Morphing Attack Detection

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

2023 EAB and CITeR Biometrics Workshop
April 19, 2023

ATHENE

MARS

NORWEGIAN BIOMETRICS LABORATORY

NTNU

Overview

Agenda

- Vulnerability of Face Recognition Systems
- Morphing Attack Detection (MAD) - Scenarios and Methods
- Automated Face Morphing Attack Detection
- Human examiners at Face Morphing Attack Detection
- Conclusion

Border Security depends on Passport Security

The passport is the security anchor

- One individual - one passport

Principle of unique link of ICAO

- ICAO - International Civil Aviation Organisation
- 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/

Border Security depends on Passport Security

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

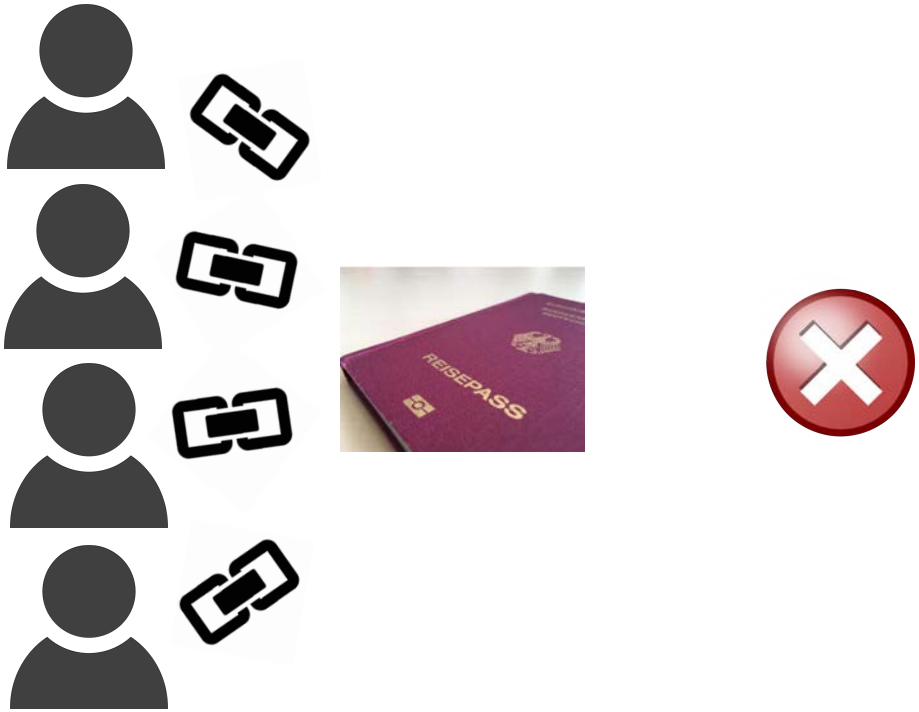


image source: https://pixabay.com/de/vectors/tick-sternchen-kreuz-rot-gr%C3%BCn-40678/

Border Control meeting Morphing Attacks

Is it a real 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

Solution for Morphing Attacks

Possible solutions to the Morphing Attack Problem:

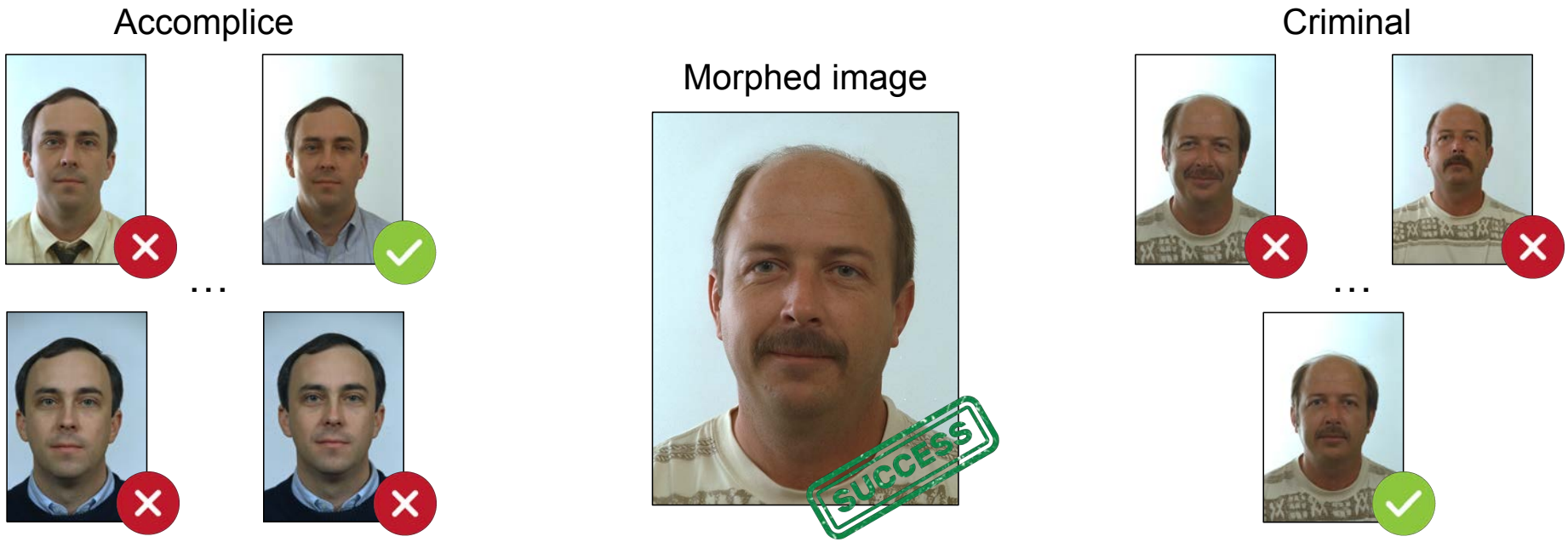
- 1.) Photo studio should digitally sign the picture taken by Photo Studio and send it to the passport application office
  - this is in progress for Finland
- 2.) Switch to live enrolment
  - that is the case for Norway, Sweden, Hungary
  - EU Regulation 2019/1157:
    on strengthening the security 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."
- 3.) Software-supported detection of morphed face images

What is the size of the problem?
What is the vulnerability of FRS?

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.



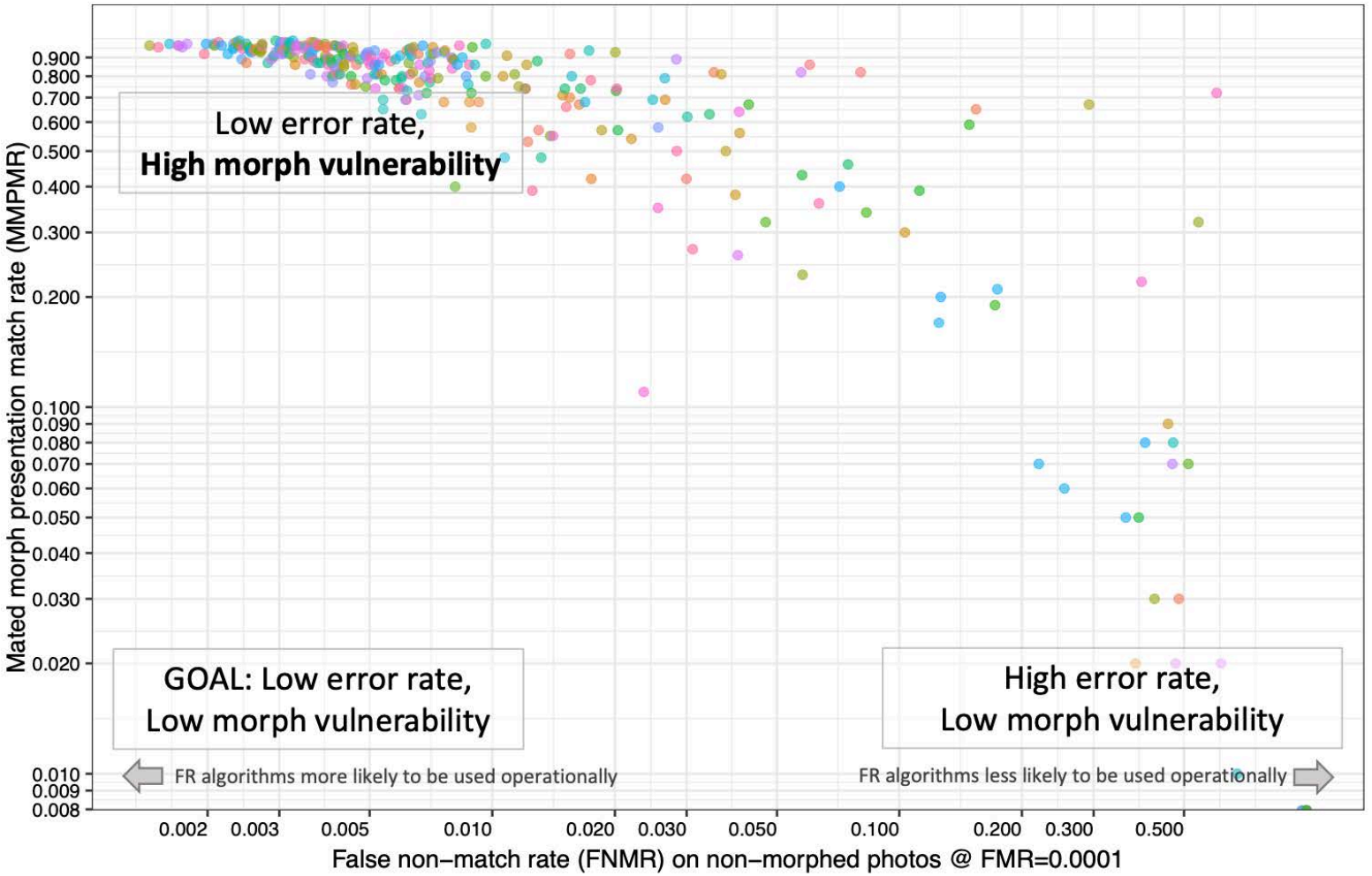
Source: M. Ferrara, IWBF-2022

[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)

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 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.

generality

MAP		# FRSs (c)			
		1	2	3	4
# attempts (r)	1	85%	73%	60%	48%
	2	80%	68%	55%	43%
	3	75%	63%	50%	38%
	4	70%	58%	45%	33%
	5	65%	53%	40%	28%

robustness

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

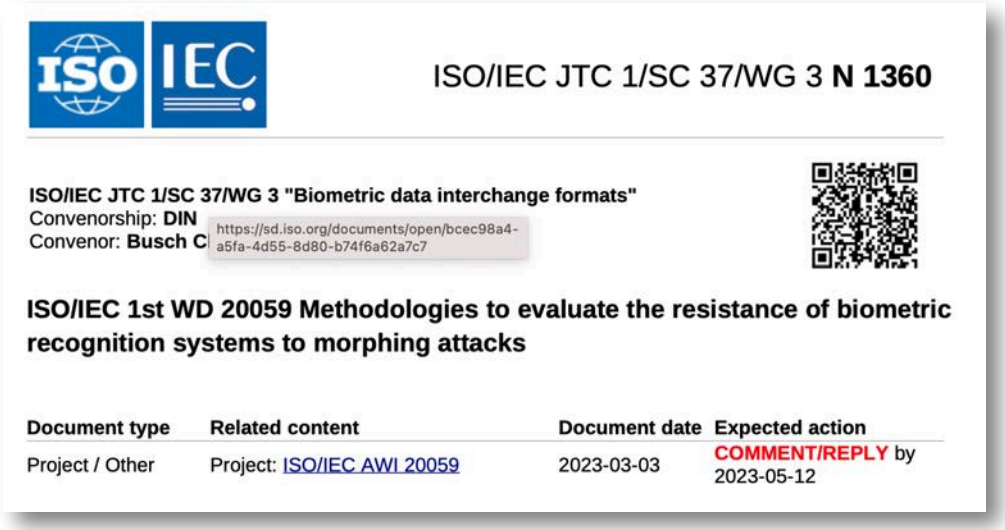
Example:
$m = 5$
$n = 4$

[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)

Standardisation

Evaluate the ~~vulnerability~~ / resistance of biometric recognition systems to morphing attacks

- ISO/IEC 20059 is based on the Morphing Attack Potential (MAP)
- Comments on the working draft are due on 2023-05-12



ISO/IEC JTC 1/SC 37/WG 3 **N 1360**

ISO/IEC JTC 1/SC 37/WG 3 "Biometric data interchange formats"
Convenorship: **DIN**
Convenor: **Busch C**
https://sd.iso.org/documents/open/bcec98a4-a5fa-4d55-8d80-b74f6a62a7c7

ISO/IEC 1st WD 20059 Methodologies to evaluate the resistance of biometric recognition systems to morphing attacks

Document type	Related content	Document date	Expected action
Project / Other	Project: ISO/IEC AWI 20059	2023-03-03	COMMENT/REPLY by 2023-05-12

- Join ISO/IEC JTC1 SC37: https://www.iso.org/members.html
- A free copy of ISO/IEC WD 20059 is available at: https://lnkd.in/dvbS6jxt

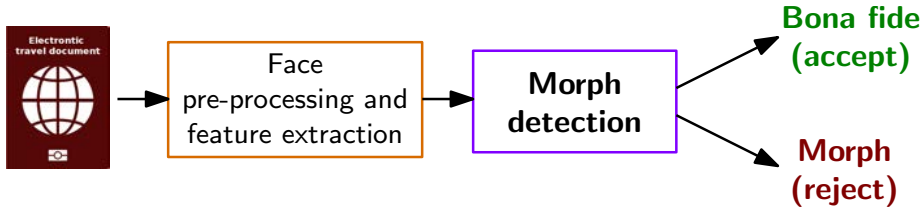
Morphing Attack Detection (MAD)

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)

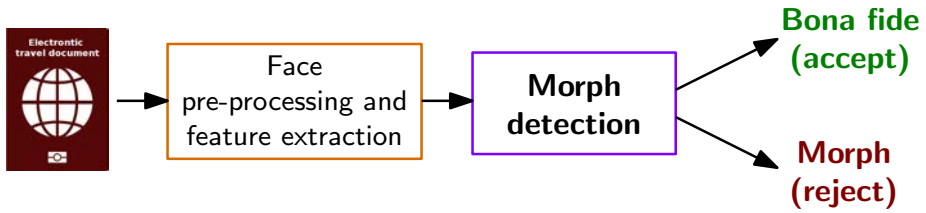


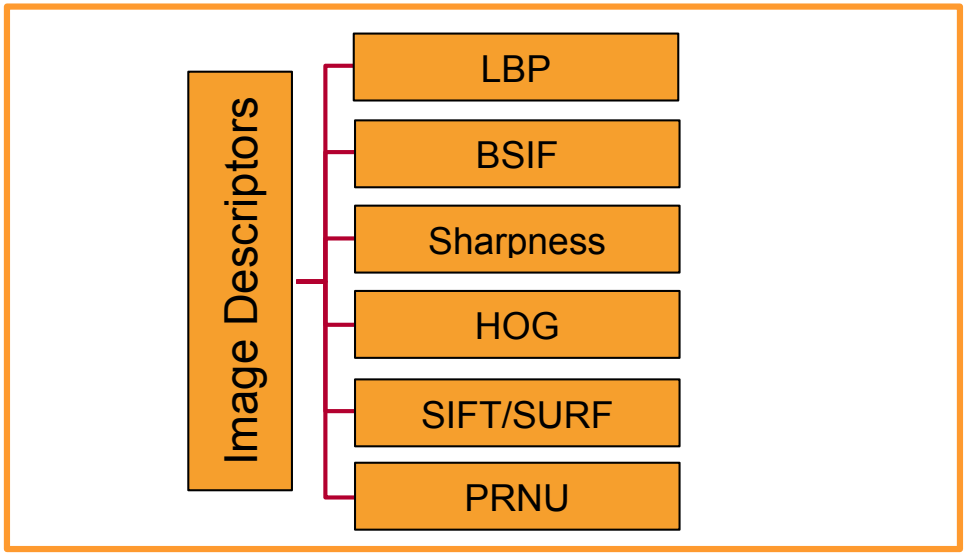
[SRB2018a] U. Scherhag, C. Rathgeb, C. Busch: "Towards Detection of Morphed Face Images in electronic Travel Documents“, in Proceedings of the 13th IAPR International Workshop on Document Analysis Systems (DAS), April 24-27, (2018)

Face Pre-processing and Feature Extraction

Morphing Attack Detection (S-MAD) with texture analysis

- Image descriptors as hand-crafted features





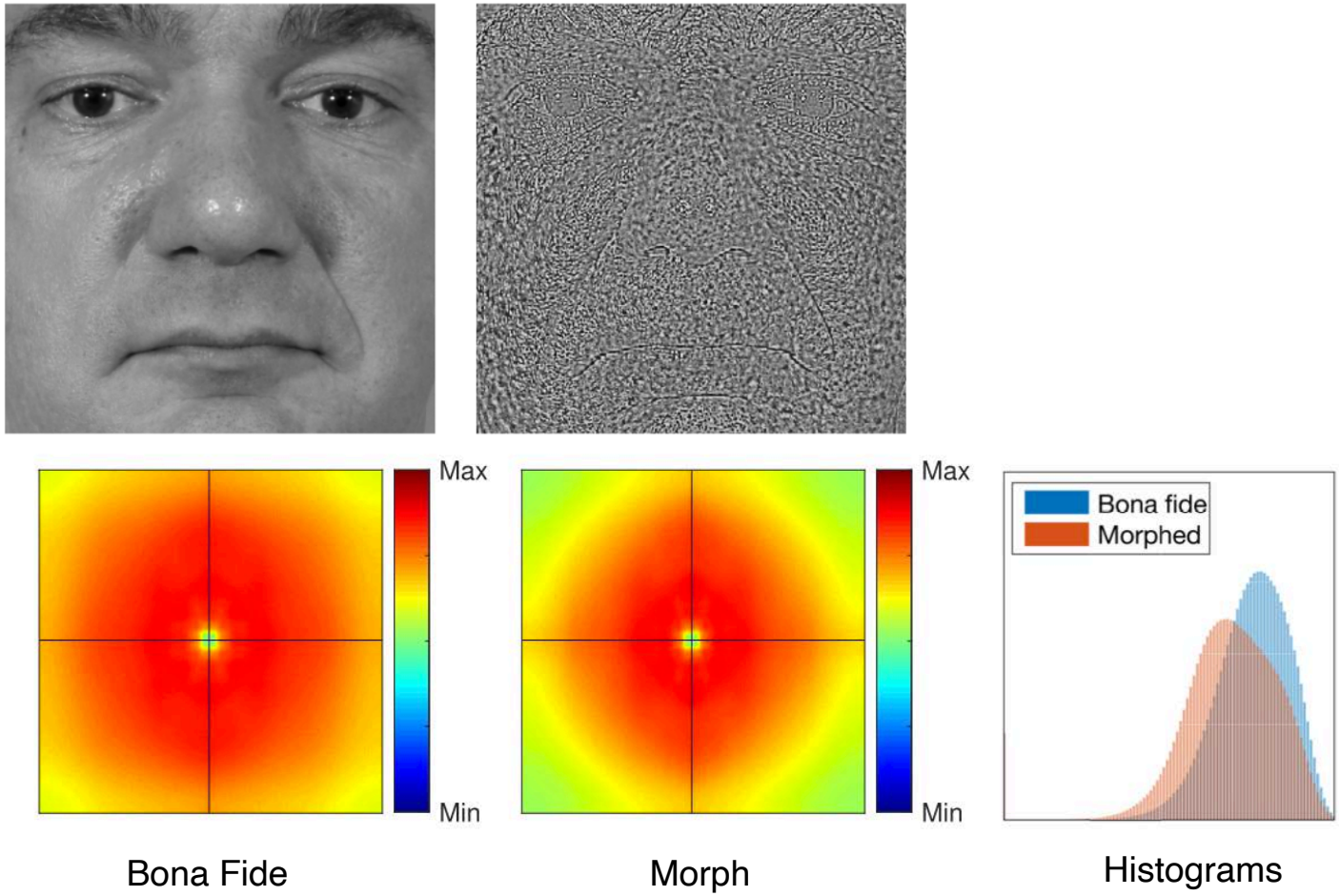
Morph Detection Classifier

[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 / forensic approach

- Photo Response Non-Uniformity (PRNU)



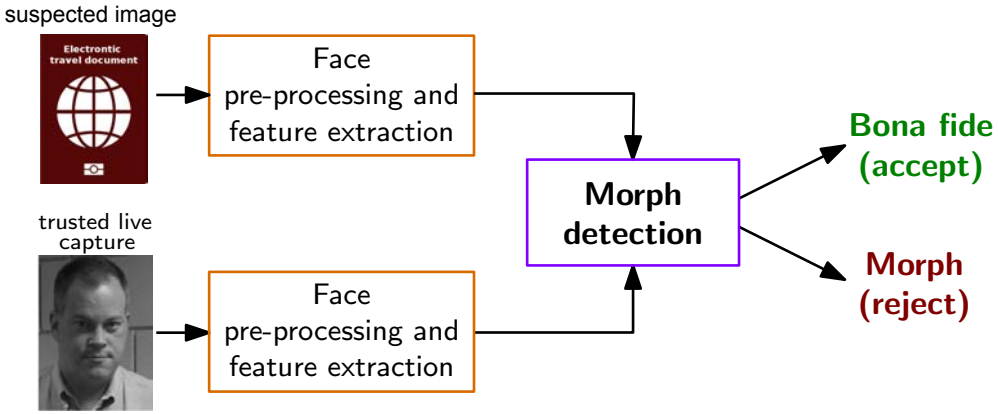
[SDRBU2019] U. Scherhag, L. Debiasi, C. Rathgeb, C. Busch and A. Uhl: "Detection of Face Morphing Attacks based on PRNU Analysis“, in IEEE TBIOM, (2019)

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)

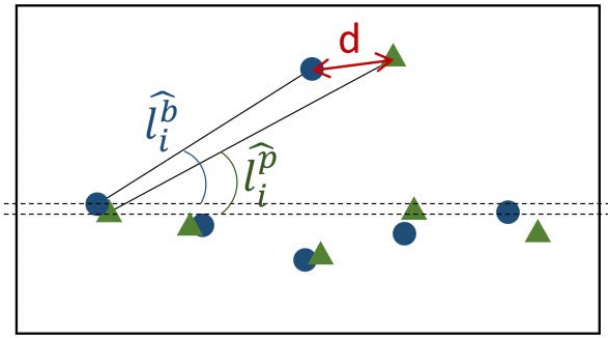


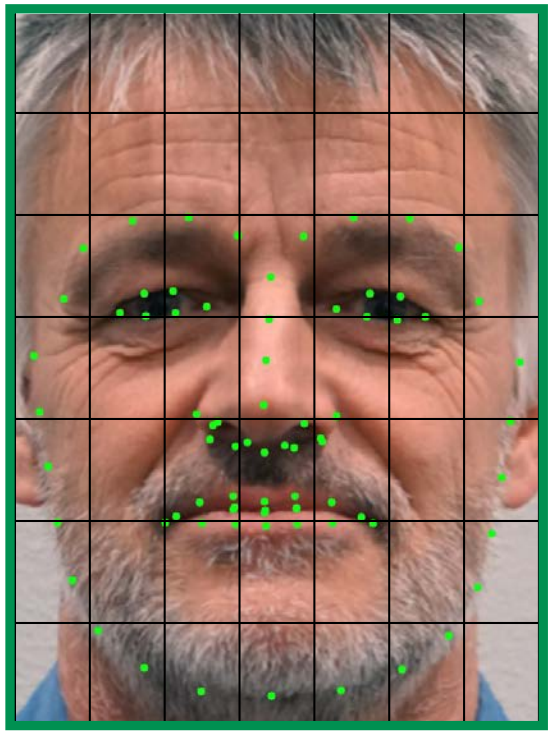
[SRB2018a] U. Scherhag, C. Rathgeb, C. Busch: "Towards Detection of Morphed Face Images in electronic Travel Documents“, in Proceedings of the 13th IAPR International Workshop on Document Analysis Systems (DAS), April 24-27, (2018)

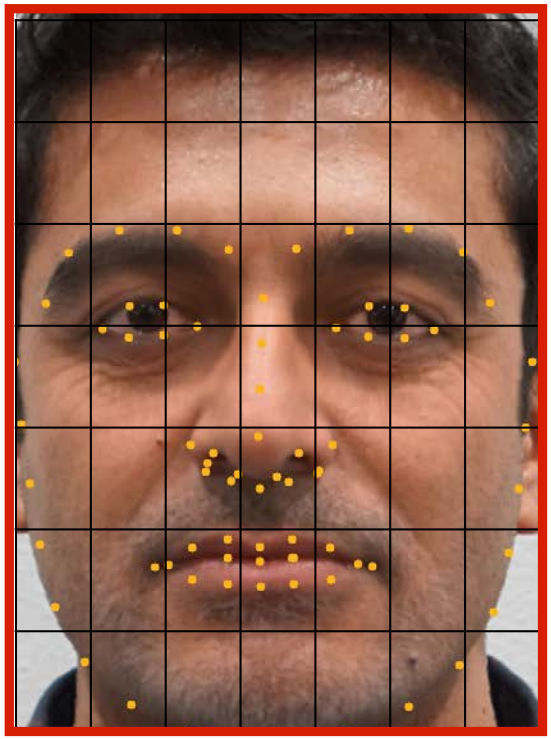
Differential Morphing Attack Detection

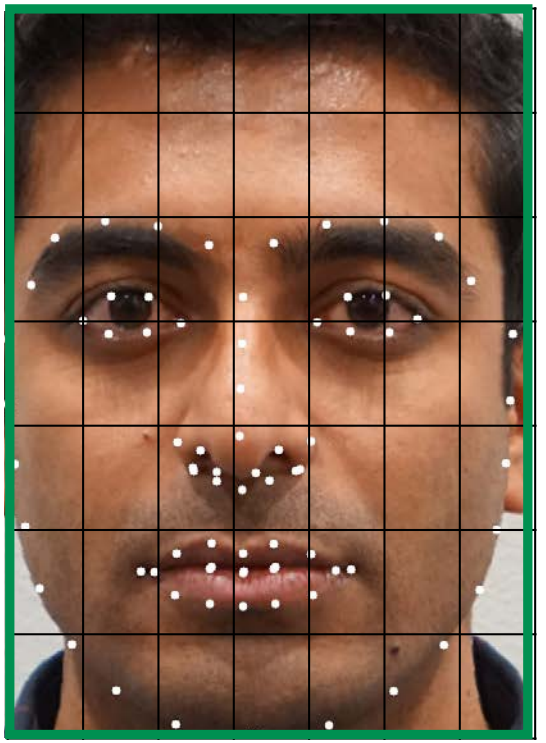
D-MAD with landmark analysis

- Angle based features
- Distance based features







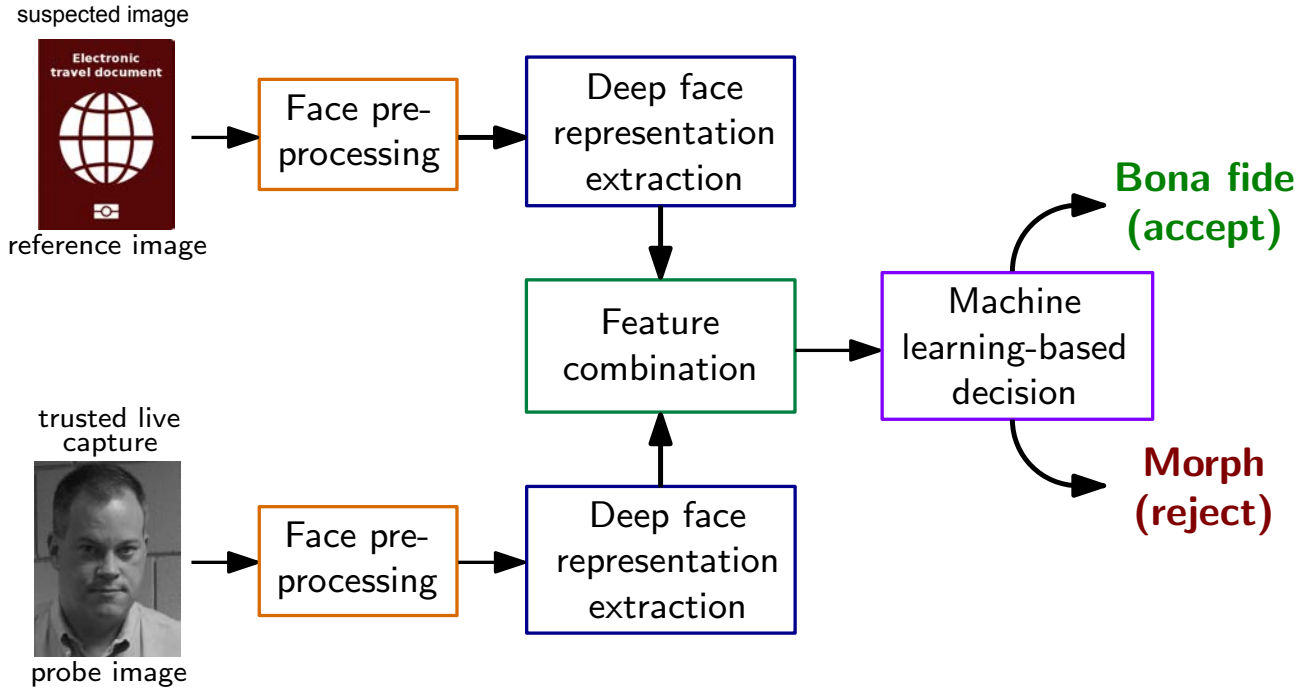


[SDGB2018] U. Scherhag, D. Budhrani, M. Gomez-Barrero, C. Busch: "Detecting Morphed Face Images Using Facial Landmarks“, in Proceedings of International Conference on Image and Signal Processing (ICISP), (2018)

Differential Morphing Attack Detection

D-MAD with deep learning

- Deep Face representations of Deep CNNs

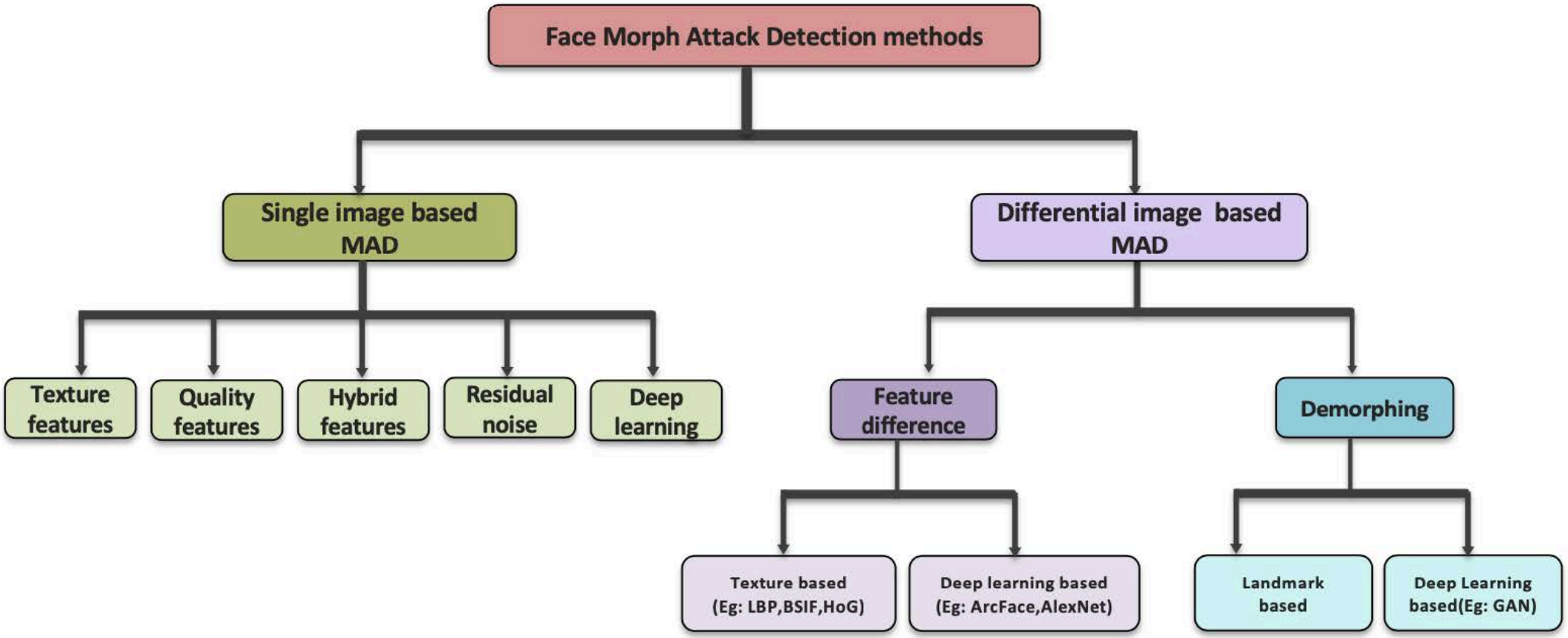


- Deep representations extracted by the neural network (on the lowest layer)
- Feature space with small dimension: 512 (for ArcFace)
- SVM with radial basis function

[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)

State of the Art - MAD Algorithms

Taxonomy of Morphing Attack Detection



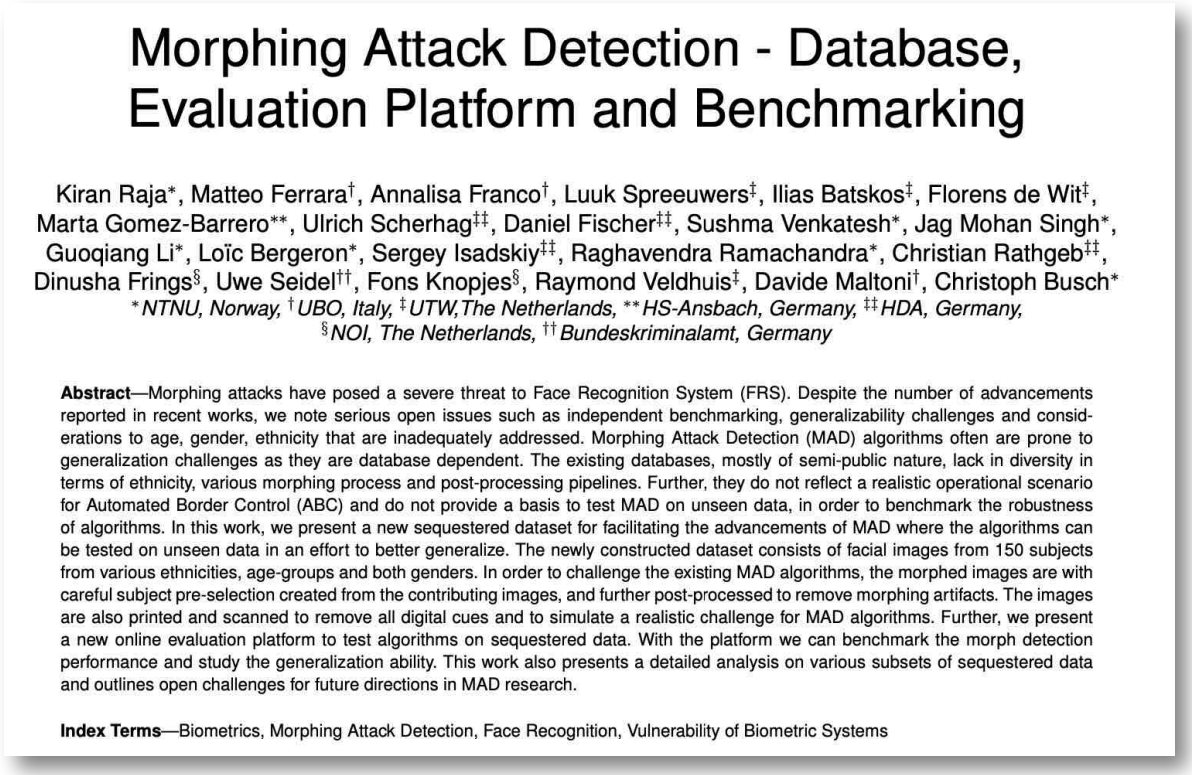
[Venkatesh2021] S. Venkatesh, R. Raghavendra, K. Raja, C. Busch: "Face Morphing Attack Generation & Detection: A Comprehensive Survey", in IEEE Transactions on Technology and Society (TTS), (2021)

MAD Evaluation

MAD Evaluation

Bologna Online Evaluation Platform (BOEP)

- SOTAMD dataset
  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.

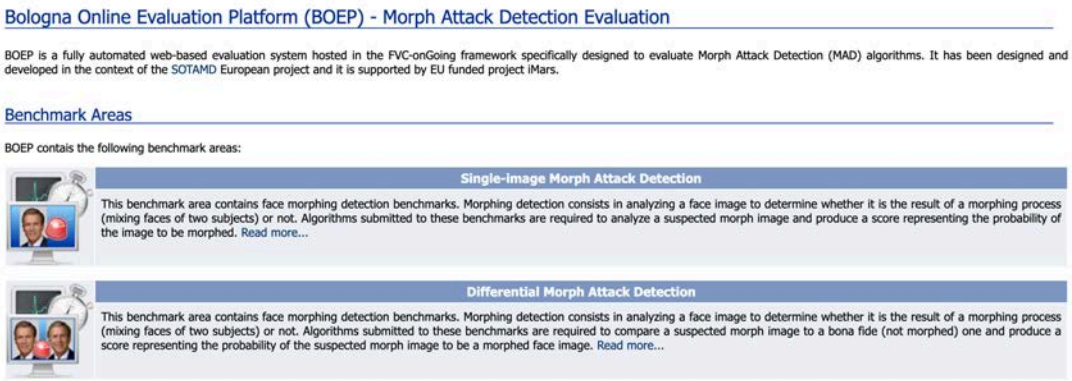
Index Terms—Biometrics, Morphing Attack Detection, Face Recognition, Vulnerability of Biometric Systems

[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.

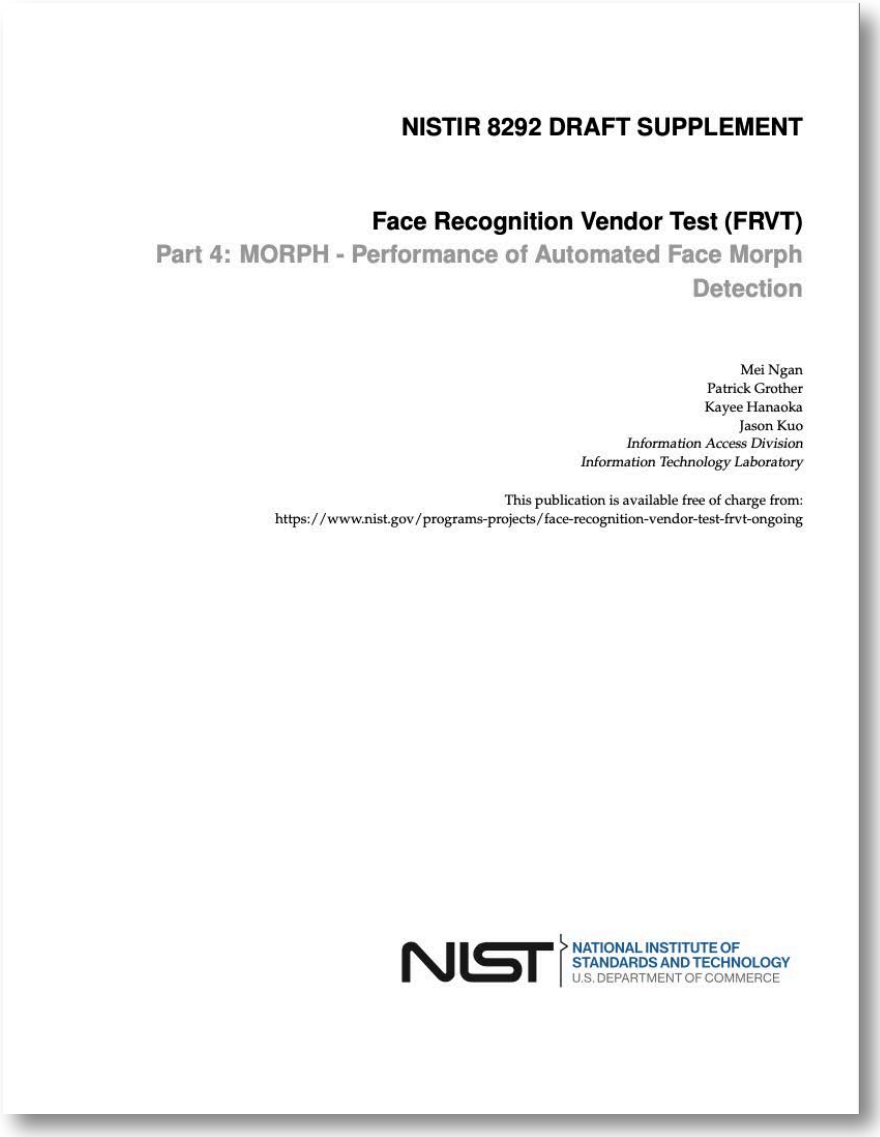
NIST FRVT MORPH

NIST IR 8292 report presented March, 2023

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

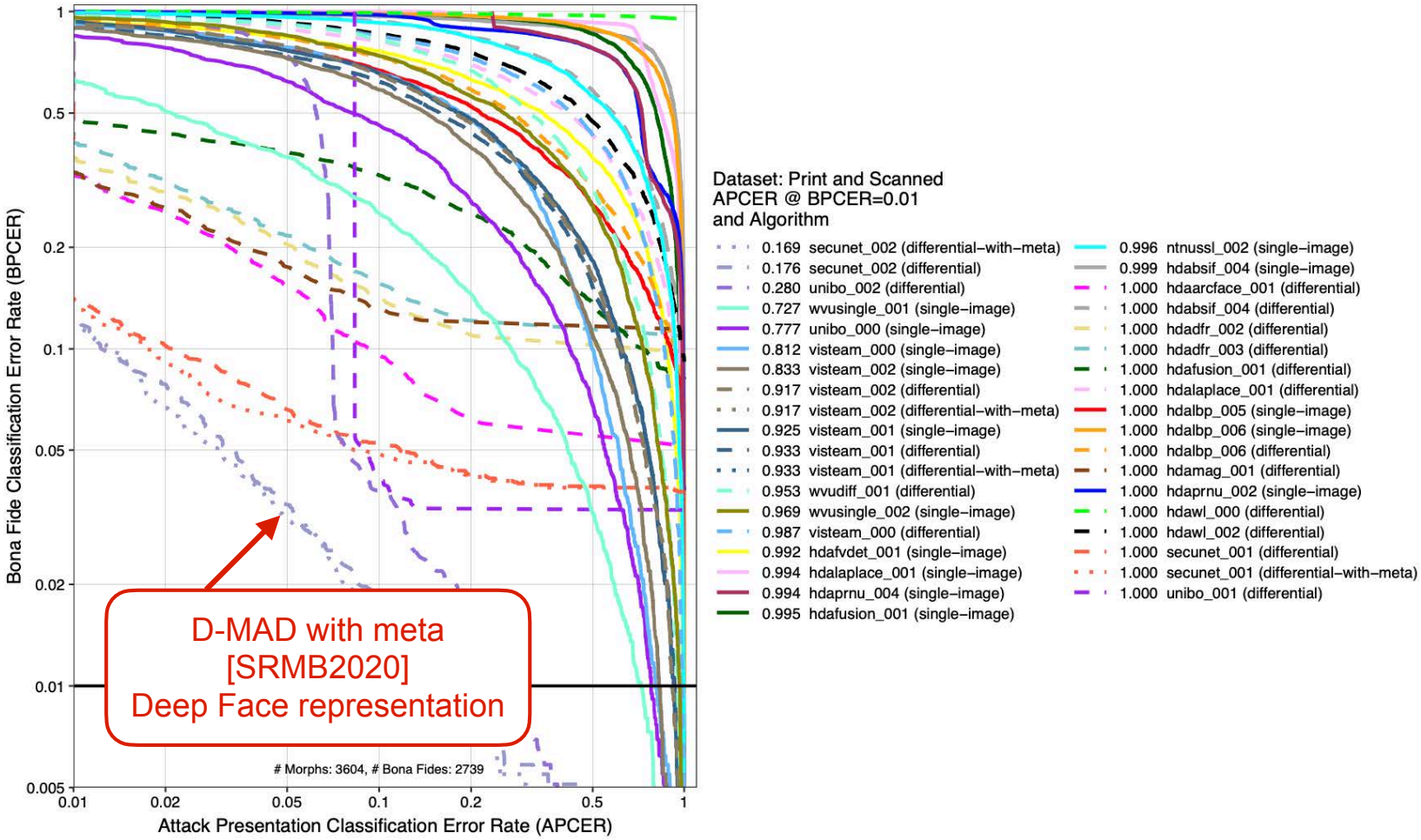
This publication is available free of charge from:
https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

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

NIST FRVT MORPH

NIST IR 8292 report presented March, 2023

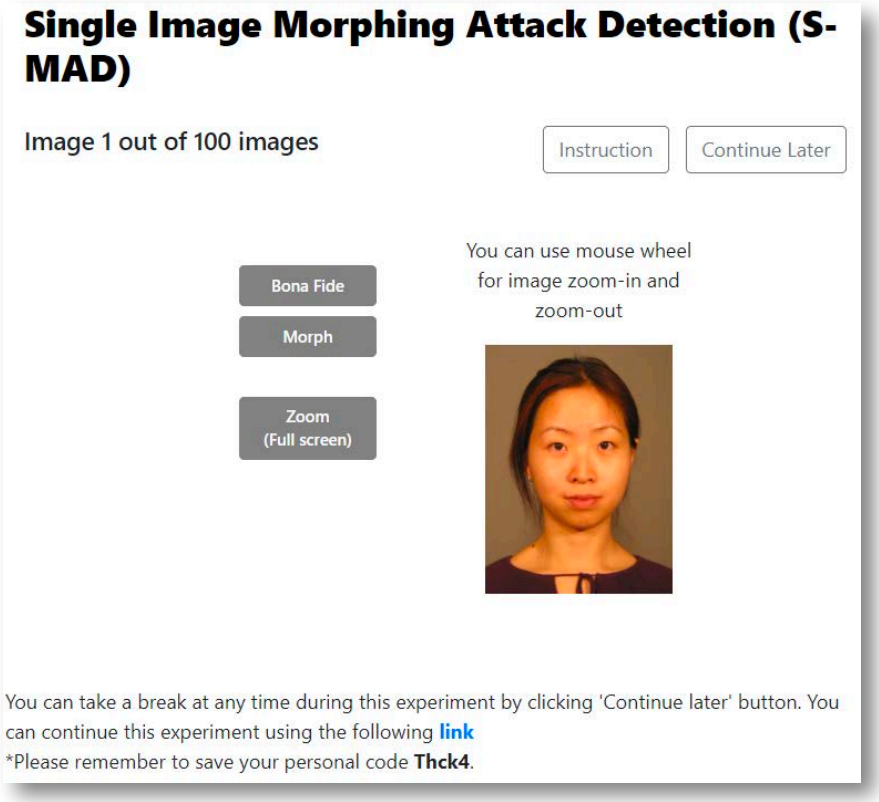
- Performance of Automated Face Morph Detection
  https://pages.nist.gov/frvt/reports/morph/frvt_morph_report.pdf
  - results for print and scanned morphs

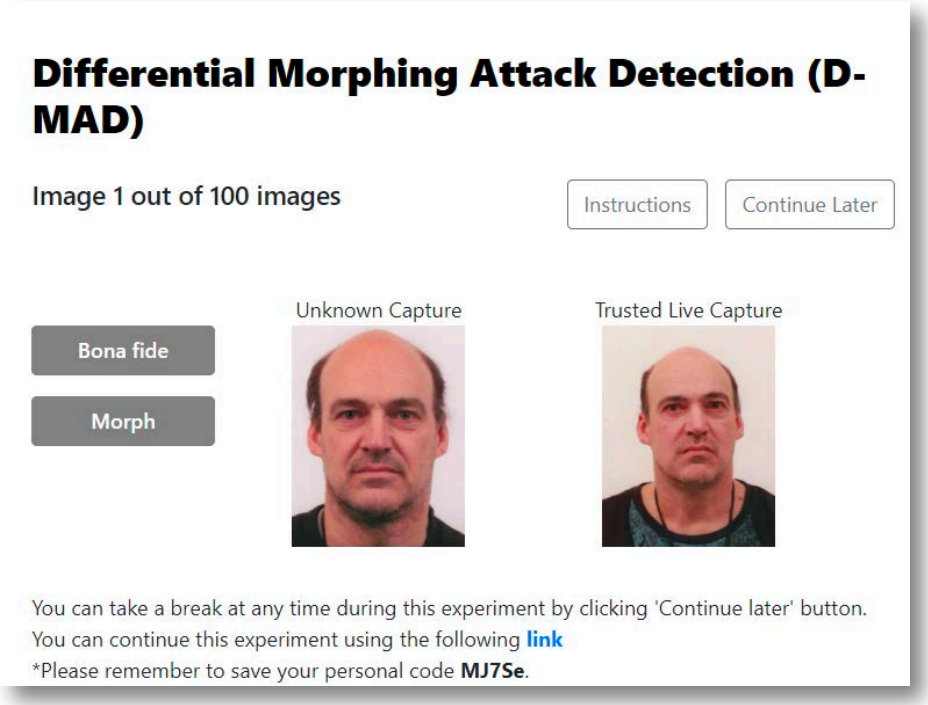


Human Experts in MAD

Border guards, case handlers, document examiners

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

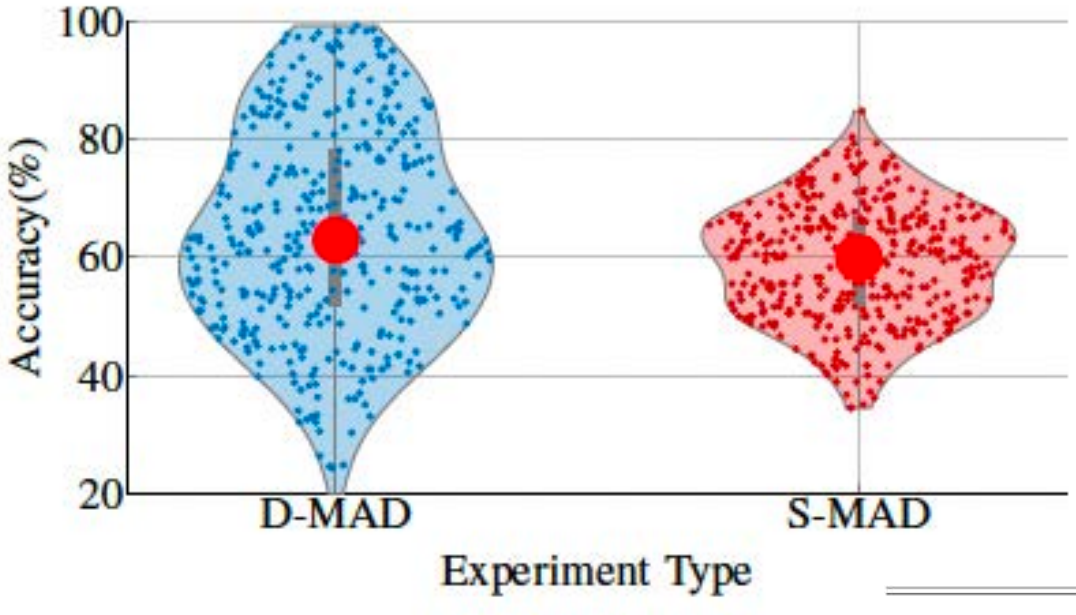




[GOD2022] S. Godage, F. Løvåsdal, S. Venkatesh, K. Raja, R. Raghavendra, C. Busch: “Analyzing Human Observer Ability in Morphing Attack Detection - Where Do We Stand?”, https://arxiv.org/abs/2202.12426

Human Experts in MAD

Overall accuracy

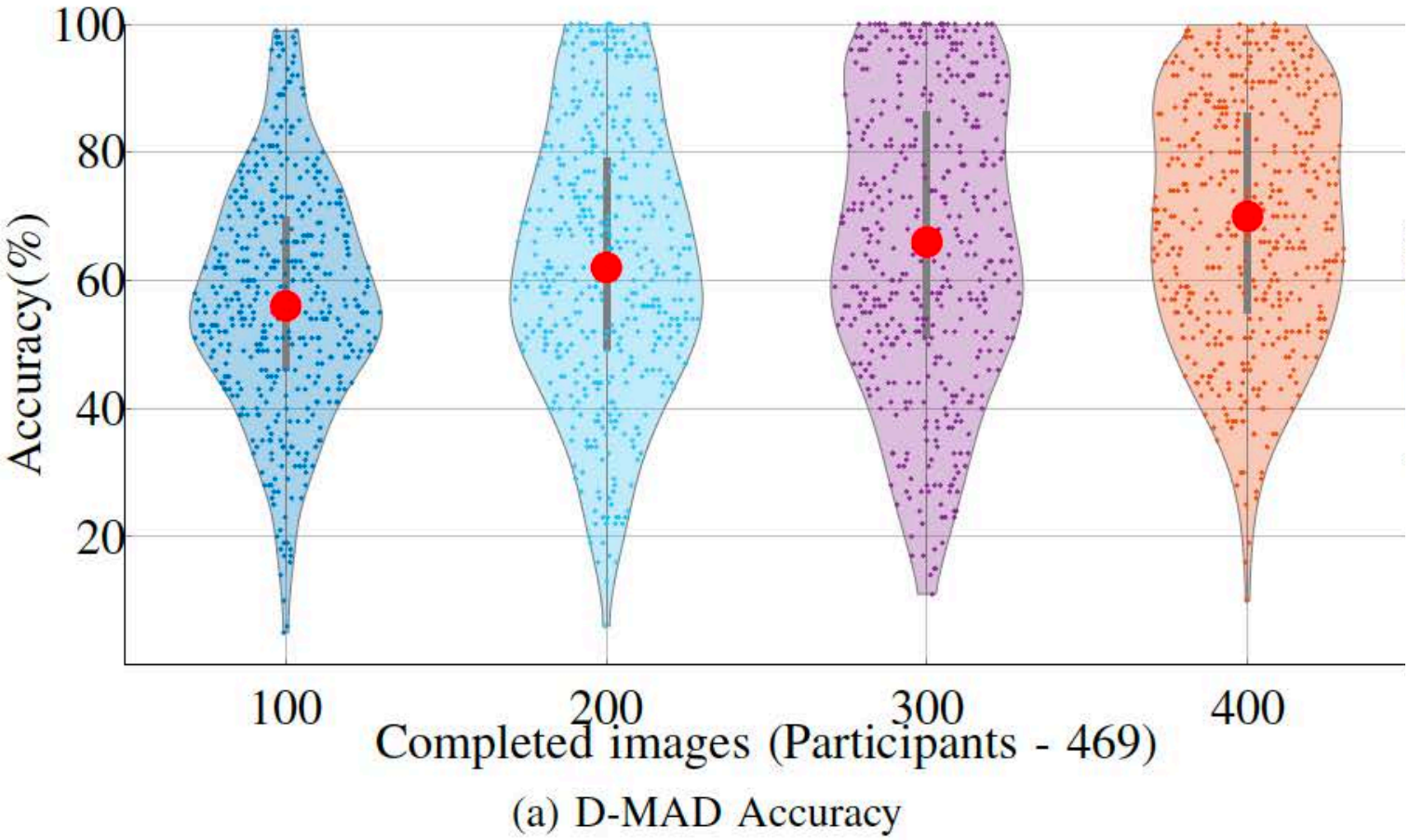


Line of work	D-MAD		S-MAD	
	Number of participants	Average Accuracy	Number of participants	Average Accuracy
Border Guard	30	64.66	26	55.17
Case handler- Passport, visas, ID, etc	150	63.45	137	56.65
Document examiner- 1st line	38	60.79	30	57.63
Document examiner- 2st line	40	68.64	34	62.56
Document examiner- 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

Further Research on MAD

With the iMARS project consortium

- 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/

iMARS
image manipulation attack resolving solutions

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

ULRICH SCHERHAG, CHRISTIAN RATHGEB, JOHANNES MERKLE, RALPH BREITHAUPT, AND CHRISTOPH BUSCH

- 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

Sushma Venkatesh Raghavendra Ramachandra Kiran Raja Christoph Busch
Norwegian University of Science and Technology (NTNU), Norway

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