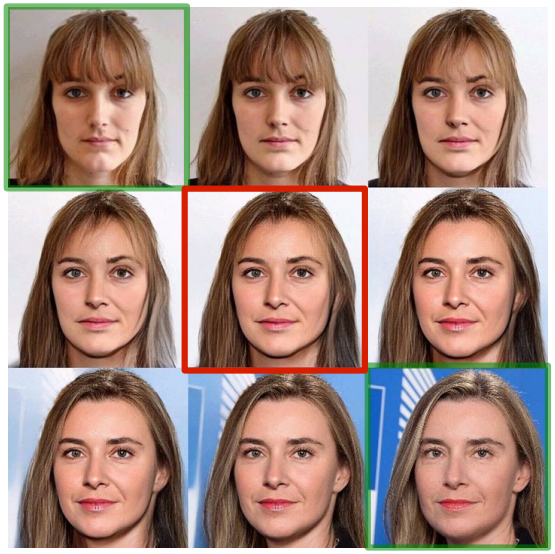


Image source: https://www.spiegel.de/netzwelt/netzpolitik/biometrie-im-reisepass-peng-kollektiv-schmuggelt-fotomontage-in-ausweis-a-1229418.html

Problem: Morphing Attacks

Message in December 2015:

- *„Brussels - we have a problem!“*

Proposed solutions to the Morphing Attack Problem:

- 1.) Photo studio should digitally sign the picture taken by Photo Studio and send it to the passport application office
  - this is in progress for Finland
- 2.) Switch to live enrolment
  - that is the case for Norway and Sweden
- 3.) Software-supported detection of morphed face images

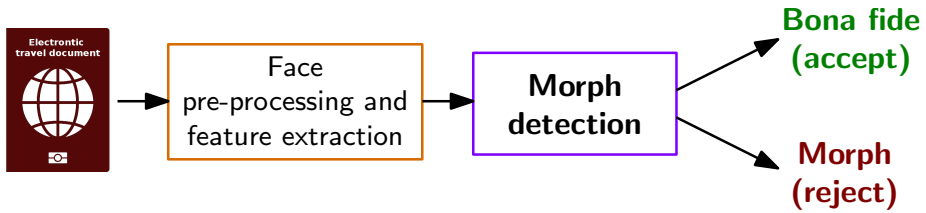
Regarding 2.) EU Regulation 2019/1157:

- on strengthening the security of identity cards in recital 32 states: *"... To this end, Member States could consider collecting biometric identifiers, particularly the facial image, by means of live enrolment by the national authorities issuing identity cards."*

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)

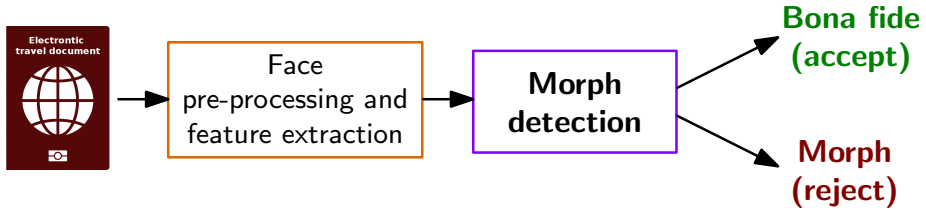


[SRB2018a] U. Scherhag, C. Rathgeb, C. Busch: "Towards Detection of Morphed Face Images in electronic Travel Documents“, in Proceedings of the 13th IAPR International Workshop on Document Analysis Systems (DAS), April 24-27, (2018)

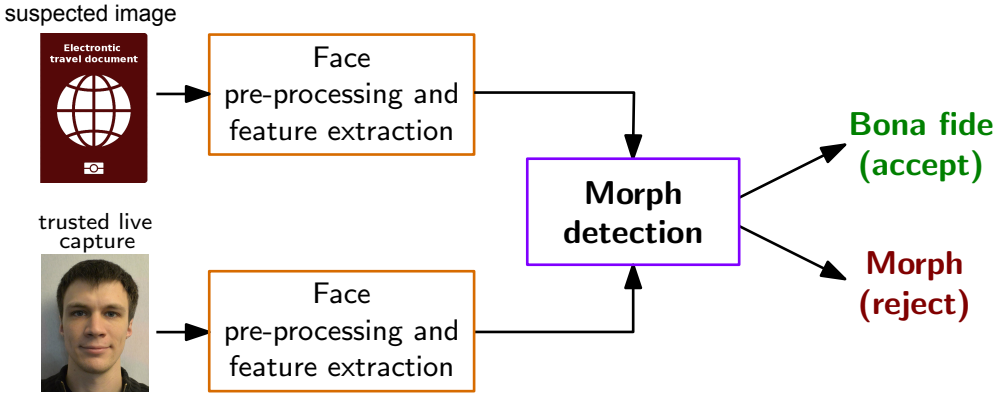
Morphing Attack Detection Scenarios

Real world scenarios

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



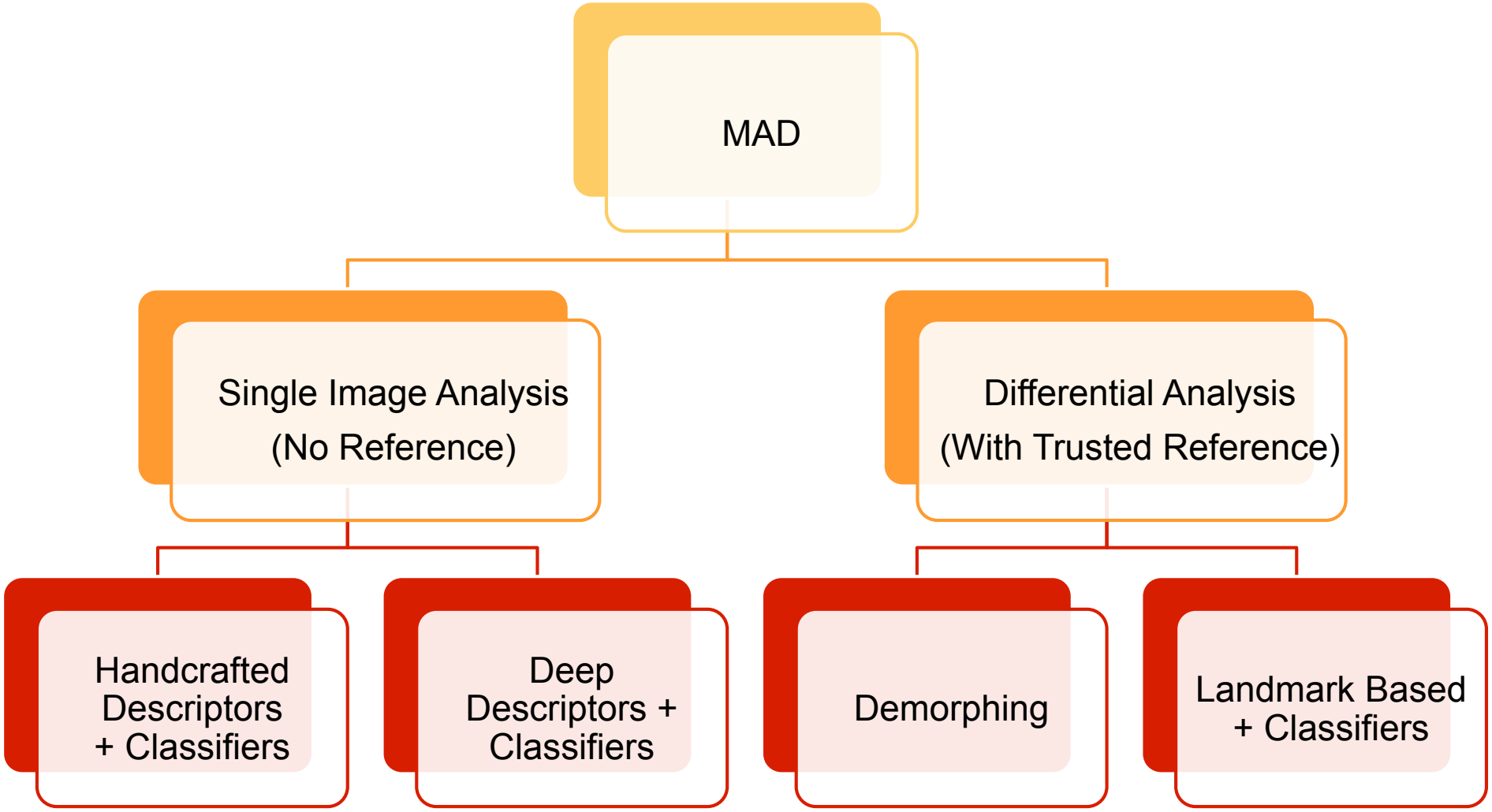
- Differential morphing attack detection (D-MAD)
  - A pair of images is analysed - and one is a trusted Bona Fide image
  - Biometric verification (e.g. at the border)



[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



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

MAD Evaluation

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

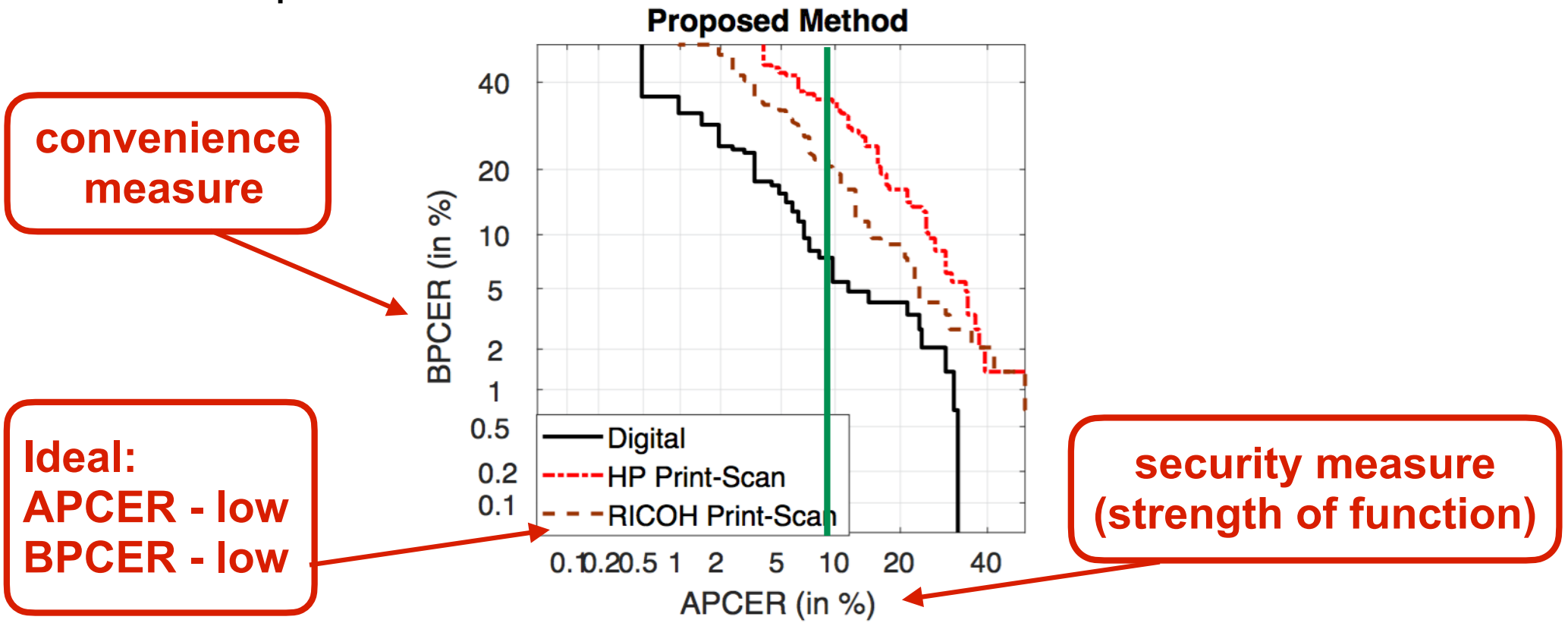
- **Bona fide presentation classification error rate (BPCER)**
  proportion of bona fide presentations incorrectly classified as attack presentations in a specific scenario

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)

MAD Evaluation Methodology

Face Morphing Attack evaluations are complex

- Evaluations must consider a dedicated methodology [SNR2017]
- Evaluations must consider many parameters

result = f (dataset-training, dataset-testing, morphing-attack,
landmark-detector, feature-extractor, classifier,
scenario (S-MAD vs. D-MAD),
post-processing, printer, scanner, ageing)

[SNR2017] U. Scherhag, A. Nautsch, C. Rathgeb, M. Gomez-Barrero, R. Veldhuis, L. Spreeuwers, M. Schils, D. Maltoni, P. Grother, S. Marcel, R. Breithaupt, R. Raghavendra, C. Busch: "Biometric Systems under Morphing Attacks: Assessment of Morphing Techniques and Vulnerability Reporting", in Proceedings of the IEEE 16th International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, September 20-22, (2017)

MAD Evaluation Methodology

Evaluations must consider many parameters

- Morphing may require manual interaction (not desired)

$$result = f(dataset\text{-}training, dataset\text{-}testing, morphing\text{-}attack, landmark\text{-}detector, feature\text{-}extractor, classifier, scenario\ (S\text{-}MAD\ vs.\ D\text{-}MAD), post\text{-}processing, printer, scanner, ageing)$$

Automated face morphing tools may introduce artifacts

In our evaluation we use

- Dlib / OpenCV
- FaceMorpher

Subject 1 | Morph (Dlib and OpenCV) | Morph (FaceMorpher) | Subject 2

MAD Evaluation Methodology

Evaluations must consider many parameters

- Postprocessing might conceal morphing effects (e.g. smoothing)

result = f (dataset-training, dataset-testing, morphing-attack, landmark-detector, feature-extractor, classifier, scenario (S-MAD vs. D-MAD), post-processing, printer, scanner, ageing)

smoothing and other effects might be compensated by the attacker

Morph

Sharpening

Histogram equalisation

MAD Evaluation Methodology

Evaluations must consider many parameters

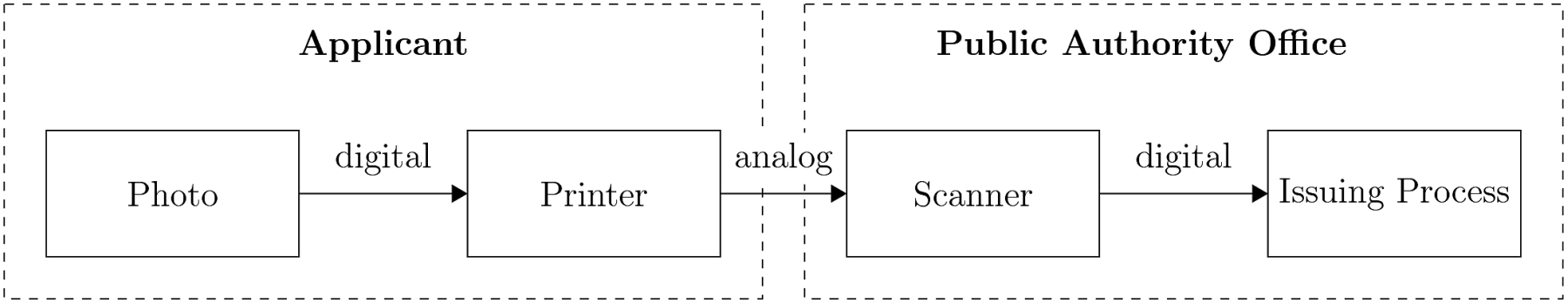
- The hardware selected for printing and scanning

$$result = f(dataset\text{-}training, dataset\text{-}testing, morphing\text{-}attack, landmark\text{-}detector, feature\text{-}extractor, classifier, scenario\ (S\text{-}MAD\ vs.\ D\text{-}MAD), post\text{-}processing, printer, scanner, ageing)$$

the image in the passport will be impacted
by fidelity and resolution of the hardware

Issuing process for the passport in most countries:

- applicant submit a printed photo



MAD Evaluation in SOTAMD

EU funded project: February 2019 – January 2020

- Partners:
  - National Office for Identity Data, NL, Bundeskriminalamt (BKA), DE
  - University of Bologna (UBO), IT, Hochschule Darmstadt (HDA), DE
  - The University of Twente (UTW), NL, NTNU, NO




Specific objectives:

- Capture face images from 150 subjects
  - with photo equipment and
  - automated border control gates
- Generate morphed face images with at least 3 algorithms
- Post-process automatically and manually
- Print and scan all morphed face images
- Test the MAD algorithms on the Bologna server
  https://biolab.csr.unibo.it/FVConGoing

D-MAD Evaluation in SOTAMD

SOTAMD achievements

- A new benchmark area for differential morphing attack detection

Differential Morph Attack Detection	Benchmarks	Leaded by
This benchmark area contains face morphing detection benchmarks. Morphing detection consists in analyzing an ISO compliant face image to determine whether it is the result of a morphing process (mixing faces of two subjects) or not. Algorithms submitted to these benchmarks are required to compare a bona fide (not morphed) image to a suspected image and produce a score representing the probability of the suspected image to be morphed. Read more...	DMAD-TEST DMAD-MORPHDB_D-1.0 DMAD-MORPHDB_P&S-1.0 DMAD-BIOLAB-1.0	Biometric System Lab University of Bologna

- Two benchmarks to evaluate different image types:
  - Digital or Printed/Scanned images

- Possibility of analysing results according to specific factors:
  - Manual or automatic morphing
  - Morphing approaches and parameters (e.g., morphing factor)
  - Gender, ethnicity, age, etc.

SOTAMD compliance with NIST-FRVT-MORPH

NIST realized FRVT MORPH

- an ongoing independent testing of face morph detection technologies.
  https://www.nist.gov/programs-projects/frvt-morph

The SOTAMD consortium decided to define

- a testing protocol perfectly compatible with the NIST interface,
- in order to minimize the effort for developers and
- promote the submission of algorithms to both evaluation platforms.

NIST only accepts Linux dynamically-linked library file;

- FVC-onGoing accepts both Windows and Linux executables

SOTAMD Results

A database with variety of morphing algorithms and automated and manual post-processing

- Demographics

Gender		Age		
Male	Female	A18-A35	A36-A55	A56-A75
86	64	87	47	16
Ethnicity				
European	African	India-Asian	East-Asian	Middle-Eastern
96	26	10	9	9

- Number of images with morphing and manual post-processing

	Automated Morphing	Manually post-processed	Total
Digital images	1475	570	2045
Printed & Scanned	1453	2250	3703
Total	2928	2820	5748

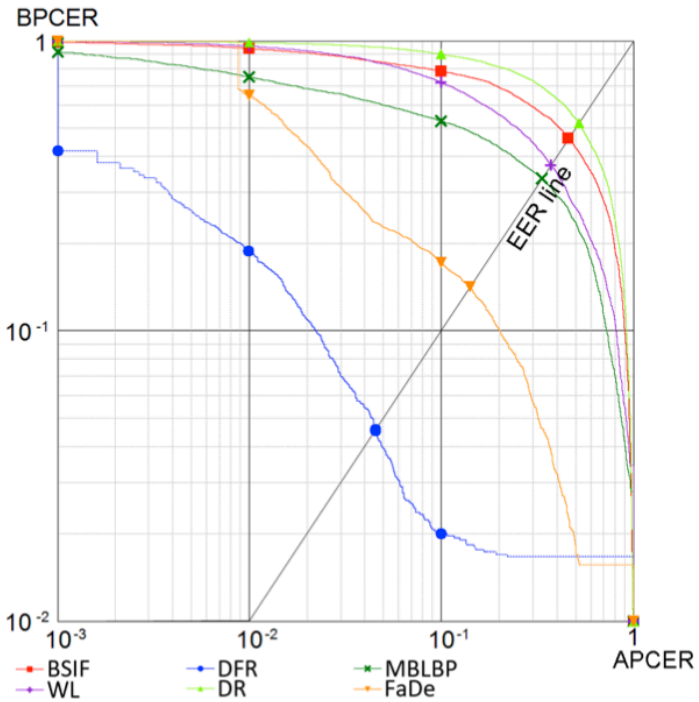
[Raja2020] K. Raja, M. Ferrara, A. Franco, L. Spreeuwers, I. Batskos, F. Wit, M. Gomez-Barrero, U. Scherhag, D. Fischer, S. Venkatesh, J. Singh, G. Li, L. Bergeron, S. Isadskiy, R. Raghavendra, C. Rathgeb, D. Frings, U. Seidel, F. Knopjes, R. Veldhuis, D. Maltoni, C. Busch: "Morphing Attack Detection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

SOTAMD Results

Detection accuracy - focused on D-MAD

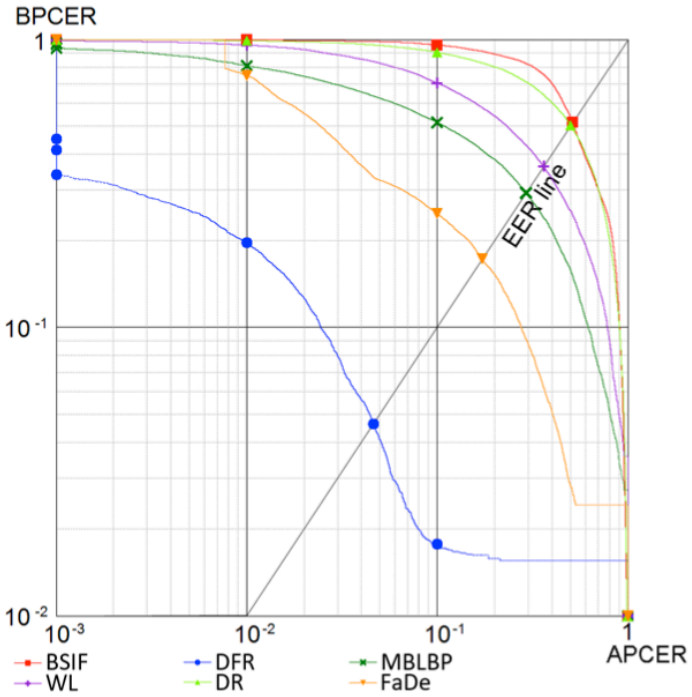
https://biolab.csr.unibo.it/FVCOnGoing/UI/Form/BenchmarkAreas/BenchmarkAreaDMAD.aspx

- 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

The iMARS Project Summary

The Key Figures

iMARS project

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

The Consortium

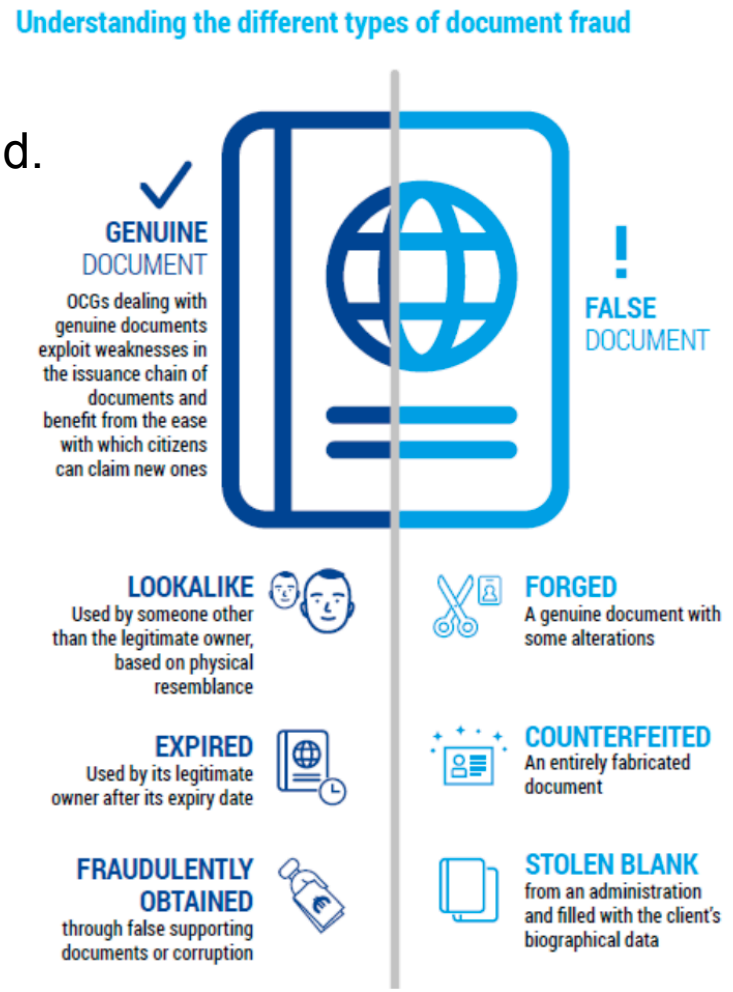
24 Partners

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

The Objectives

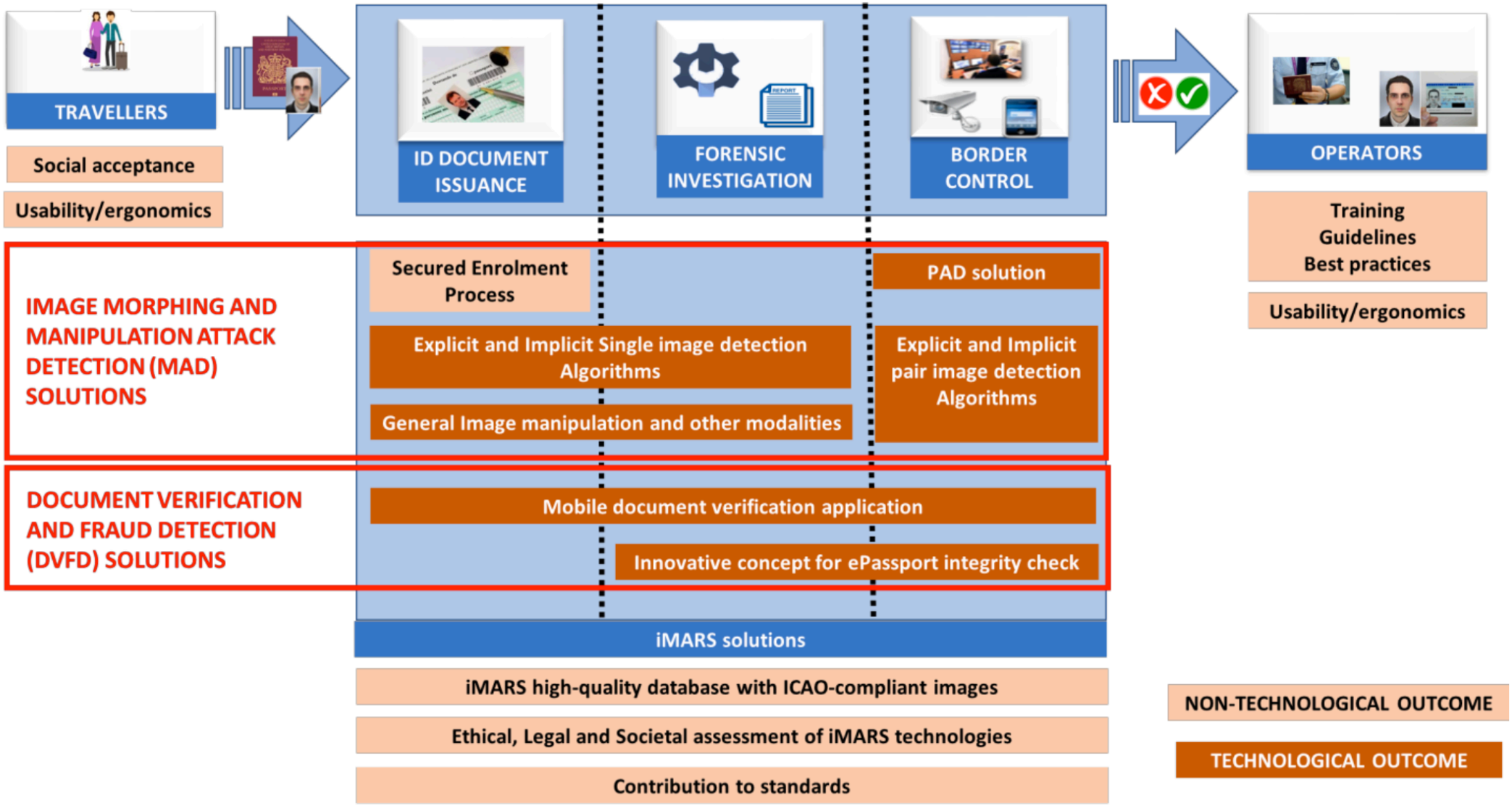
Technologies to enhance border and external security

- The iMARS project will provide:
  - Image Morphing and manipulation Attack Detection (MAD) solutions to assess ID documents validity against document fraud.
    - focus on attacks during enrolment steps and at the border crossing stations
  - Document Verification and Fraud Detection (DVFD) solutions to support border guards in the verification process by providing mobile tools and training.
- The solutions developed in iMARS will:
  - focus on electronic ID documents
  - be flexible enough to enable the integration with existing solutions and serving various use cases:
    - ID Document application or renewal
    - border control
    - forensic investigation of ID Documents.



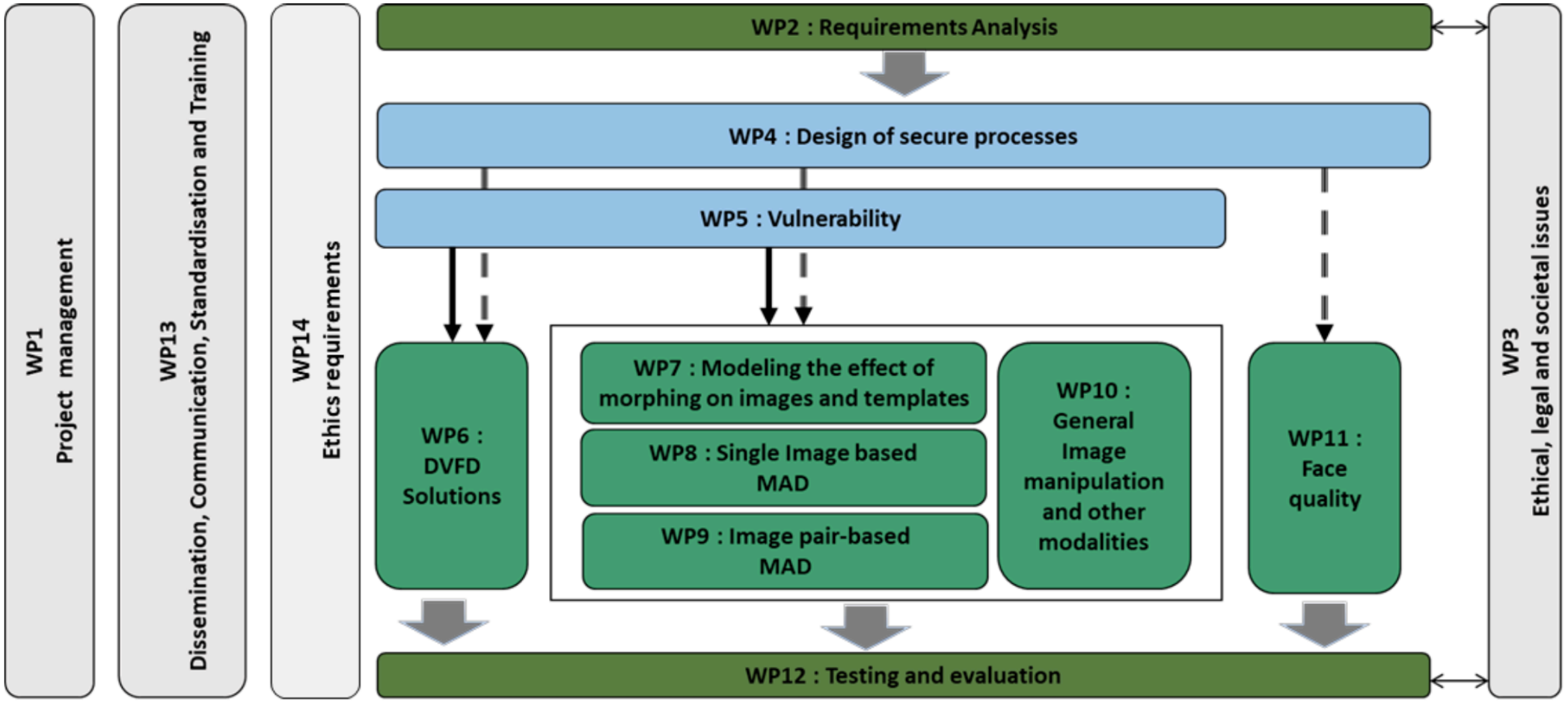
The iMARS Research

The iMARS overall concept



The Work Packages

The iMARS work packages dependencies



What needs to be done -

after the SOTAMD project is completed?

MAD Action Plan

1.) Establish consensus amongst stakeholders

- Europe should immediately start an action to secure
  - the trusted link between a MRTD and the document holder meaning to switch to live enrolment !
    - Note: The German parliament is discussing a revision of the passport law these days
  - and to develop and deploy technical mechanisms that can detect a morph passport at borders.
- Support the iMARS-consortium, that is ready to jointly work on the morphing challenges
  - iMARS is a pan-European approach that is supported by the European Association for Biometrics (EAB)

MAD Action Plan

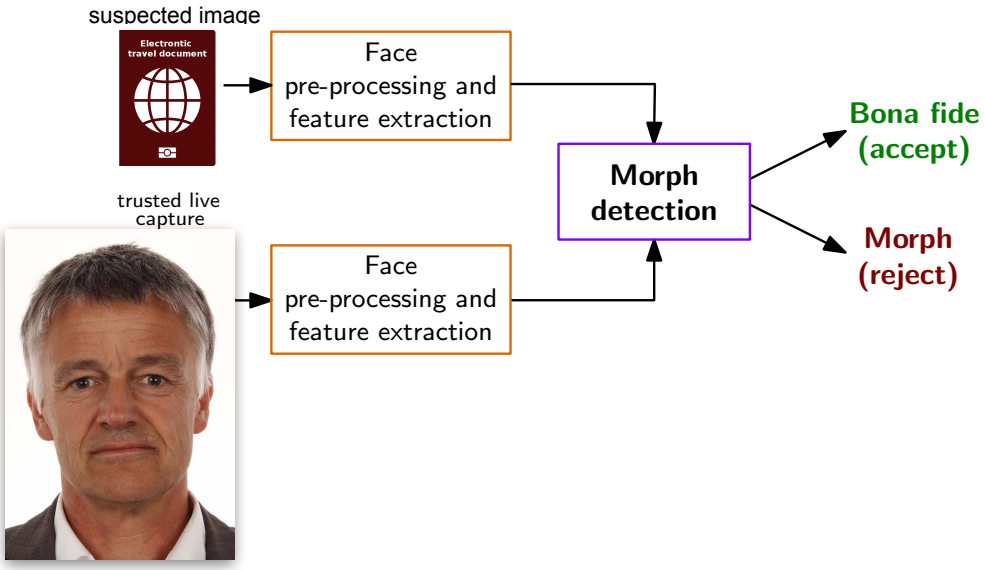
2.) Standardise the passport application process

- A European regulation should enforce that all Member States switch to live enrolment, as it is already operational e.g. in Norway and Sweden.
  - Only then, with full control of the biometric capture process by a civil servant in the passport application office, trust in the link of passport holder to reference data can be assured.
- The iMARS consortium has proposed to define a secure ID Document application process:
  - Make it difficult to apply for an ID document with a photograph that has been morphed or manipulated otherwise (e.g. data subjects want to look younger)
  - Take precautions to detect a case that someone tries to enrol with a well-crafted facemask (avoid a presentation attack with a morphed face image on the mask)
  - The capture device certification scheme will be recorded in the data record, as defined in the new extensible interchange format ISO/IEC 39794-5

MAD Action Plan - iMARS Project

3.) Detect automatically Morph Passports at Borders

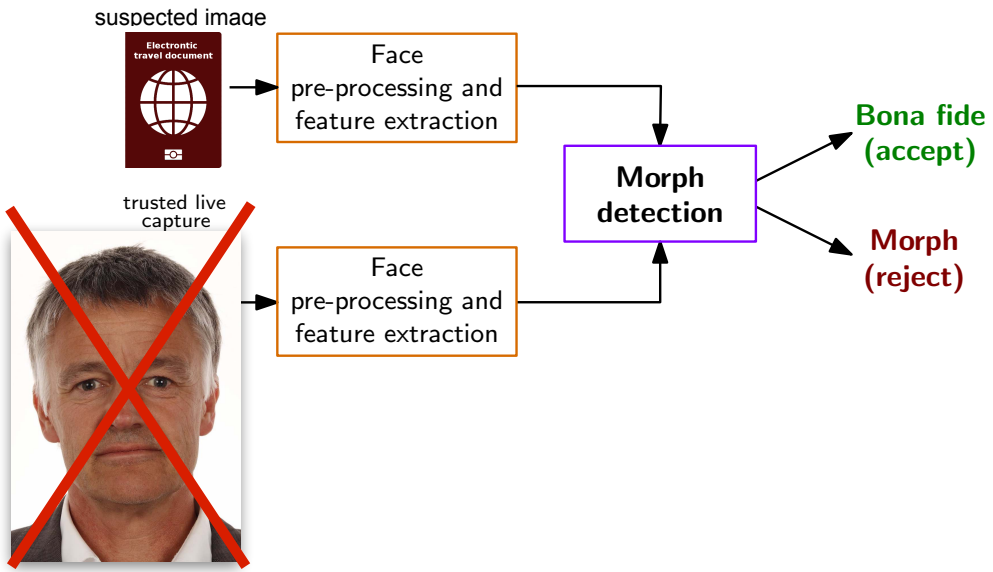
- After the completed transition to live enrolment in all MS we must anticipate that European passports - potentially containing a morphed image - are presented at least for the next 10 years.
  - Robust border control processes based on a differential morphing attack analysis, where the quality of probe image varies.
  - Trusted live capture images must be in realistic degraded quality!

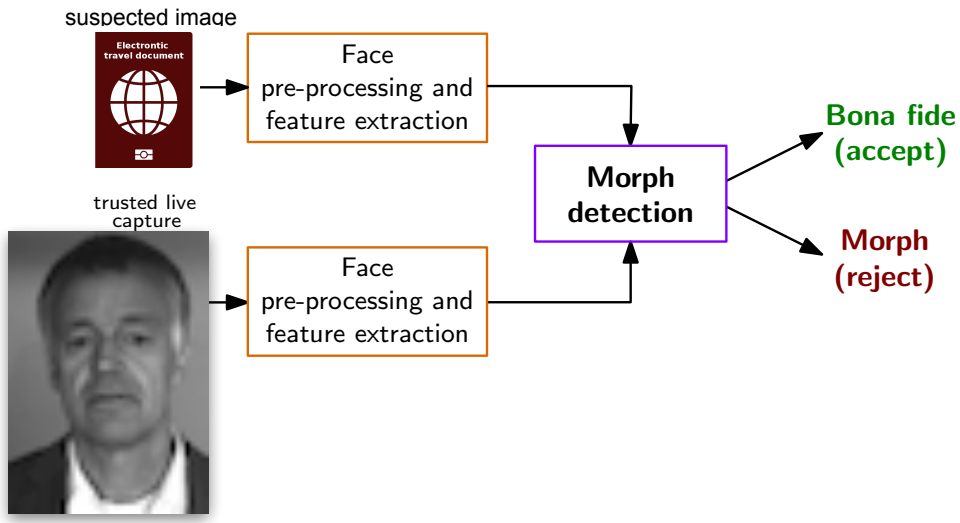


MAD Action Plan - iMARS Project

3.) Detect automatically Morph Passports at Borders

- After the completed transition to live enrolment in all MS we must anticipate that European passports - potentially containing a morphed image - are presented at least for the next 10 years.
  - Robust border control processes based on a differential morphing attack analysis, where the quality of probe image varies.
  - Trusted live capture images must be in realistic degraded quality!





- Explicit and implicit D-MAD algorithms

MAD Action Plan

4.) Detect Morph Passports in Forensic Investigations

- A forensic investigator has a single image only
- In support of forensic investigations, we need single image MAD
  - also known as no-reference MAD or forensic MAD
  - explicit MAD and implicit MAD with transfer learning
  - trained with large-scale face morph databases.
  - based on the relatively low-resolution digital image stored in the passport,
  - print and scan MAD robustness
  - fusion of multiple MAD subsystems.

MAD Action Plan

5.) Compose Test Data and Online Evaluation Platform

- Testing of MAD solution can't be done without appropriate data.
- Need for an iMARS mixed quality dataset and diversification
  - more subjects
  - more enrolment processes / print and scan equipment
  - more morphing tools
  - high AND controlled degrading quality
- Augment the Bologna-Online-Evaluation-Platform (BOEP)
  - Provide open access benchmark tests.
  - Include S-MAD evaluation:
    https://biolab.csr.unibo.it/FVCOnGoing/UI/Form/BenchmarkAreas/BenchmarkAreaSMAD.aspx
  - Thus national border control agencies will be able to evaluate
    if the MAD State-of-the Art meets the operational requirements.

MAD Action Plan

6.) Standardise Testing of MAD Solutions

- Find consensus, how we test
  - Measures for vulnerability and detection accuracy
- Morphing vulnerability metric based on the Mated-Morph-Presentation-Match-Rate (MMPMR)
  - anchor the MAD evaluation methodology in the ISO/IEC 30107 multipart standard
  - Find consensus in the MAD research community
- Standardise metrics to evaluate the performance of MAD methods
  - APCER - Attack Presentation Classification Error Rate
  - BPCER - Bona Fide Presentation Classification Error Rate
  - corresponding DET-Plots
- Border control agencies of EU Member State shall be motivated to participate in this standardisation process

MAD Action Plan - iMARS Project

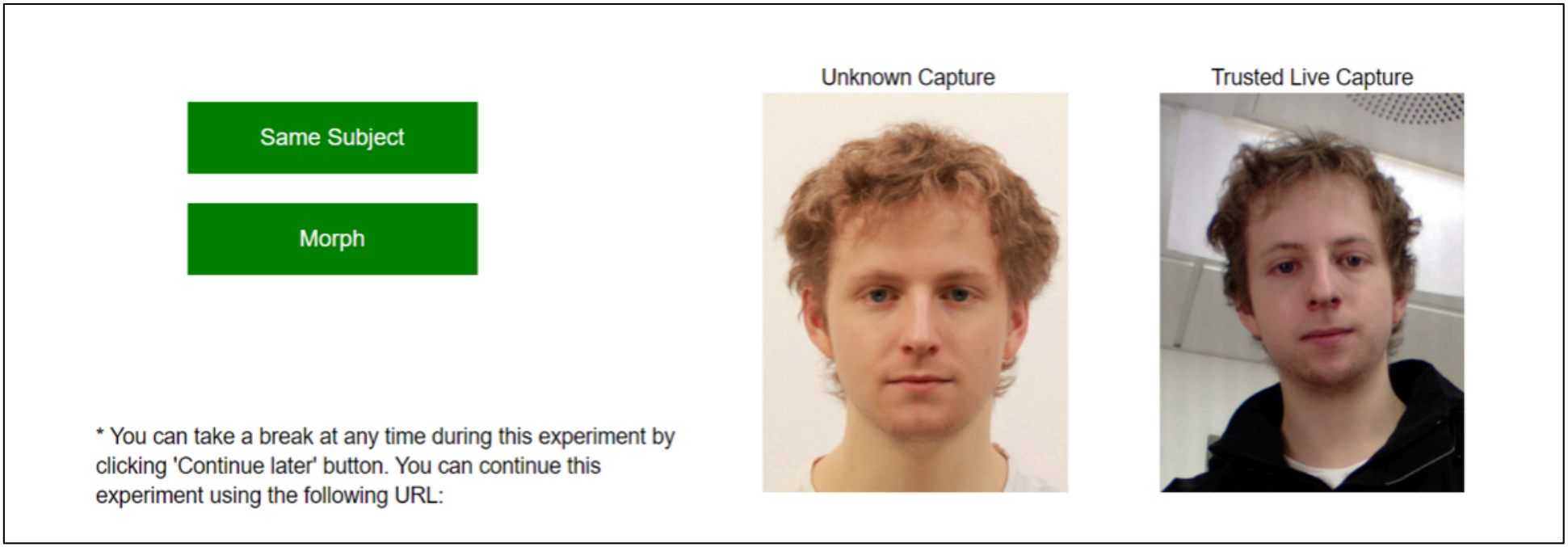
7.) Develop Face Image Quality Metrics

- We need the equivalent to NFIQ2.0 for facial images
- Ensure that captured samples that are sufficiently good in terms of illumination, sharpness, or pose
- Align with the framework for biometric sample quality described in ISO/IEC 29794-1:2016
  - align with ISO/IEC NP 29794-5 https://www.iso.org/standard/81005.html
- Develop an automatic face image quality assessment software,
  - which can predict recognition accuracy
- Once predictive face quality metrics are available,
  - MAD evaluation can be adapted to the three relevant scenarios (ID Document issuance, border control, and forensic investigation)
  - we can report the impact of face image quality on morphing attack detection

MAD Action Plan

8.) Train Communication Personnel and Border Officers

- Train the agencies staff, how to react
  - to mitigate public excitement and explain attack resolving solutions against morphing attacks,
- Develop best practices for improving the officers' skills on manipulated/morphed image and document fraud detection
  - show to border guards that the MAD tools will not replace, but complement, their expertise.



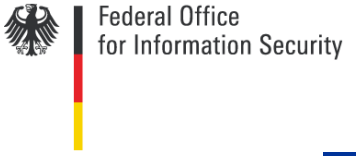
Thanks

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 — Borders and Visa

- 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.

Conclusion

We are facing a situation, where

- Passports with morphs are already in circulation
  - 1000+ reported cases
  - Switch to live enrolment is a good decision, but does not solve the problem
- Passports with morphed face images will have a major impact on border security (introduction of EU's entry/exit system, global migration flows)
- In combination with passport brokers a dramatic problem
  - the darknet offers numerous such opportunities …

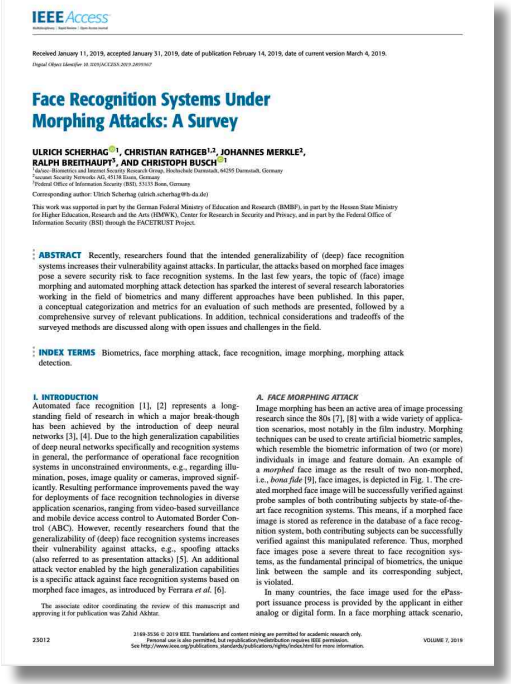
More information

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,

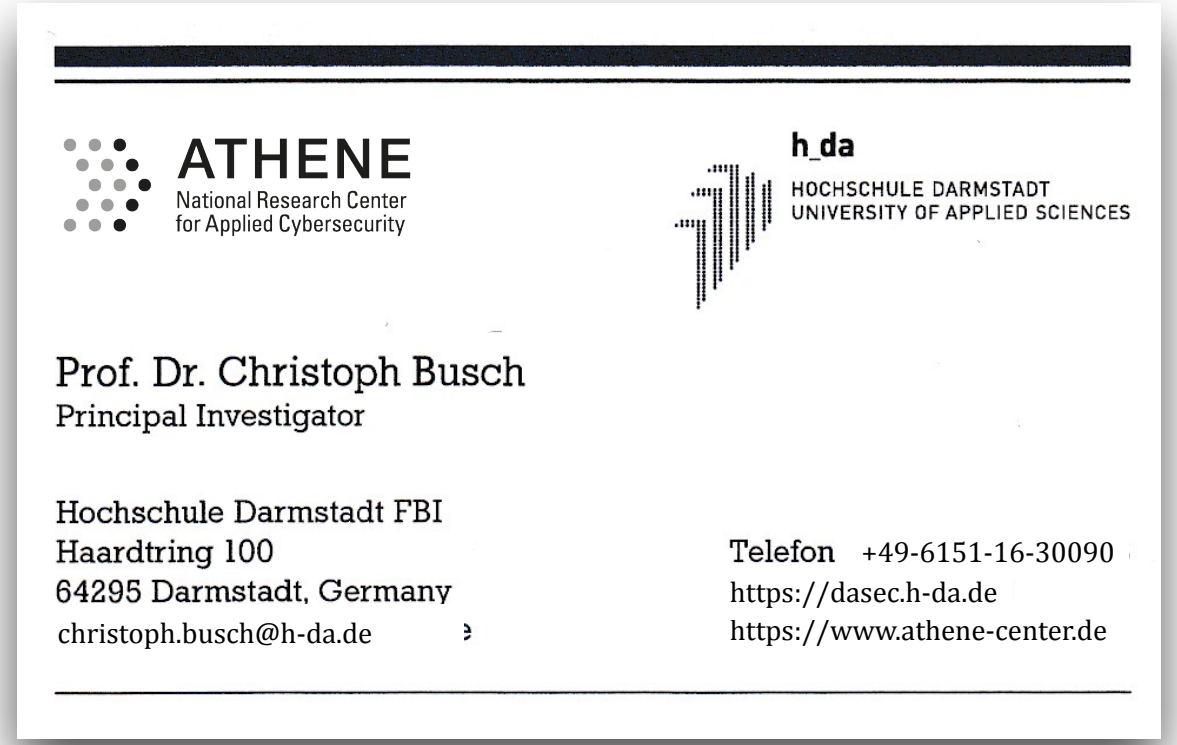
Contact

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

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