

Morphing Attack Detection Overview

Christoph Busch, Ulrich Scherhag, Christian Rathgeb, Marta Gomez-Barrero, Kiran Raja, Raghu Ramachandra, Sushma Venkatesh, Jag Singh, Loic Bergeron, Guoqiang Li, Daniel Fischer, Sergey Isadskiy

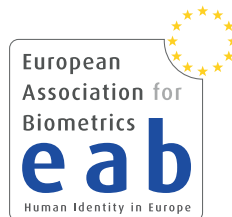
copy of slides available at:

<https://www.christoph-busch.de/projects-mad.html>

NBF, 2019-05-09



CRISP
Center for Research
in Security and Privacy



Overview

Agenda

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

Problem Description

Problem: Morphing Attacks

Enrolment attack with morphed facial images



Subject A



Morph = Subject A + Subject C



Subject C

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.

Problem: Morphing Attacks

Morphing attack scenario

- Passport application of the accomplice A



Problem: Morphing Attacks

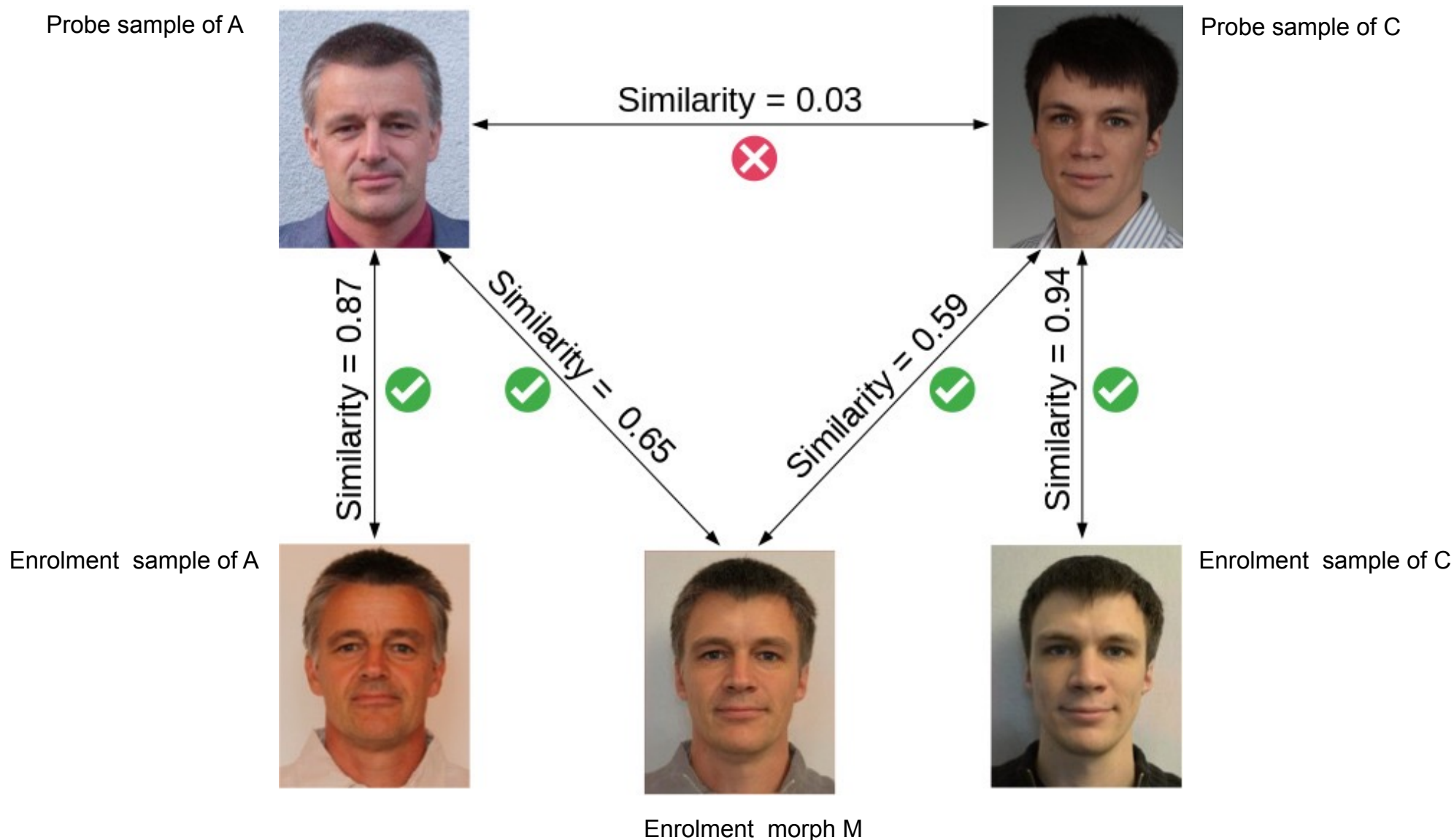
Morphing attack scenario

- Border control



Problem: Morphing Attacks

Verification against morphed facial images



Problem: Morphing Attacks

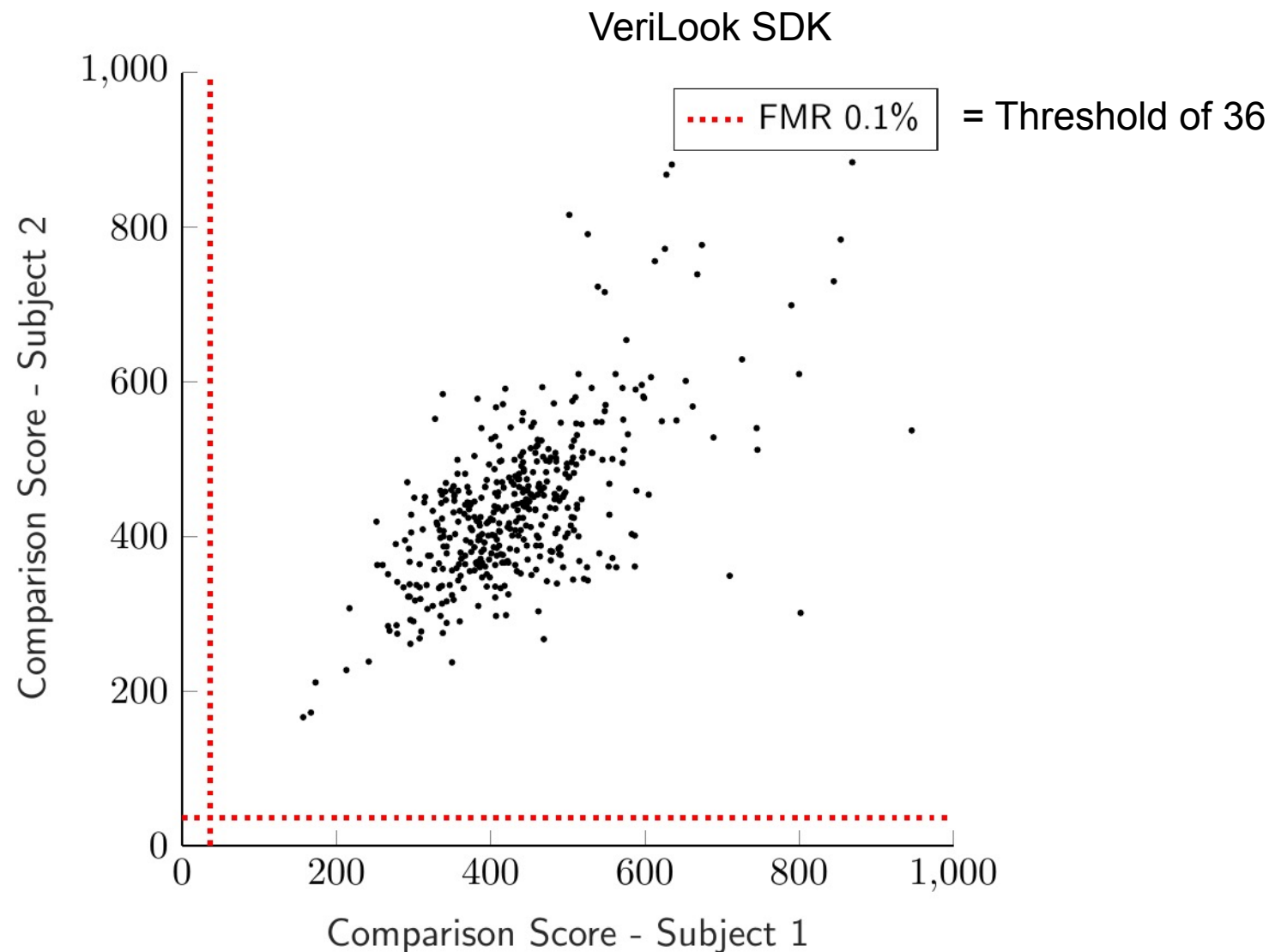
FIDELITY conclusion (December 2015)

- The **current procedure**, where a printed face photo can be provided by the citizen, **poses serious security risks**
- Solutions:
 - ▶ Photo studio should digitally sign the picture and send it to the passport application office (this is in progress for Finland)
 - ▶ Switch to **live enrolment** (that is the case for Norway and Sweden)
 - ▶ Software-supported **detection** of **morphed face images**

What is the vulnerability?

Scale of the Problem: Vulnerability

Vulnerability of face recognition systems to morphing attacks



Scale of the Problem: Vulnerability

A metric to measure the vulnerability of face recognition systems

- A morphed image is only successful, if all contributing subjects can reach a match (i.e. **all subjects will be verified**)
- Mated Morph Presentation Match Rate (MMPMR)

$$MMPMR = \frac{1}{M} \cdot \sum_{m=1}^M \left\{ \left[\min_{n=1, \dots, N_m} S_m^n \right] > \tau \right\}$$

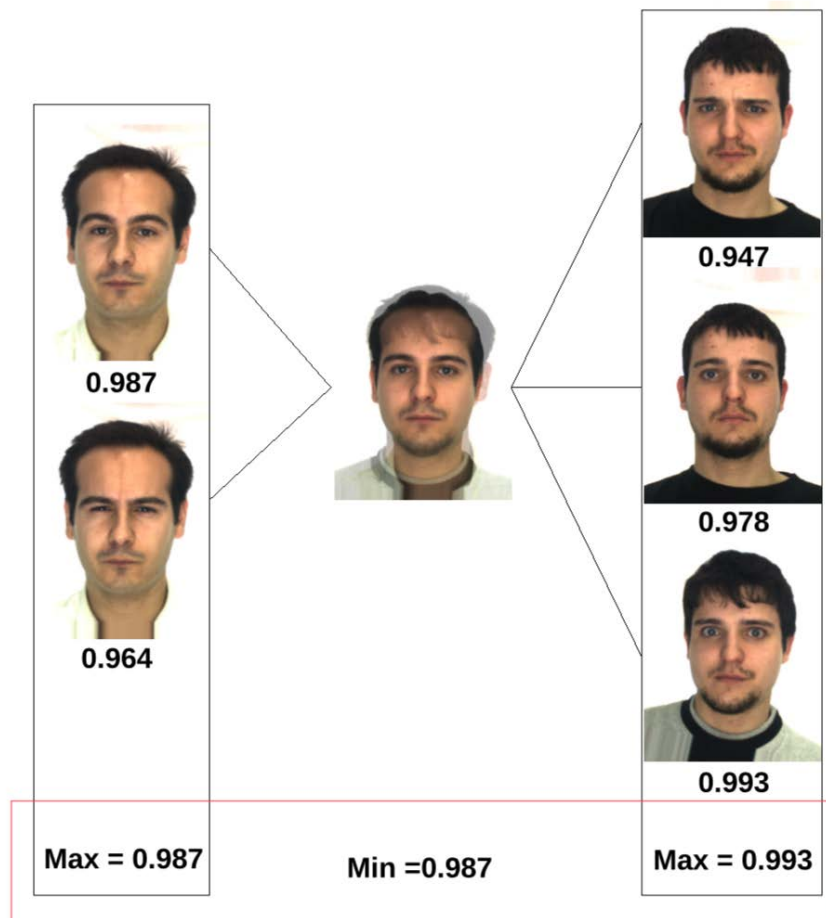
- ▶ τ is the verification threshold
- ▶ S_m^n is the mated morph comparison score of the n -th subject of morph m
- ▶ M is the total number of morphed images
- ▶ N_m is the total number of subjects contributing to morph m

[SNRG+17] U. Scherhag, A. Nautsch, C. Rathgeb, M. Gomez-Barrero, R. Veldhuis, L. Spreeuwes, 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

Example for the metric

- MinMax-Mated Morph Presentation Match Rate



[SNRG+17] U. Scherhag, A. Nautsch, C. Rathgeb, M. Gomez-Barrero, R. Veldhuis, L. Spreeuwes, 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

Human Capabilities: Experts (44 border guards)



[MFM2016] 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)

Standardised Metrics for Attack Detection

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-3

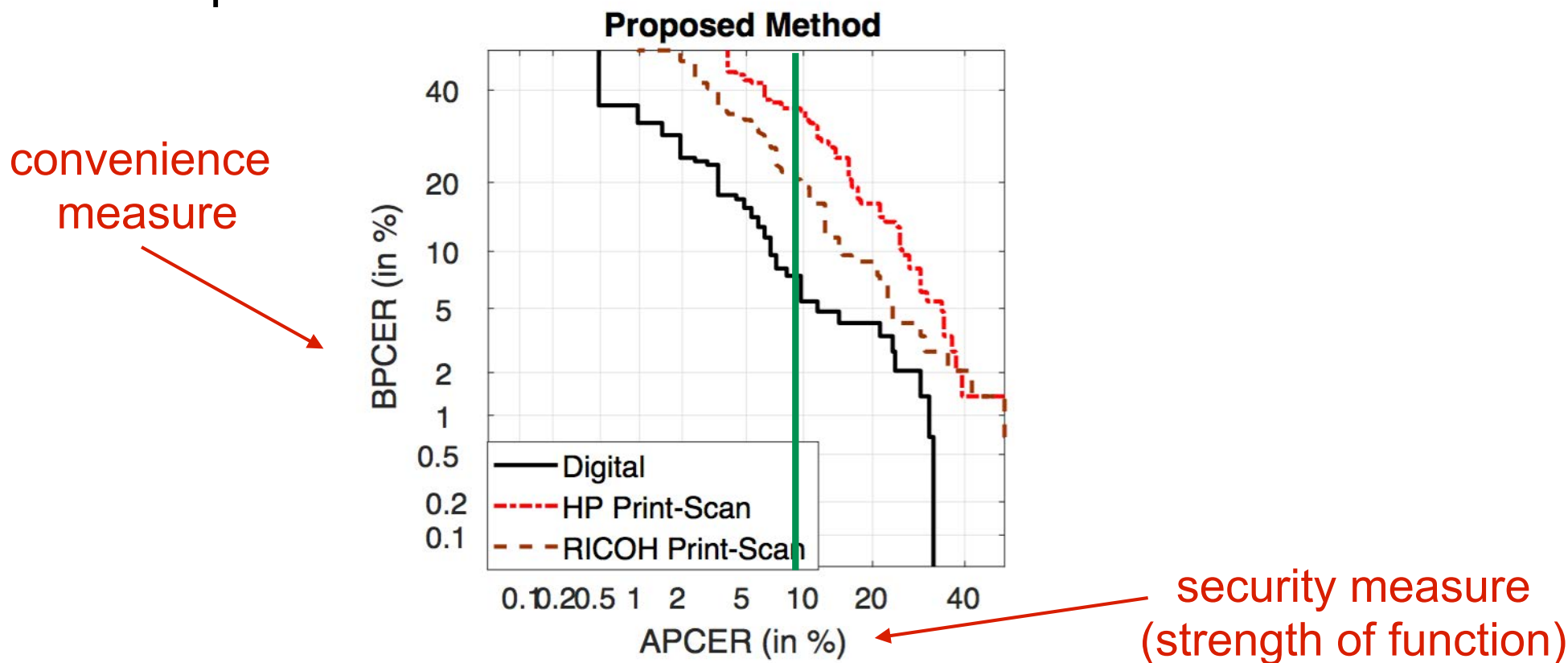
- Testing the **PAD subsystem** with false-negative and false-positive errors:
- **Attack presentation classification error rate (APCER)**
*proportion of **attack presentations** using the same PAI species incorrectly **classified as bona fide presentations** in a specific scenario*
- **Bona fide presentation 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

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-3

- DET curve analyzing operating points for various **security** measures and **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)

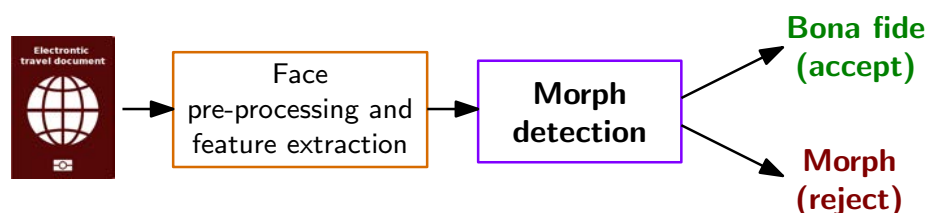
Morphing Attack Detection (MAD)

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)



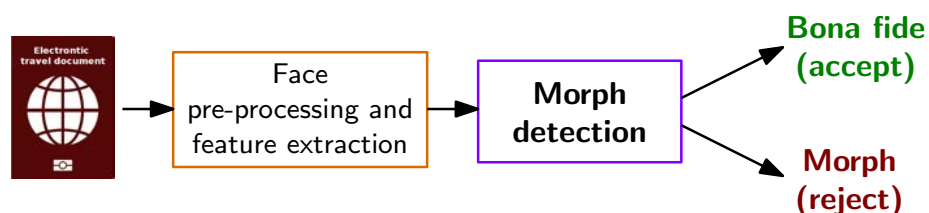
[SRB18a] U. Scherhag, C. Rathgeb, C. Busch: "Towards Detection of Morphed Face Images in electronic Travel Documents", in Proceedings of the 13th IAPR International Workshop on Document Analysis Systems (DAS 2018), April 24-27, (2018)

Morphing Attack Detection Scenarios

Real world scenarios

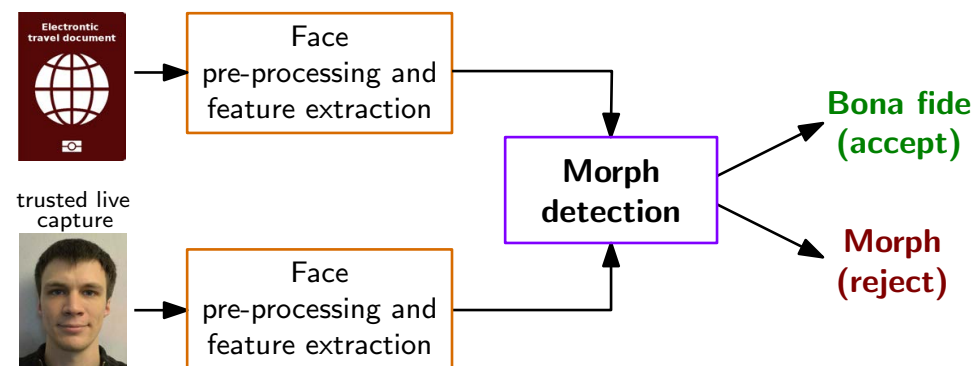
- No-reference morph detection

- ▶ 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)

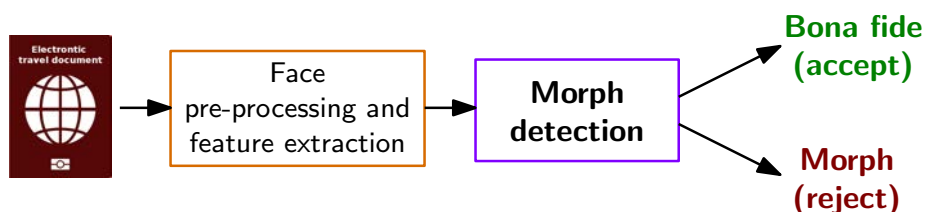


[SRB18a] U. Scherhag, C. Rathgeb, C. Busch: "Towards Detection of Morphed Face Images in electronic Travel Documents", in Proceedings of the 13th IAPR International Workshop on Document Analysis Systems (DAS 2018), April 24-27, (2018)

Face Pre-processing and Feature Extraction

Morphing Attack Detection (MAD) with texture analysis

- Image descriptors as **hand-crafted** features

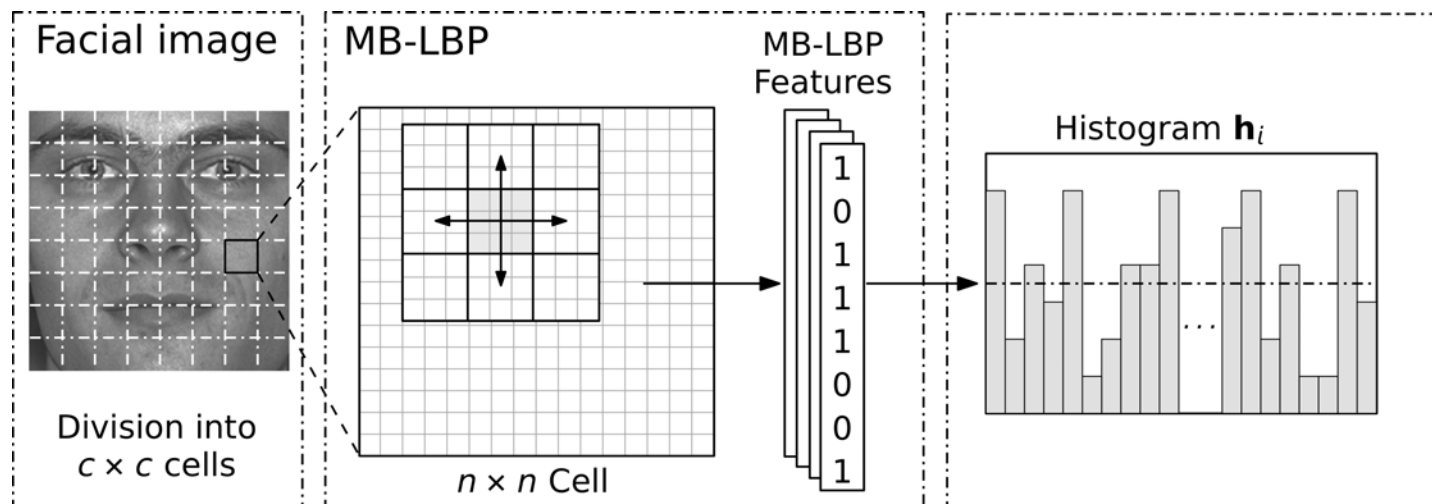


[SRB18b] U. Scherhag, C. Rathgeb, C. Busch: „Detection of Morphed Faces from Single Images: a Multi-Algorithm Fusion Approach“, in Proceedings of the 2nd International Conference on Biometric Engineering and Applications (ICBEA 2018), Amsterdam, The Netherlands, May 16-18, (2018)

Face Pre-processing and Feature Extraction

MAD with image descriptor

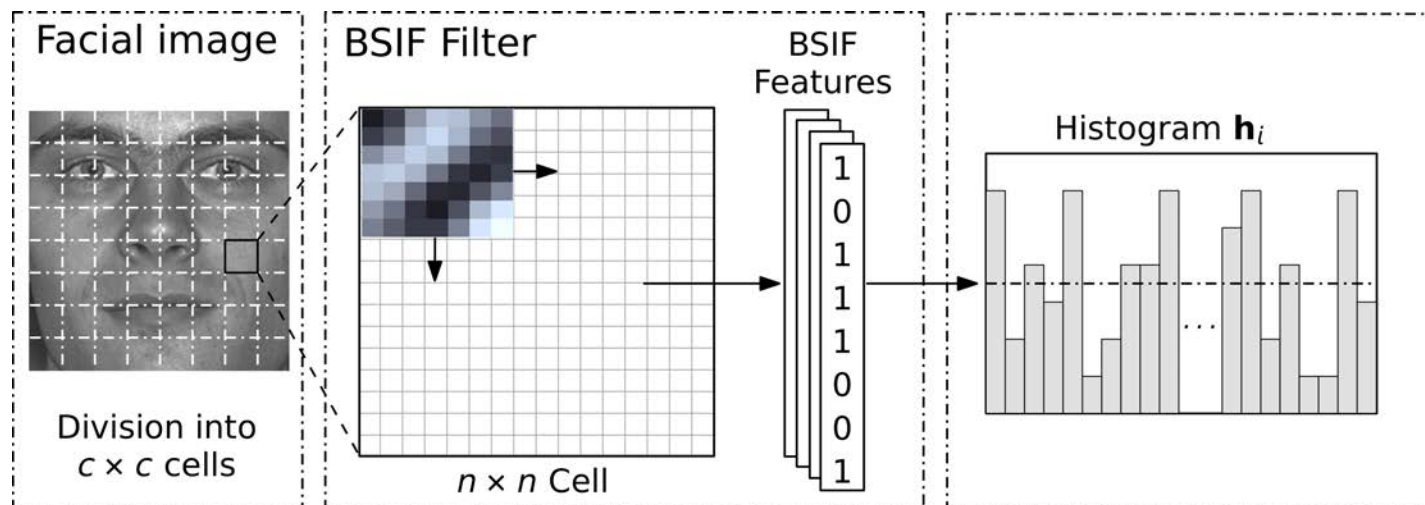
- Local Binary Pattern (LBP)



Face Pre-processing and Feature Extraction

MAD with image descriptor

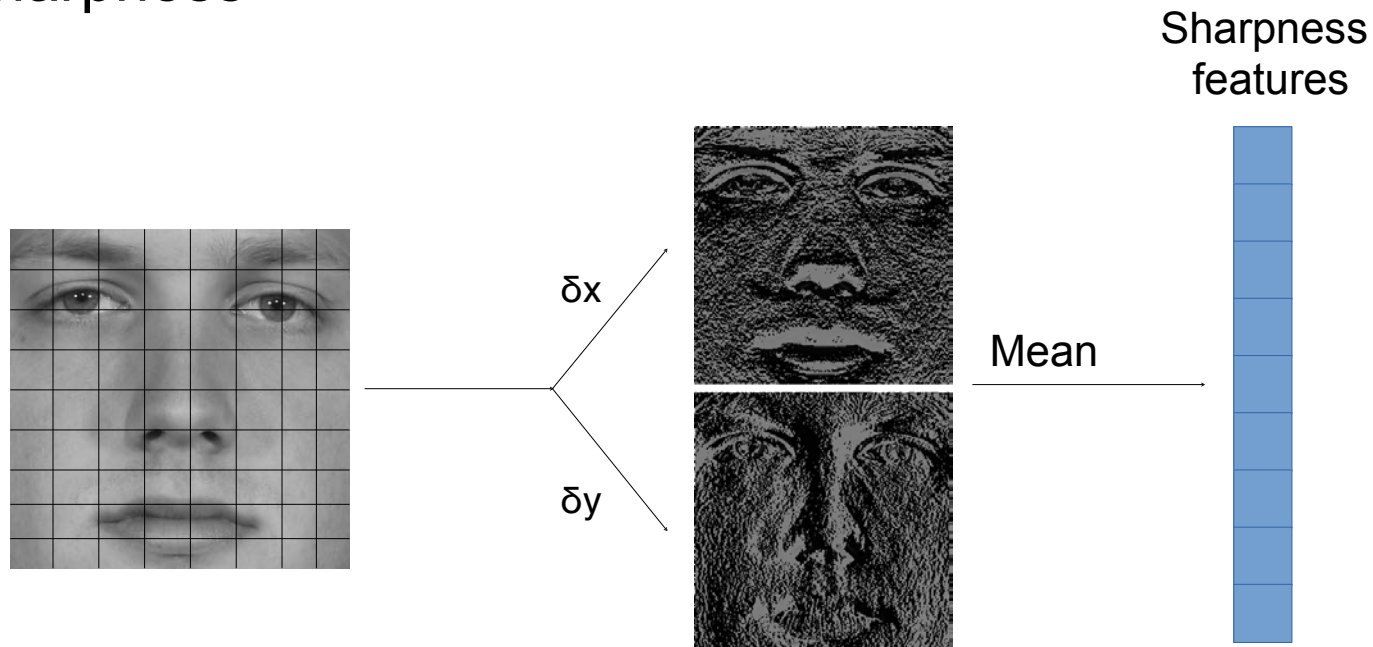
- Binarized Statistical Image Features (BSIF)



Face Pre-processing and Feature Extraction

MAD with image descriptor

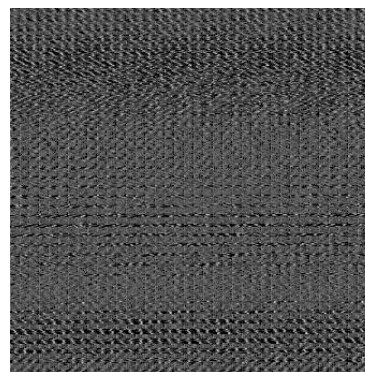
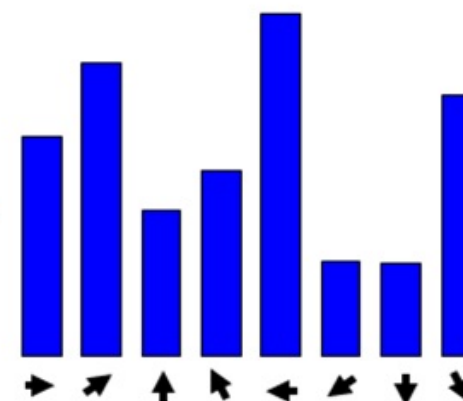
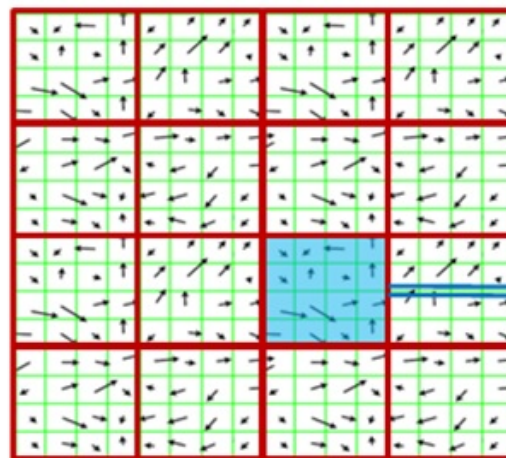
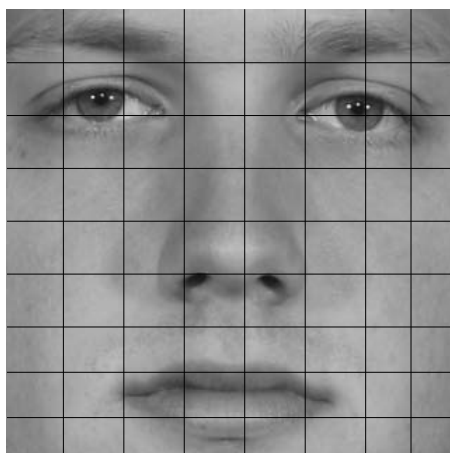
- Sharpness



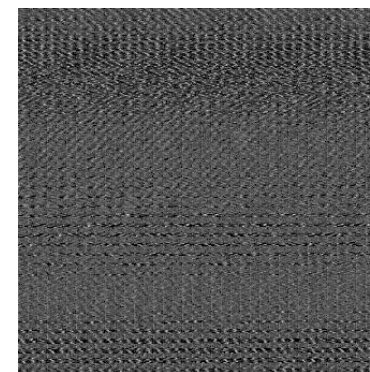
Face Pre-processing and Feature Extraction

MAD with image descriptor

- Histogram of Gradients (HOG)



Morph

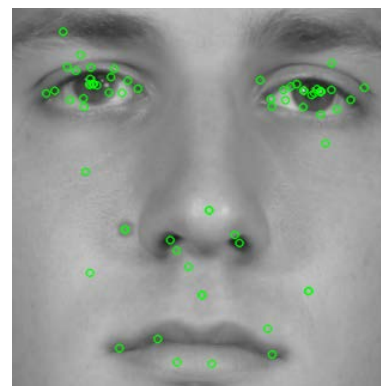
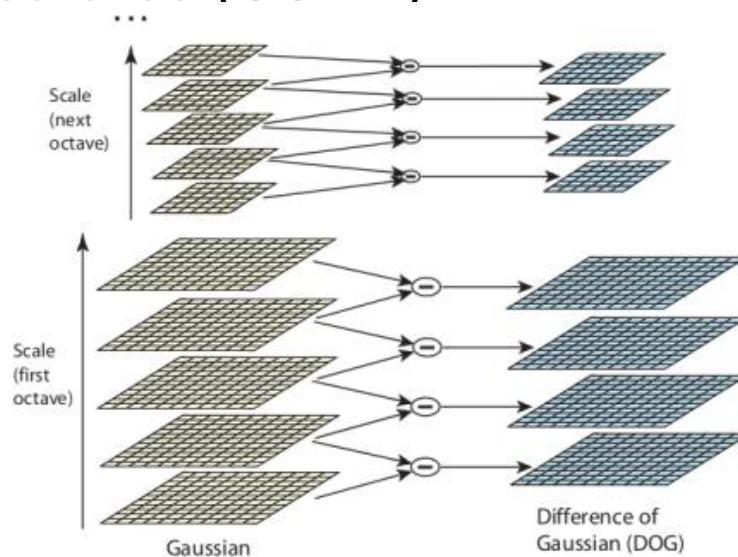
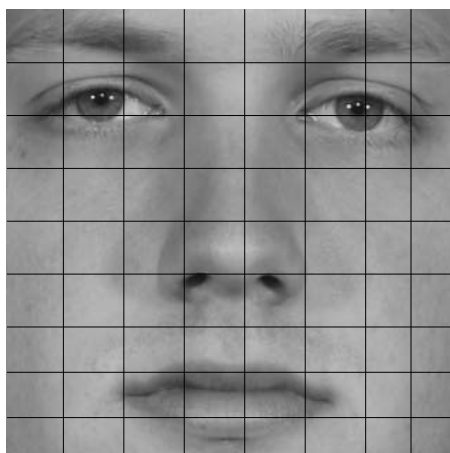


Bona Fide

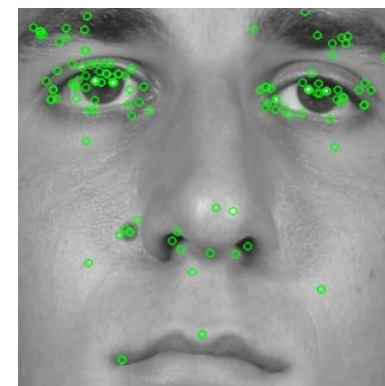
Face Pre-processing and Feature Extraction

MAD with image descriptor

- Scale Invariant Feature Transform (SIFT)
- Speeded up Robust Features (SURF)



Morph

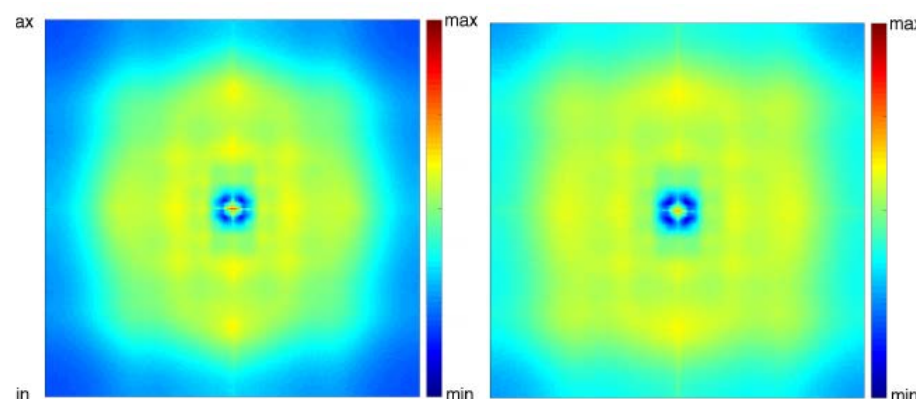
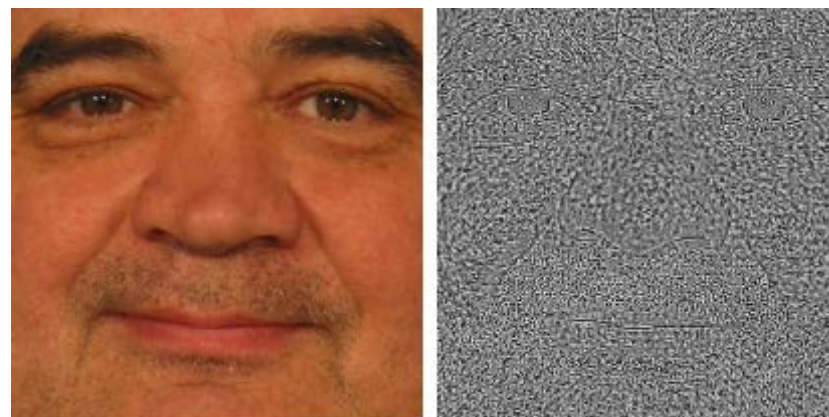


Bona Fide

Face Pre-processing and Feature Extraction

MAD with image descriptor / forensic approach

- Photo Response Non-Uniformity (PRNU)



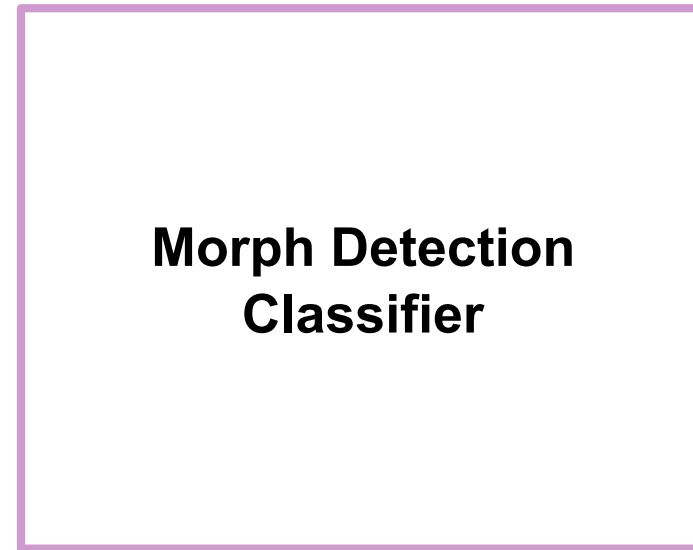
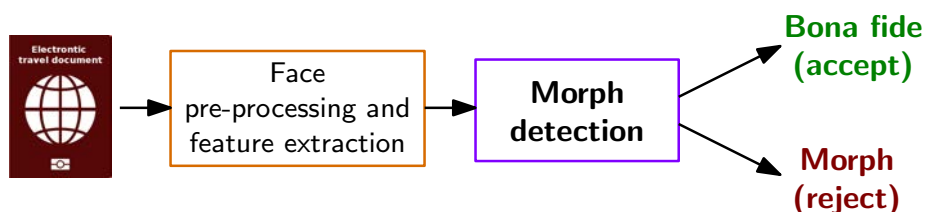
Morph

Bona Fide

Face Pre-processing and Feature Extraction

Morphing Attack Detection (MAD) with texture analysis

- Image descriptors as **Deep features**

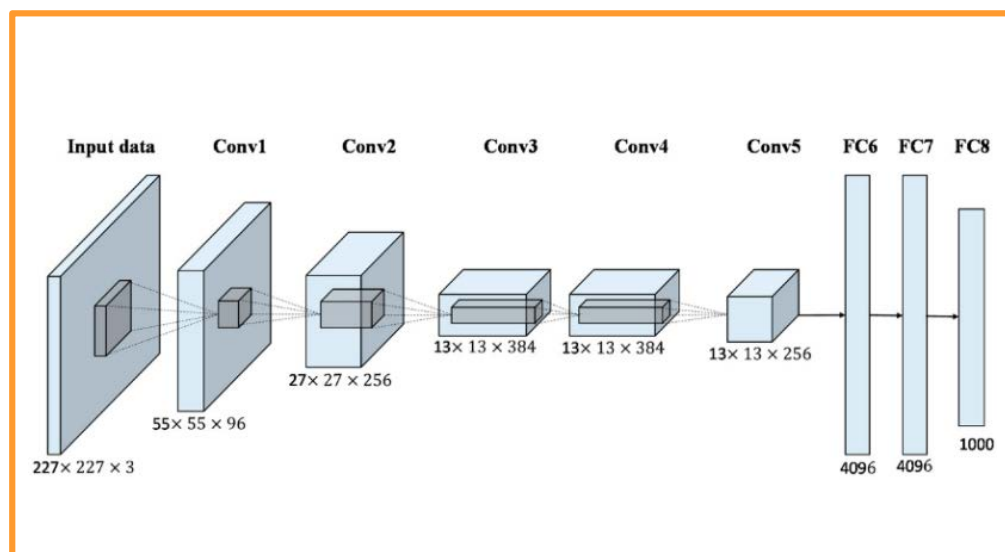


Face Pre-processing and Feature Extraction

MAD with deep learning

- **Deep Features**

- ▶ pre-trained Convolutional Neural Network (CNN)
- ▶ OpenFace



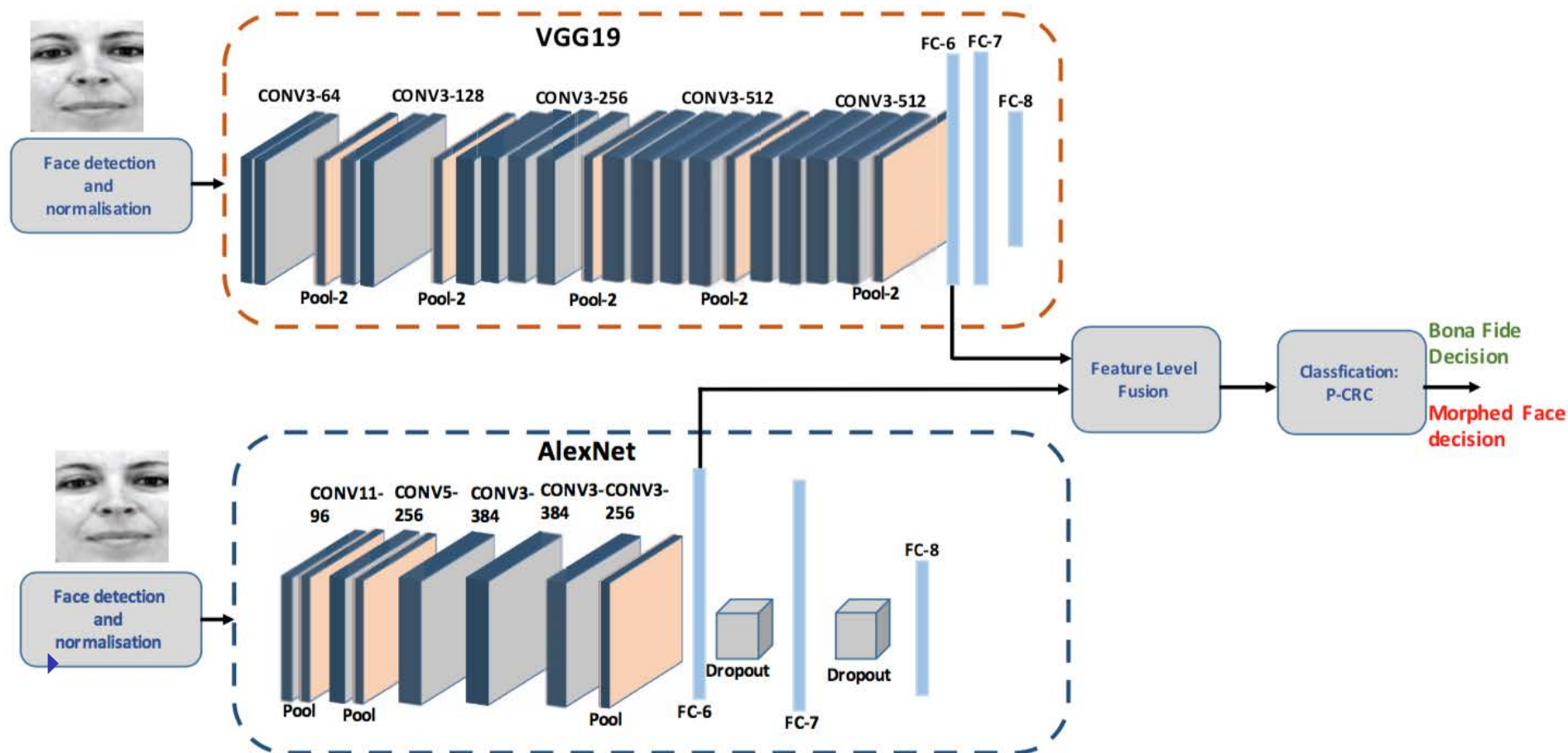
**Morph Detection
Classifier**

[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

MAD Evaluation Methodology

Face Morphing Attack **evaluations** are complex

- Evaluations must consider a dedicated **methodology** [SNR17]
- Evaluations must consider **many parameters**

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

[SNR17] U. Scherhag, A. Nautsch, C. Rathgeb, M. Gomez-Barrero, R. Veldhuis, L. Spreeuwiers, M. Schils, D. Maltoni, P. Grother, S. Marcel, R. Breithaupt, R. Raghavendra, C. Busch: "Biometric Systems under Morphing Attacks: Assessment of Morphing Techniques and Vulnerability Reporting", in Proceedings of the IEEE 16th International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, September 20-22, (2017)

MAD Evaluation Methodology

Evaluations must consider **many parameters**

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

Quality of the passport image under investigation

- hopefully ICAO 9303 compliant
- and
- ISO/IEC 39794-5 compliant



MAD Evaluation Methodology

Evaluations must consider many parameters

- For a **differential** MAD evaluation

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

Quality of the **passport image** under investigation
and quality of the **trusted probe image**



In our evaluation we use

- The FERET dataset for training
<https://www.nist.gov/programs-projects/face-recognition-technology-feret>
- The FRGCv2 dataset for testing
<https://www.nist.gov/programs-projects/face-recognition-grand-challenge-frgc>
- Both data sets were filtered to reach ICAO compliance

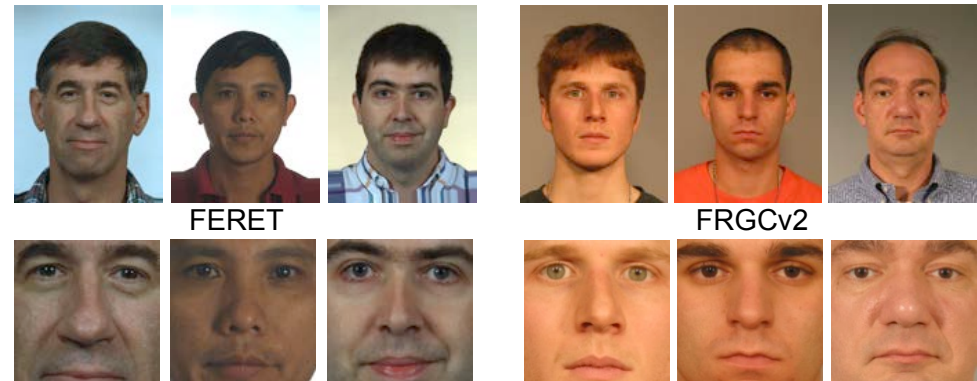
MAD Evaluation Methodology

Evaluations must consider many parameters

- Dataset preparation requires **pre-processing**

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

Facial images are **cropped** and **aligned** to a normalized **size**



Resulting images are

- cropped** to 320x320 pixel
- aligned according to Dlib landmarks, such that eyes are at **identical coordinates**

MAD Evaluation Methodology

Evaluations must consider many parameters

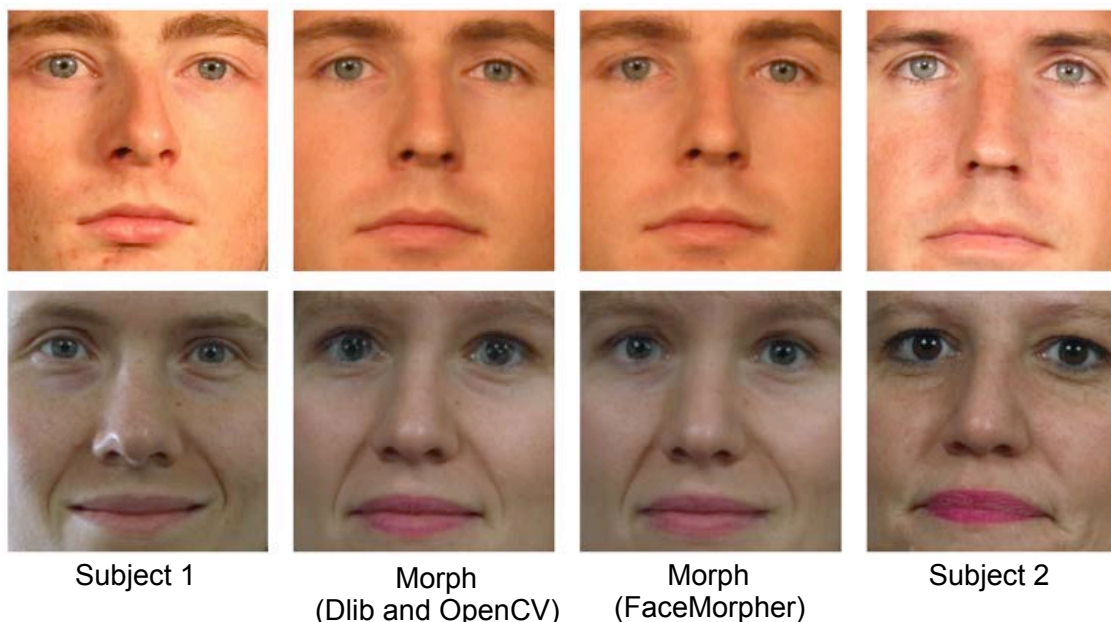
- Morphing may require **manual interaction** (not desired)

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

Automated face morphing tools may introduce artifacts

In our evaluation we use

- Dlib / OpenCV
- FaceMorpher

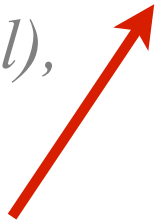


MAD Evaluation Methodology

Evaluations must consider many parameters

- From machine learning tools we select a **classifier**

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



Simplicity and **generalisation capability** are desired properties

In our evaluation we use

- Support Vector Machine (SVM)
 - with radial basis function as kernel
- AdaBoost
 - with 200 estimates and a decision stump

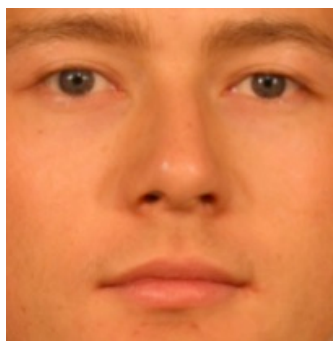
MAD Evaluation Methodology

Evaluations must consider many parameters

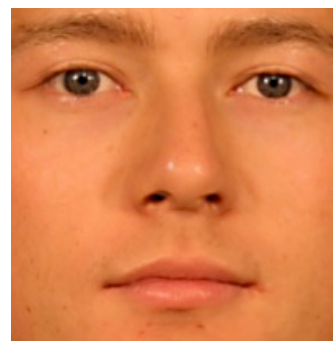
- Postprocessing might **conceal** morphing effects (e.g. **smoothing**)

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

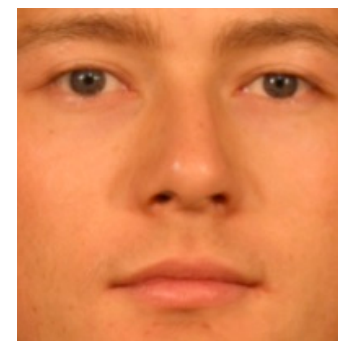
smoothing and other effects might be compensated by the attacker



Morph



Sharpening



Histogram
equalisation

In our evaluation
we show results for

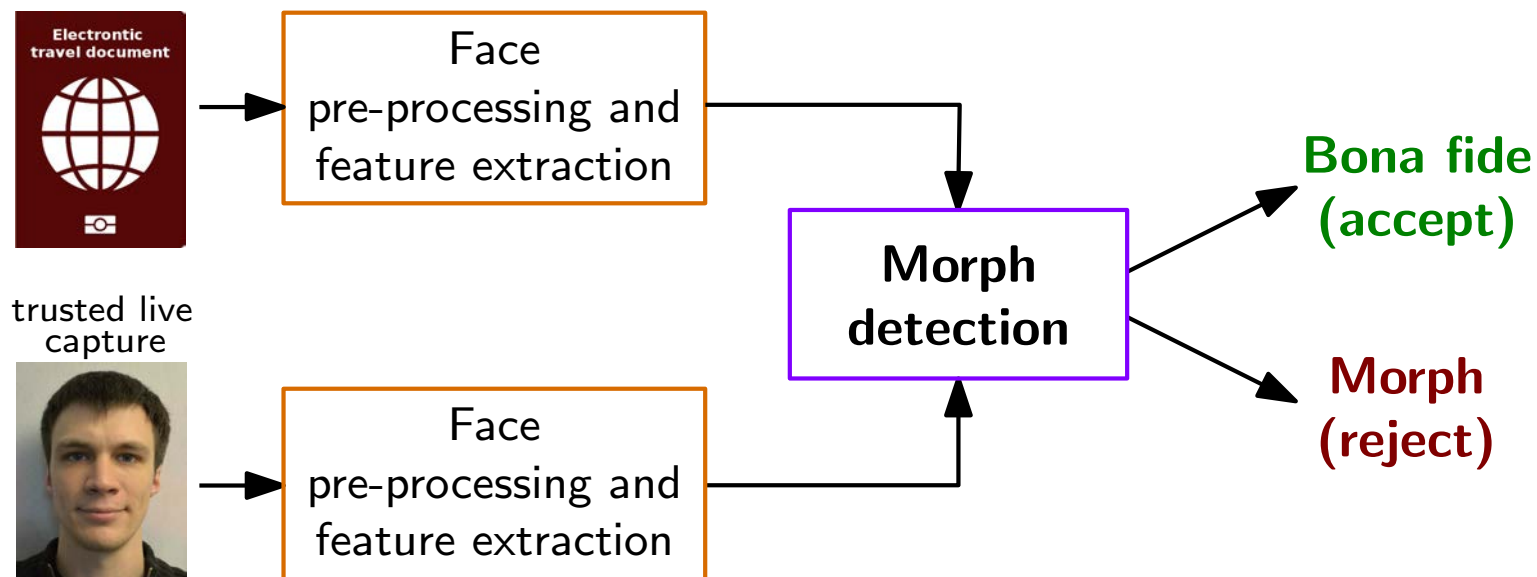
- Sharpening

Results

MAD Evaluation

Generalising evaluation - **differential** scenario

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



MAD Evaluation

Generalising evaluation - differential scenario

- training on FERET, testing on FRGCv2
 - hand-crafted feature extractors perform well
 - no post-processing of morph images

MAD-method	Classifier	Morphing Algorithm (Training)	Morphing Algorithm (Test)	D-EER
LBP	SVM	Dlib und OpenCV	Dlib und OpenCV	0,0228
LBP (4x4 cells)	SVM	Dlib und OpenCV	Dlib und OpenCV	0,0997
LBP	AdaBoost	Dlib und OpenCV	Dlib und OpenCV	0,0645
LBP (4x4 cells)	AdaBoost	Dlib und OpenCV	Dlib und OpenCV	0,0471
BSIF	SVM	Dlib und OpenCV	Dlib und OpenCV	0,0775
BSIF (4x4 cells)	SVM	Dlib und OpenCV	Dlib und OpenCV	0,0656
BSIF	AdaBoost	Dlib und OpenCV	Dlib und OpenCV	0,0695
BSIF (4x4 cells)	AdaBoost	Dlib und OpenCV	Dlib und OpenCV	0,0742
OpenFace	SVM	Dlib und OpenCV	Dlib und OpenCV	0,1253
OpenFace	AdaBoost	Dlib und OpenCV	Dlib und OpenCV	0,1373
FaceNet	SVM	Dlib und OpenCV	Dlib und OpenCV	0,1943
FaceNet	AdaBoost	Dlib und OpenCV	Dlib und OpenCV	0,1745
LBP	SVM	FaceMorpher	FaceMorpher	0,0025
LBP (4x4 cells)	SVM	FaceMorpher	FaceMorpher	0,0023
LBP	AdaBoost	FaceMorpher	FaceMorpher	0,0453
LBP (4x4 cells)	AdaBoost	FaceMorpher	FaceMorpher	0,0000
BSIF	SVM	FaceMorpher	FaceMorpher	0,0253
BSIF (4x4 cells)	SVM	FaceMorpher	FaceMorpher	0,0085
BSIF	AdaBoost	FaceMorpher	FaceMorpher	0,0126
BSIF (4x4 cells)	AdaBoost	FaceMorpher	FaceMorpher	0,0695
OpenFace	SVM	FaceMorpher	FaceMorpher	0,1432
OpenFace	AdaBoost	FaceMorpher	FaceMorpher	0,1404
FaceNet	SVM	FaceMorpher	FaceMorpher	0,2054
FaceNet	AdaBoost	FaceMorpher	FaceMorpher	0,1745

MAD Evaluation

Generalising evaluation - differential scenario

- training on FERET, testing on FRGCv2
- now we focus on **LBP** only
 - and again no post-processing of morph images

MAD-method	Classifier	Morphing Algorithm (Training)	Morphing Algorithm (Test)	D-EER
LBP	SVM	Dlib und OpenCV	FaceMorpher	0,0153
LBP	AdaBoost	Dlib und OpenCV	FaceMorpher	0,0471
LBP	SVM	FaceMorpher	Dlib und OpenCV	0,0251
LBP	AdaBoost	FaceMorpher	Dlib und OpenCV	0,1369

We reach in the best case

- approx 1 % EER (between APCER and BPCER)

MAD Evaluation

Generalising evaluation - differential scenario

- training on FERET, testing on FRGCv2
- now we focus on LBP only
- post-processing of morph images with the **sharpening** operator

MAD-method	Classifier	Morphing Algorithm (Training)	Morphing Algorithm (Test)	D-EER
LBP	SVM	Dlib und OpenCV	FaceMorpher	0,0108
LBP	AdaBoost	Dlib und OpenCV	FaceMorpher	0,0414
LBP	SVM	FaceMorpher	Dlib und OpenCV	0,0417
LBP	AdaBoost	FaceMorpher	Dlib und OpenCV	0,1289

We still reach in the best case

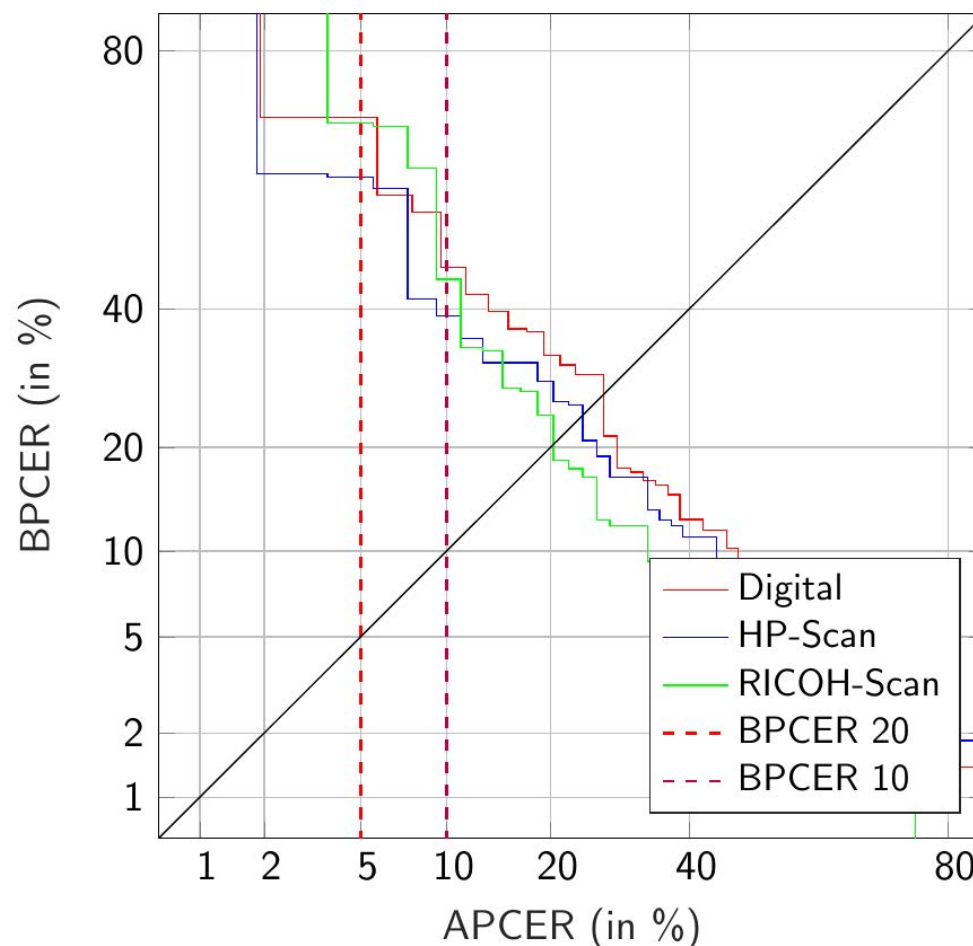
- approx 1 % EER (between APCER and BPCER)

Results and Print and Scan

IWBF 2017 - Evaluation

Texture based morphing detection

- Binarized Statistical Image Features as texture descriptor
- Support Vector Machine (SVM) as classifier



Future - What needs to be done?

MAD Evaluations on Digital Images

First investigations on morphing attack detection

- are 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

MAD Evaluations on Digital Images

Our submissions to NIST-FRVT-MORPH / SOTAMD:

- LBP-MAD proposed in [RRB16], [SRB18a] and [SRB18b]
- PRNU-MAD proposed in [DSRUB18a] and [DSRUB18b]
- SSF-MAD proposed in [RVRB19]

[RRB16] 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, Niagara Falls, USA, (2016)

[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)

[SRB18b] U. Scherhag, C. Rathgeb, C. Busch: „Detection of Morphed Faces from Single Images: a Multi-Algorithm Fusion Approach“, in Proceedings of the 2nd International Conference on Biometric Engineering and Applications (ICBEA 2018), Amsterdam, The Netherlands, May 16-18, (2018)

[DSRUB18a] L. Debiase, 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)

[DSRUB18b] L. Debiase, 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)

[RVRB19] 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)

What needs to be Done ?

Evaluations must consider the printing process

- There are numerous parameters to explore for this

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



Printer / Scanner of choice

Resolution (spatial sampling rate)

What needs to be Done ?

Multiple dimensions to explore:

- Large scale datasets evaluation in NIST FRVT MORPH
- **Generalisation** on public datasets
 - FERET, FRGCv2, FEI, ARface
- Morphing mechanism
 - Fantamorph, OpenCV, Splicing, GIMP, ...
- **Number** of contributing **subjects** (broker model)
- The most effective **alpha-factor** (50:50 or 20:80)
- Random or **lookalike** morphs
 - Same gender, same skin-color as selection criteria
- Digital samples versus digital-analog-digital transition

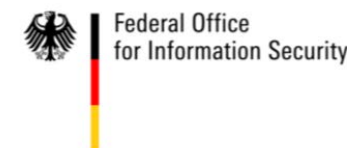
Publications available <https://www.christoph-busch.de/projects-mad.html>

- 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 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)

Sponsors

This research is kindly sponsored by

- Federal Office for Information Security (BSI)
 - ▶ FACETRUST
- Center for Research in Security and Privacy:
 - ▶ LOEWE/BMBF CRISP <http://www.crisp-da.de/>
- Norwegian Research Council
 - ▶ IKTPLUSS SWAN http://nislabs.no/biometrics_lab/swan
- Norwegian University of Science and Technology
- The EU ISF Project SOTAMD
 - ▶ <https://www.christoph-busch.de/projects-sotamd.html>



Contact

Contact:



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

**CRISP**
Center for Research
in Security and Privacy

**h_da**
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

Prof. Dr. Christoph Busch
Principal Investigator

Hochschule Darmstadt FBI
Haardtring 100
64295 Darmstadt, Germany
christoph.busch@crisp-da.de

Telefon +49-6151-16-30090
www.dasec.h-da.de
www.crisp-da.de
