Face Image Morphing

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

2022 International Joint Conference on Biometrics (IJCB 2022)
October 11, 2022

ATHENE

MARS

NORWEGIAN BIOMETRICS LABORATORY

NTNU

Overview

Agenda

- Introduction - Problem description
- Morphing Attack Detection (MAD) - Scenarios and Methods
- Automated Face Morphing Attack Detection
- Human examiners at Face Morphing Attack Detection
- Conclusion

Biometric Characteristic

Biometric activities

- Lecturer in Darmstadt, Gjøvik and Copenhagen
- Convener of the Working Group 3 on Biometric Data Interchange Formats in ISO/IEC JTC1 SC37
- Board-member European Association for Biometrics
- Chair of the TeleTrusT working group on Biometrics
- Co-Chair of the Norsk Biometri Forum

Research related to Biometrics

- ATHENE research area on Biometrics https://ngbs.athene-center.de/
- EU H2020 iMARS https://imars-project.eu/

ATHENE National Research Center for Applied Cybersecurity

iMARS

ATHENE NGBS Fraunhofer IGD 2015 h_da

ISO IEC 2003

European Association for Biometrics eab 2011

NTNU 2007

Passports and Identity Cards

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
OPTIONAL	ISSUING STATE OR ORGANIZATION DATA	Encoded Identification Feature(s)	Global Interchange Feature	DG2	Encoded Face
			Additional Feature(s)	DG3	Encoded Finger(s)
				DG4	Encoded Eye(s)
		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

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

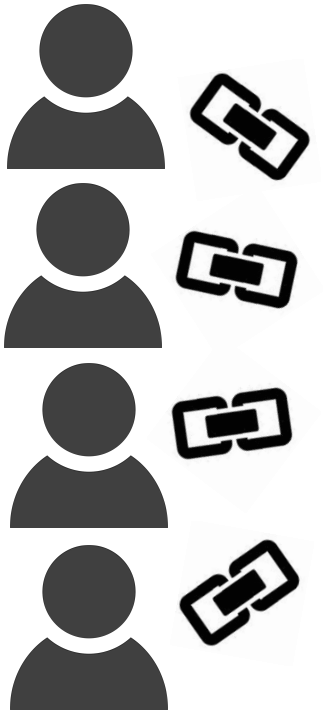


image source: https://pixabay.com/de/vectors/tick-sternchen-kreuz-rot-gr%C3%BCn-40678/

What is Morphing?

What is Morphing?

Do you remember the story

- if you kiss a frog …

What is Morphing?

Do you remember the story

- if you kiss a frog …
- … the frog will turn into a prince

Source: www.promipool.de

What is Morphing?

Or with minor modification of the story:

- if you kiss a frog …
- … the frog will turn into a princess

What is Morphing?

Or with minor modification of the story:

- if you kiss a frog …
- … the frog will turn into a princess
- Morphing can make this dream possible (even without the kiss)
  - with the frog and the princess as actors

Image source: https://www.myposter.de/motive/frosch-bild

Therese Johaug acting as princess in this talk

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

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

What is Morphing?

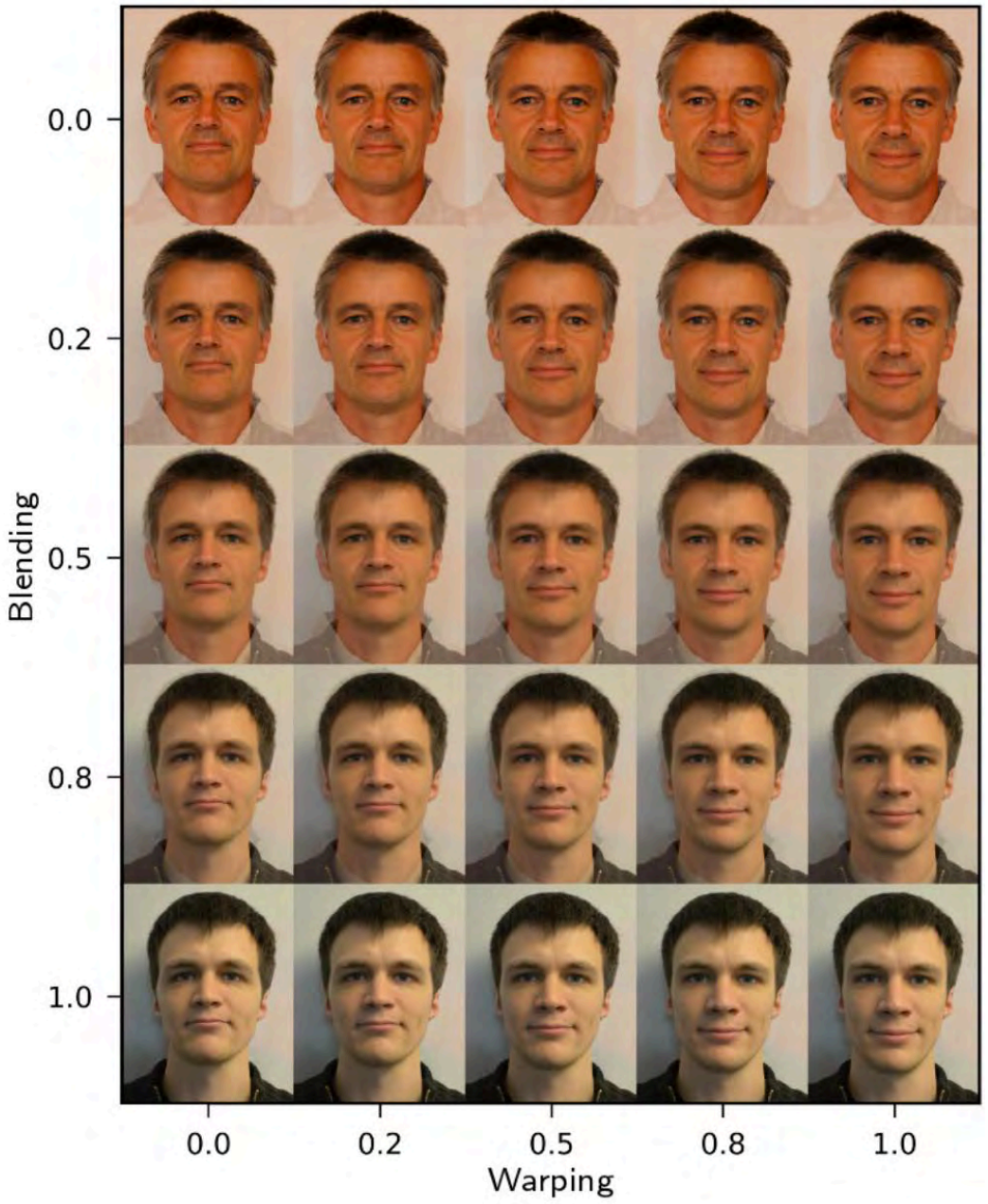
Warping and blending

- controlled by the alpha factor
- Landmark positions

$$\vec{x}_m = (1 - \alpha_w) \cdot \vec{x}_1 + \alpha_w \cdot \vec{x}_2$$

- Colour

$$C_m = (1 - \alpha_b) \cdot C_1 + \alpha_b \cdot C_2$$



A good Morph …

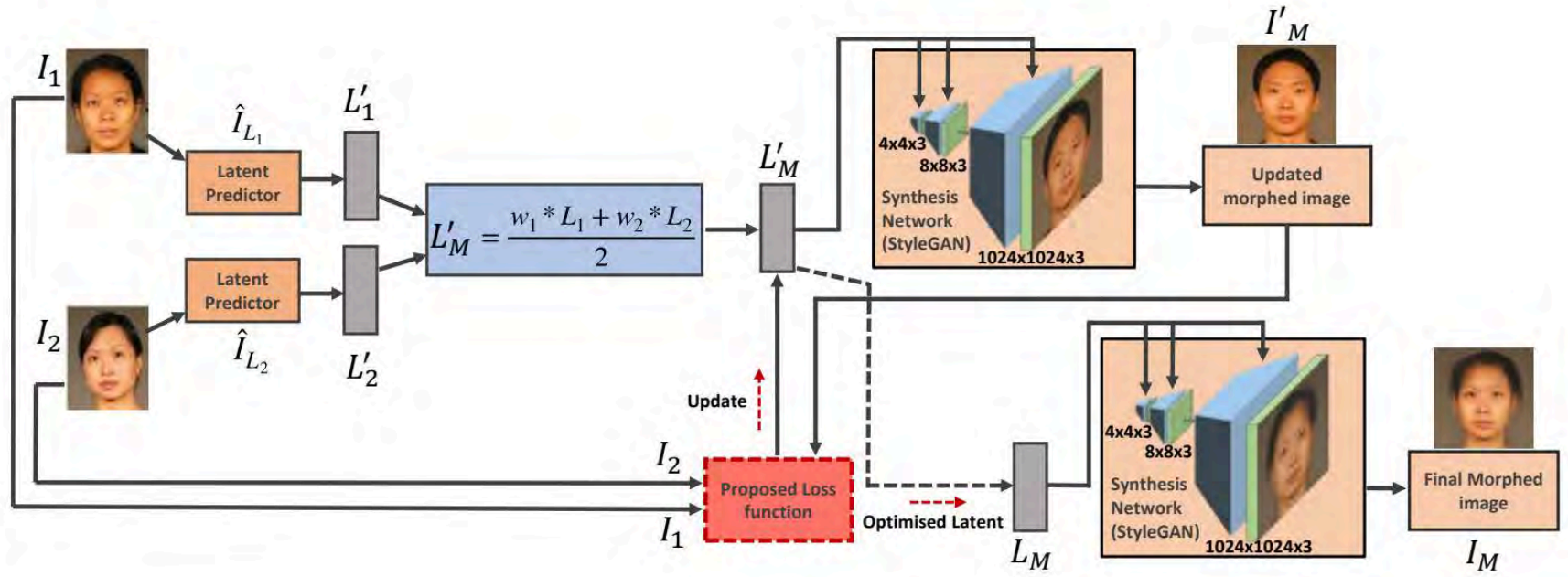
… is not as simple as you think

- Alignment at inner and outer eyecorner landmarks, will cause artifacts (e.g. iris shadows)

A good Morph …

… generated with MIP-GAN

- Morphing through Identity Prior driven Generative Adversarial Network
  - high quality morphs
  - enforced identity priors



[Zhang2021] H. Zhang, S. Venkatesh, R. Raghavendra, K. Raja, N. Damer, C. Busch: "MIPGAN - Generating Strong and High Quality Morphing Attacks Using Identity Prior Driven GAN", in IEEE Transactions on Biometrics, Behavior, and Identity Science (TBIOM), (2021)

Problem Description

Problem: Morphing Attacks

Morphing attack scenario

- Passport application of the accomplice A

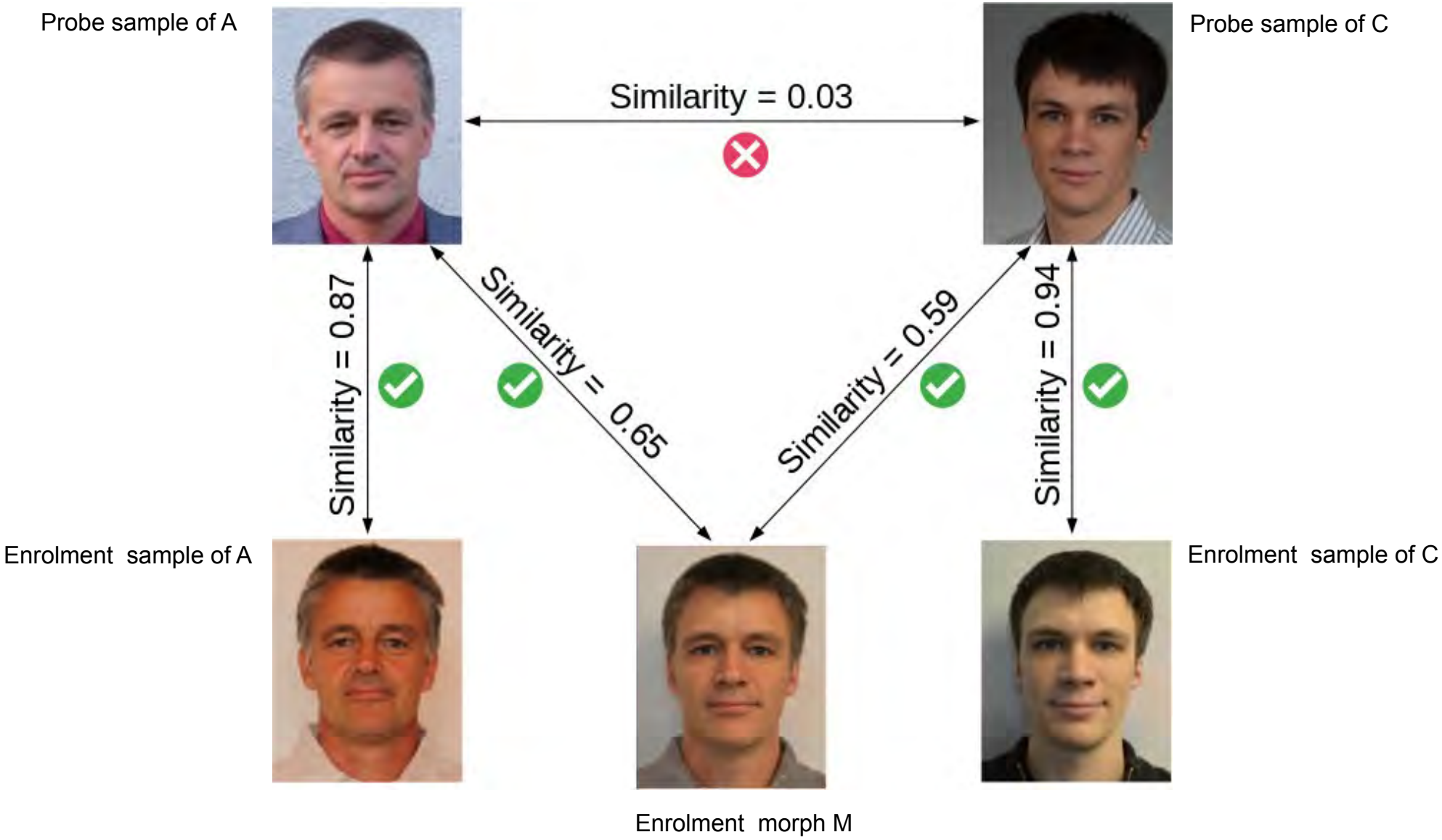
Problem: Morphing Attacks

Morphing attack scenario

- Border control

Problem: Morphing Attacks

Verification against morphed facial images



Problem: Morphing Attacks

Is it a really problem ? - YES!

- In September 2018 German activists
  - used a morphed images of Federica Mogherini (High representative of the European Union for Foreign Affairs and Security Policy) and a member of their group
  - and received an authentic German passport.

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

Problem: Morphing Attacks

Is it a really problem ? - YES!

Report by the Slovenian Police [Tork2021]

- Reported in September 2021 that
  in last 12 month more than 40 morphing cases
  - were detected at Airport Police in Ljubljana
- Business model:
  - Albanian citizens, applying for a Slovenian passport
  - offered as a professional service travel route
    via Vienna and Warsaw to Canada

[Tork2021] Matjaž Torkar: “Morphing Cases in Slovenia”, German Biometric Working Group, (2021), https://eab.org/events/program/220

Problem: Morphing Attacks

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."*

What is the vulnerability of FRS?

Automatic Border Control

The verification process

- at an Automatic Border Control (ABC) gate
- is comparing the reference image from the ePass against multiple consecutive frames acquired live.

ABC gates of different manufacturers use different FRSs.

- Different FRSs use a different number of live frames during the verification process

Image source: BSI

Measure the Vulnerability

When is a morphing attack considered successful?

- Only if all contributing subjects reach successfully a match when being compared against the morphed reference sample.

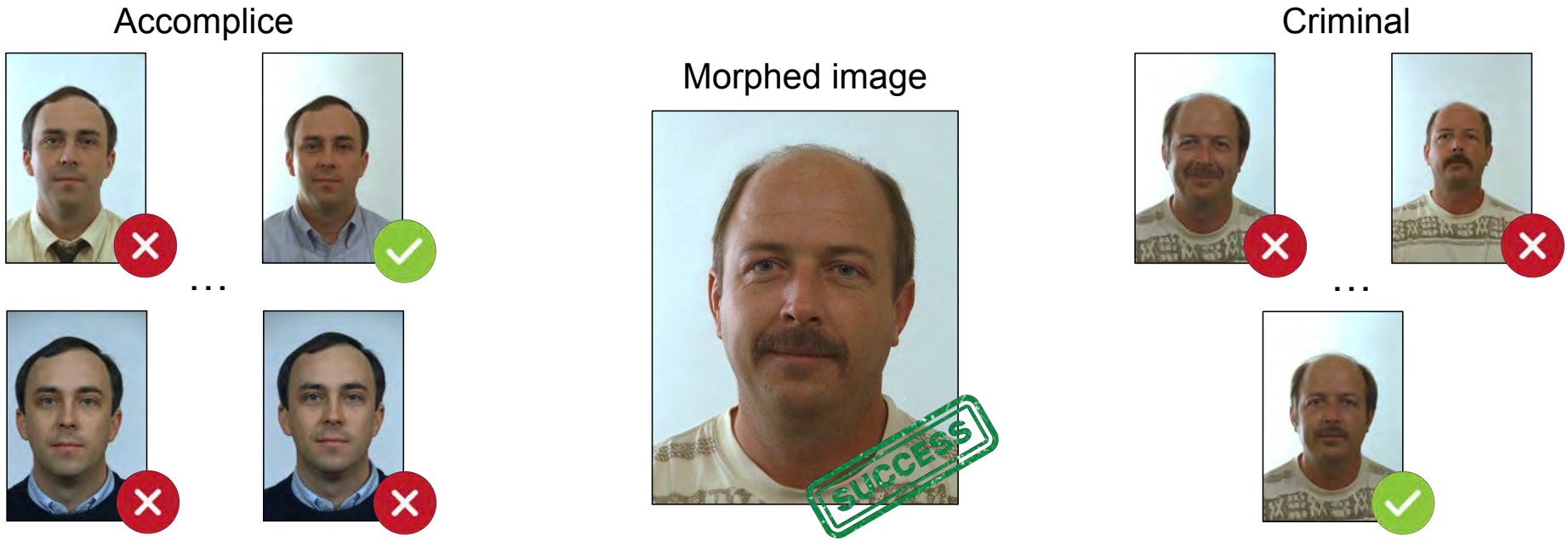
The vulnerability to morphing is usually measured on specific databases of morphed images.

- It is quantified as the proportion of morphed images that are erroneously verified as bona fide (i.e. pristine) with all contributing subjects.
- Two metrics have been introduced for vulnerability assessment
  - MMPMR
  - FMMPMR

Measure the Vulnerability

Mated Morph Presentation Match Rate (MMPMR)

- A morphing attack succeeds if the morphed image can be successfully verified against at least one of the probe images of each subject.



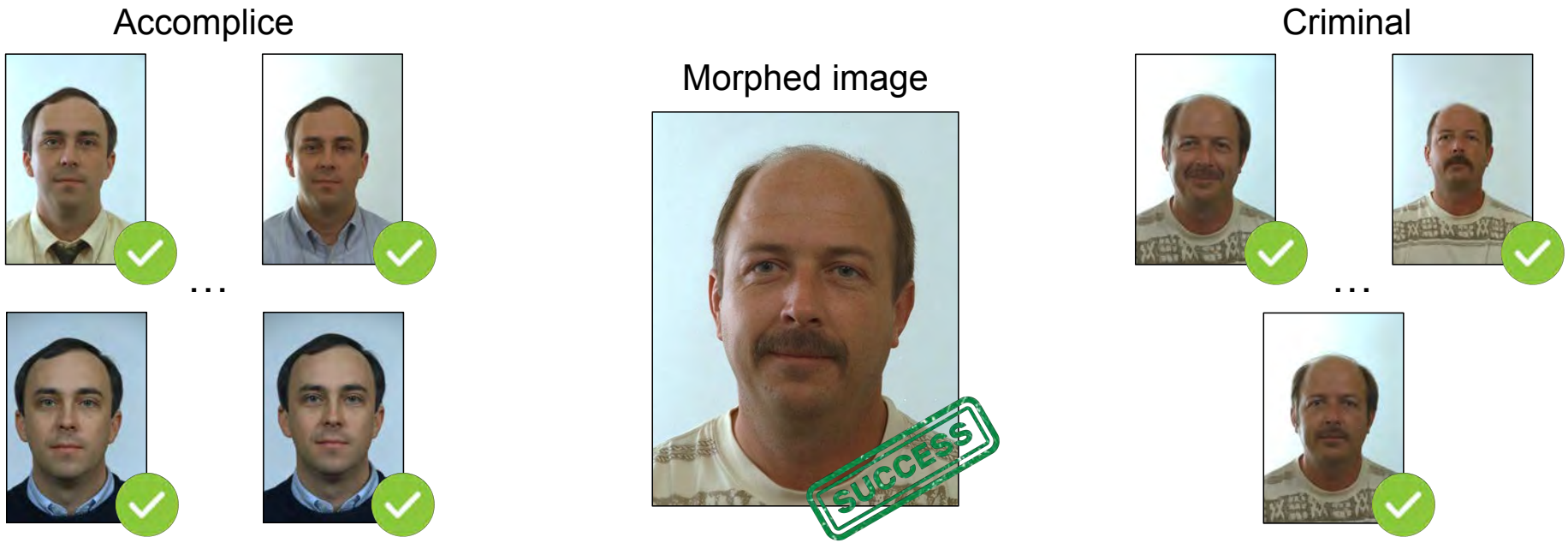
Source: M. Ferrara, IWBF-2022

[SNRG+17] 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 BIOSIG, (2017)

Measure the Vulnerability

Fully Mated Morph Presentation Match Rate (FMMPMR)

- A morphing attack succeeds if the morphed image can be successfully verified against all probe images of each subject.



Source: M. Ferrara, IWBF-2022

[Venk2020] S. Venkatesh, R. Raghavendra, K. Raja, C. Busch. "Face Morphing Attack Generation & Detection: A Comprehensive Survey." IEEE-TTS, (2021)

Morphing Attack Potential

The MMPMR and FMMPMR

- can only partially estimate the attack potential.

They do not take into account:

- multiple FRSs (generality);
- a variable number of verified probe images (robustness).

To extend these concepts [Fera2022]

- proposed a new metric called Morphing Attack Potential (MAP)
- that considers a variable number of attempts (frames acquired live at the gate) and multiple FRSs.

[Fera2022] M. Ferrara, A. Franco, D. Maltoni, C. Busch: "Morphing Attack Potential", in Proceedings of 10th International Workshop on Biometrics and Forensics (IWBF 2022), Salzburg, AT, April 20-21, (2022)

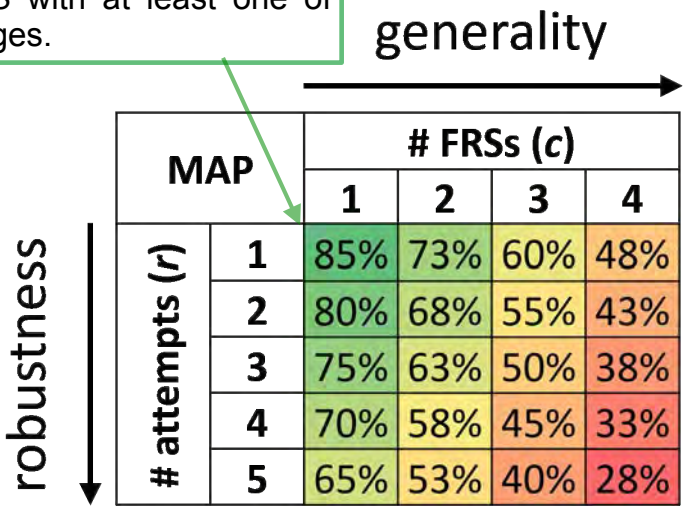
Morphing Attack Potential

Definition of Morphing Attack Potential (MAP)

- Given a dataset of morphed images $\mathbb{M}$, m probe images for each contributing subject and n FRSs to evaluate, MAP is defined as a matrix of size $m \; x \; n$ whose element $MAP[r,c]$ reports the proportion of morphed images successfully verified with both contributing subjects with at least r probe images by at least c FRSs.

85% of the morphed images fool at least one FRS with at least one of the probe images.

Example:
$m = 5$
$n = 4$



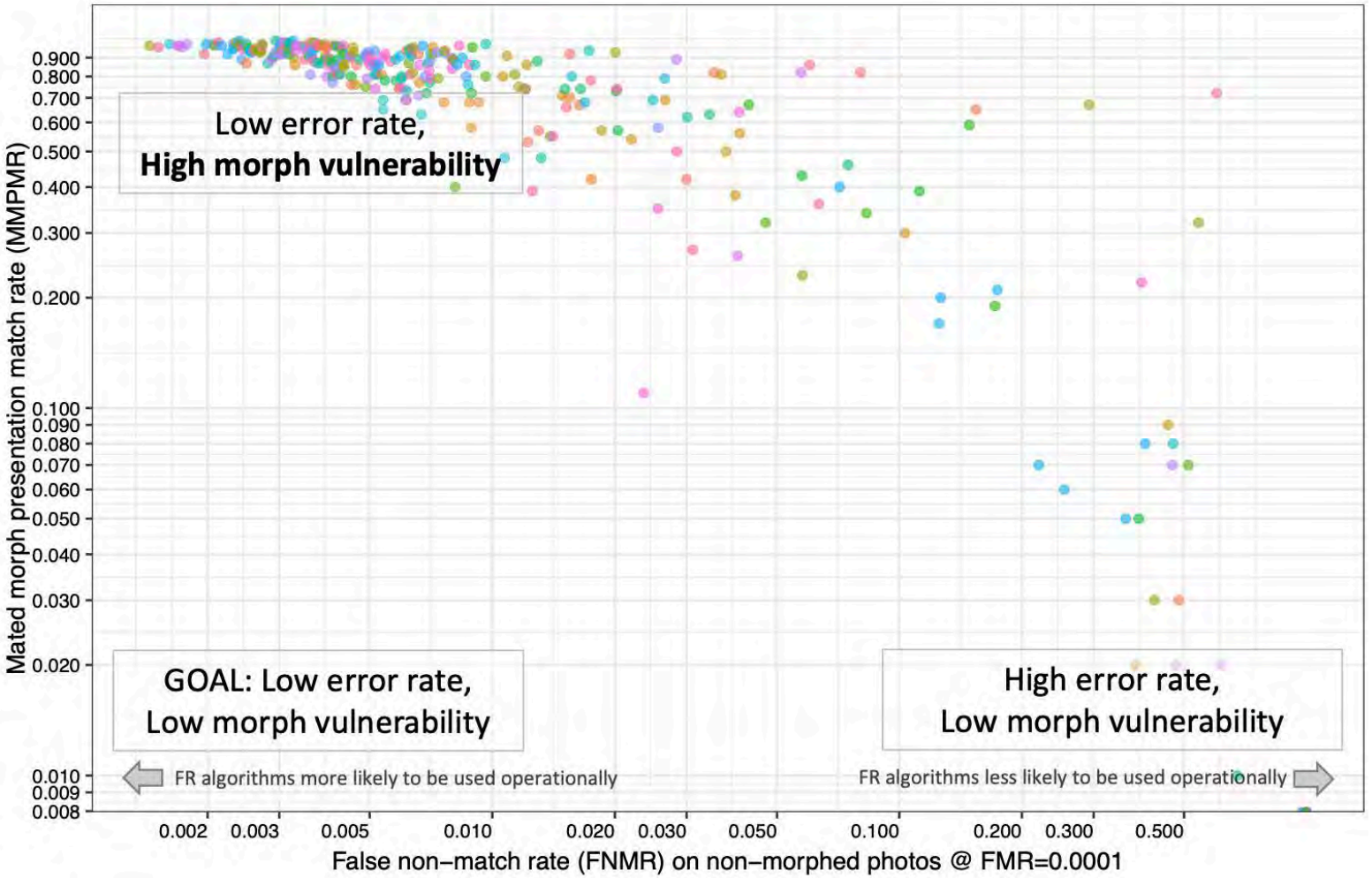
28% of the morphed images fool all four FRSs with all five probe images (MOST DANGEROUS).

[Fera2022] M. Ferrara, A. Franco, D. Maltoni, C. Busch: "Morphing Attack Potential", in Proceedings of 10th International Workshop on Biometrics and Forensics (IWBF 2022), Salzburg, AT, April 20-21, (2022)

Scale of the Problem: Vulnerability of FRS

NIST IR 8430 report on FRS vulnerability [Ngan2022]

- Accurate FRS are more vulnerable!



[Ngan2022] NIST IR 8430: "FRVT MORPH: Utility of 1:N Face Recognition Algorithms for Morph Detection", 2022
https://pages.nist.gov/frvt/reports/morph/frvt_morph_4A_NISTIR_8430.pdf

Scale of the Problem: Vulnerability of FRS

The morphing attack paradox

- The better the face recognition system (FRS)
  - the lower the false non-match rate (FNMR)
  - the more tolerant is the FRS at the defined FMR (e.g. 0.01 %)
- The more tolerance the FRS has
  - the more vulnerability we can observe
- Accurate FRS are more vulnerable!

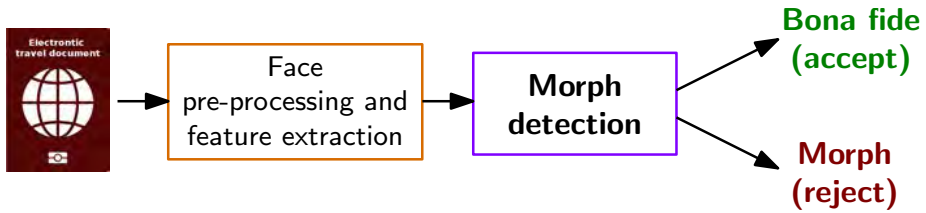
Morphing Attack Detection (MAD)

Scenarios and Methods

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)

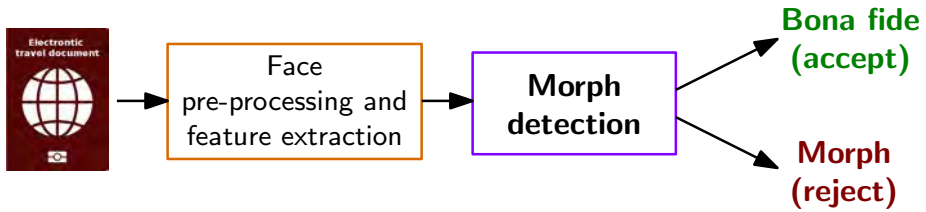


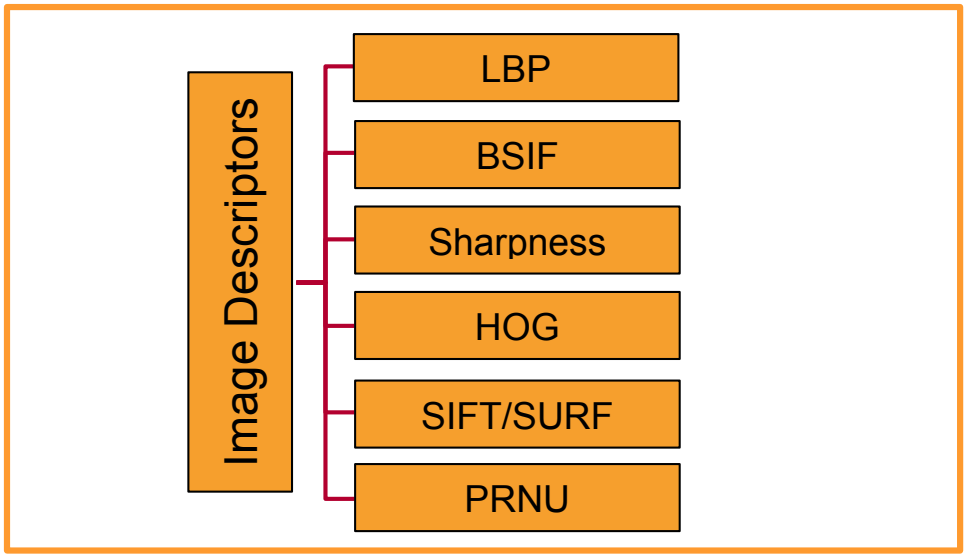
[SRB2018a] U. Scherhag, C. Rathgeb, C. Busch: "Towards Detection of Morphed Face Images in electronic Travel Documents“, in Proceedings of the 13th IAPR International Workshop on Document Analysis Systems (DAS), April 24-27, (2018)

Face Pre-processing and Feature Extraction

Morphing Attack Detection (S-MAD) with texture analysis

- Image descriptors as hand-crafted features





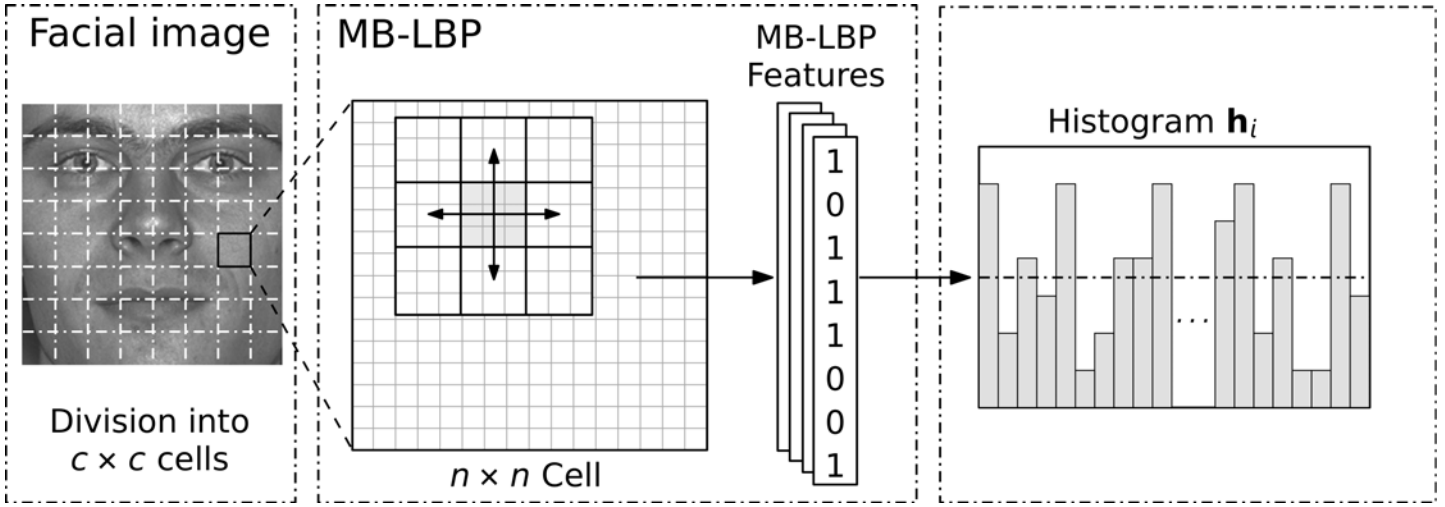
Morph Detection Classifier

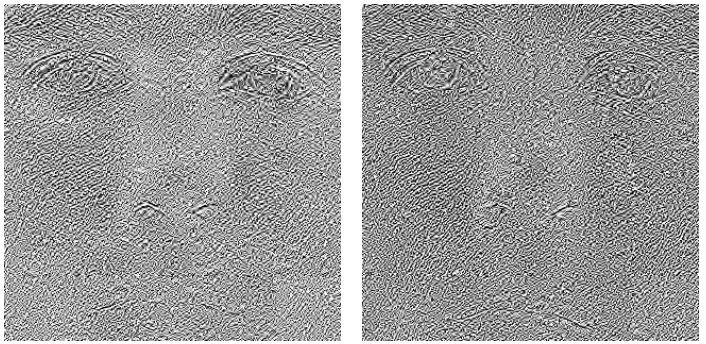
[SRB2018b] U. Scherhag, C. Rathgeb, C. Busch: „Detection of Morphed Faces from Single Images: a Multi-Algorithm Fusion Approach“, in Proceedings if of the 2nd International Conference on Biometric Engineering and Applications (ICBEA), Amsterdam, The Netherlands, May 16-18, (2018)

Face Pre-processing and Feature Extraction

S-MAD with image descriptor

- Local Binary Pattern (LBP)





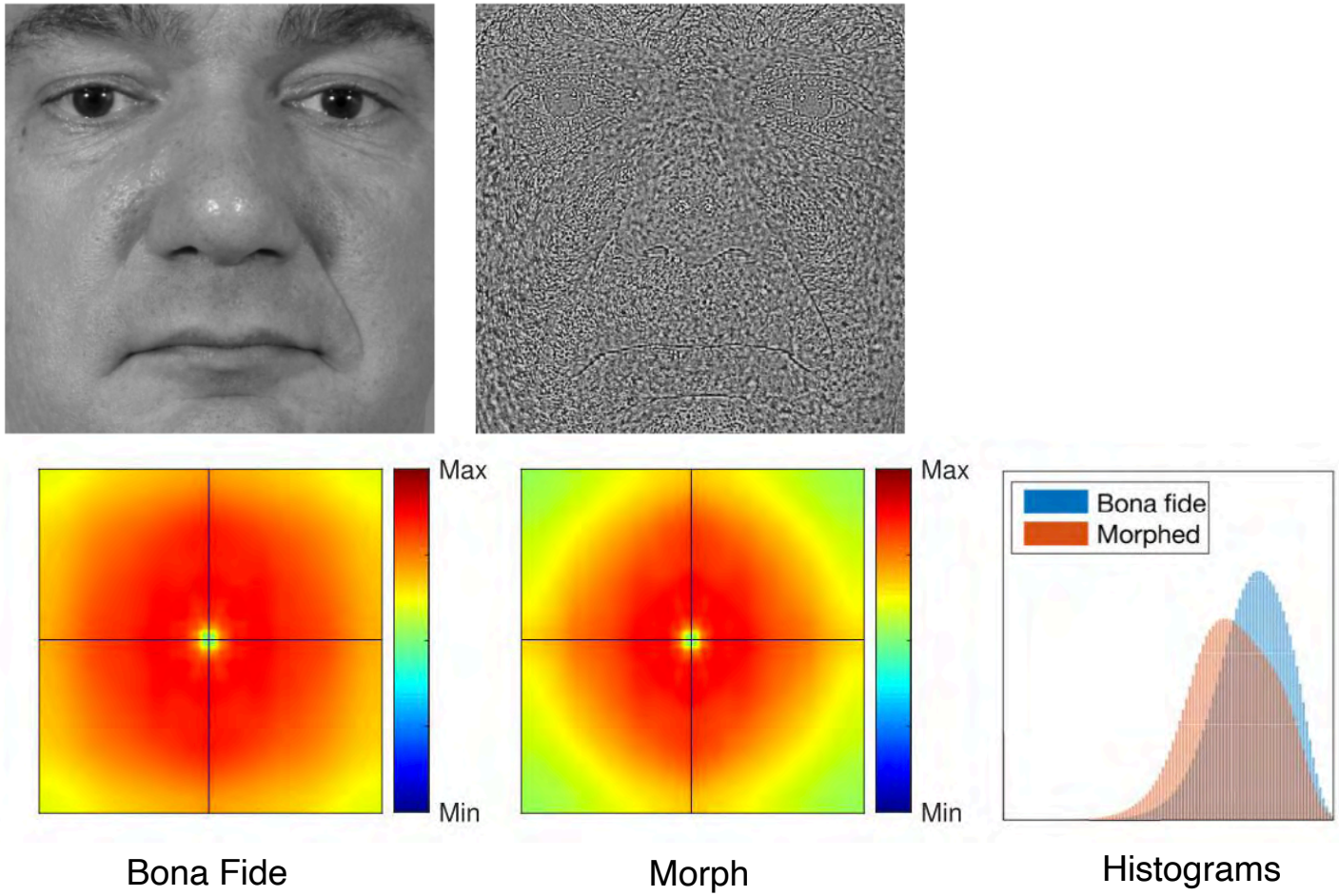
Morph

Bona Fide

Face Pre-processing and Feature Extraction

S-MAD with image descriptor / forensic approach

- Photo Response Non-Uniformity (PRNU)



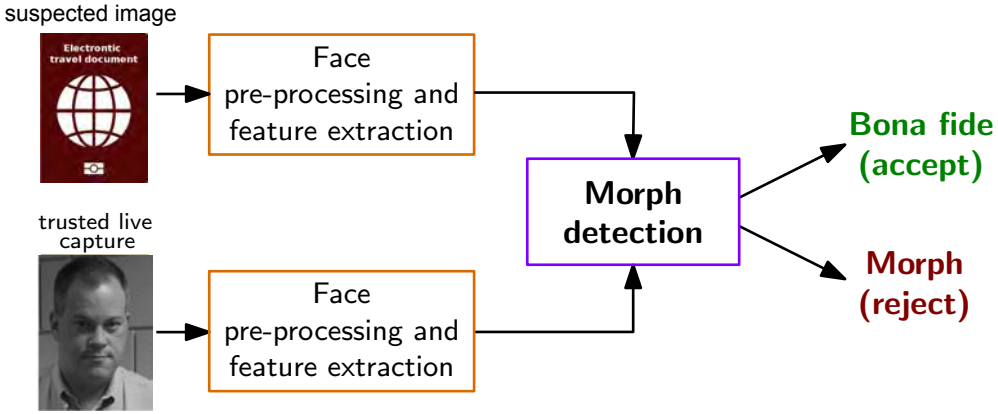
[SDRBU2019] U. Scherhag, L. Debiasi, C. Rathgeb, C. Busch and A. Uhl: "Detection of Face Morphing Attacks based on PRNU Analysis“, in IEEE TBIOM, (2019)

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)

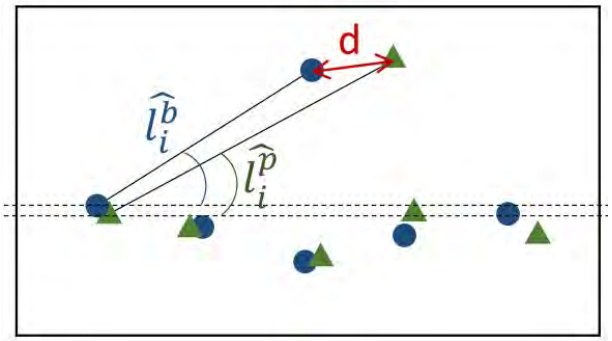


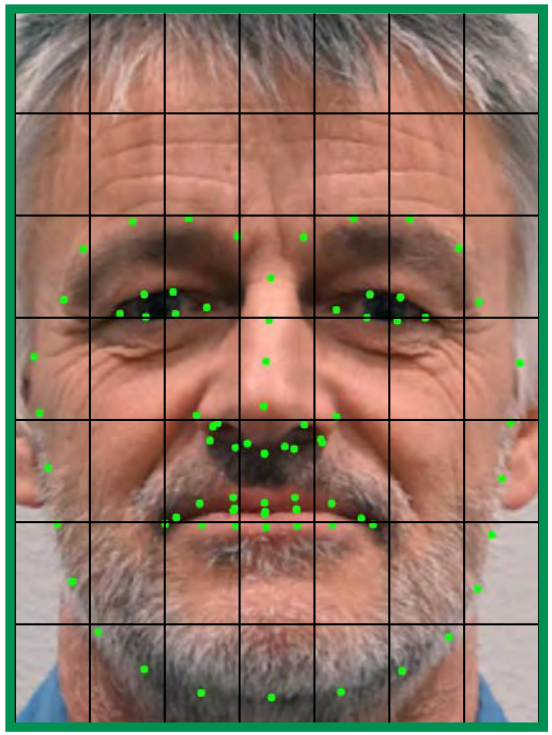
[SRB2018a] U. Scherhag, C. Rathgeb, C. Busch: "Towards Detection of Morphed Face Images in electronic Travel Documents", in Proceedings of the 13th IAPR International Workshop on Document Analysis Systems (DAS), April 24-27, (2018)

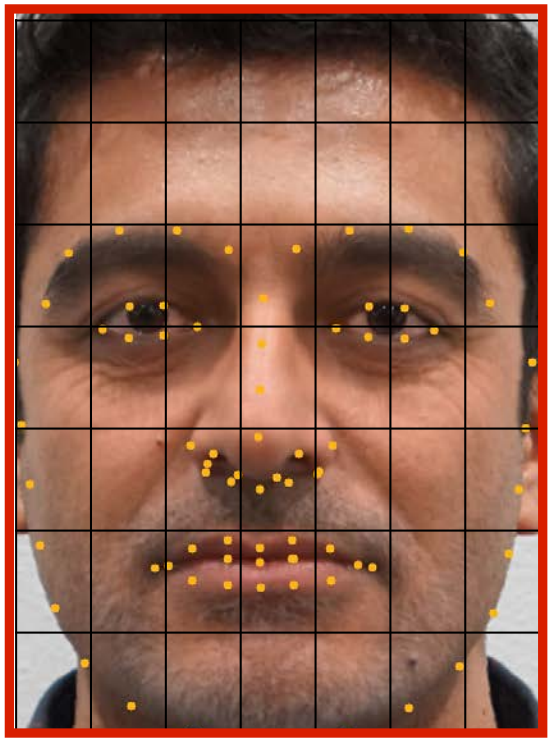
Differential Morphing Attack Detection

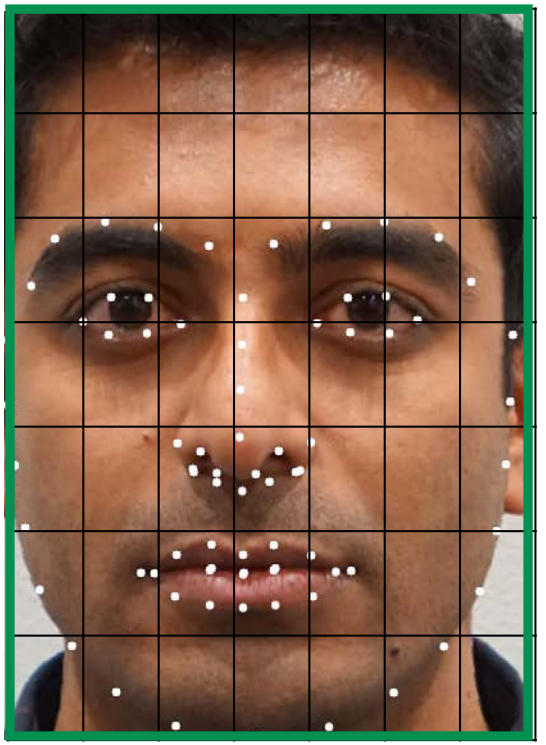
D-MAD with landmark analysis

- Angle based features
- Distance based features







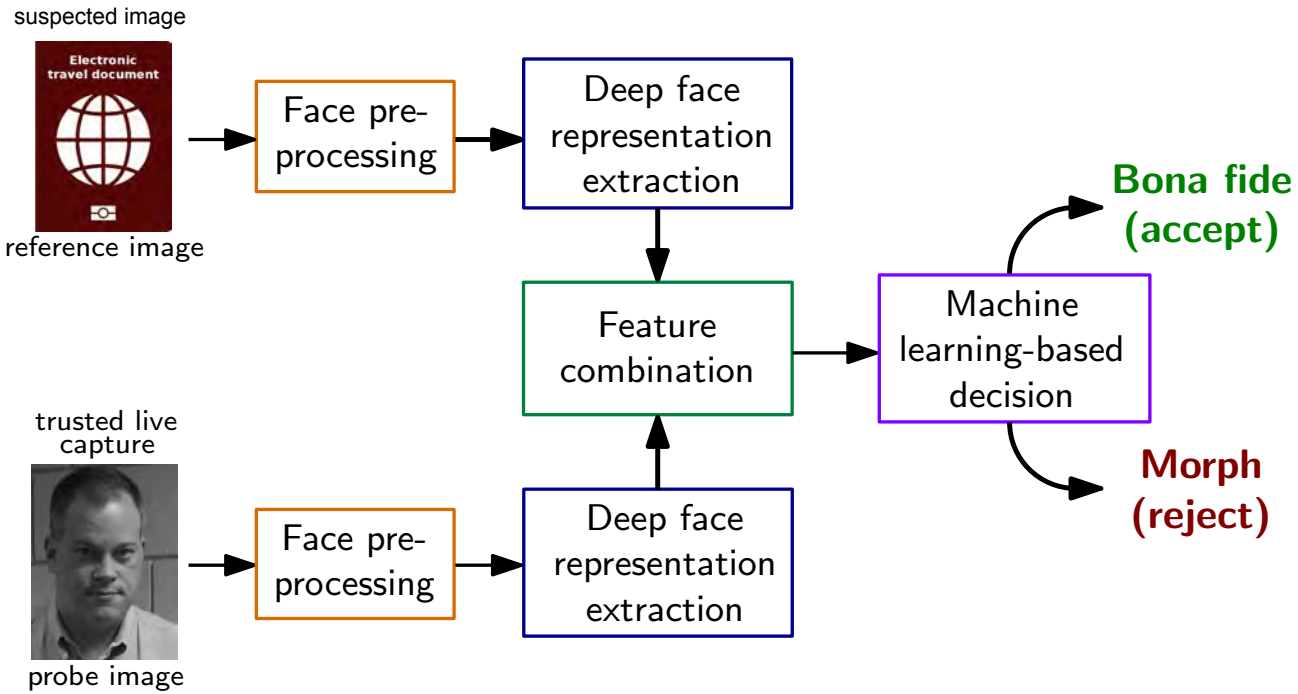


[SDGB2018] U. Scherhag, D. Budhrani, M. Gomez-Barrero, C. Busch: "Detecting Morphed Face Images Using Facial Landmarks“, in Proceedings of International Conference on Image and Signal Processing (ICISP), (2018)

Differential Morphing Attack Detection

D-MAD with deep learning

- Deep Face representations of Deep CNNs



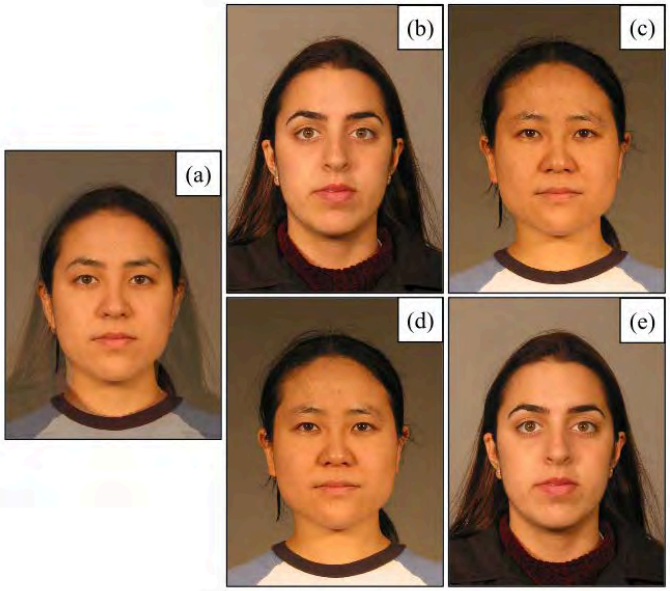
- Deep representations extracted by the neural network (on the lowest layer)
- Feature space with small dimension: 512 (for ArcFace)
- SVM with radial basis function

[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)

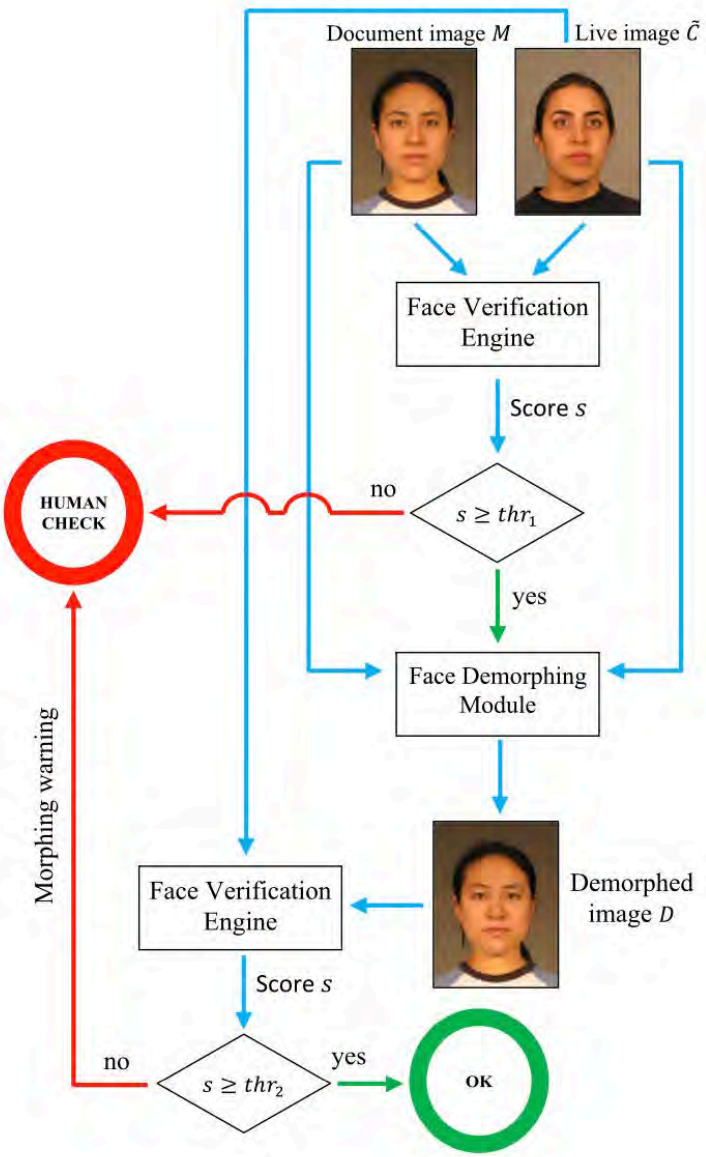
Differential Morphing Attack Detection

D-MAD with Demorphing

- Invert the morphing process
- Then confirm the similarity score



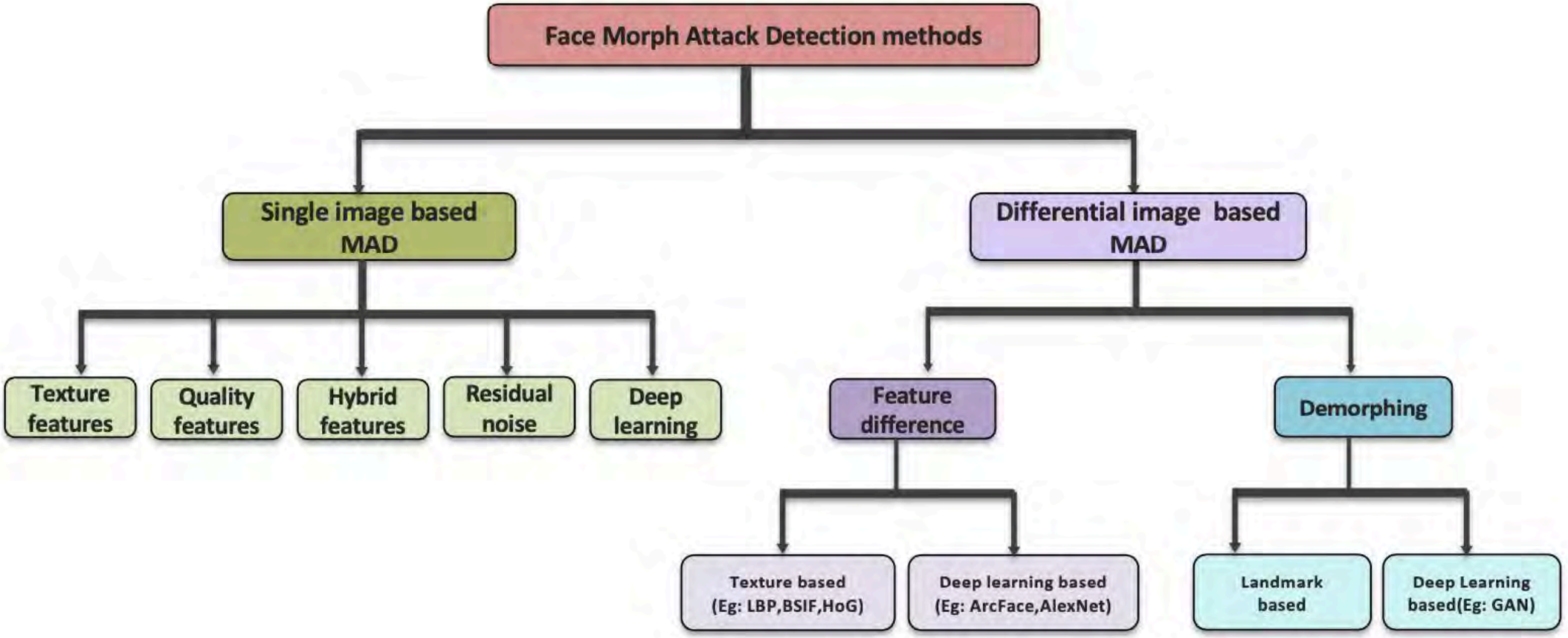
a): morphed image / suspected image
b) and c): trusted live capture image
d): recovered image obtained from a) and b)
e): recovered image obtained from a) and c)



[Ferrara2018] M. Ferrara, A. Franco, D. Maltoni: "Face Demorphing“, in IEEE Transactions on Information Forencics and Security (TIFS), (2018)

State of the Art - MAD Algorithms

Taxonomy of Morphing Attack Detection



[Venkatesh2021] 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)

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

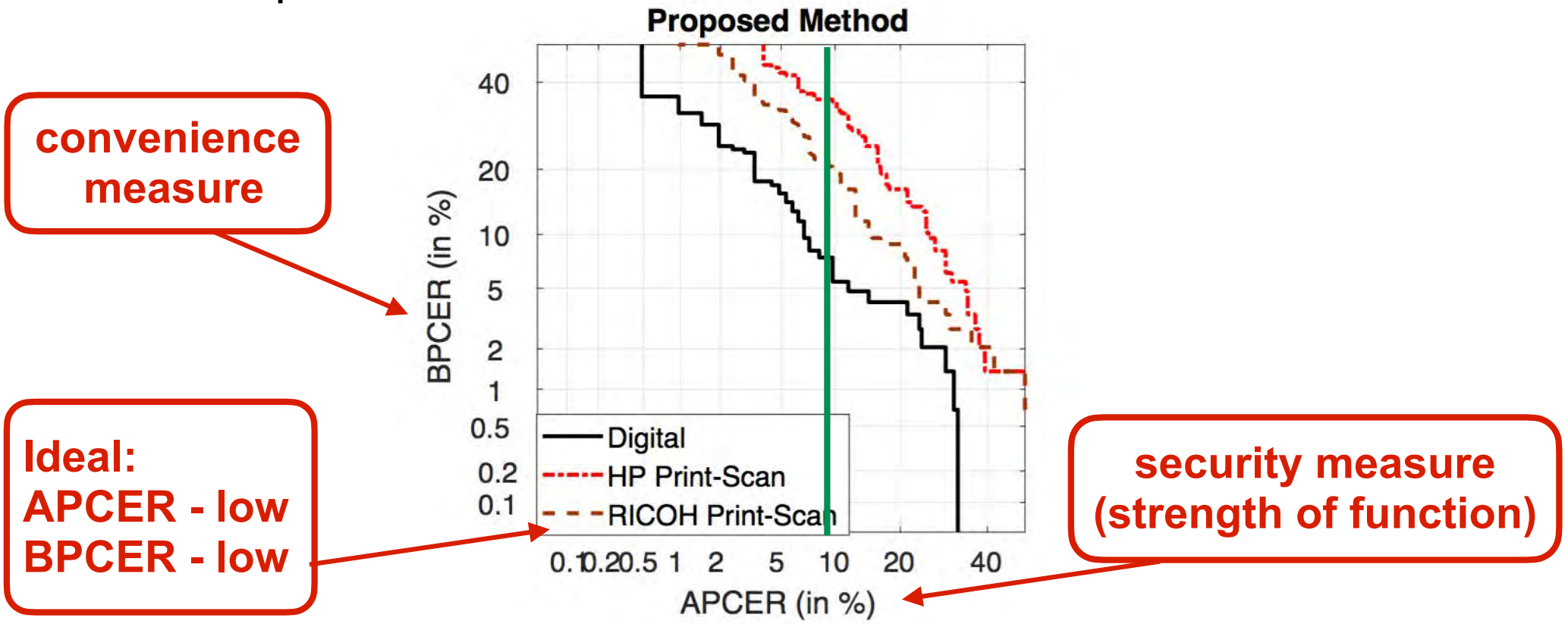
- **Bona fide presentation classification error rate (BPCER)**
  proportion of bona fide presentations incorrectly classified as attack presentations in a specific scenario

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 convenience measures over security 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 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



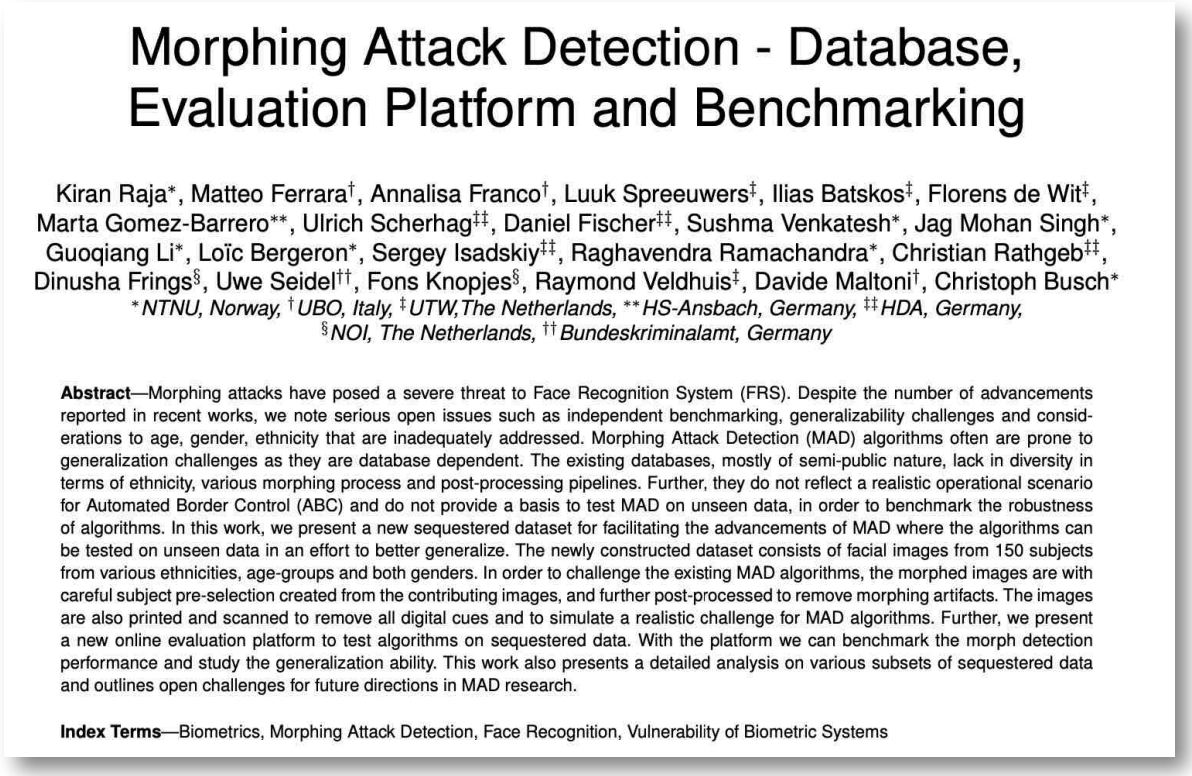

Specific objectives:

- Capture face images from 150 subjects
  - with photo equipment and automated border control gates
- Generate morphed face images with multiple algorithms
- Post-process automatically and manually
- Print and scan all morphed face images
- MAD Test on the Bologna-Online-Evaluation-Platform (BOEP)
  - Provide open access benchmark tests.
  - D-MAD evaluation:
    https://biolab.csr.unibo.it/FVCOnGoing/UI/Form/BenchmarkAreas/BenchmarkAreaDMAD.aspx

Research on Morphing Attack Detection

MAD Evaluation in SOTAMD

- SOTAMD dataset and BOEP testing platform
  https://ieeexplore.ieee.org/document/9246583



Morphing Attack Detection - Database, Evaluation Platform and Benchmarking

Kiran Raja*, Matteo Ferrara†, Annalisa Franco†, Luuk Spreeuwers‡, Ilias Batskos‡, Florens de Wit‡, Marta Gomez-Barrero**, Ulrich Scherhag‡‡, Daniel Fischer‡‡, Sushma Venkatesh*, Jag Mohan Singh*, Guoqiang Li*, Loïc Bergeron*, Sergey Isadskiy‡‡, Raghavendra Ramachandra*, Christian Rathgeb‡‡, Dinusha Frings§, Uwe Seidel††, Fons Knopjes§, Raymond Veldhuis‡, Davide Maltoni†, Christoph Busch*
*NTNU, Norway, †UBO, Italy, ‡UTW,The Netherlands, **HS-Ansbach, Germany, ‡‡HDA, Germany, §NOI, The Netherlands, ††Bundeskriminalamt, Germany

Abstract—Morphing attacks have posed a severe threat to Face Recognition System (FRS). Despite the number of advancements reported in recent works, we note serious open issues such as independent benchmarking, generalizability challenges and considerations to age, gender, ethnicity that are inadequately addressed. Morphing Attack Detection (MAD) algorithms often are prone to generalization challenges as they are database dependent. The existing databases, mostly of semi-public nature, lack in diversity in terms of ethnicity, various morphing process and post-processing pipelines. Further, they do not reflect a realistic operational scenario for Automated Border Control (ABC) and do not provide a basis to test MAD on unseen data, in order to benchmark the robustness of algorithms. In this work, we present a new sequestered dataset for facilitating the advancements of MAD where the algorithms can be tested on unseen data in an effort to better generalize. The newly constructed dataset consists of facial images from 150 subjects from various ethnicities, age-groups and both genders. In order to challenge the existing MAD algorithms, the morphed images are with careful subject pre-selection created from the contributing images, and further post-processed to remove morphing artifacts. The images are also printed and scanned to remove all digital cues and to simulate a realistic challenge for MAD algorithms. Further, we present a new online evaluation platform to test algorithms on sequestered data. With the platform we can benchmark the morph detection performance and study the generalization ability. This work also presents a detailed analysis on various subsets of sequestered data and outlines open challenges for future directions in MAD research.

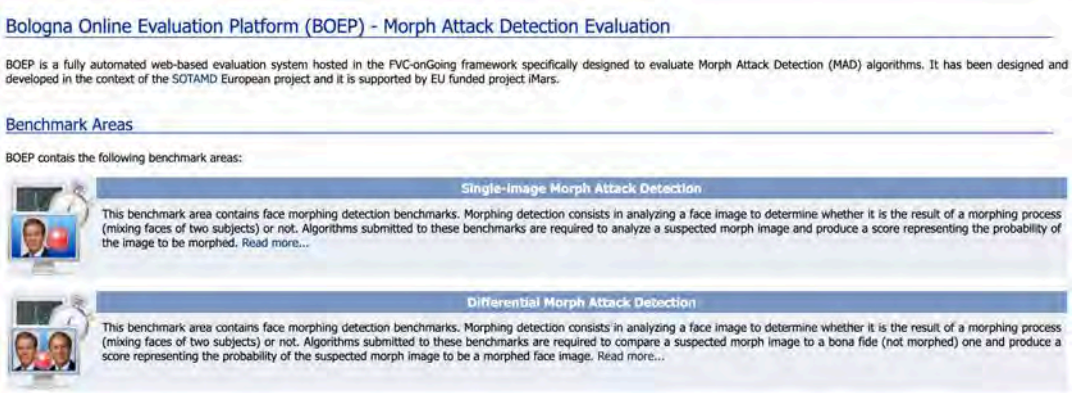
Index Terms—Biometrics, Morphing Attack Detection, Face Recognition, Vulnerability of Biometric Systems

[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)

MAD Evaluation

Bologna Online Evaluation Platform (BOEP)

- A new benchmark area for morphing attack detection
  https://biolab.csr.unibo.it/fvcongoing/UI/Form/BOEP.aspx



- Both scenarios: D-MAD and S-MAD
- 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.

NIST FRVT MORPH

NIST IR 8292 report presented September, 2022

FRVT MORPH

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

- results for MAD algorithms from six research labs:
  - University of Bologna (UBO)
  - Norwegian University of Science and Technology (NTNU)
  - Hochschule Darmstadt (HDA)
  - West Virginia University (WVU)
  - Universidade de Coimbra (VIS)
  - secunet (SEC)

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

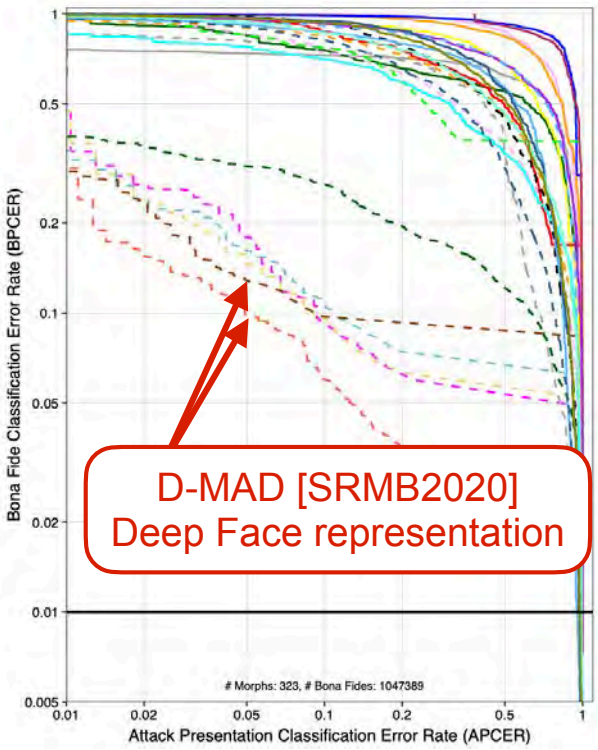
This publication is available free of charge from:
https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

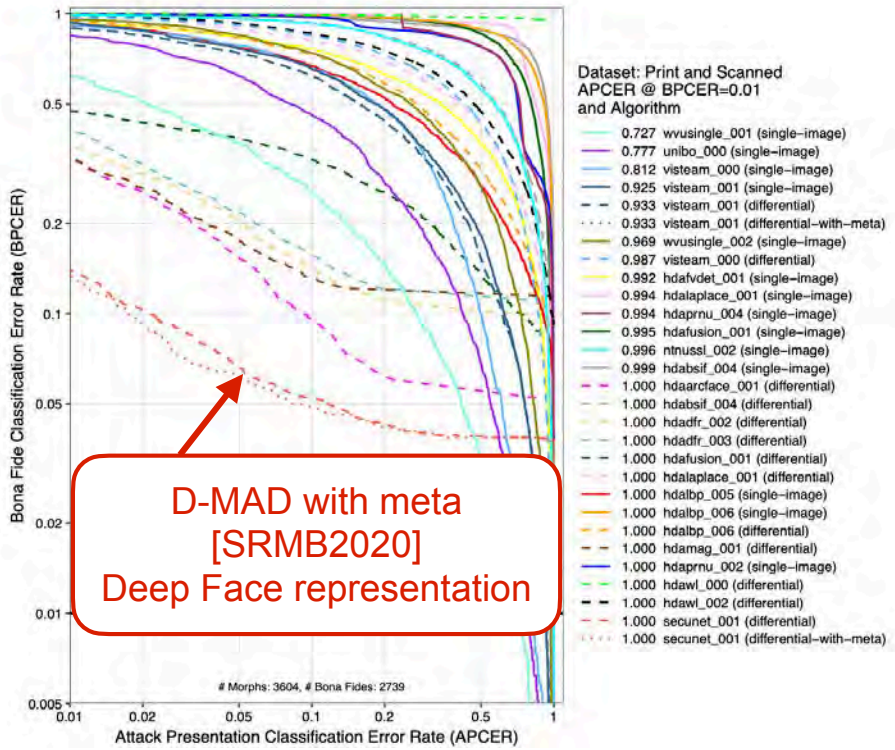
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

NIST FRVT MORPH

NIST IR 8292 report presented September, 2022

- 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 morphs
  - note the low number of print and scanned images





The iMARS Project on MAD

The Key Figures

iMARS project

- image Manipulations Attack Resolving Solutions (iMARS)
- Start date: 1 September 2020
- End date: 31 August 2024
- H2020-SU-SEC-2019
- Grant agreement ID: 883356
- Topic:
  - SU-BES02-2018-2019-2020 -
    Technologies to enhance border and external security
- Overall budget: € 6 988 521,25
- Website: https://imars-project.eu/

The iMARS Consortium

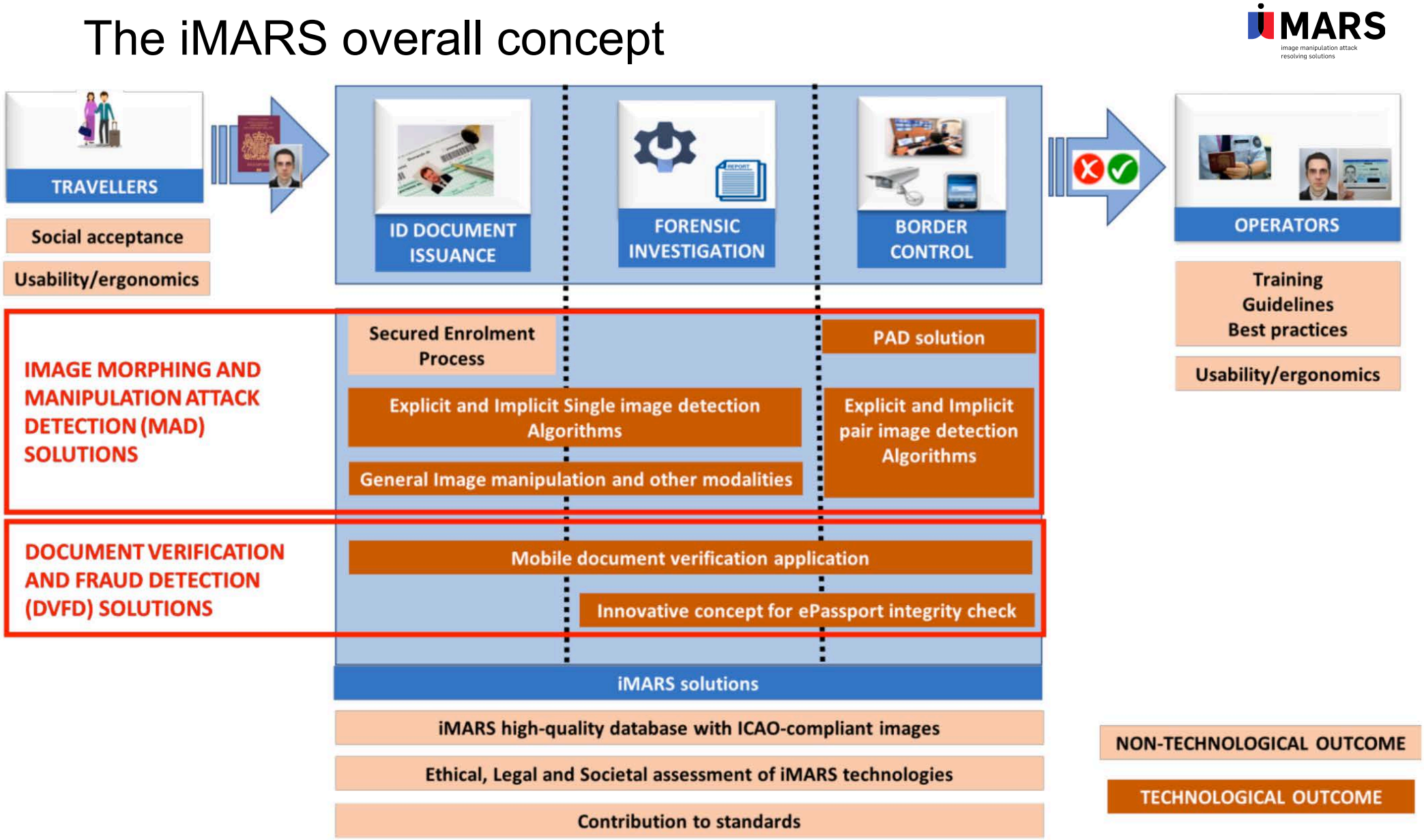
24 Partners

- 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)
- UTW - UNIVERSITY OF TWENTE (NL)
- 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)

iMARS
image manipulation attack
resolving solutions

The iMARS Research

The iMARS overall concept



Human Experts in MAD

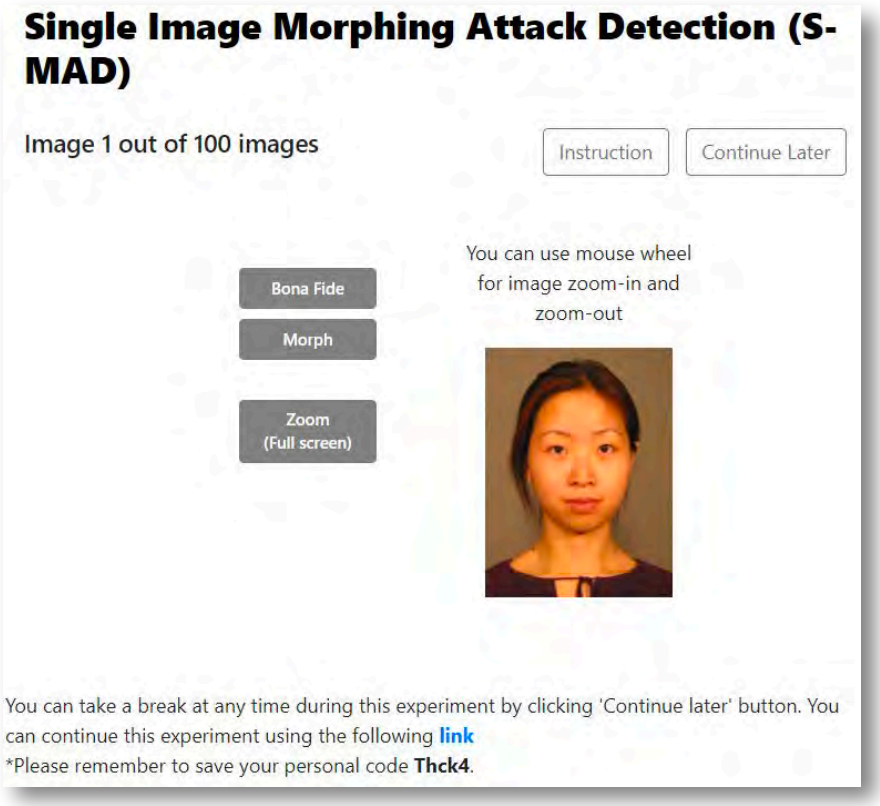
Many unanswered questions:

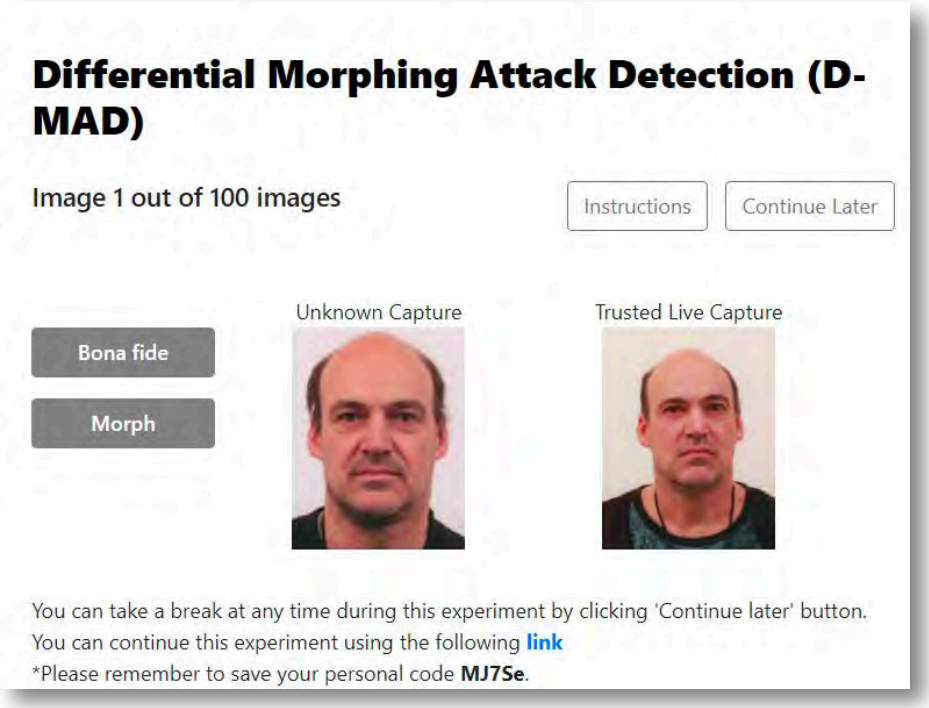
- How good are ID document examiners at detecting morphing attacks?
- Are human observers with certain types of training better than others at detecting morphing attacks?
- Are expert observers with training or experience in checking identity/identity documents better than those without training?
- How do machine-based MAD algorithms perform compared to human observers in D-MAD and S-MAD?

Human Experts in MAD

Border guards, case handlers, document examiners, ID experts

- S-MAD: 410 participants, 400 trials (4 x 100 tasks)
- D-MAD: 469 participants, 180 trials

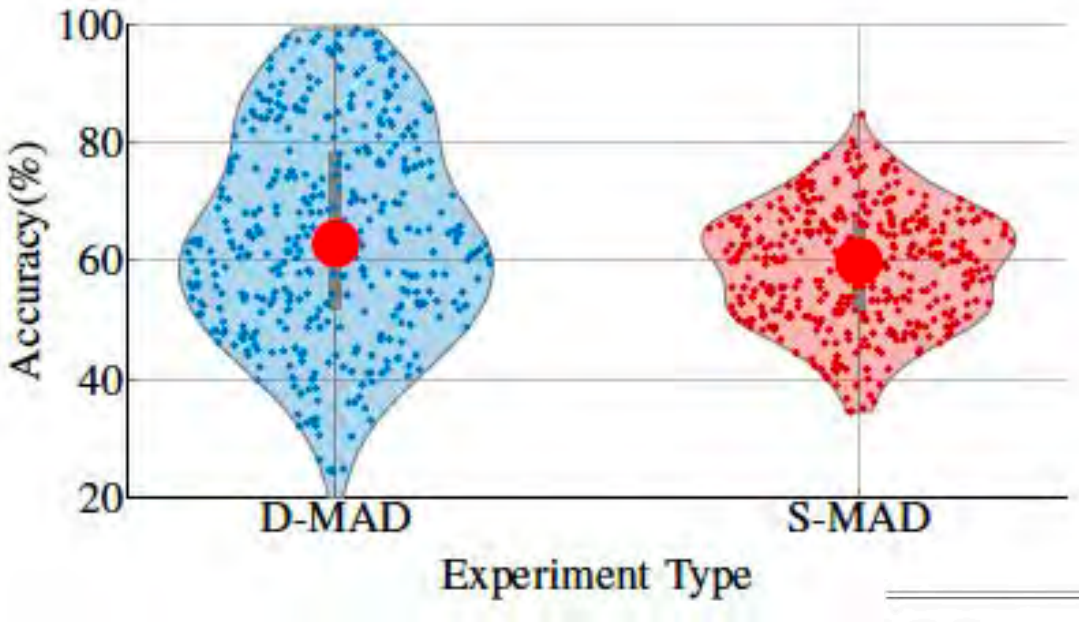




[GOD2022] S. Godage, F. Løvåsdal, S. Venkatesh, K. Raja, R. Raghavendra, C. Busch: “Analyzing Human Observer Ability in Morphing Attack Detection - Where Do We Stand?”, https://arxiv.org/abs/2202.12426

Human Experts in MAD

Overall accuracy

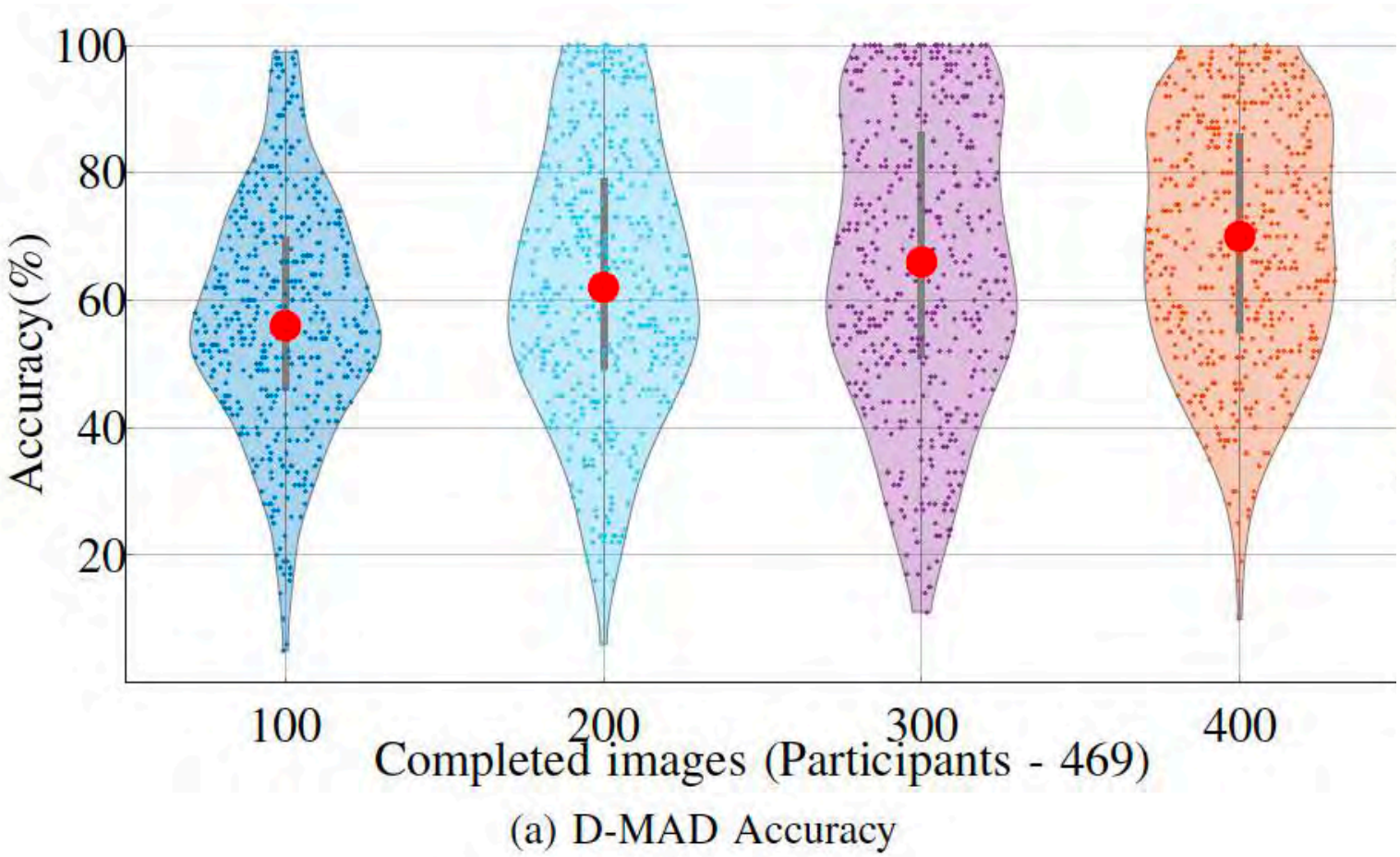


Line of work	D-MAD		S-MAD	
	Number of participants	Average Accuracy	Number of participants	Average Accuracy
Border Guard	30	64.66	26	55.17
Case handler- Passport, visas, ID, etc	150	63.45	137	56.65
Document examiner- 1st line	38	60.79	30	57.63
Document examiner- 2st line	40	68.64	34	62.56
Document examiner- 3rd line	30	65.74	25	61.51
Face comparison expert (Manual examination)	44	72.56	39	64.63
ID Expert	53	63.09	50	57.21
Other	84	64.66	69	55.17
Student	103	56.91	-	-
Total participants	572		410	
Experts	469		410	

[GOD2022] S. Godage, F. Løvåsdal, S. Venkatesh, K. Raja, R. Raghavendra, C. Busch: “Analyzing Human Observer Ability in Morphing Attack Detection - Where Do We Stand?”, https://arxiv.org/abs/2202.12426

Human Experts in MAD

Does exposure to morphed images help?



(a) D-MAD Accuracy

[GOD2022] S. Godage, F. Løvåsdal, S. Venkatesh, K. Raja, R. Raghavendra, C. Busch: “Analyzing Human Observer Ability in Morphing Attack Detection - Where Do We Stand?”, https://arxiv.org/abs/2202.12426

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 - at least for the upcoming 10 years
- Passports with morphed face images
  will have a major impact on border security
  - introduction of EU's entry/exit system
- In combination with passport brokers a dramatic problem
  - the darknet offers numerous opportunities …

- Summary: MAD is the hardest challenge that I have seen
  in my 25 research years on biometrics

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

More information on MAD

The 2021 NBL - EAB workshop

https://eab.org/events/program/229

- Luuk Spreeuwers (University of Twente) - recorded talk
  - Morphing Attacks on Face Recognition Systems
- David Robertson (University of Strathclyde) - recorded talk
  - Psychological Experiments on Morphed Faces
- Kiran Raja (NTNU) - recorded talk
  - Morphing Attack Detection Approaches
- Matteo Ferrara (University of Bologna) - recorded talk
  - Bologna Online Evaluation Platform
- Frøy Løvåsdal (Norwegian Police) - recorded talk
  - Morphing Attack Detection Capabilities of Human Examiners
- Mei Ngan (NIST) - recorded talk
  - Face Morphing Detection Evaluation
- Naser Damer (Fraunhofer IGD) - recorded talk
  - Generating Morphs with Generative Adversarial Networks
- Christian Rathgeb (Hochschule Darmstadt) - recorded talk
  - Detection of Face Beautification Manipulations
- Uwe Seidel (BKA)
  - Research Needs for Morphing Attack Detection

More Information on MAD

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.
- Free membership for master and PhD students!
  https://eab.org/membership/types_of_membership.html

More Information on MAD

National Institute of Standards and Technology (NIST)

- Will host the virtual
  3rd International Face Performance Conference (IFPC)
- November 15 - 17, 2022.
- The registration is open and free.
- The first draft agenda is posted at:
  https://www.nist.gov/news-events/events/2022/11/international-face-performance-conference-ifpc-2022
- The presentations:
  - Matjaž Torkar (Ministry of the Interior Police, Slovenia)
    - Morphing Cases in Slovenia
  - Matteo Ferrara (University of Bologna)
    - Morphing Attack Potential (MAP)
  - Nasser Nasrabadi (West Virginia University)
    - Face Morph Generation and Attack Detection
  - Kiran Raja (Norwegian University of Science and Technology)
    - Overview on Morph Attack Detection Development
  - Frøy Løvåsdal (National Police Directorate, Norway)
    - Morphing Attack Detection - Analysing Human Observer Ability

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.

Thanks

I would like to thank my colleagues working on this topic:

- In the NBL - HDA research group:
  - Kiran Raja, Raghu Ramachandra, Loic Bergeron, Sankini Godage, Guoqiang Li, Jag Mohan Singh, Sushma Venkatesh, Haoyu Zhang
  - Ulrich Scherhag, Christian Rathgeb, Daniel Fischer, Siri Lorenz, Robert Nichols Sergey Isadskiy, Marta Gomez-Barrero, Juan Tapia, Mathias Ibsen
- In the FACETRUST-Project:
  - Ralph Breithaupt, Johannes Merkle
- In the SOTAMD-Project and iMARS-Project:
  - Dinusha Frings, Fons Knopjes, Uwe Seidel, Frøy Løvåsdal
  - Davide Maltoni, Matteo Ferrara, Analisa Franco
  - Raymond Veldhuis, Luuk Spreeuwers,
- In the NIST-FRVT-MORPH-Project:
  - Mei Ngan, Patrick Grother, Kayee Hanaoka, Jason Kuo

Contact

Research opportunities

- Darmstadt (Germany) https://dasec.h-da.de/
- Gjøvik (Norway) https://www.ntnu.edu/nbl
- Internships possibility for Msc and PhD students with travel grant
- Collaboration with governmental and industrial partners