Morphing Attacks on Face Recognition Systems

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

IAM Exchange, October 30, 2020

ATHENE

European Association for Biometrics eab Human Identity in Europe

NTNU

Overview

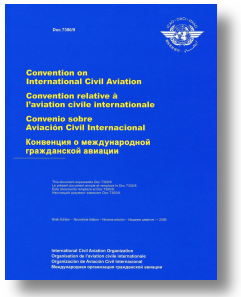
Agenda

- Introduction - Problem description
- Morphing Attack Detection - Scenarios and Methods
- Status: Face Morphing Attack Detection
- Future - what needs to be done?
- Conclusion

Passports

Standardised Travel Documents

ICAO - International Civil Aviation Organisation



- A specialised UN agency (Headquarter Montreal)
- 193 member states
- ICAO's mandate for standards development
  - The Convention on International Civil Aviation - Doc 7300 signed in December 1944 ("Chicago Convention")
  - ICAO works to achieve its vision of safe, secure and sustainable development of civil aviation through the cooperation of its Member States
- Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD)
- Cooperation with International Organisation for Standardisation (ISO/IEC JTC1)
  - SC17 and SC37

ePassport Data Group Details

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

ePassport Details

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

New in 2020

  - 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).

Principles

Principle of equality - in our society

- One individual - one passport

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

Principles

Principle of equality - in our society

- One Carlos Ghosen - multiple passports

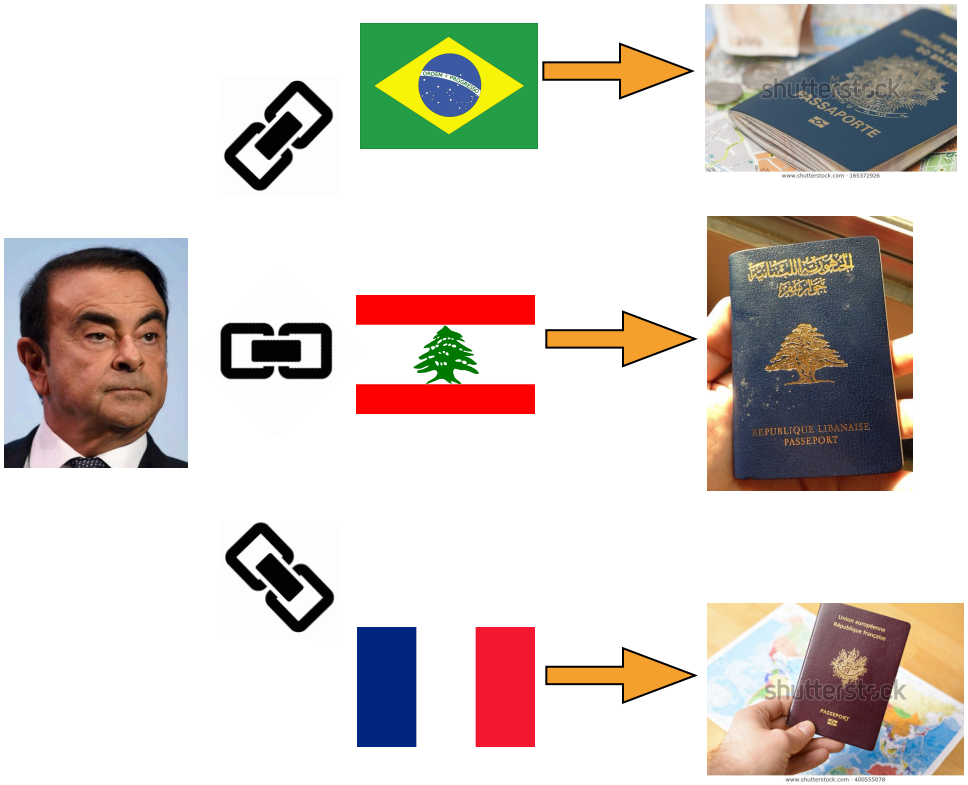
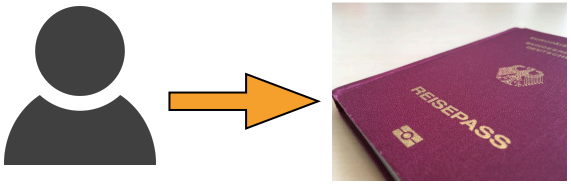


image source: https://www.shutterstock.com/image-photo/passport-hand-worlds-maps-background-400555078
image source: https://stateofmind13.com/2016/01/06/everything-you-need-to-know-about-the-new-lebanese-passport-rules/
image source: https://www.shutterstock.com/image-photo/brazilian-passport-above-map-governmentissued-document-165372926
image source: https://www.stern.de/wirtschaft/carlos-ghosn--die-filmreife-flucht-des-frueheren-star-managers-9069770.html

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

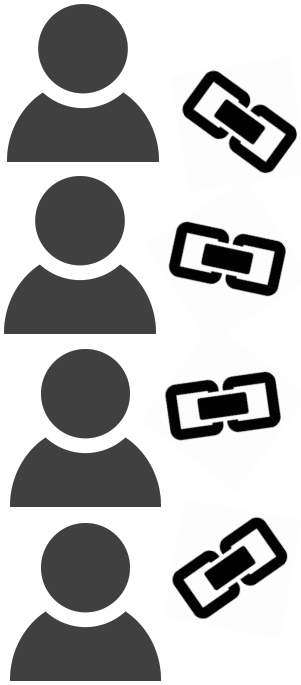


image source: https://pixabay.com/de/vectors/tick-sternchen-kreuz-rot-gr%C3%BCn-40678/

What is Morphing?

What is Morphing?

In our real world morphing can become a threat

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

What is Morphing?

In our real world morphing can become a threat

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

What is Morphing?

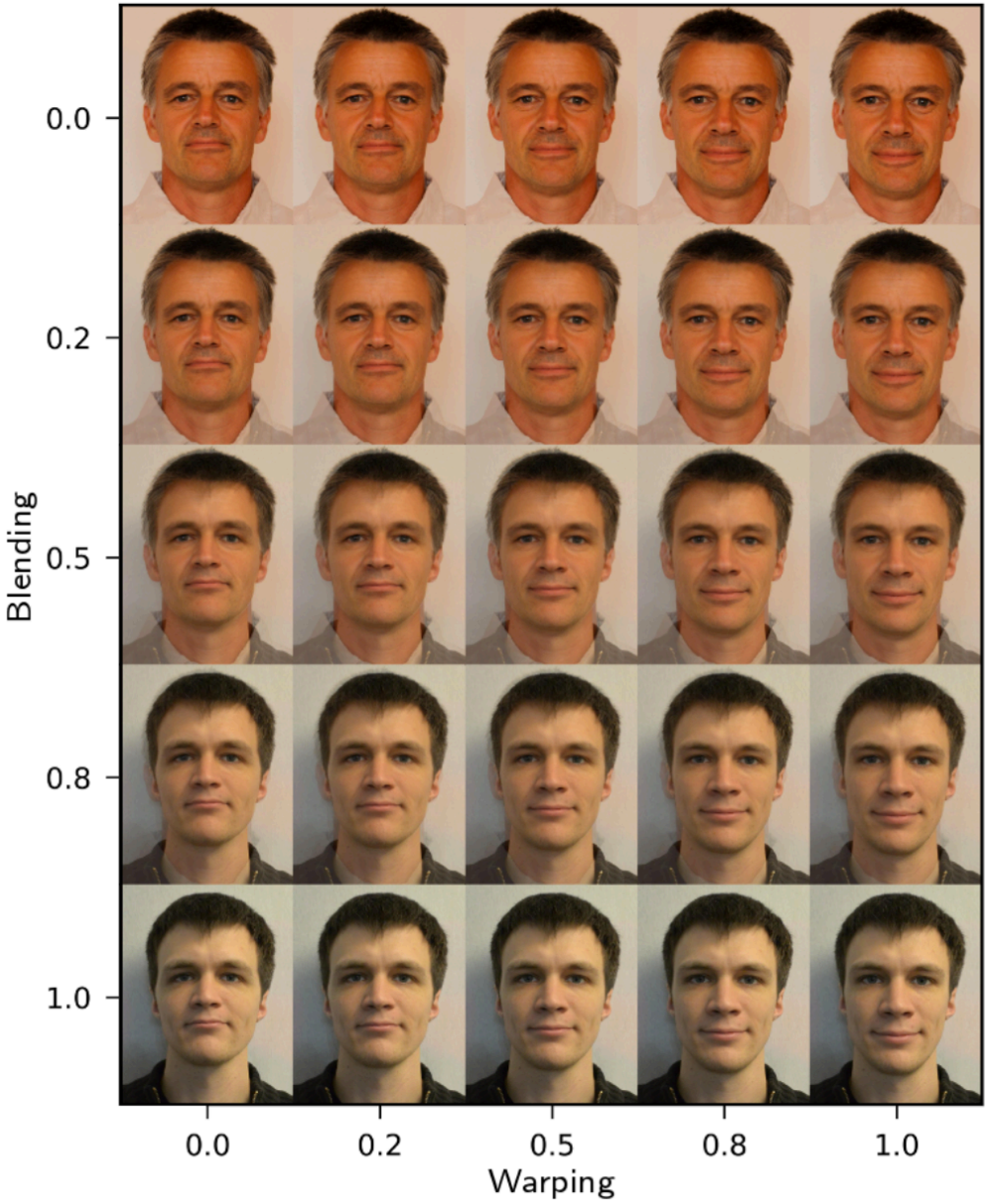
Warping and blending

- controlled by the alpha factor
- Landmark positions

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

- Colour

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



Problem Description

Problem: Morphing Attacks

Morphing attack scenario

- Passport application of the accomplice A

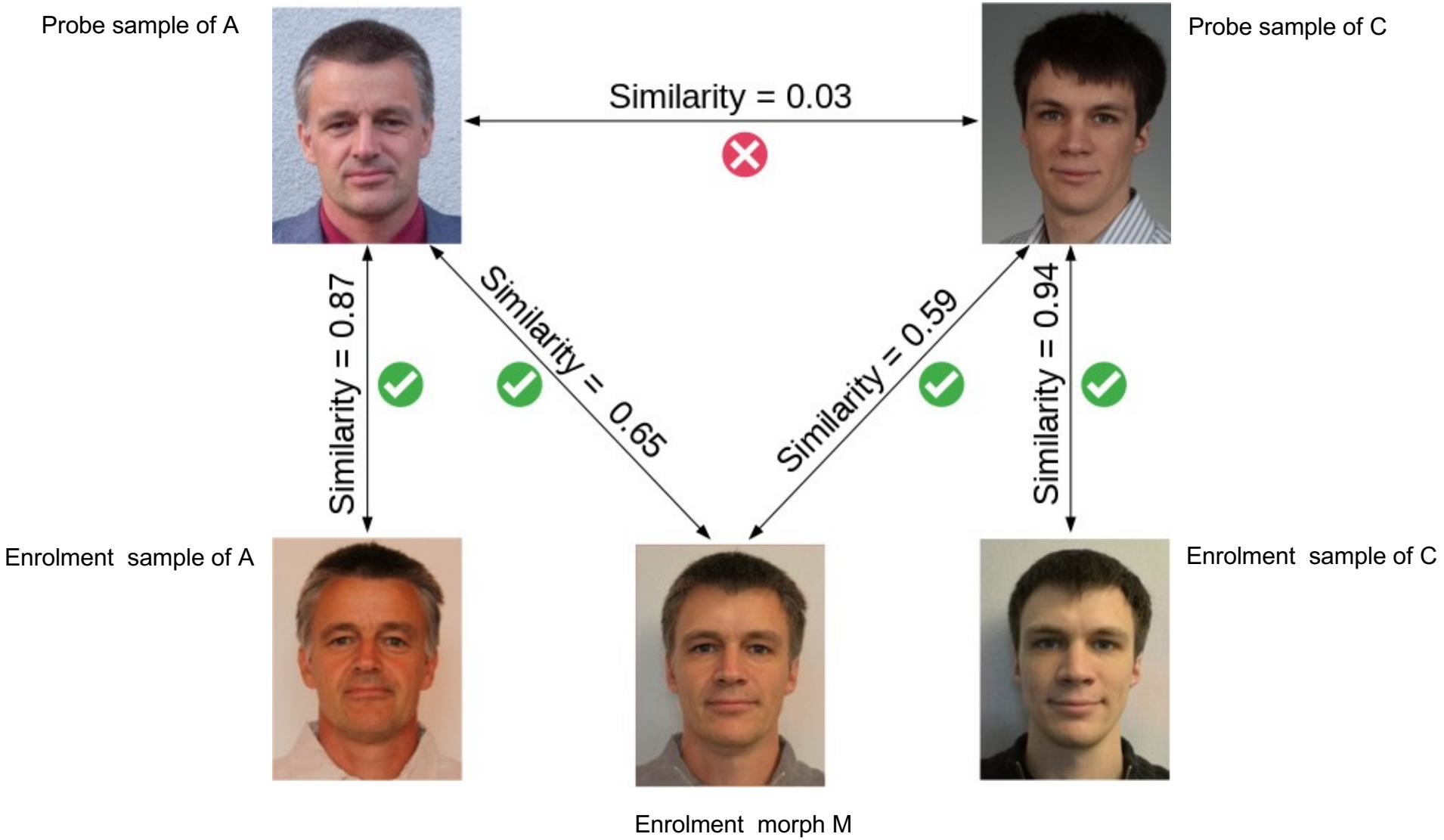
Problem: Morphing Attacks

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.

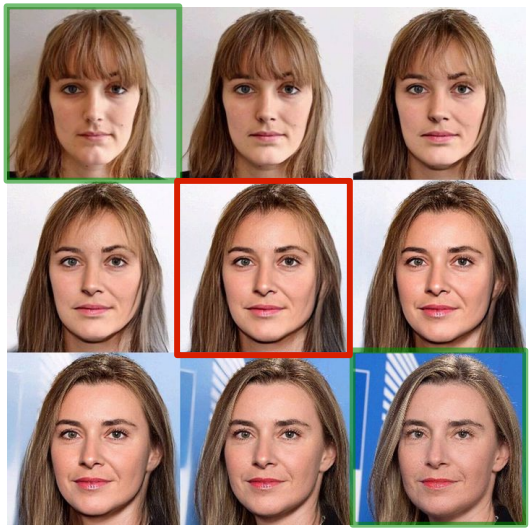


Image source: https://www.spiegel.de/netzwelt/netzpolitik/biometrie-im-reisepass-peng-kollektiv-schmuggelt-fotomontage-in-ausweis-a-1229418.html

Problem: Morphing Attacks

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."*

What is the vulnerability?

Scale of the Problem: Vulnerability

Human Experts Capabilities - (44 border guards)

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

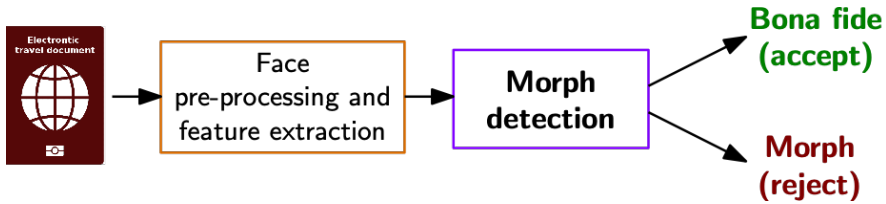
Morphing Attack Detection (MAD)

Scenarios and Methods

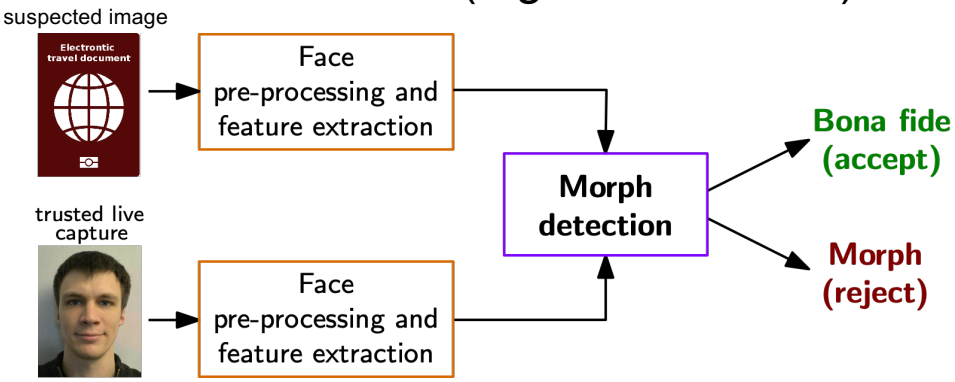
Morphing Attack Detection Scenarios

Real world scenarios

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



- 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)

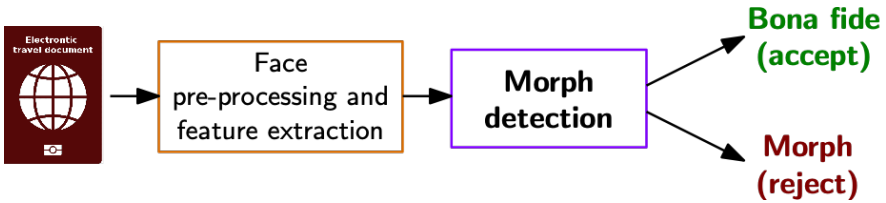


[SRB2018a] U. Scherhag, C. Rathgeb, C. Busch: "Towards Detection of Morphed Face Images in electronic Travel Documents", in Proceedings of the 13th IAPR International Workshop on Document Analysis Systems (DAS), April 24-27, (2018)

Face Pre-processing and Feature Extraction

Morphing Attack Detection (S-MAD) with texture analysis

- Image descriptors as hand-crafted features

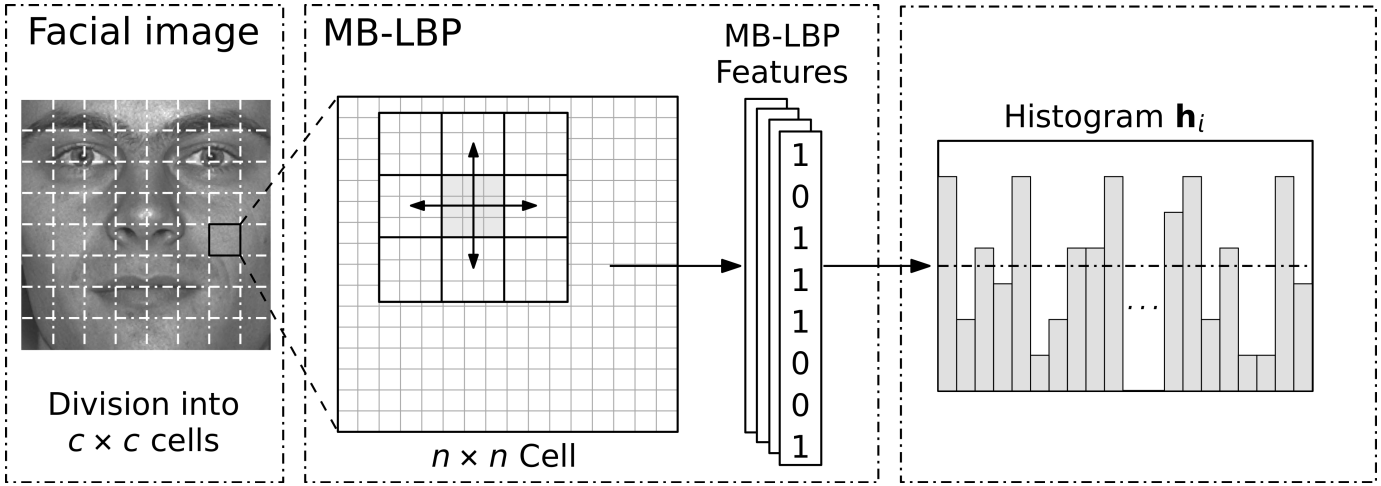


[SRB2018b] U. Scherhag, C. Rathgeb, C. Busch: „Detection of Morphed Faces from Single Images: a Multi-Algorithm Fusion Approach“, in Proceedings if of the 2nd International Conference on Biometric Engineering and Applications (ICBEA), Amsterdam, The Netherlands, May 16-18, (2018)

Face Pre-processing and Feature Extraction

S-MAD with image descriptor

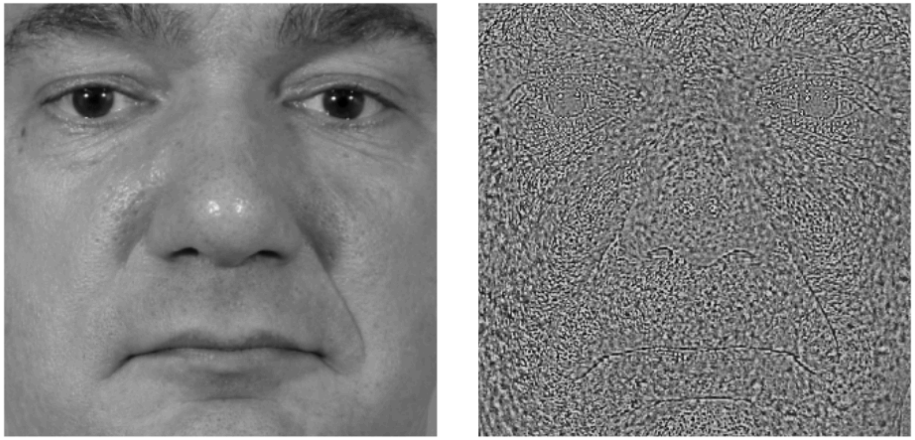
- Local Binary Pattern (LBP)

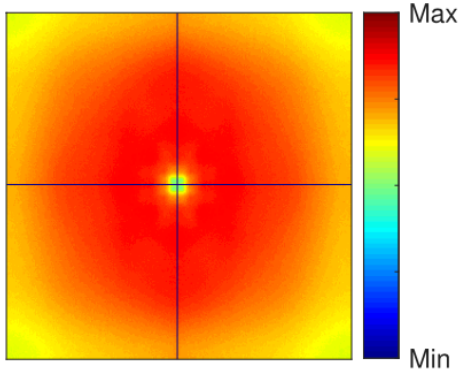


Face Pre-processing and Feature Extraction

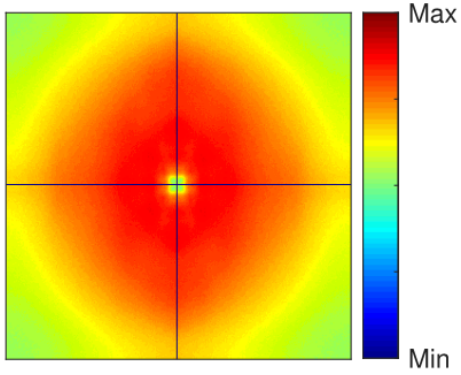
S-MAD with image descriptor / forensic approach

- Photo Response Non-Uniformity (PRNU)

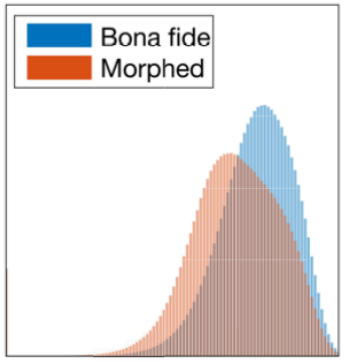




Bona Fide



Morph



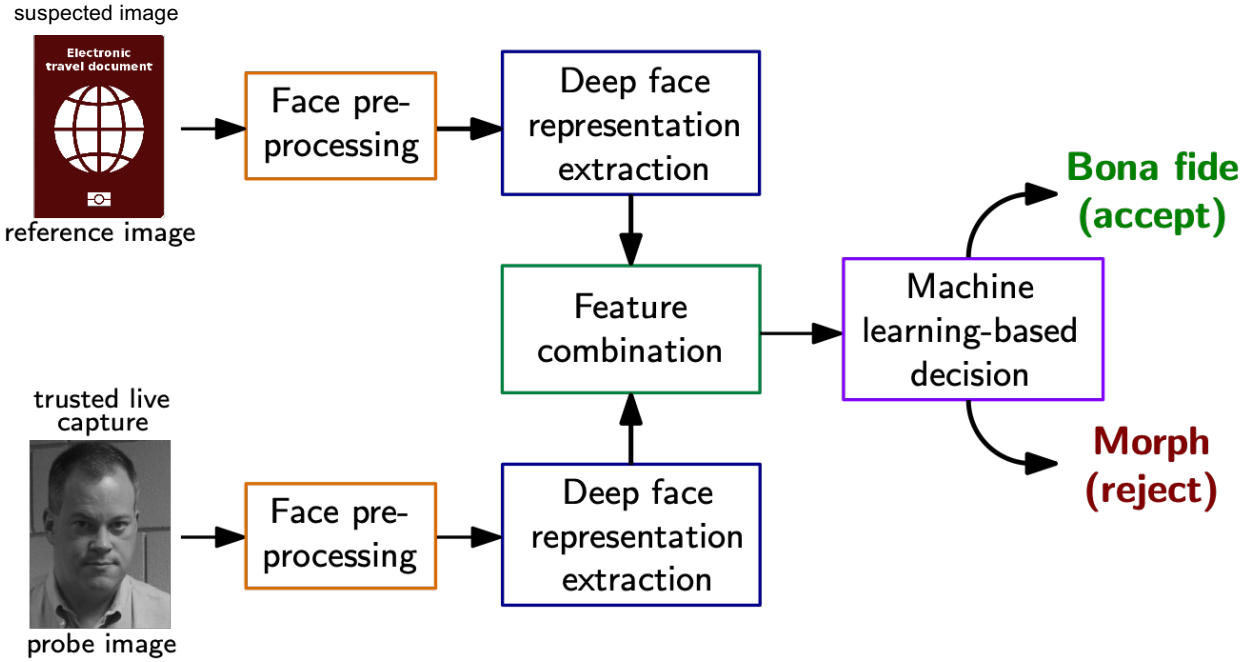
Histograms

[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)

Differential Morphing Attack Detection

D-MAD with deep learning

- Deep Face representations of Deep CNNs

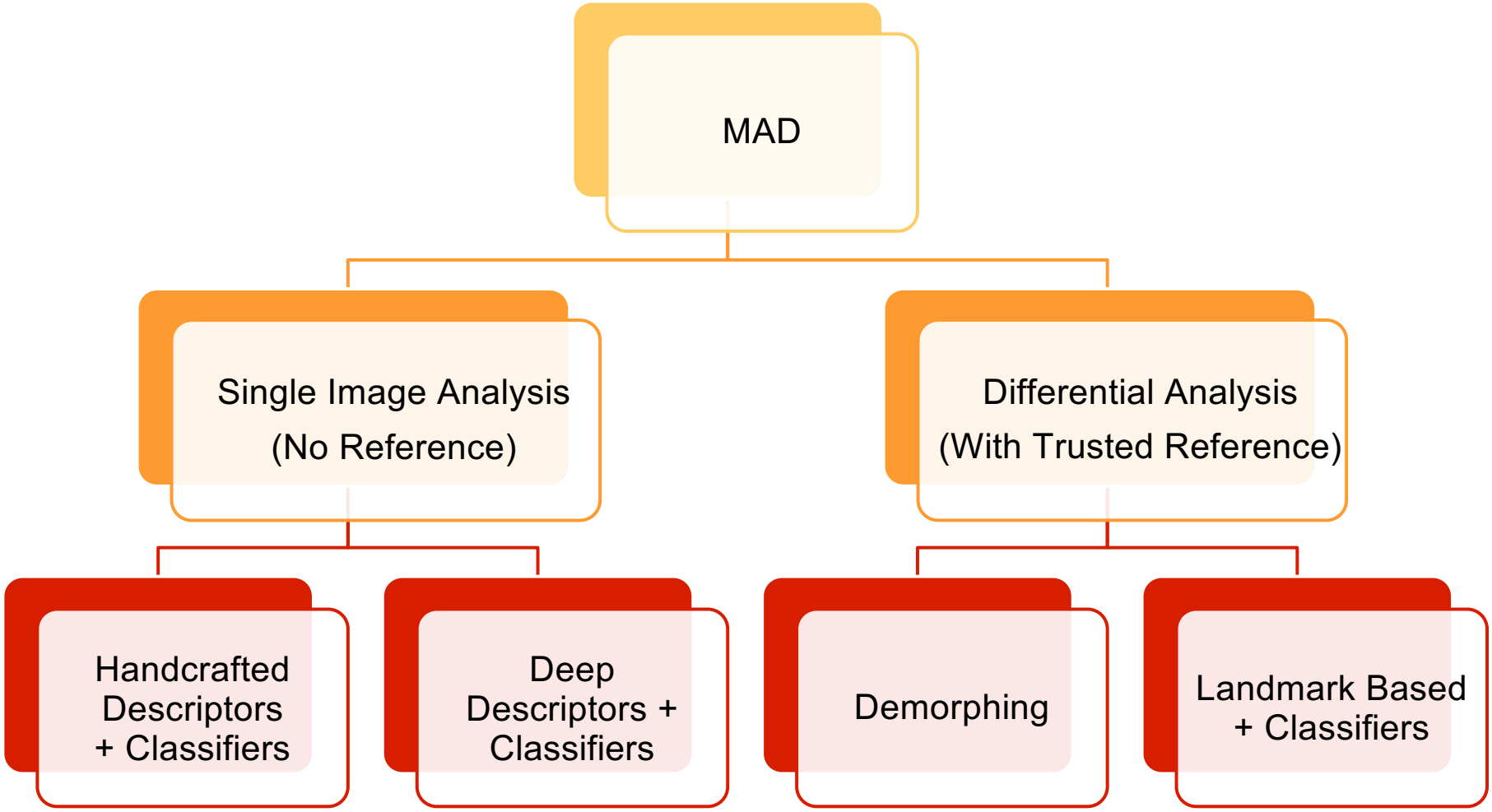


- Deep representations extracted by the neural network (on the lowest layer)
- Feature space with small dimension: 512 (for ArcFace and FaceNet)
- SVM with radial basis function

[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)

Summary of 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 Methodology

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

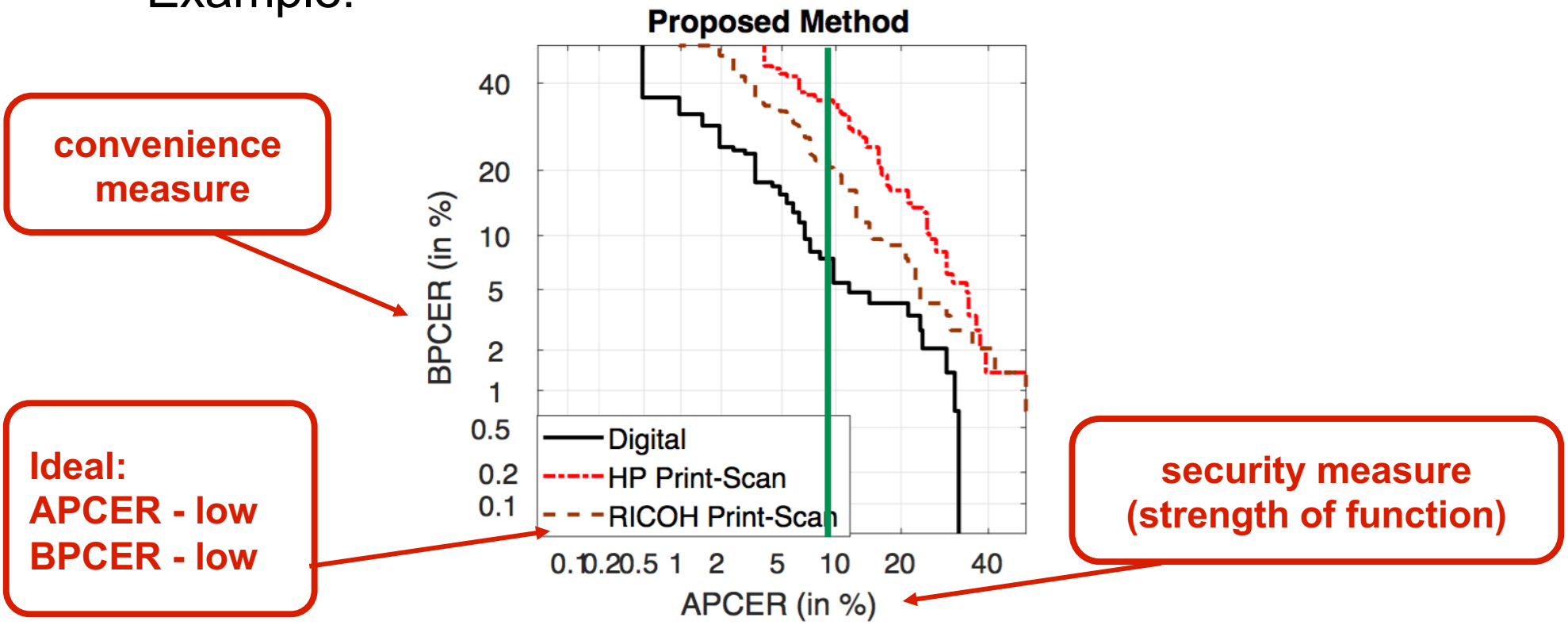
- **Bona fide presentation classification error rate (BPCER)**
  proportion of bona fide presentations incorrectly classified as attack presentations in a specific scenario

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

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

[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)

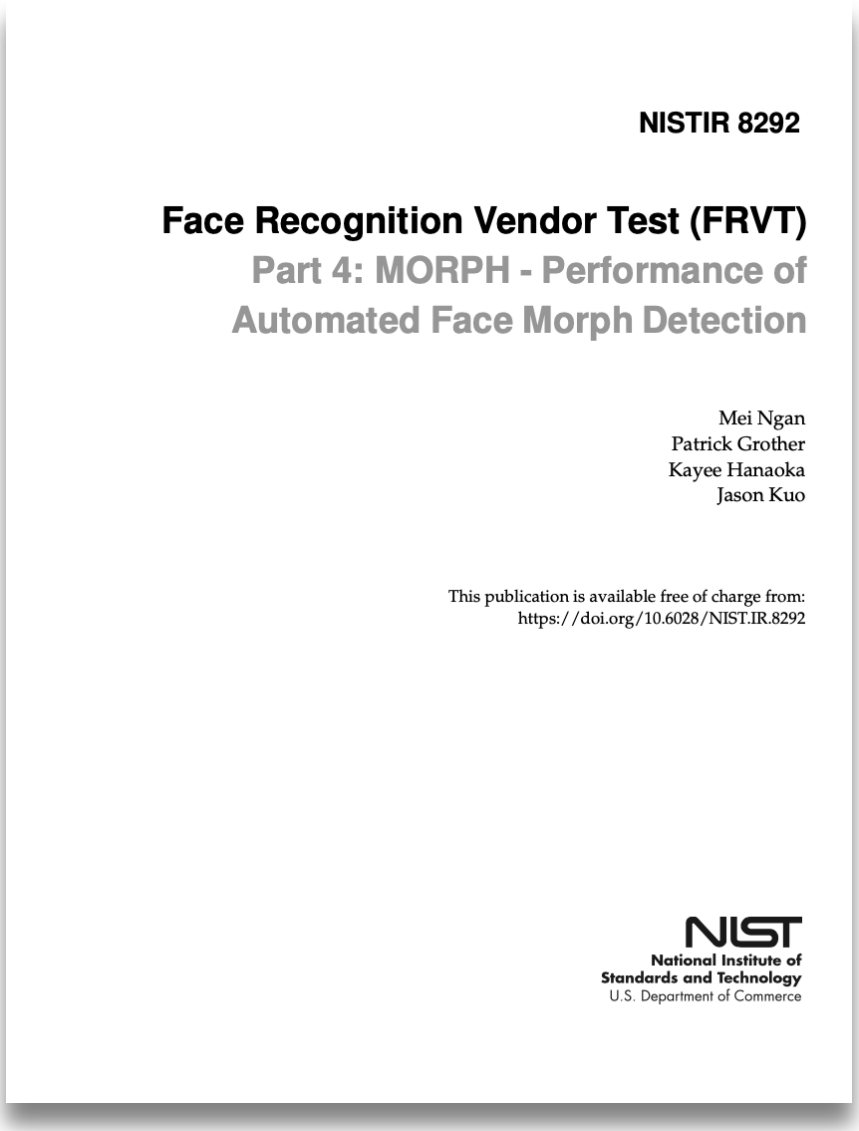
NIST-FRVT-MORPH

NIST IR 8292 report presented July, 2020

FRVT-MORPH

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

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



NISTIR 8292

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

Mei Ngan
Patrick Grother
Kayee Hanaoka
Jason Kuo

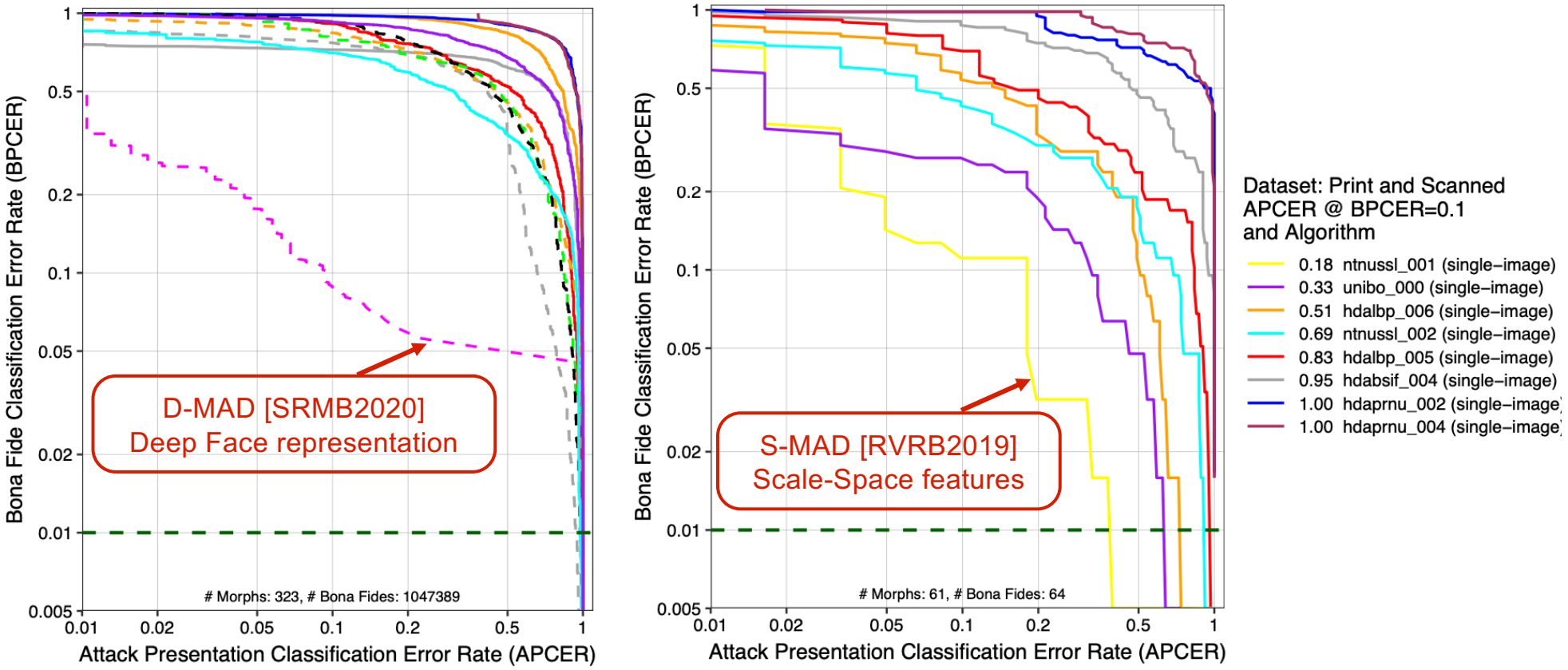
This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8292

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

NIST-FRVT-MORPH

NIST IR 8292 report presented July, 2020

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



What needs to be done?

MAD Action Plan

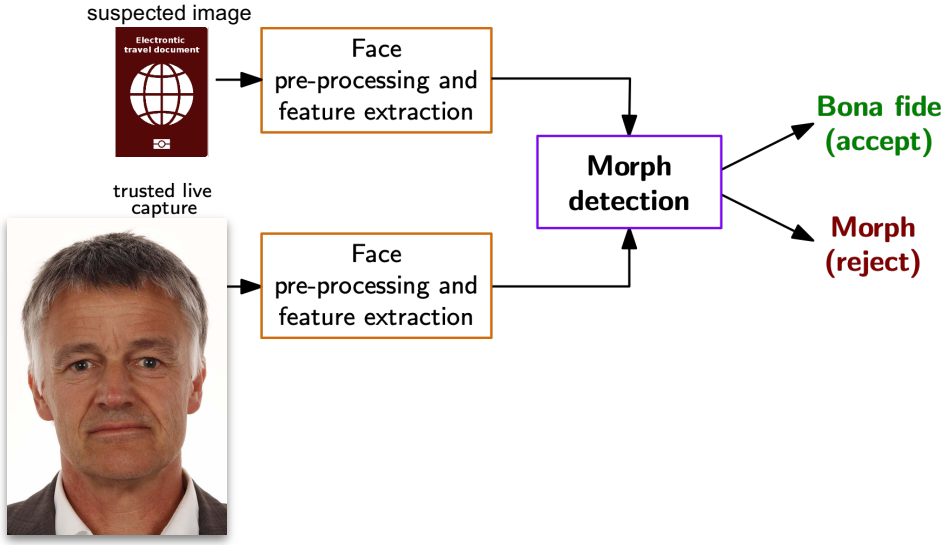
I.) Establish consensus amongst stakeholders

- Europe should immediately start an action to secure
  - the trusted link between a MRTD and the document holder meaning to switch to live enrolment!
  - 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 = image Manipulation Attack Resolving Solutions (H2020 proposal)
  - The iMARS consortium consists of Idemia, NTNU, University Bologna, University Twente, Hochschule Darmstadt, University Leuven, Dutch National Office for Identity Data, German Bundeskriminalamt, Vision-Box, Cognitec, Mobai, IBS, EAB and various end users (border control agencies)
  - iMARS is a pan-European approach that is supported by the European Association for Biometrics (EAB)

MAD Action Plan - iMARS Project

II.) 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

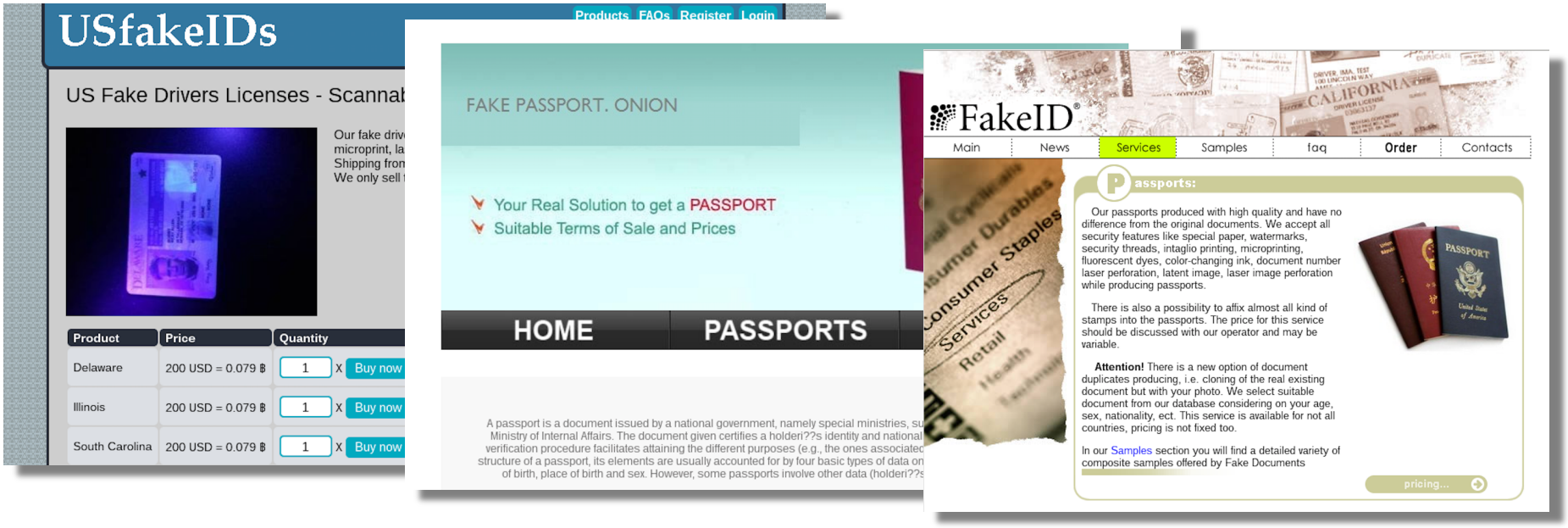
III.) Develop Face Image Quality Metrics

- 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 24357 and ISO/IEC 29794-5
- 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

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 (GlobalWarming, Information, Services)
- In combination with passport brokers a dramatic problem
  - the darknet offers numerous such opportunities:



References

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

- U. Scherhag, C. Ratgeb, J. Merkle, C. Busch: "Deep Face Representations for Differential Morphing Attack Detection", in IEEE Transactions on Information Forensics and Security (TIFS), (2020)
- S. Venkatesh, H. Zhang, R. Raghavendra, K. Raja, N. Damer, C. Busch: "Can GAN Generated Morphs Threaten Face Recognition Equally as Landmark Based Morphs? - Vulnerability and Detection", in Proceedings of 8th International Workshop on Biometrics and Forensics (IWBF 2020), Porto, PT, April 29 - 30, (2020)
- S. Venkatesh, R. Raghavendra, K. Raja, L. Spreeuwers, R. Veldhuis, C. Busch: "Detecting Morphed Face Attacks Using Residual Noise from Deep Multi-scale Context Aggregation Network", in Proceedings of Winter Conference on Applications of Computer Vision (WACV '20), Colorado, US, March 1-5, (2020)
- J. Merkle, C. Rathgeb, U. Scherhag, C. Busch: "Morphing-Angriffe: Ein Sicherheitsrisiko für Gesichtserkennungssysteme", in Datenschutz und Datensicherheit (DuD), Vol. 44, no. 1, pp. 26-31, (2020)
- J. Singh, S. Venkatesh, K. Raja, R.Raghavendra, C. Busch: "Detecting Finger-Vein Presentation Attacks Using 3D Shape & Diffuse Reflectance Decomposition", in Proceedings of the 15th International Conference on Signal Image Technology & Internet Based Systems (SITIS 2019), November 26-29, Sorrento - Naples, IT, (2019)
- S. Venkatesh, R. Raghavendra, K. Raja, L. Spreeuwers, R. Veldhuis, C. Busch: "Morphed Face Detection Based on Deep Color Residual Noise", in Proceedings of the ninth International Conference on Image Processing Theory, Tools and Applications (IPTA 2019), Istanbul, Turkey, November 6-9, (2019)
- U. Scherhag, L. Debiasi, C. Rathgeb, C. Busch and A. Uhl: "Detection of Face Morphing Attacks based on PRNU Analysis", in IEEE TBIOM, (2019)
- U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, C. Busch: "Face Recognition Systems und Morphing Attacks: A Survey", in IEEE Access, (2019)
- R.Raghavendra, S. Venkatesh, K. Raja, C. Busch: "Towards making Morphing Attack Detection robust using hybrid Scale-Space Colour Texture Features", in Proceedings of 5th International Conference on Identity, Security and Behaviour Analysis (ISBA 2019), Hyderabad, IN, January 22-24, (2019)
- L. Debiasi, C. Rathgeb, U. Scherhag, A. Uhl, C. Busch: "PRNU Variance Analysis for Morphed Face Image Detection", in Proceedings of 9th International Conference on Biometrics: Theory, Applications and Systems (BTAS 2018), Los Angeles, US, October 22-25, (2018)
- R.Raghavendra, S. Venkatesh, K. Raja, C. Busch: "Detecting Face Morphing Attacks with Collaborative Representation of Steerable Scale-Space Features", in Proceedings of 3rd International Conference on Computer Vision and Image Processing (CVIP 2018), Japalpur, IN, September 29 - October 1, (2018)
- 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), Cherbourg, FR, July 2-4, (2018)
- U. Scherhag, C. Rathgeb, C. Busch: "Performance Variation of Morphed Face Image Detection Algorithms across different Datasets", in Proceedings of 6th International Workshop on Biometrics and Forensics (IWBF 2018), Sassari, IT, June 7-8, (2018)
- L. Debiasi, U. Scherhag, C. Rathgeb, A. Uhl, C. Busch: "PRNU-based Detection of Morphed Face Images", in Proceedings of 6th International Workshop on Biometrics and Forensics (IWBF 2018), Sassari, IT, June 7-8, (2018)
- 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 2018), Amsterdam, The Netherlands, May 16-18, (2018)
- U. Scherhag, C. Rathgeb and 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 2018), Vienna, Austria, April 24-27, (2018)
- M. Gomez-Barrero, C. Rathgeb, U. Scherhag, C. Busch: „Predicting the Vulnerability of Biometric Systems to Attacks based on Morphed Biometric Samples", in IET Biometrics, (2018)
- C. Rathgeb, C. Busch: "On the Feasibility of Creating Morphed Iris-Codes", in Proceedings of International Joint Conference on Biometrics (IJCB 2017), Denver, Colorado, October 1-4, (2017)
- R. Raghavendra, K. Raja, S. Venkatesh, C. Busch: "Face Morphing Versus Face Averaging: Vulnerability and Detection", in Proceedings of International Joint Conference on Biometrics (IJCB 2017), Denver, Colorado, October 1-4, (2017)
- 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)
- 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)
- M. Gomez-Barrero, C. Rathgeb, U. Scherhag, C. Busch: "Is Your Biometric System Robust to Morphing Attacks?", in Proceedings of 5th International Workshop on Biometrics and Forensics (IWBF 2017), Coventry, UK, April 4-5, (2017)
- U. Scherhag, R. Raghavendra, K. Raja, M. Gomez-Barrero, C. Rathgeb, C. Busch: "On The Vulnerability Of Face Recognition Systems Towards Morphed Face Attacks", in Proceedings of 5th International Workshop on Biometrics and Forensics (IWBF 2017), Coventry, UK, April 4-5, (2017)
- R. Raghavendra, K. Raja, C. Busch: "Detecting Morphed Facial Images", in Proceedings of 8th IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS-2016), September 6-9, Niagra Falls, USA, (2016)

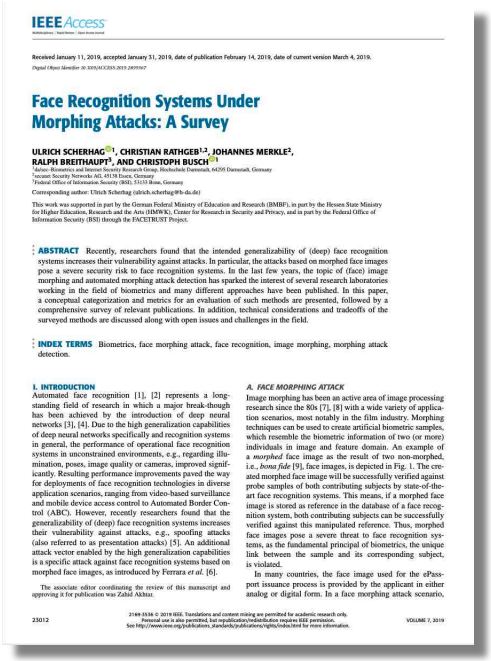
More information

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

Face Recognition Systems Under Morphing Attacks: A Survey

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

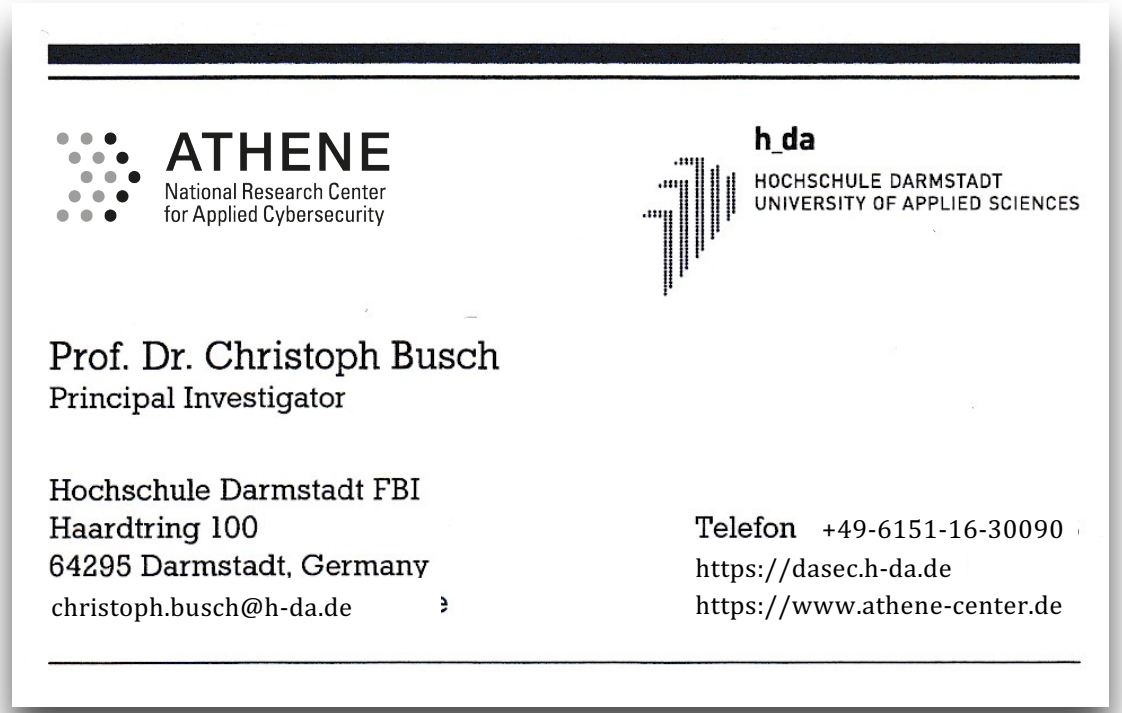
Contact

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