Travel Documents and Morphing Attacks on Face Recognition Systems

Christoph Busch

copy of slides available at:
https://www.christoph-busch.de/about-talks-slides.html

Notre Dame University, January 15, 2020

ATHENE

European Association for Biometrics eab Human Identity in Europe

NTNU

Principles

Principle of redundancy

- One individual - multiple credit cards

Principles

Principle of equality - in our society

- One individual - multiple votes

image source: https://pixabay.com/vectors/ballot-election-vote-1294935/

Principles

Principle of equality - in our society

- One individual - one passport

image source: https://pixabay.com/photos/passport-pass-travel-document-id-1051697/

Principles

Principle of equality - in our society

- One Carlos Ghosen - multiple passports

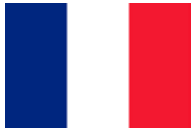


image source: https://www.shutterstock.com/image-photo/passport-hand-worlds-maps-background-400555078
image source: https://stateofmind13.com/2016/01/06/everything-you-need-to-know-about-the-new-lebanese-passport-rules/
image source: https://www.shutterstock.com/image-photo/brazilian-passport-above-map-governmentissued-document-165372926
image source: https://www.voanews.com/east-asia-pacific/fugitive-tycoon-ghosn-ready-stand-trial-fair-system

A personal Principle:

one Christoph - two research labs

Biometrics and Internet Security
Research Group
da/sec

Darmstadt Research Team

da/sec - Biometrics and Internet-Security Research Group

- Faculty-Members / PostDocs:
  - Harald Baier
  - Christoph Busch
  - Christian Rathgeb
  - Marta Gómez-Barrero
- PhD-Students / Lab-Engineers:
  - Pawel Drozdowski
  - Daniel Fischer
  - Thomas Göbel
  - Sergey Isadskiy
  - Jascha Kolberg
  - Lorenz Liebler
  - Hareesh Mandalapu
  - Jannis Priesnitz
  - Ulrich Scherhag
  - Janier Soler

2019

- Key-factors - since 2009:
  - 3 European funded projects,
    10 German funded projects
    5 research projects funded by the German BSI,
    2 industrial projects,
  - cooperated with > 30 research partners

https://dasec.h-da.de/

IT-Security in Darmstadt

National Research Center for Applied Cybersecurity (ATHENE)

- 400+ scientist from 47+ countries

TECHNISCHE UNIVERSITÄT DARMSTADT

CYSEC research group at TU Darmstadt

CYSEC Cybersecurity TU Darmstadt

Fraunhofer SIT

Fraunhofer Institute for Secure Information Technology SIT

Fraunhofer IGD

Fraunhofer Institute for Computer Graphics Research IGD

h_da HOCHSCHULE DARMSTADT UNIVERSITY OF APPLIED SCIENCES

da/sec research group at Hochschule Darmstadt

da/sec BIOMETRICS AND INTERNET-SECURITY RESEARCH GROUP

Darmstadt in the Rhine Valley

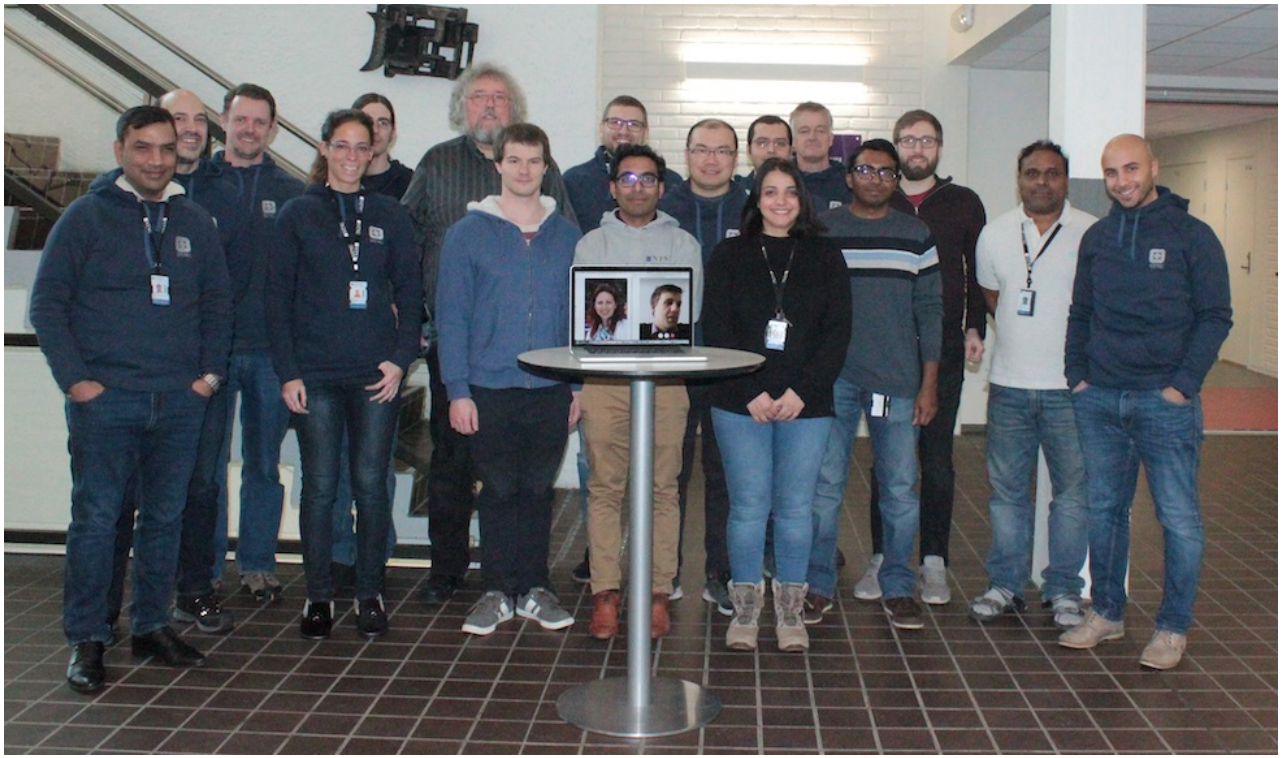
Darmstadt in the Rhine Valley

Darmstadt in the Rhine Valley

Norwegian Biometrics Laboratory

Norwegian Biometrics Laboratory (NBL)

- Faculty-Members / PostDocs:
  - Christoph Busch
  - Patrick Bours
  - Raghu Ramachandra
  - Kiran Raja
  - Guoqiang Li
  - Koshorkumar Upla
  - Mudasir Wani
  - Mohammad Derawi
  - Marta Gomez-Barrero
  - Patrick Schuch
  - Bian Yang
- PhD-Students / Lab-Engineers:
  - Alexander Kipfel
  - Ali Khodabakhsh
  - Edlira Martiri
  - Hareesh Mandalapu
  - Jag Mohan Singh
  - Lars Erik Pedersen
  - Loic Bergeron
  - Martin Stokkenes
  - Pankaj Wasnik
  - Parisa Borj
  - Pawel Drozdowski
  - Sushma Venkatesh
  - Tobias Scheer



2019

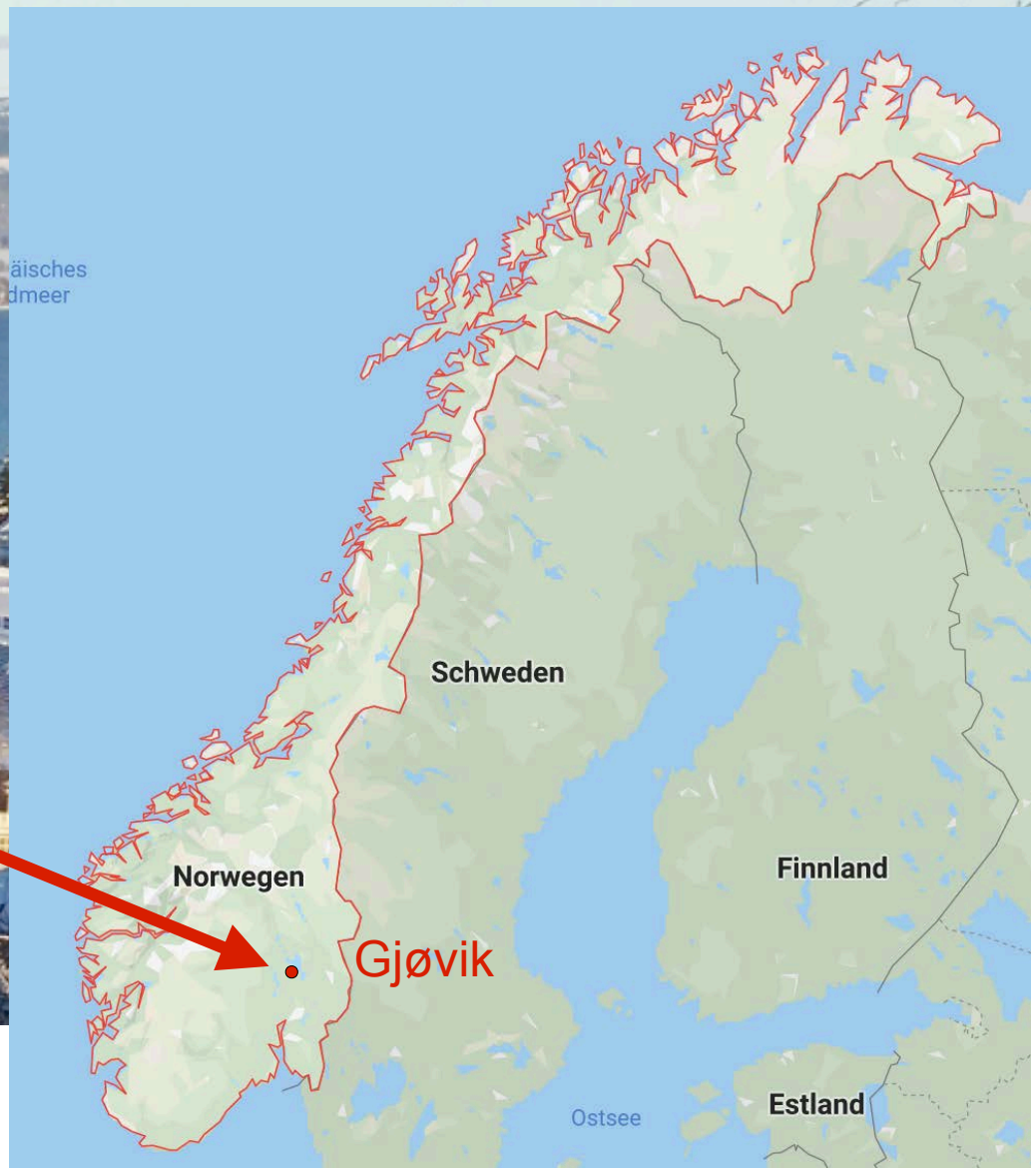
- represents an active focus point of the Department Department of Information Security and Communication Technology (IIK)
- keyfactors - since 2008:
  7 European funded projects,
  2 Norwegian funded projects
  2 US-government funded project,
  3 research projects funded by the German BSI,
  4 industrial projects

Gjøvik at Lake Mjøsa

Gjøvik at Lake Mjøsa

- Gjøvik is at the western shore of lake Mjøsa
  - the largest fresh water lake in Norway
    117 km long and 440m deep
- Gjøvik was part of the 1994
  winter olympic games
  - that took place in the triangle:
    Lillehammer - Hamar - Gjøvik
  - Since those days Gjøvik has the famous fjellhalle

Gjøvik at Lake Mjøsa



There are Days with Sunshine in Norway

Research Topics

Biometric research

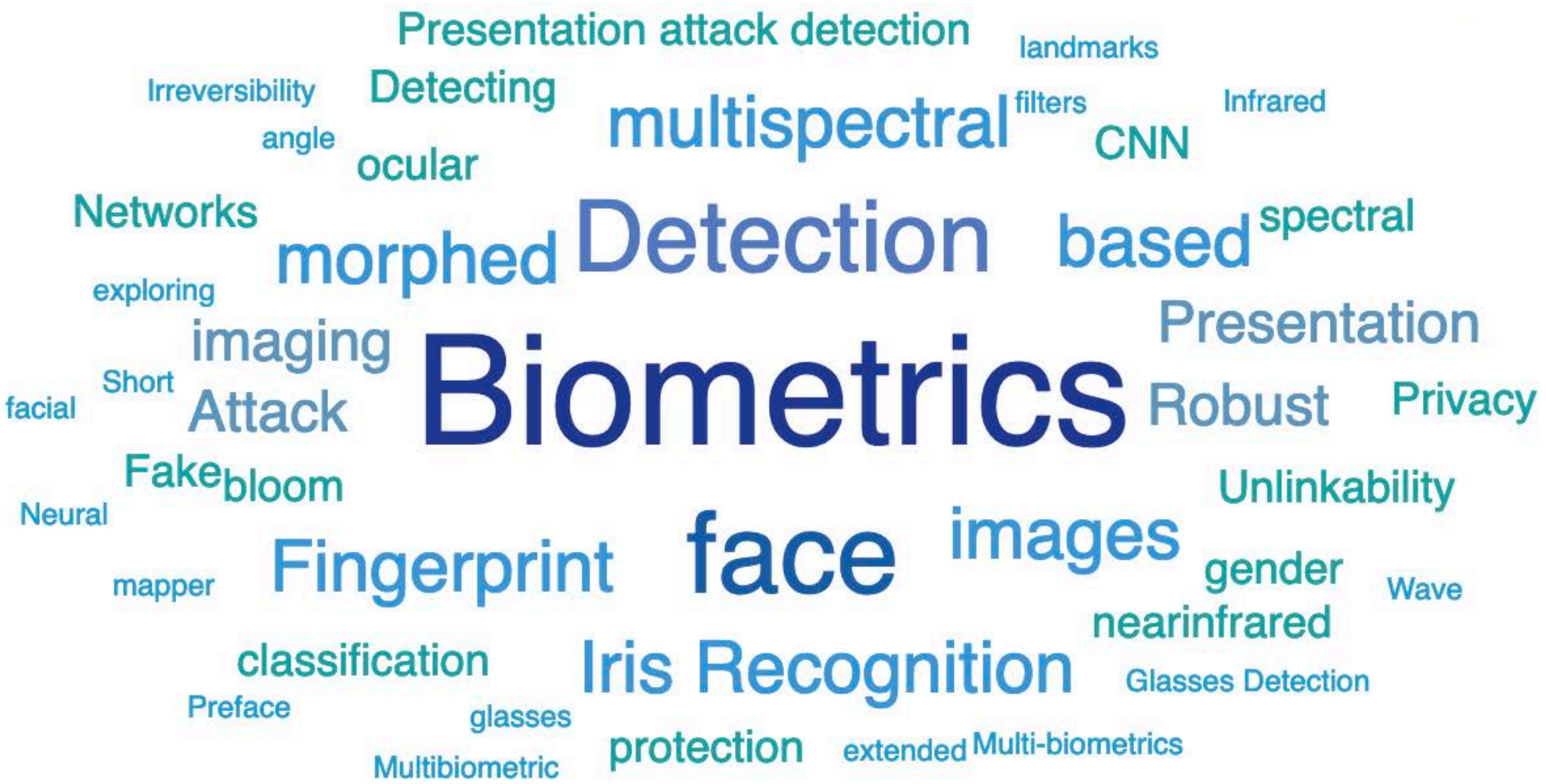
- Covering various physiological and behavioral biometrics: 2D- and 3D-face recognition, iris and periocular recognition, fingerprint recognition, fingervein recognition, ear recognition, signature recognition, speaker recognition, gait recognition, keystroke recognition, gesture recognition and mouse dynamics.
- Focus on biometric template protection and presentation attack detection / morphing attack detection

Projects

- National: BioKeyS, NID, NFIQ2.0, OCT-II, SWAN, BioMobile-II, BioBiDa, DIRECT-PAD, FACETRUST
- EU: TURBINE, BEST Network, FIDELITY, INGRESS, PIDaaS, ORIGINS, SMILE, SOTAMD, TReSPAsS, PRIMA
- US: NIST-BTPMetric, IARPA-BATL
- Industry: IDEX, Idemia-Morpho, Secunet Dermalog, CrossMatch, Fujitsu,

Norwegian Biometrics Laboratory (NBL)

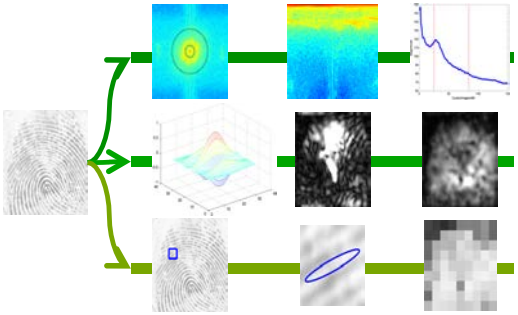
Our 2018 publication tag cloud



Application Oriented Research

Quality metrics for fingerprint images - NFIQ2.0

- Performance improvements can be achieved by improving data quality and integrity.



- Providing constructive feedback only possible if cause of poor quality is known.

character behavior environment Imaging/system

- Research results constitute the content of ISO/IEC 29794-4 and will be used in enrolment for the Visa Information System

https://christoph-busch.de/projects-nfiq2.html

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

Federal Office for Information Security

Bundeskriminalamt

secunet

Fraunhofer IGD

Travel Documents

Standardised Travel Documents

ICAO - International Civil Aviation Organisation

- A specialised UN agency (Headquarter Montreal)
- 191 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

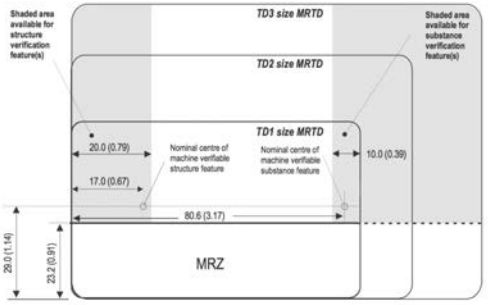
Biometrics and ePassports

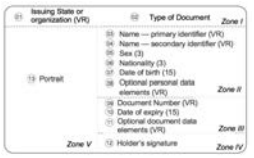
- ICAO - New Orleans Resolution - March 2003
  - *"ICAO TAG-MRTD/NTWG recognises that Member States currently and will continue to utilise the facial image as the primary identifier for MRTDs and as such endorses the use of standardised digitally stored facial images as the globally interoperable biometric to support facial recognition technologies for machine assisted identity verification with machine-readable travel documents.*
  - *ICAO TAG-MRTD/NTWG further recognises that in addition to the use of a digitally stored facial image, Member States can use standardised digitally stored fingerprint and/or iris images as an additional globally interoperable biometrics in support of machine assisted verification and/or identification.*
  - *Member States, in their initial deployment of MRTDs with biometrics identifiers, are encouraged to adopt contactless IC media of sufficient capacity to facilitate on-board storage of additional MRTD data and biometric identifiers."*

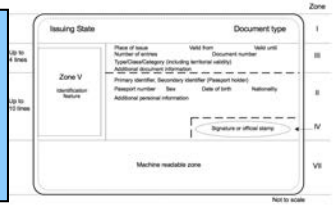
ICAO International Specifications

Doc 9303: relevant parts

Part 2: Specification for the Security of the Design	sizes of MRTD: TD1 (cards), TD2, TD3 (passports)
Part 3: Specifications Common to all MRTDs	physical characteristics, visual zone, MRZ, conventions, face image
Part 4: TD3 size MRTDs electronic Passports (MRP)	MRP data page (design and data fields), primary identifier, check digits
Part 5:TD1 size MRTDs electronic citizen cards	sequence of data elements, truncation rules
Part 7: Machine Readable Visas (MRV)	specification which allow both visual and machine readable means
Part 10: Logical Data Structure (LDS)	specification for both visual and mach. readable







Encoded Identification Feature(s)	Global Interchange Feature	DG2	Encoded Face
	Additional Feature(s)	DG3	Encoded Finger(s)
		DG4	Encoded Eye(s)

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
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

ePassport Details

Data size 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)

New in 2020

- 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 by April 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 Revisited

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

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

- Multiple individuals - one passport

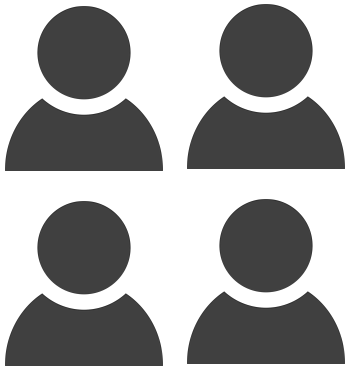


image source: https://pixabay.com/de/vectors/tick-sternchen-kreuz-rot-gr%C3%BCn-40678/

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

Problem Description

History - 2014

Integrated Project FIDELITY

http://www.fidelity-project.eu/

- Fast and trustworthy Identity Delivery and check with ePassports leveraging Traveler privacy
- 4 years project (2012-2016)
  - European 7th Framework Programme
- Objectives:
  - To improve the ePassport issuing process
    - Security of birth certificates and other evidence of identity
    - Quality of biometric data in the chip
    - One individual one passport (duplicate enrolment check)
  - To demonstrate solutions that enable faster and more secure and efficient real-time authentication of individuals at border crossing
  - To protect privacy of the travel document holders with a privacy-by-design approach.

[FFM2014] M. Ferrara, A. Franco, D. Maltoni, “The Magic Passport”, in Proceedings IEEE IJCB 2014

Problem: Morphing Attacks

Morphing attack scenario

- Passport application of the accomplice A

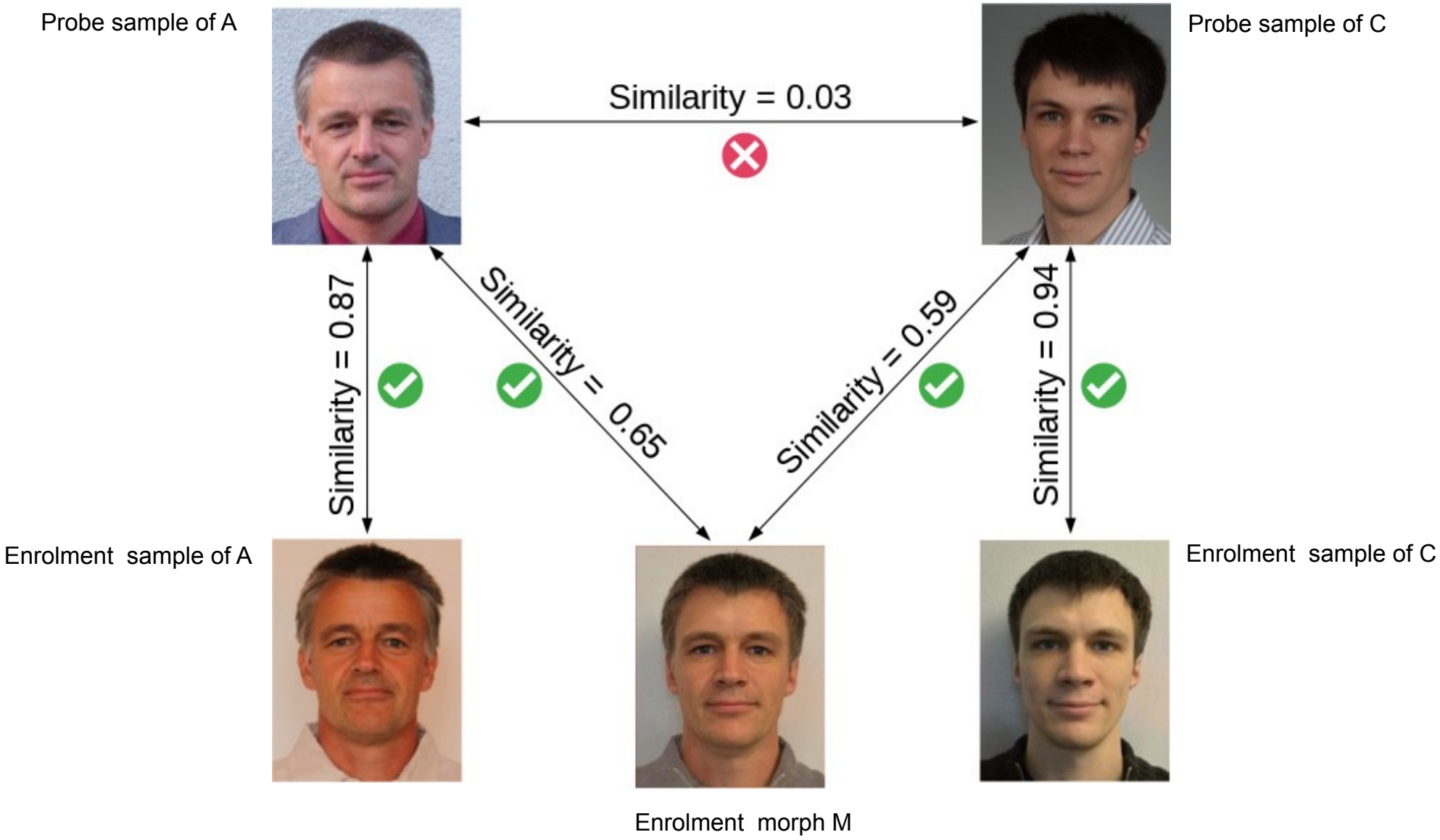
Problem: Morphing Attacks

Morphing attack scenario

- Border control

Problem: Morphing Attacks

Verification against morphed facial images



Problem: Morphing Attacks

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)

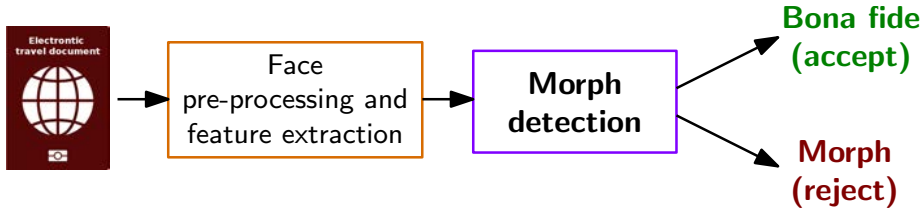
Morphing Attack Detection (MAD)

Scenarios and Methods

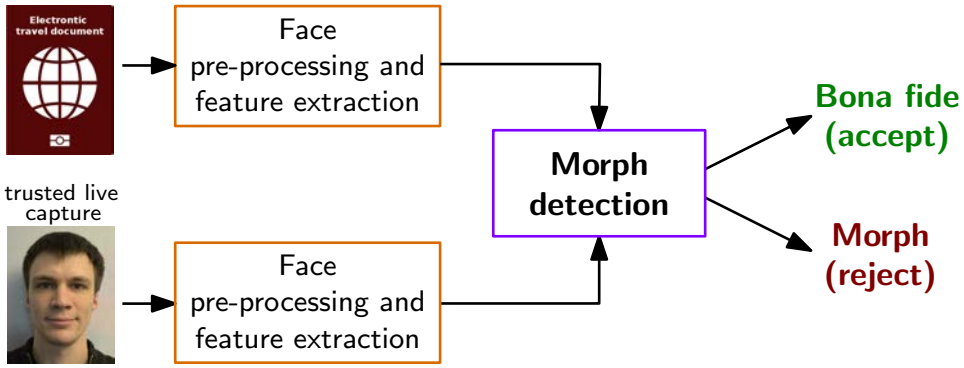
Morphing Attack Detection Scenarios

Real world scenarios

- No-reference morph detection
  - One single facial image is analysed (e.g. in the passport application office)



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

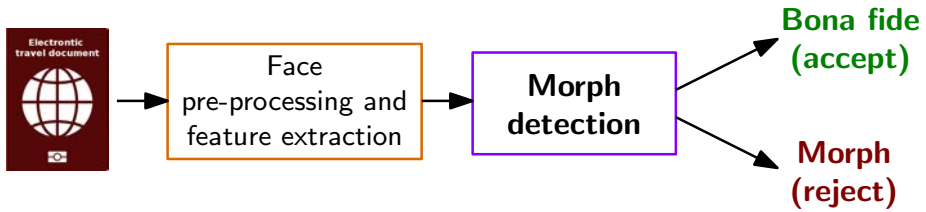


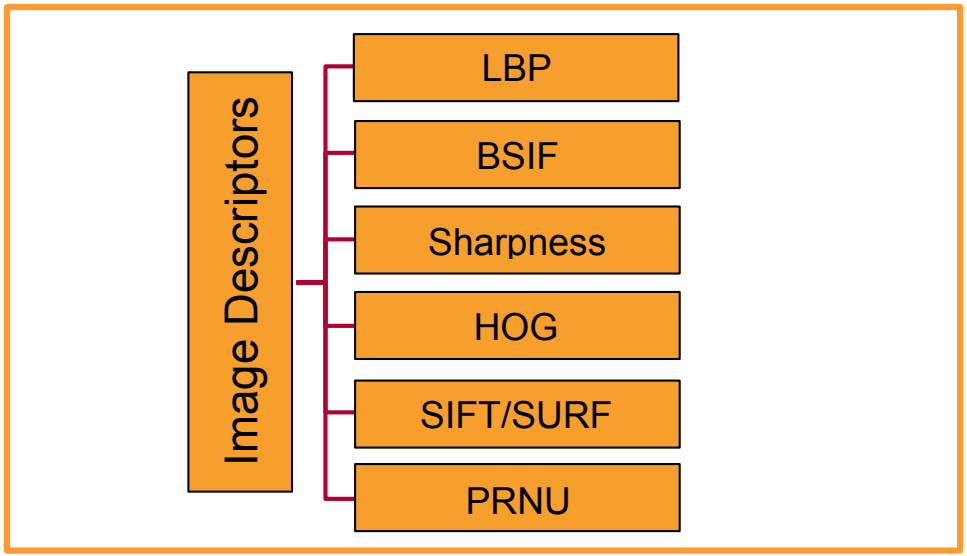
[SRB18a] U. Scherhag, C. Rathgeb, C. Busch: "Towards Detection of Morphed Face Images in electronic Travel Documents", in Proceedings of the 13th IAPR International Workshop on Document Analysis Systems (DAS 2018), April 24-27, (2018)

Face Pre-processing and Feature Extraction

Morphing Attack Detection (MAD) with texture analysis

- Image descriptors as hand-crafted features





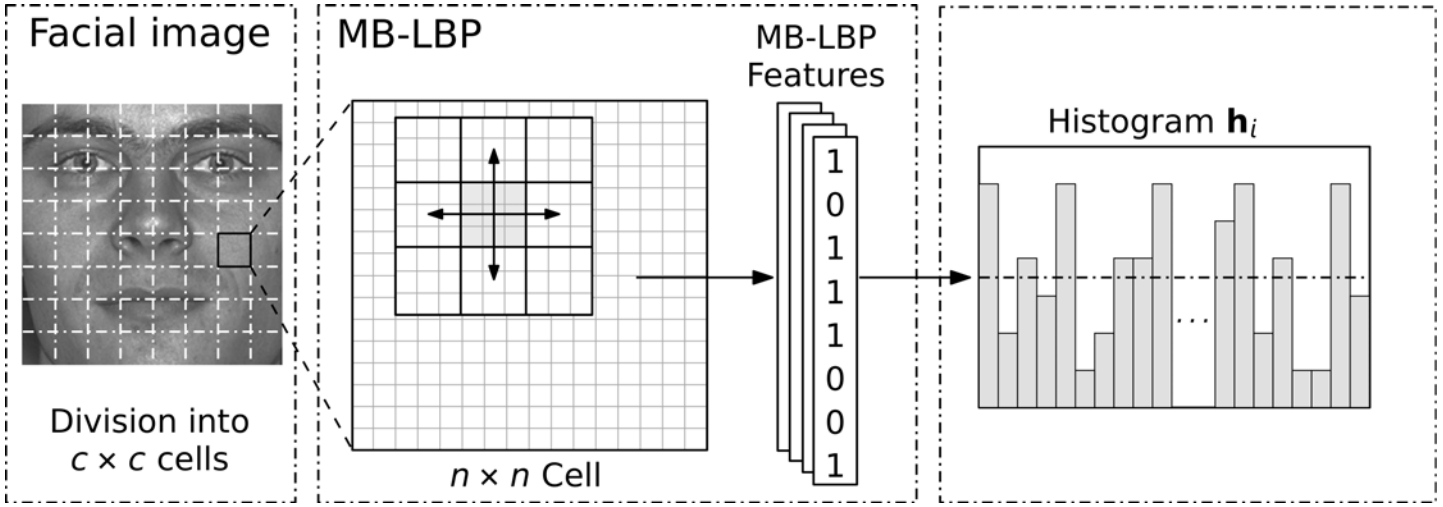
Morph Detection Classifier

[SRB18b] 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)

Face Pre-processing and Feature Extraction

MAD with image descriptor

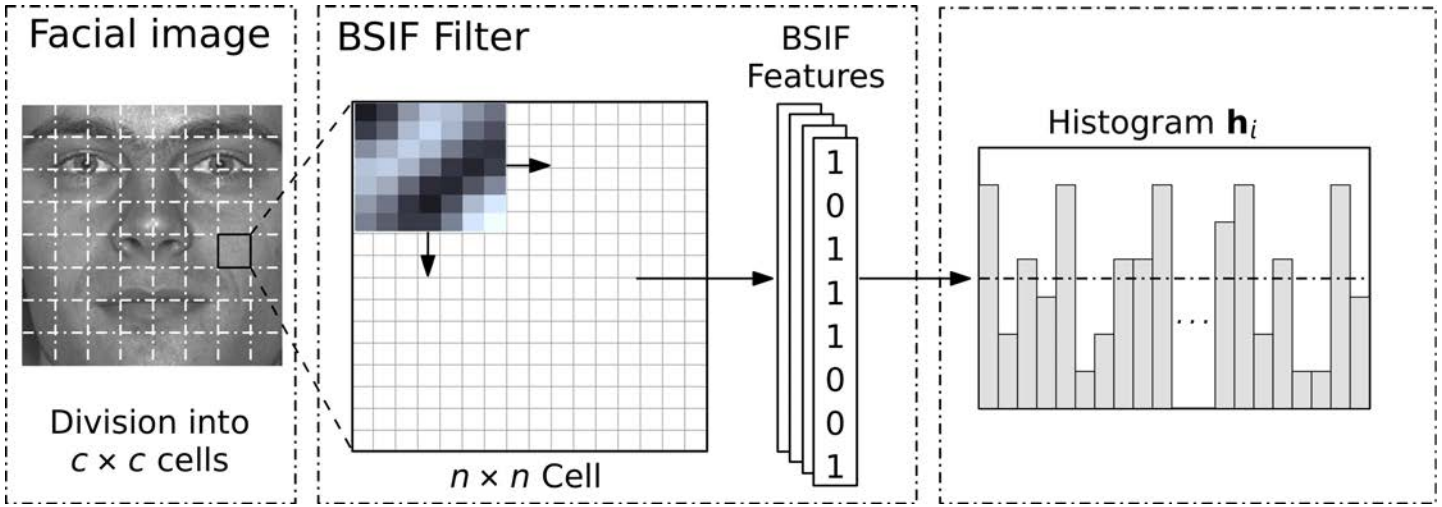
- Local Binary Pattern (LBP)



Face Pre-processing and Feature Extraction

MAD with image descriptor

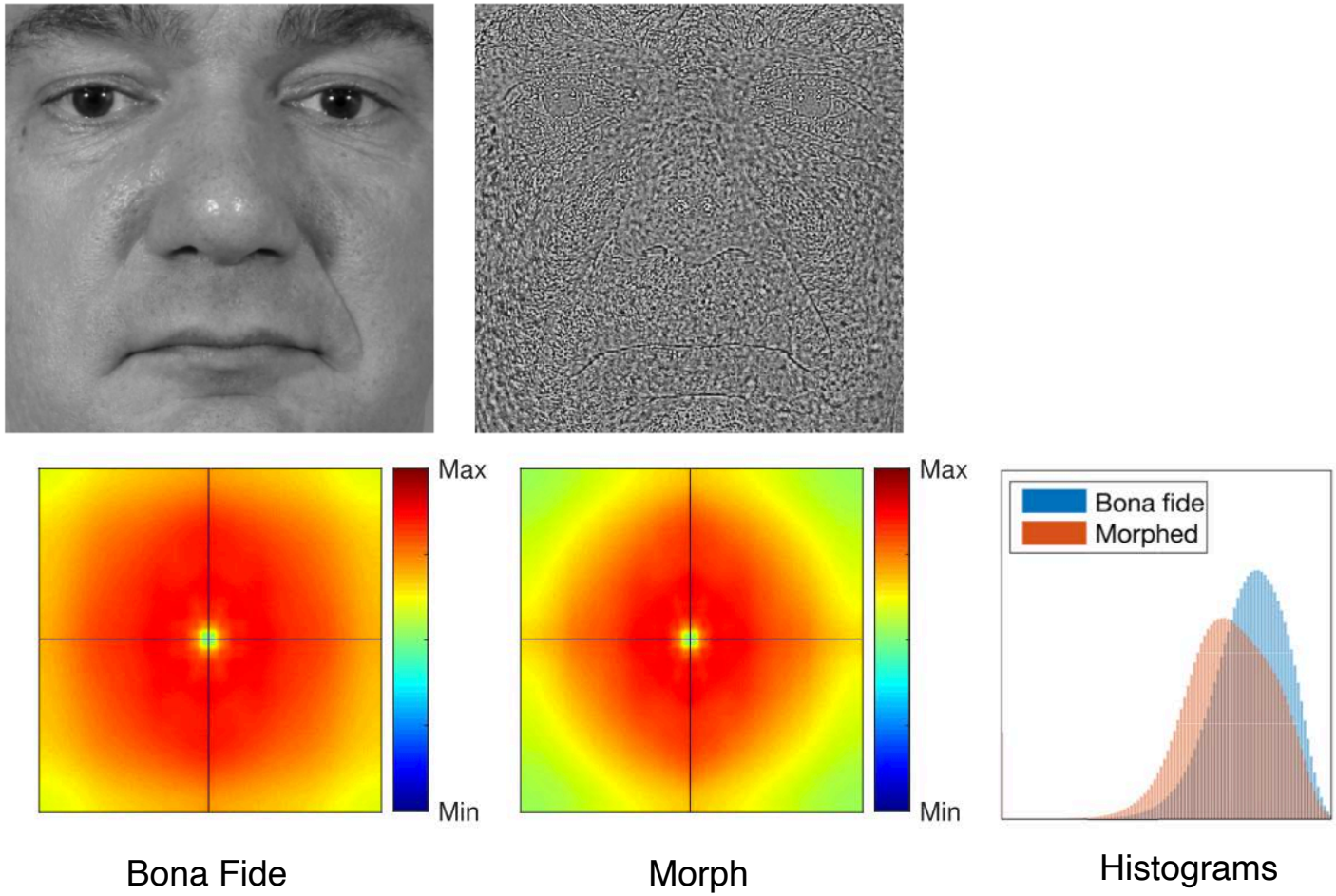
- Binarized Statistical Image Features (BSIF)



Face Pre-processing and Feature Extraction

MAD with image descriptor / forensic approach

- Photo Response Non-Uniformity (PRNU)



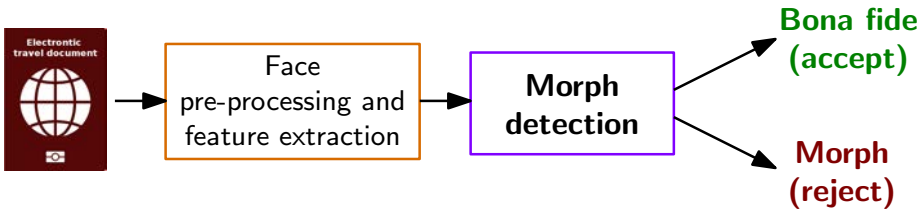
Bona Fide | Morph | Histograms

[SDRBU19] U. Scherhag, L. Debiasi, C. Rathgeb, C. Busch and A. Uhl: "Detection of Face Morphing Attacks based on PRNU Analysis“, in IEEE TBIOM, (2019)

Face Pre-processing and Feature Extraction

Morphing Attack Detection (MAD) with texture analysis

- Image descriptors as Deep features



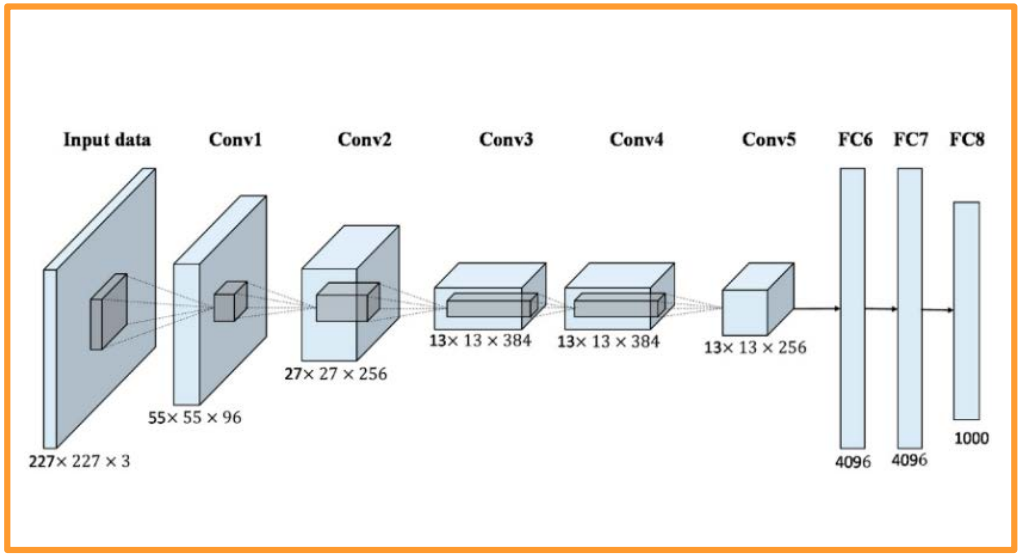
CNN BlackBox

Morph Detection Classifier

Face Pre-processing and Feature Extraction

MAD with deep learning

- Deep Features
  - pre-trained Convolutional Neural Network (CNN)
  - OpenFace



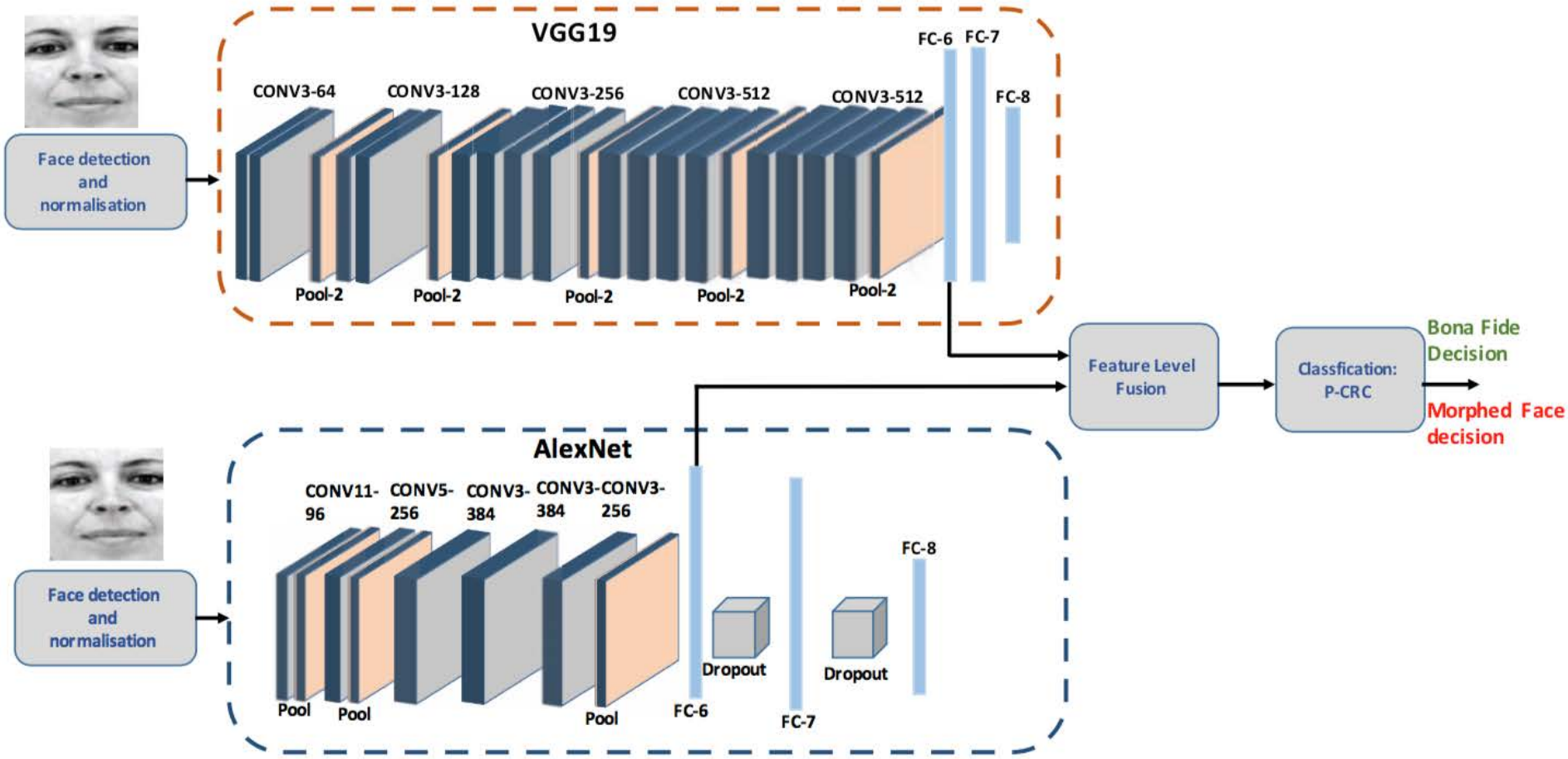
Morph Detection Classifier

[Amos16] B. Amos, B. Ludwiczuk und M. Satyanarayanan: „Open-Face: A general-purpose face recognition library with mobile applications“, Technical report, CMU School of Computer Science, (2016)

No-Reference Morph Detection

MAD with deep learning

- Feature level fusion of Deep CNNs



[RRVBu17] 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), July 21-26, (2017)

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

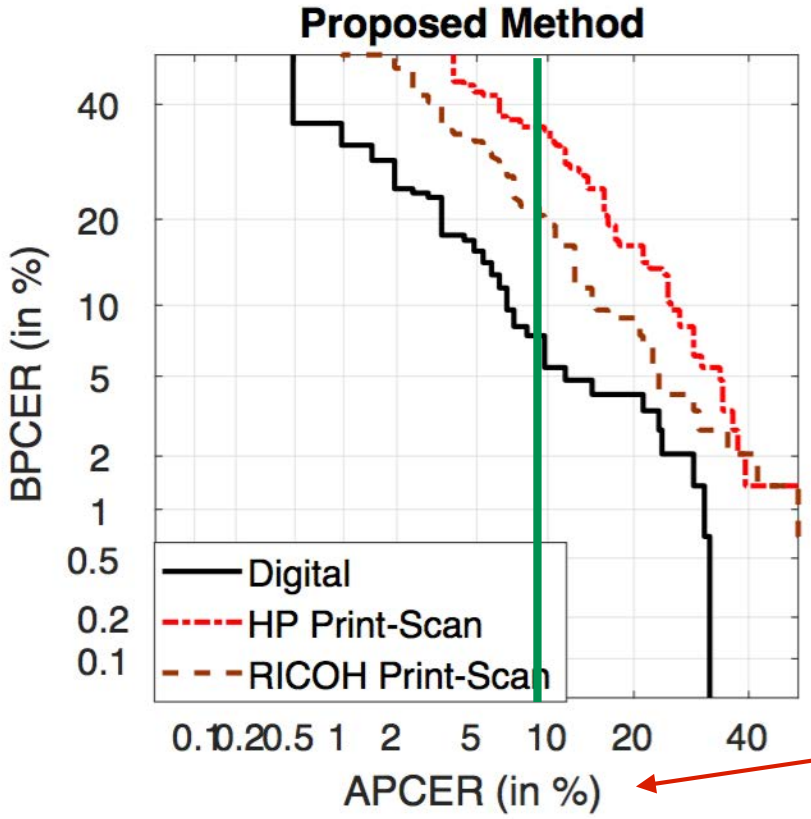
source: [ISO/IEC 30107-3] SO/IEC 30107-3, “Biometric presentation attack detection - Part 3: Testing and reporting”, (2016)
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67381

Standardized Testing Metrics

Definition of PAD metrics in ISO/IEC 30107-3

- DET curve analyzing operating points for various thresholds and plot security measures versus convenience measures
- Example:

convenience measure



security measure (strength of function)

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 [SNR17]
- Evaluations must consider many parameters

$$result = f\,(dataset\text{-}training,\ dataset\text{-}testing,\ morphing\text{-}attack,\ landmark\text{-}detector,\ feature\text{-}extractor,\ classifier,\ scenario\ (no\text{-}reference\ vs.\ differential),\ post\text{-}processing,\ printer,\ scanner)$$

[SNR17] 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 at least 3 algorithms
- Post-process automatically and manually
- Print and scan all morphed face images
- Adapt and integrate and test at least 3 MAD algorithms
- Test the MAD algorithms on the Uni Bologna server https://biolab.csr.unibo.it/FVConGoing

MAD Evaluation in SOTAMD

Benchmarks

- A new benchmark area for differential morphing 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 recently 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.

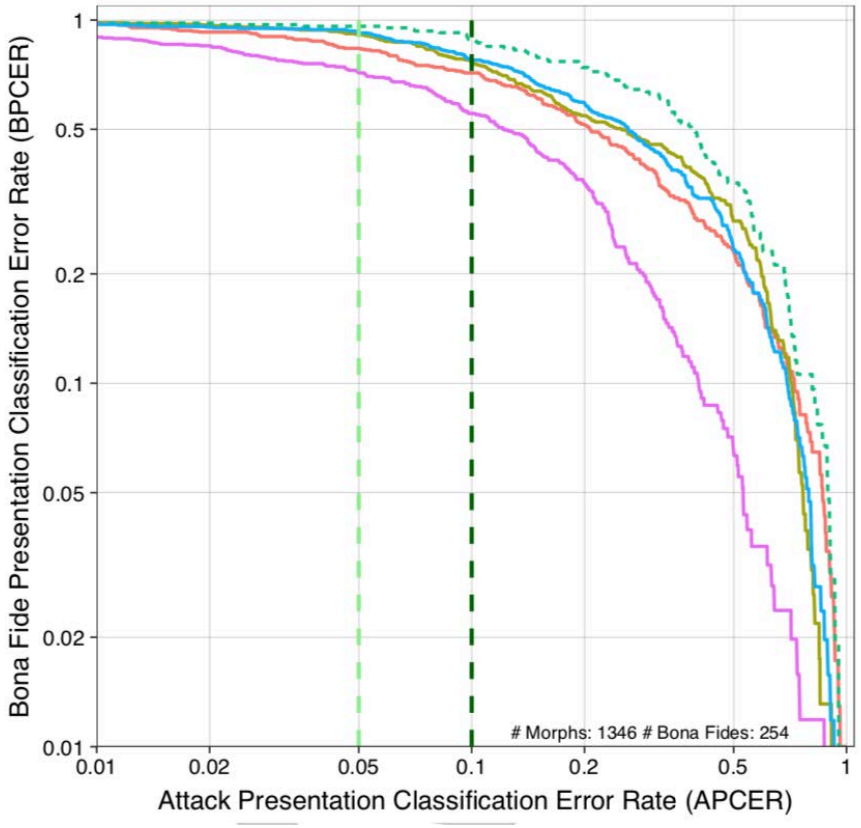
NIST only accepts Linux dynamically-linked library file;

- FVC-onGoing will accept both Windows and Linux executables

NIST-FRVT-MORPH

NIST draft report presented in September 2019

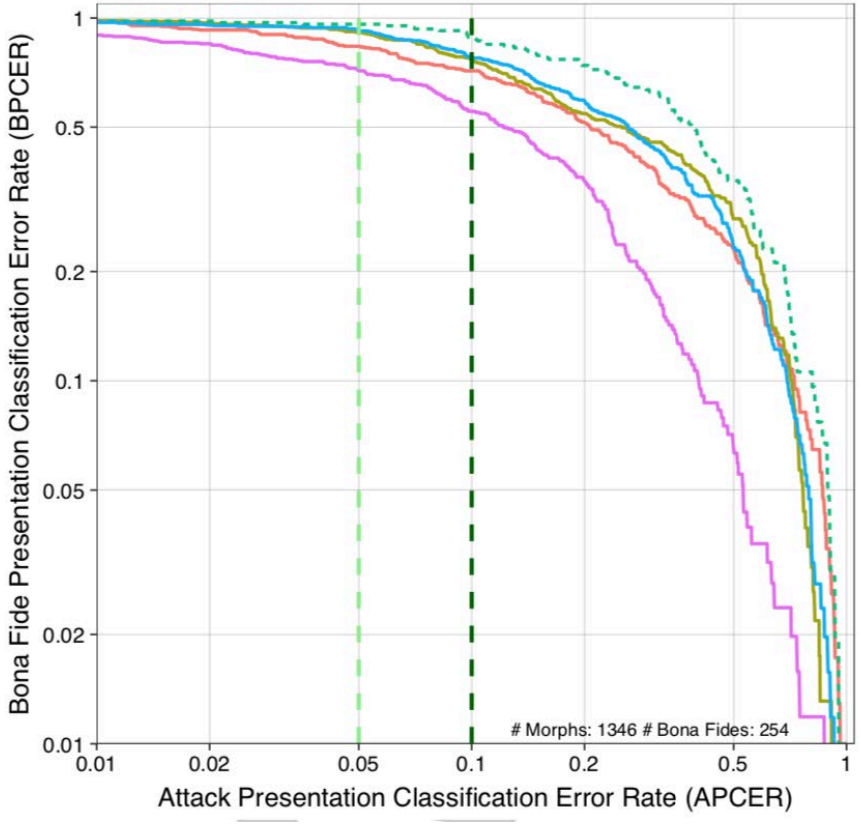
- for public review and comment
  https://www.nist.gov/sites/default/files/documents/2019/09/18/draft_frvt_morph_report_2019sept17.pdf
- results for automated morphs

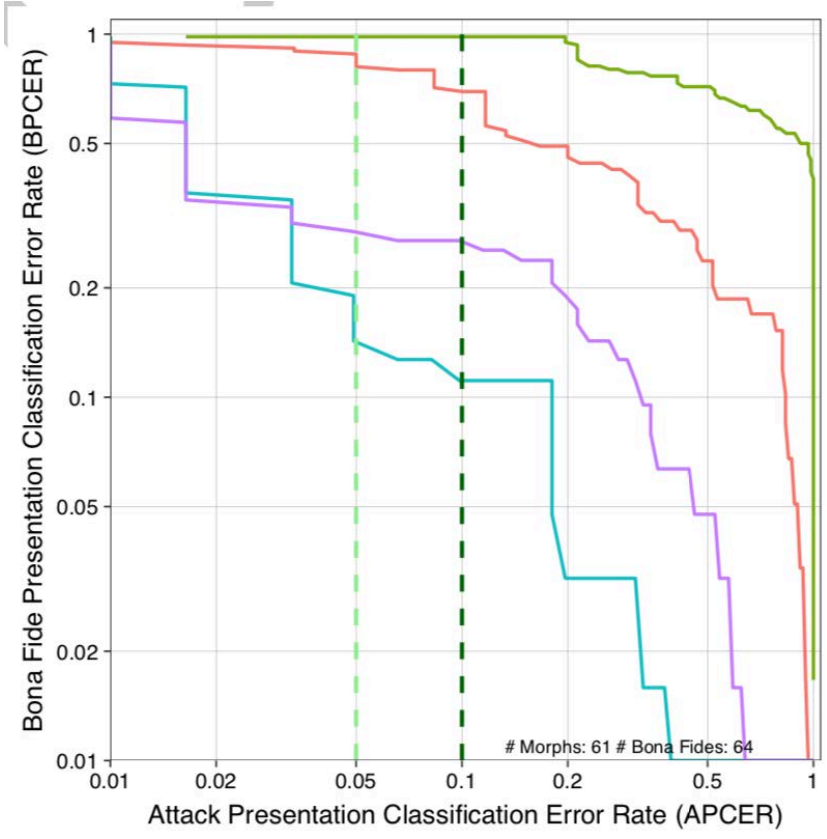


NIST-FRVT-MORPH

NIST draft report presented in September 2019

- for public review and comment
  https://www.nist.gov/sites/default/files/documents/2019/09/18/draft_frvt_morph_report_2019sept17.pdf
- results for automated morphs versus print and scanned
- note the low number of test samples





What needs to be done?

MAD Evaluations on Digital Images

First scientific publications on morphing attack detection

- Are based on a small dataset
- Addressing only digital application process
  (applicable for New Zealand, Estonia, Irland, Finland)

The upcoming evaluations

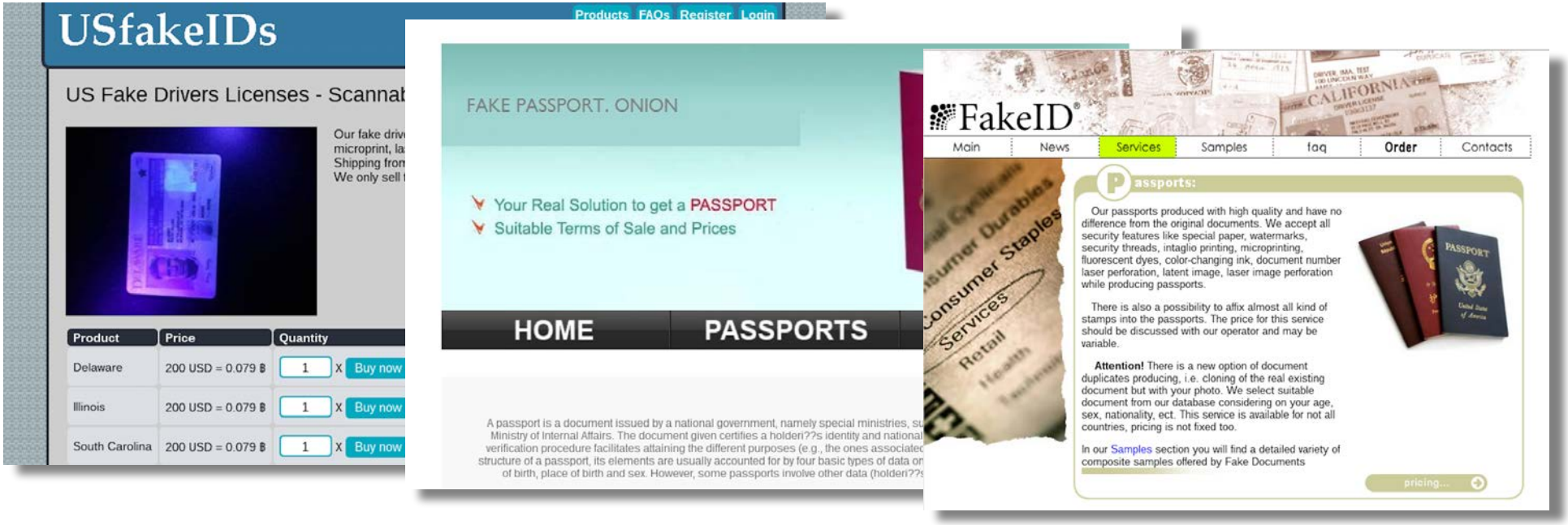
- NIST-FRVT-MORPH evaluation
- SOTAMD evaluation

will provide valuable insights

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

- 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

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

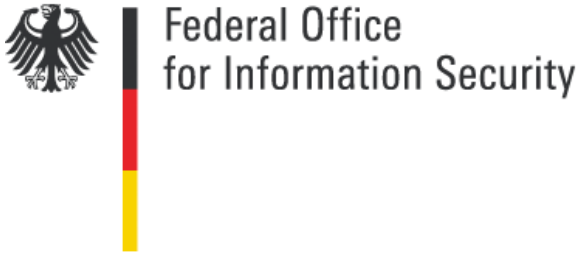
A. FACE MORPHING ATTACK

Thanks

I would like to thank the sponsors of this work:

- NGBS-Project funded by ATHENE

- FACETRUST-Project funded by BSI



- SOTAMD-Project funded by the European Union's Internal Security Fund — Borders and Visa

  - 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 da/sec - NBL team:
  - Ulrich Scherhag, Christian Rathgeb, Daniel Fischer, Sergey Isadskiy, Marta Gomez-Barrero, Kiran Raja, Raghu Ramachandra, Loic Bergeron, Jag Mohan Singh, Sushma Venkatesh
- In the FACETRUST-Project:
  - Ralph Breithaupt, Johannes Merkle
- In the SOTAMD-Project:
  - Dinusha Frings, Fons Knopjes, Uwe Seidel,
  - Davide Maltoni, Matteo Ferrara, Analisa Franco
  - Raymond Veldhuis, Luuk Spreeuwers,

If you are a PhD student consider

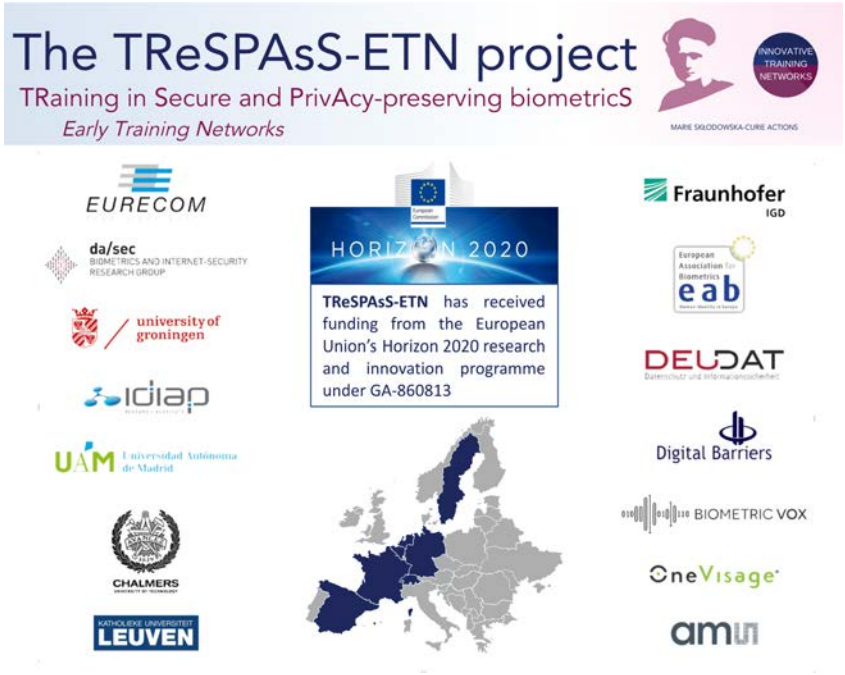
Darmstadt Biometric Week in September 2020

- 7th EAB research projects conference (EAB-RPC)
  - September 14-16, 2020 in Darmstadt, Germany
  - https://www.eab.org/events/program/151
- 19th IEEE BIOSIG conference
  - September 16-18, 2020 in Darmstadt, Germany
  - www.biosig.org/biosig-2020

If you are a Master student consider

The new European Training Networks

- 28 open PhD-positions!
- TReSPAsS: TRaining in Secure and PrivAcy preserving BiometricS
  - contact: christian.rathgeb@h-da.de for a position in Darmstadt
- PRIMA: PRIvacy MAtters
  - contact: bian.yang@ntnu.no for a position in Gjøvik



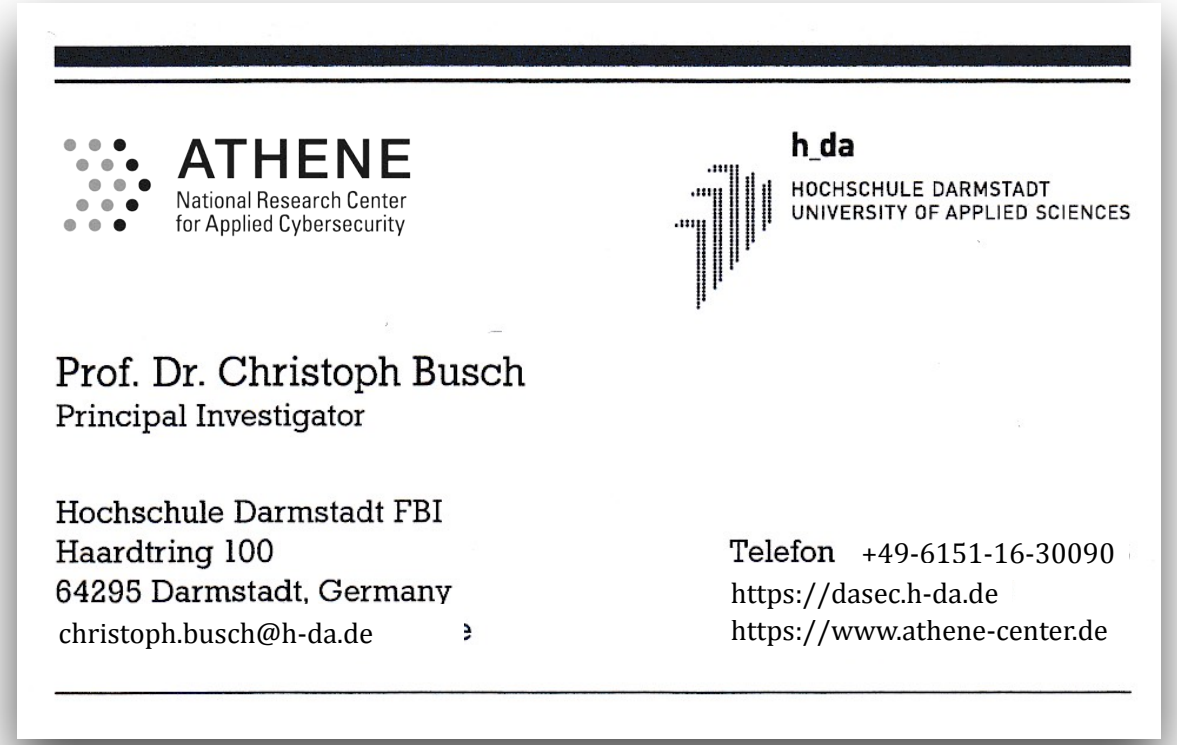
Contact

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