Biometric Attack Detection

Christoph Busch

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

latest news at:
https://twitter.com/busch_christoph

NTNU

European Association for Biometrics
eab
Human Identity in Europe

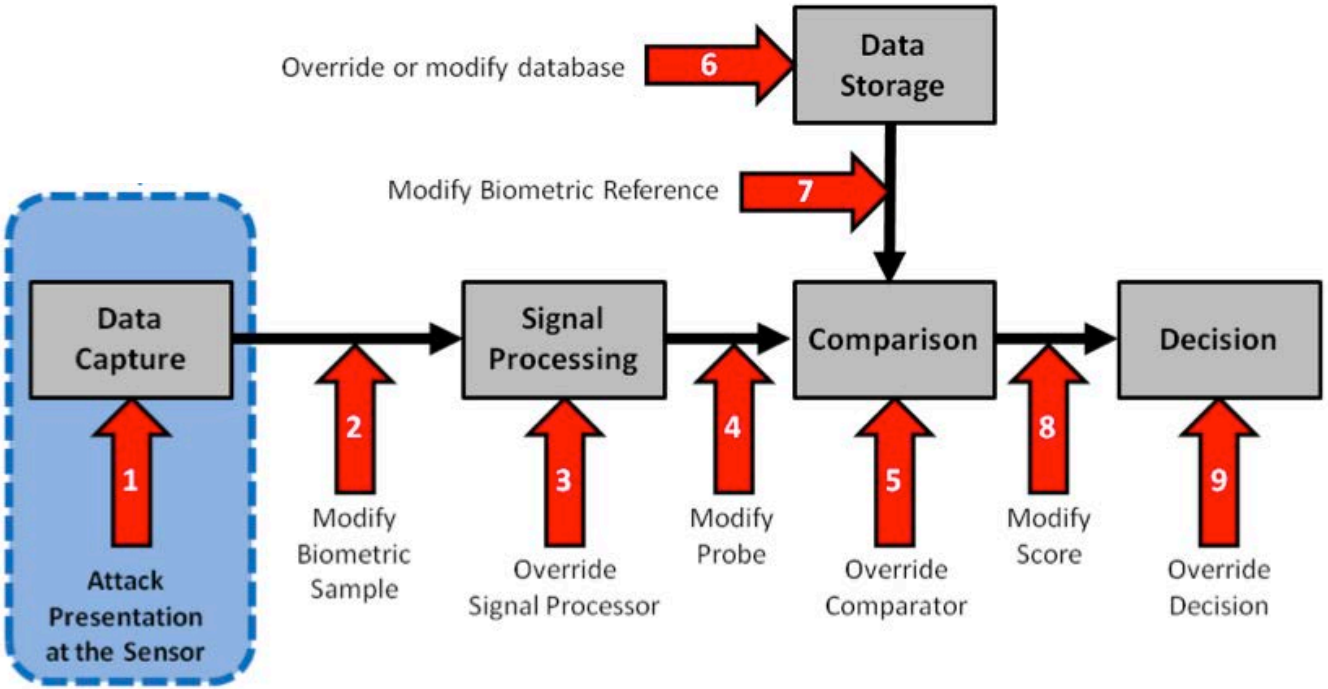
ATHENE

da/sec
BIOMETRICS AND INTERNET-SECURITY RESEARCH GROUP

Weakness of Biometric Systems

Three main points for a targeted attack

- Capture device (1): Camera, optical- / capacitive sensor
  - Attacks must be countered by presentation attack detection
- Data transmission (2): USB, firewire etc.
  - Susceptibility to attacks on data transmission channel
  - Enrolment attacks (i.e. face morphing attacks)
- Data storage (6): Database, token



Source: ISO/IEC 30107-1:2016

Overview

Structure of this session

- Presentation attack detection
  - Fingerprint capture devices
  - Face capture devices
- Morphing attack detection
  - at enrolment
  - at borders

Fingerprint Presentation Attacks

Fingerprint Presentation Attacks

Attack without support of an enrolled individual

1971

- James Bond: Diamonds Are Forever

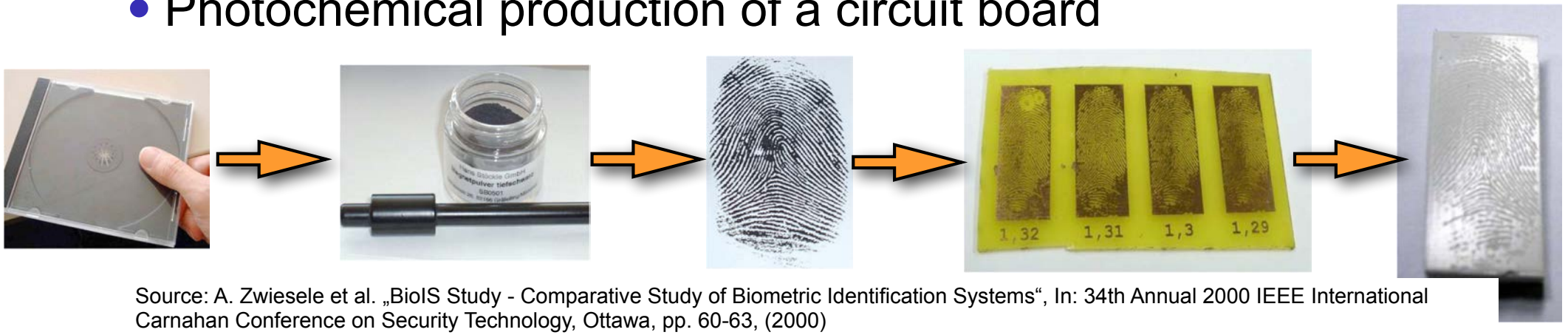
Source: https://www.imdb.com/title/tt0066995 (1971)

Fingerprint Presentation Attacks

Attack without support of an enrolled individual

1999

- Recording of an analog fingerprint from flat surface material
  - z.B. glass, CD-cover, etc.
    with iron powder and tape
- Scanning and post processing:
  - Correction of scanning errors
  - Closing of ridge lines (as needed)
  - Image inversion
- Print on transparent slide
- Photochemical production of a circuit board



Source: A. Zwiesele et al. „BioIS Study - Comparative Study of Biometric Identification Systems“, In: 34th Annual 2000 IEEE International Carnahan Conference on Security Technology, Ottawa, pp. 60-63, (2000)

Fingerprint Presentation Attacks

2002

- A thin shopping bag filled with warm water can circumvent liveness tests for capacitive sensors, activating latent prints
- Sometimes the same can also be achieved by warm breath

Source: c‘t - Magazin für Computertechnik, 11/02 p.114-123

Fingerprint Presentation Attacks

2013

Overlay attack without support

- Recording of an analog fingerprint from the phone

Source: https://www.ccc.de/en/tags/apple, (2013)

Fingerprint Alteration

Example for fingerprint alterations

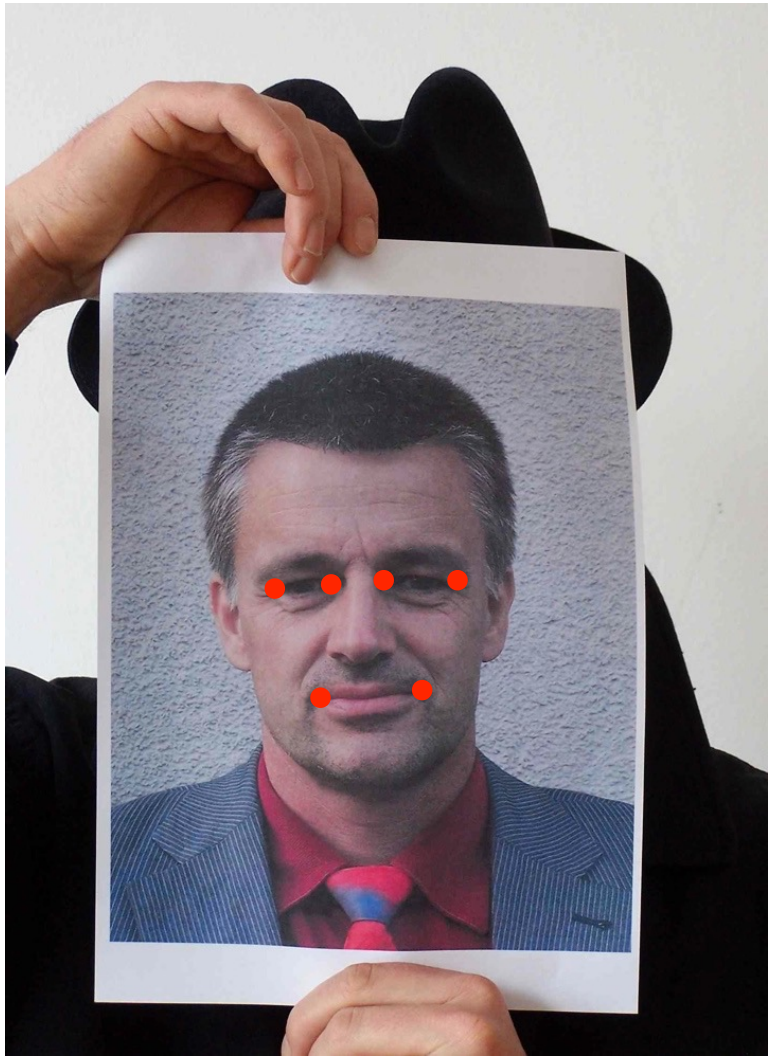
1997

- Z-shaped alteration (Finger of Jose Izquierdo)

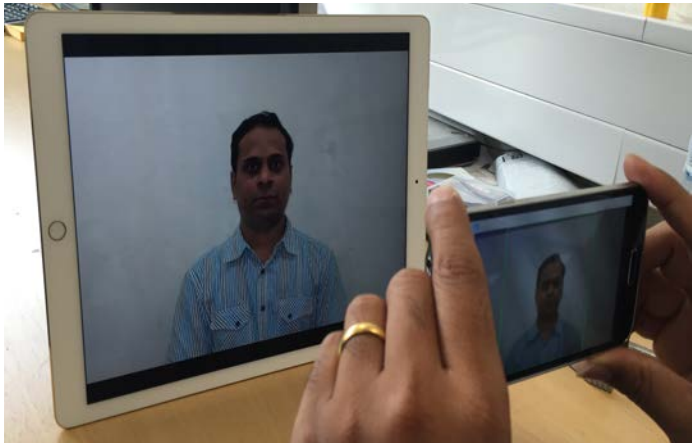
Image Source: S. Yoon, J. Feng, and A. Jain, “Altered fingerprints: Analysis and detection,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 34, no. 3, pp. 451–464, Mar. 2012

Face Presentation Attacks

Face Presentation Attacks



Face Presentation Attacks

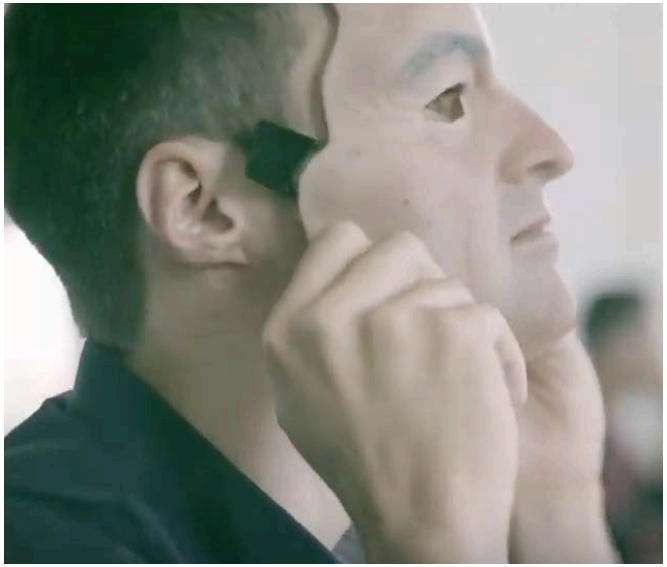


Face Presentation Attacks

2018

3D silicone mask

- Targeted attack with 3D silicone custom mask
- Cost more than 3000 USD

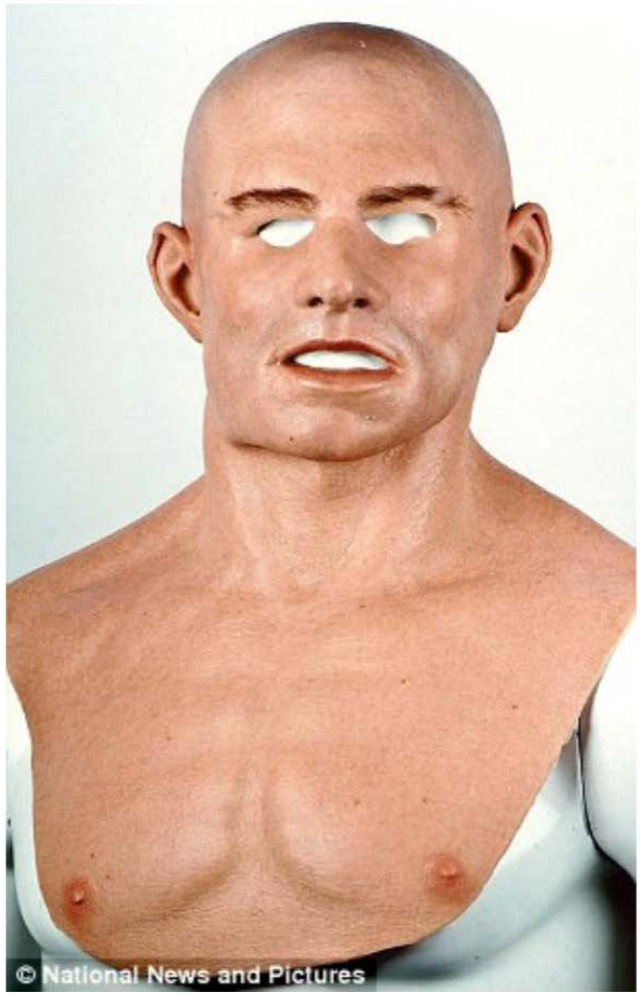


Concealer Presentation Attack

Face disguise for organized crime

2012

- http://www.dailymail.co.uk/news/article-2153346/Black-armed-robber-disguised-white-man-using-latex-mask.html



The man in the latex mask: BLACK serial armed robber disguised himself as a WHITE man to rob betting shops

- **Henley Stephenson wore the disguise during a 12-year campaign of hold-ups at betting shops and other stores across London**
- **He was part of a three-man gang jailed for a total of 28 years**
- **CCTV footage showed him firing a semi-automatic pistol into the ceiling during a raid on a betting shop**
- **The mask was bought from the same London shop which supplied masks used in the £40m Graff Diamonds heist**

By ROB PREECE and REBECCA CAMBER FOR THE DAILY MAIL

PUBLISHED: 17:22 GMT, 1 June 2012 | **UPDATED:** 16:21 GMT, 2 June 2012

Most masked robbers opt for a balaclava to hide their identity.

Not this one. Henley Stephenson, 41, eluded police for more than ten years thanks to an extraordinarily lifelike latex mask, which turned him into a white skinhead.

Officers discovered that their man was in fact black when they finally caught up with Stephenson after a string of armed raids dating back to 1999.

Face Presentation Attacks

Make-Up attack

Image Source: http://upshout.net/game-of-thrones-make-up

(a) before (b) after (c) target

Image Source: http://www.antitza.com/makeup-datasets.html

Why is this called Presentation Attack Detection (PAD) and not Liveness Detection ?

Categories of Presentation Attacks

Impostor

- impersonation attack
  - positive access 1:1 (two factor application)
  - positive access 1:N (single factor application)
- finding a look-a-like
- making appearance similar to the reference
- artefact presentation

Image Source: http://upshout.net/game-of-thrones-make-up

Concealer

- evasion from recognition
  - negative 1:N identification (watchlist application)
- depart from standard pose

- evade face detection

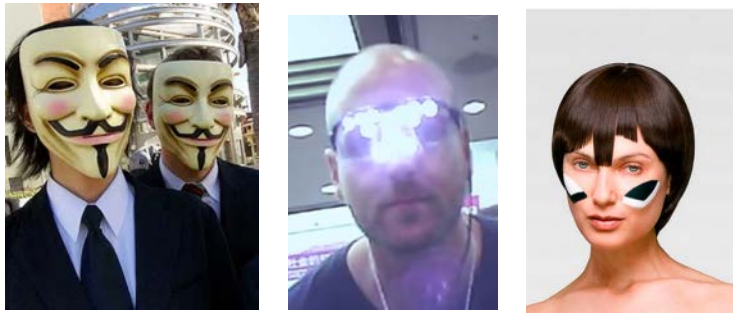


Image Source: https://www.youtube.com/watch?v=LRj8whKmN1M

Image Source: https://cvdazzle.com

Presentation Attack Detection

Definitions in ISO/IEC 30107 PAD - Part 1: Framework

- **presentation attack**
  presentation to the biometric capture subsystem with the goal of interfering with the operation of the biometric system
- **presentation attack detection (PAD)**
  automated determination of a presentation attack

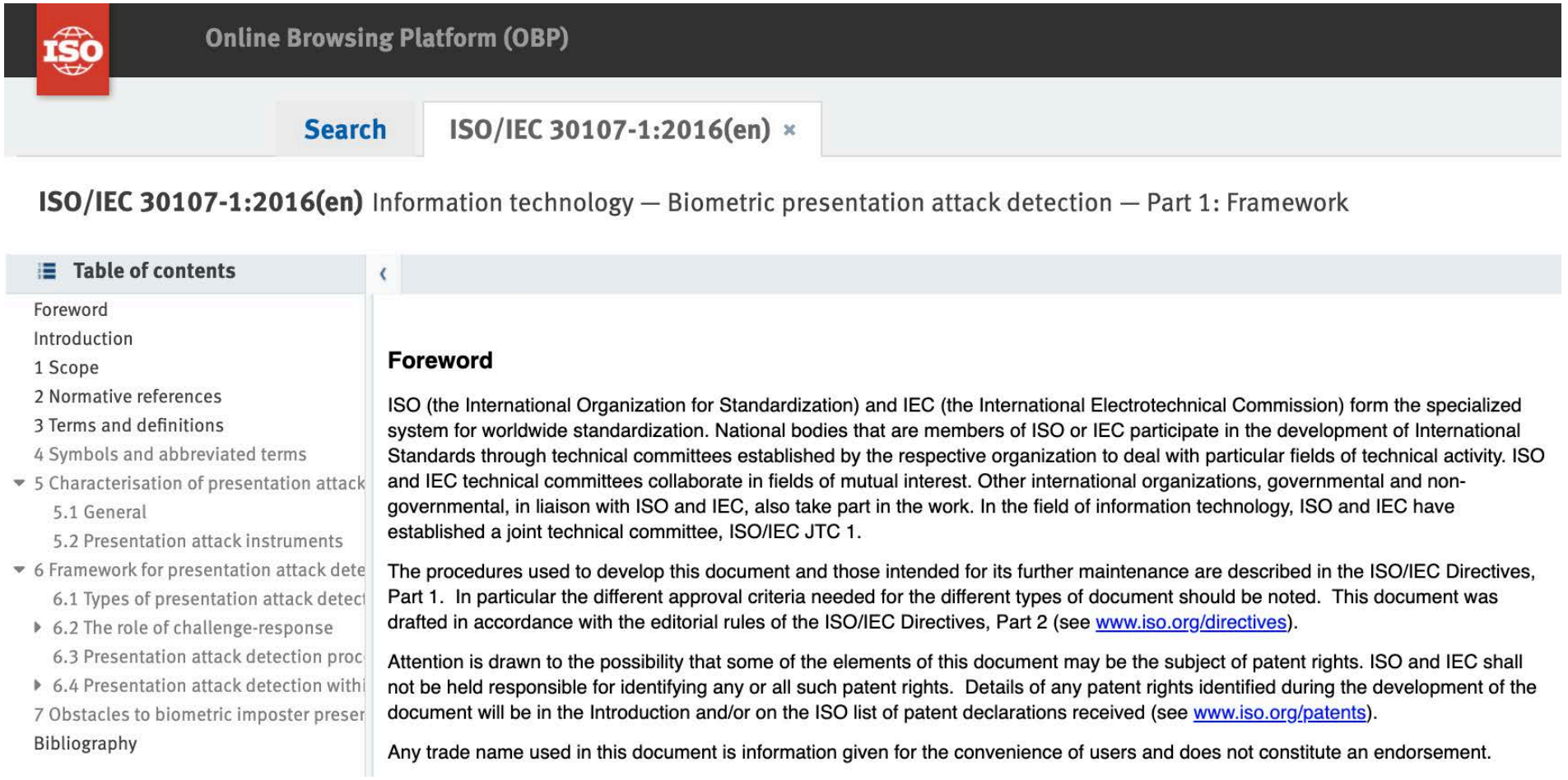
Definitions in ISO/IEC 2382-37: Vocabulary
http://www.christoph-busch.de/standards.html

- **impostor**
  subversive biometric capture subject who attempts to being matched to someone else's biometric reference
- **identity concealer**
  subversive biometric capture subject who attempts to avoid being matched to their own biometric reference

Presentation Attack Detection - Framework

ISO/IEC 30107-1

- provides the taxonomy
- freely available in the ISO-Portal
  http://standards.iso.org/ittf/PubliclyAvailableStandards/c053227_ISO_IEC_30107-1_2016.zip



Presentation Attack Detection

ISO/IEC 30107-1 - Definitions

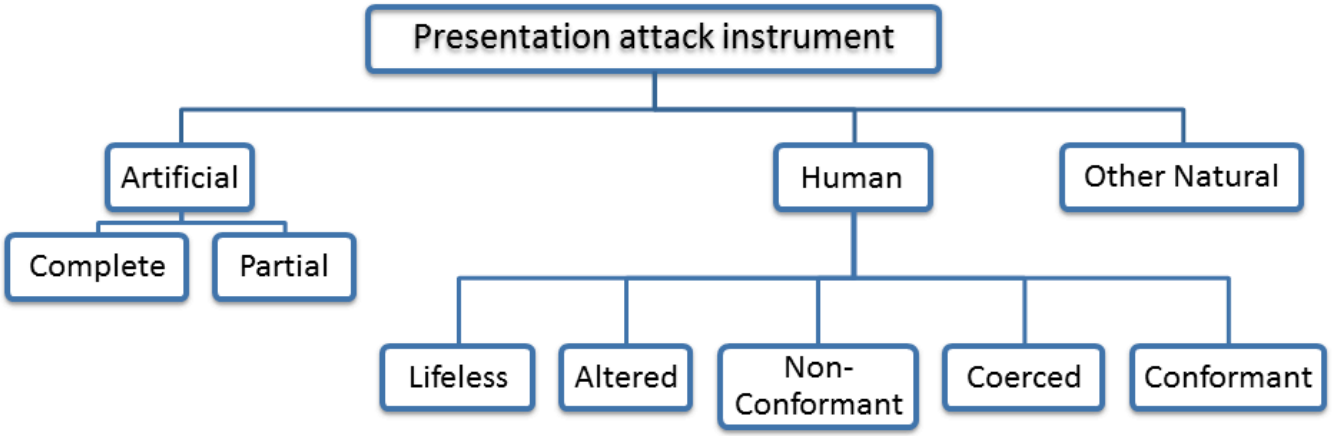
- **presentation attack instrument (PAI)**
  biometric characteristic or object used in a presentation attack
- **artefact**
  artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns

Types of presentation attacks

(General Noun)

(Adjectives describing categories)

(Qualifying adjectives)



Source: ISO/IEC 30107-1

PAD Testing

Presentation Attack Detection - Testing

Definition of detection capabilities metrics

- 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*

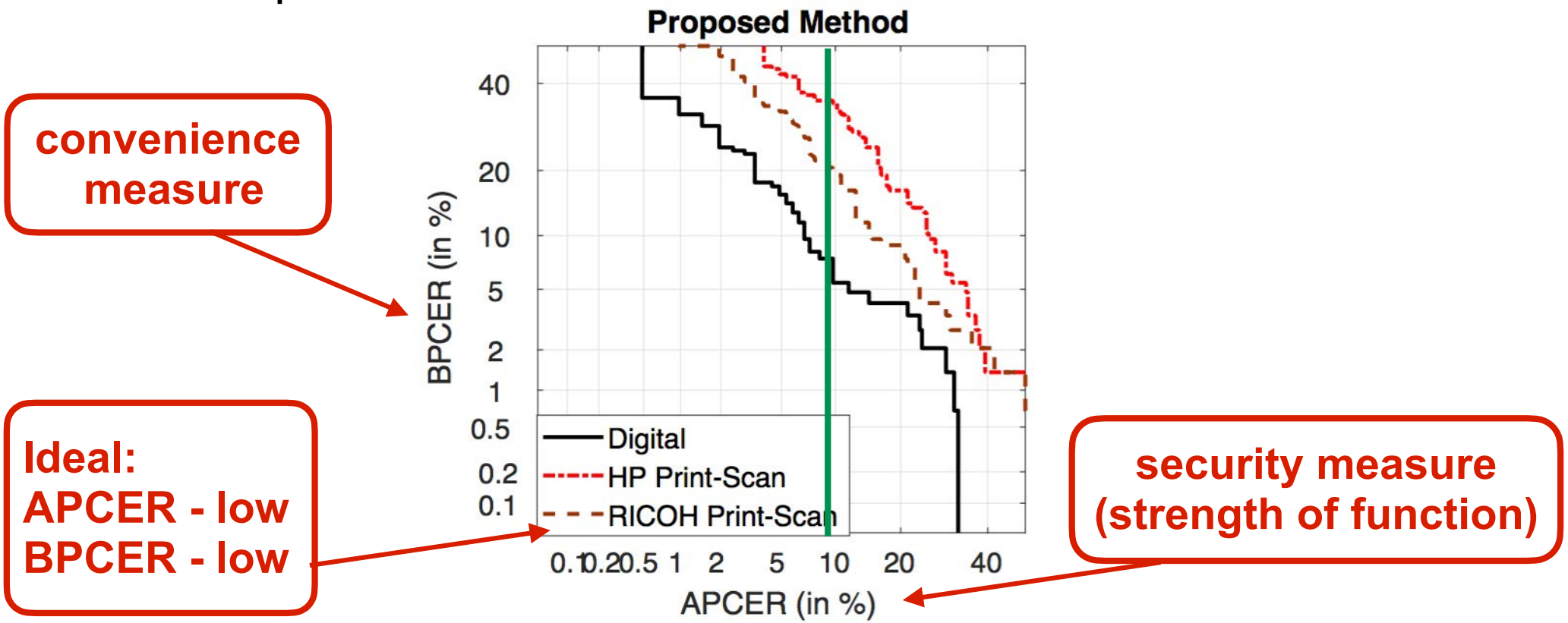
- **Bona fide presentation classification error rate (BPCER)** *proportion of bona fide presentations incorrectly classified as attack presentations in a specific scenario*

Source: ISO/IEC 30107-3

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-3

- DET curve reports operating points for various thresholds showing 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)

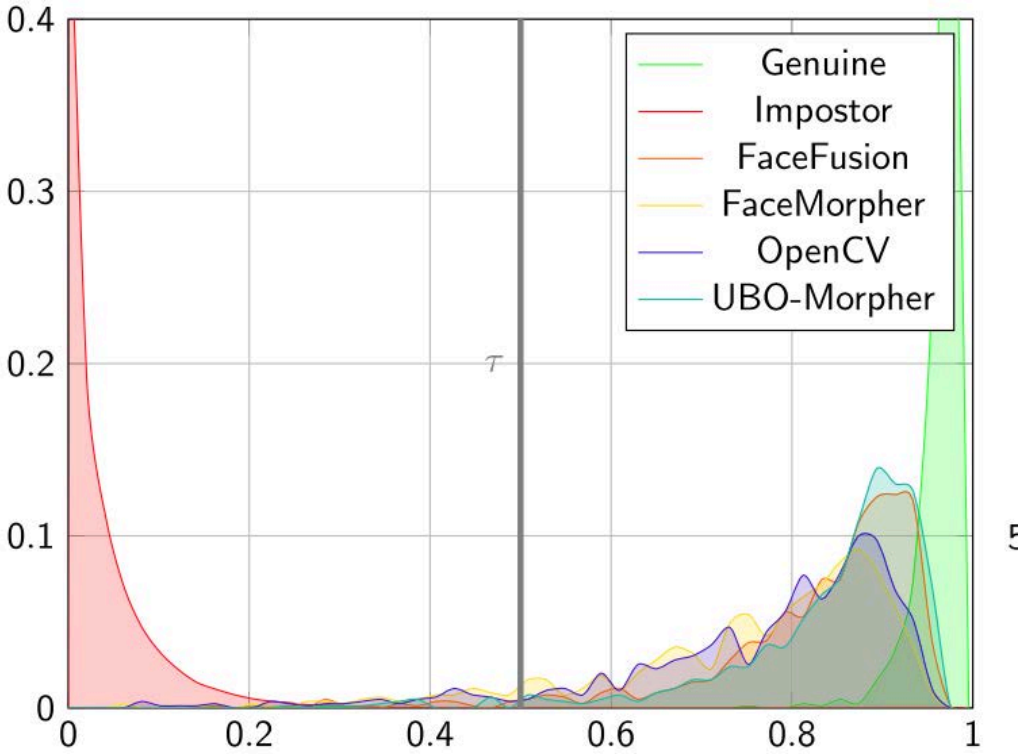
PA Vulnerability Testing

Presentation Attack Detection - Testing

Definition of full system vulnerability metric w.r.t attacks

- **Impostor attack presentation match rate (IAPMR)**
  <in a full-system evaluation of a verification system> the proportion of impostor attack presentation using the same PAI species in which the target reference is matched

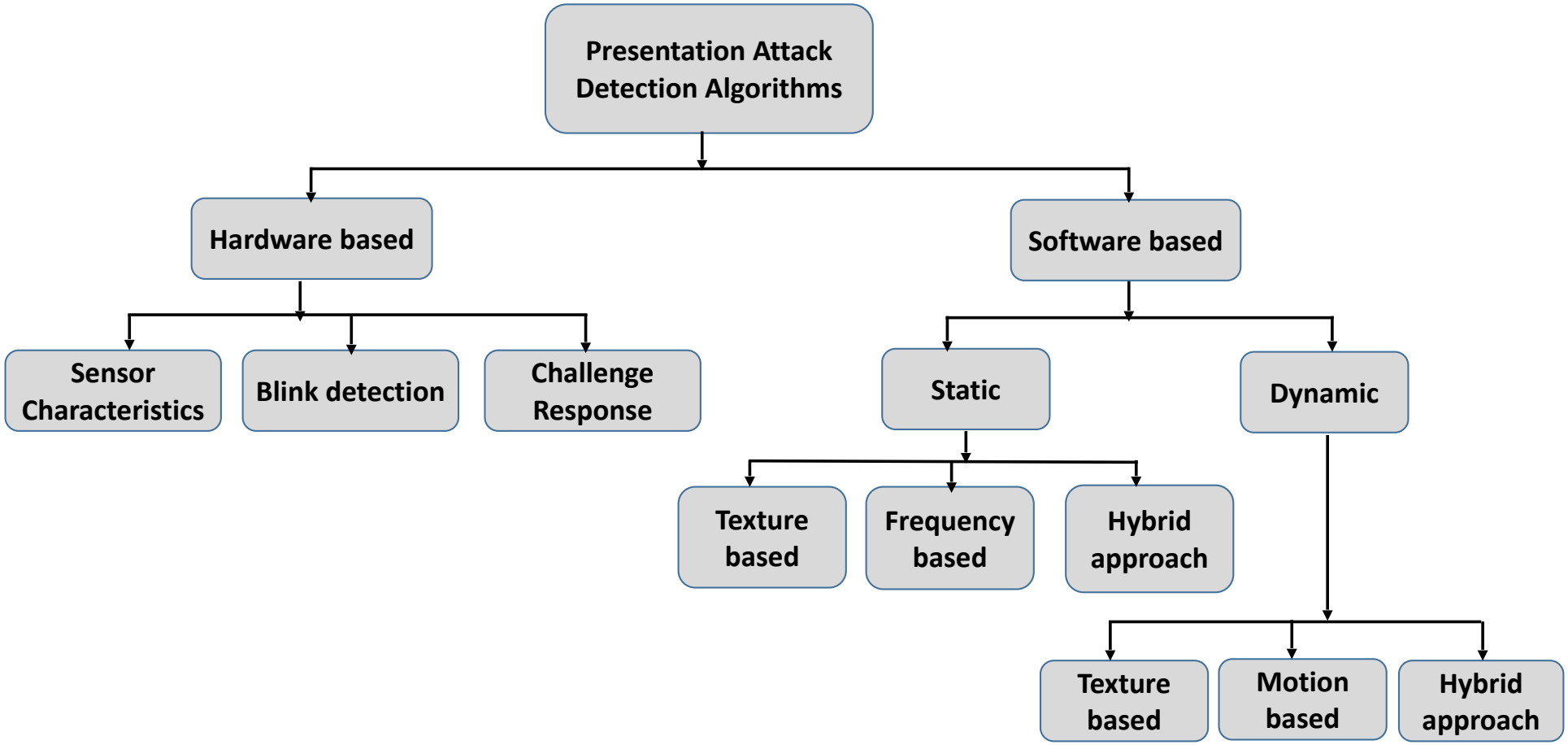
Source: ISO/IEC 30107-3



Source: 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)

A Taxonomy on PAD

Taxonomy Presentation Attack Detection



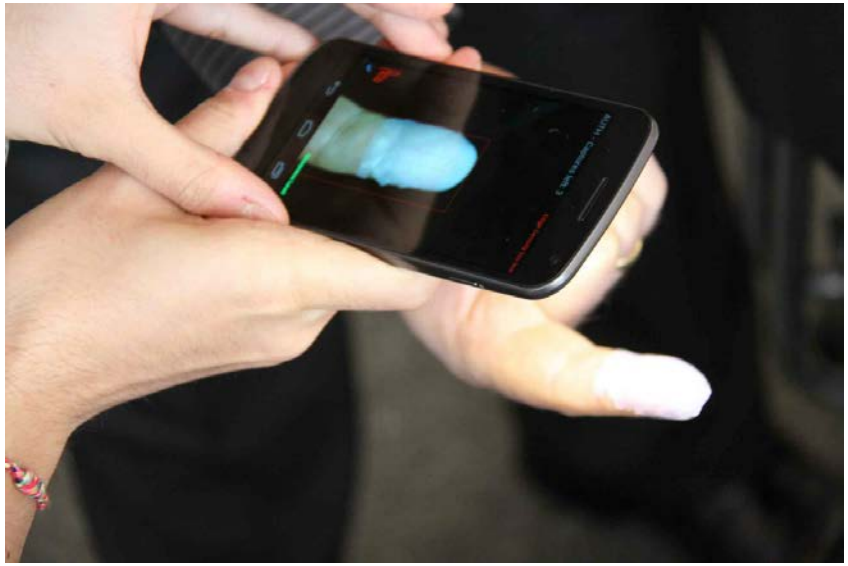
Fingerprint PAD

Fingerprint Capture Device Security

BSI BEZ (www.bsi.bund.de)

- collecting & evaluating publicly known fakes
- development of new artefact types
  - BSI-Fake-Toolbox

Source: BSI



Smartphone Access Control

Finger recognition study - 2012/2013

- Observation
  - significant strong light reflection near the fingertip
  - from the cameras LED
- Reflection depends on
  - Shape of the finger
  - Consistency of the finger
  - Angle of the finger to the camera

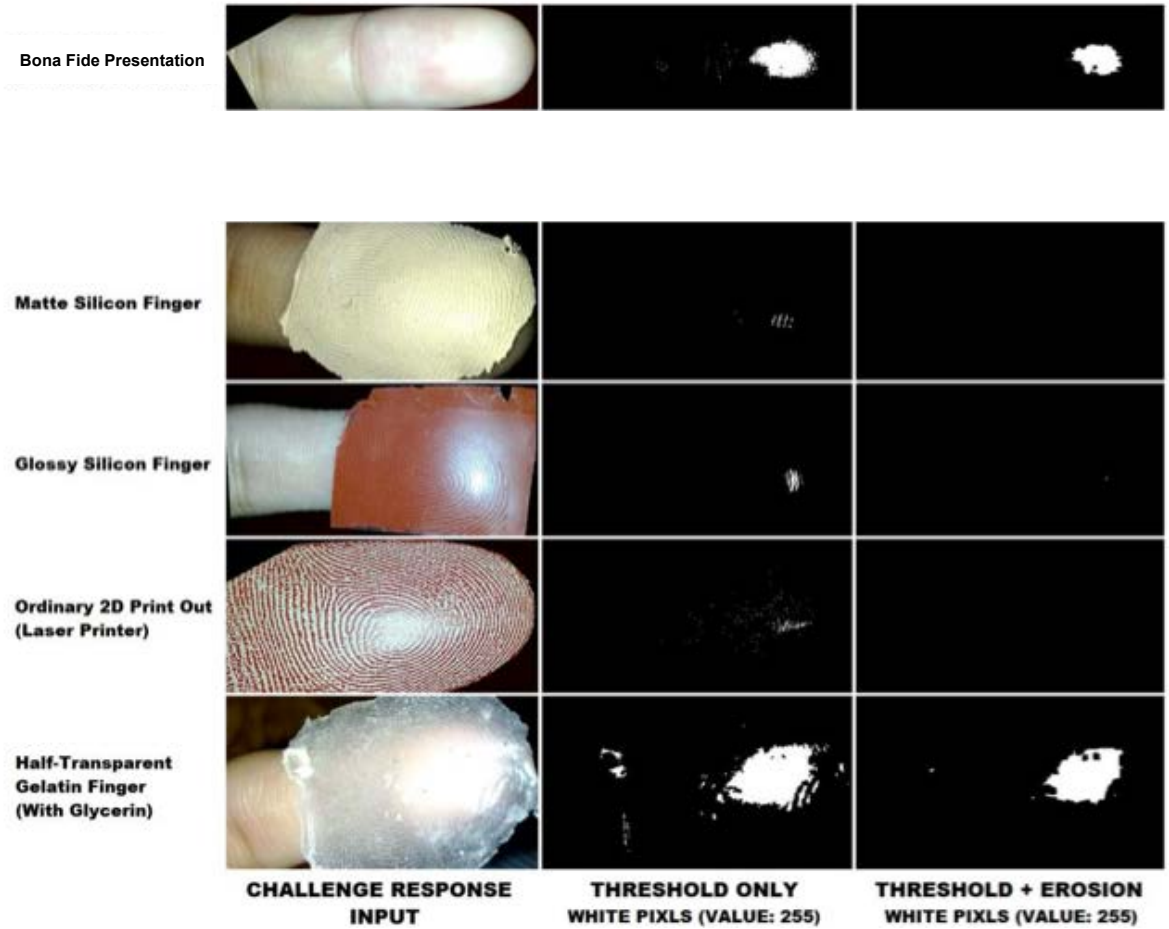
- Attack detection, as light reflection differs from artefacts to Bona Fide fingers

[SBB13] C. Stein, V. Bouatou, C. Busch, „Video-based Fingerphoto Recognition with Anti-spoofing Techniques with Smartphone Cameras“, Proceedings 12th Intern. Conference of the Biometrics Special Interest Group (BIOSIG), (2013)

Smartphone Access Control - with PAD

Finger recognition study - 2012/2013

- Results: Presentation Attack Detection (PAD)

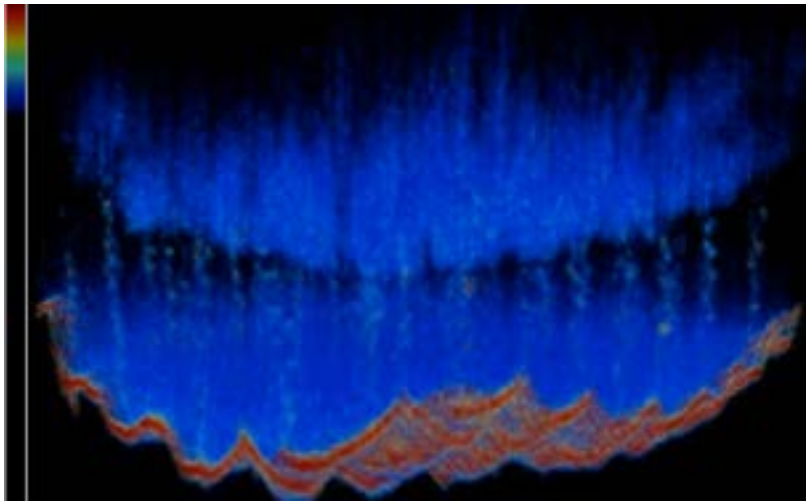


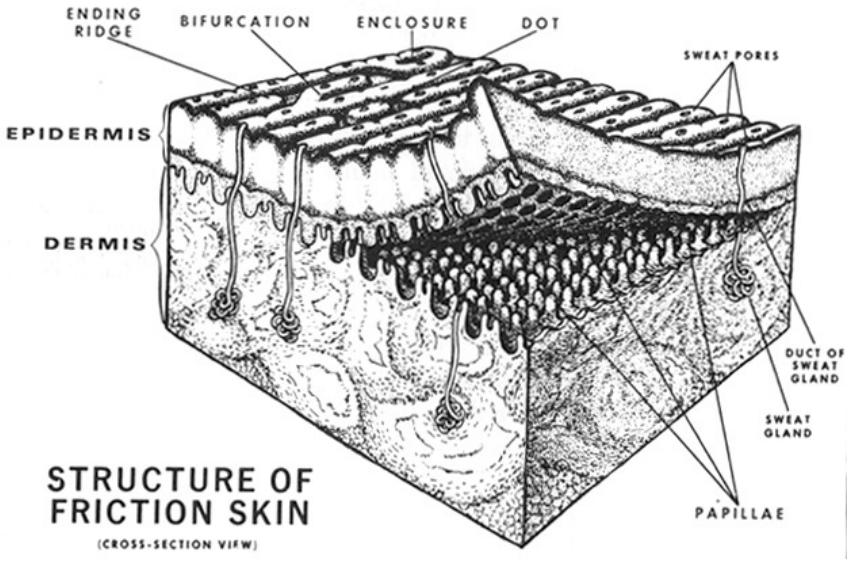
- Conclusion:
  better Presentation Attack Detection than capacitive sensors

Fingerprint Capture Device Security

Countermeasures

- Observation of the live skin properties
- Observation of the sweat glandes
- Sensors
  - Optical Coherence Tomography (OCT)

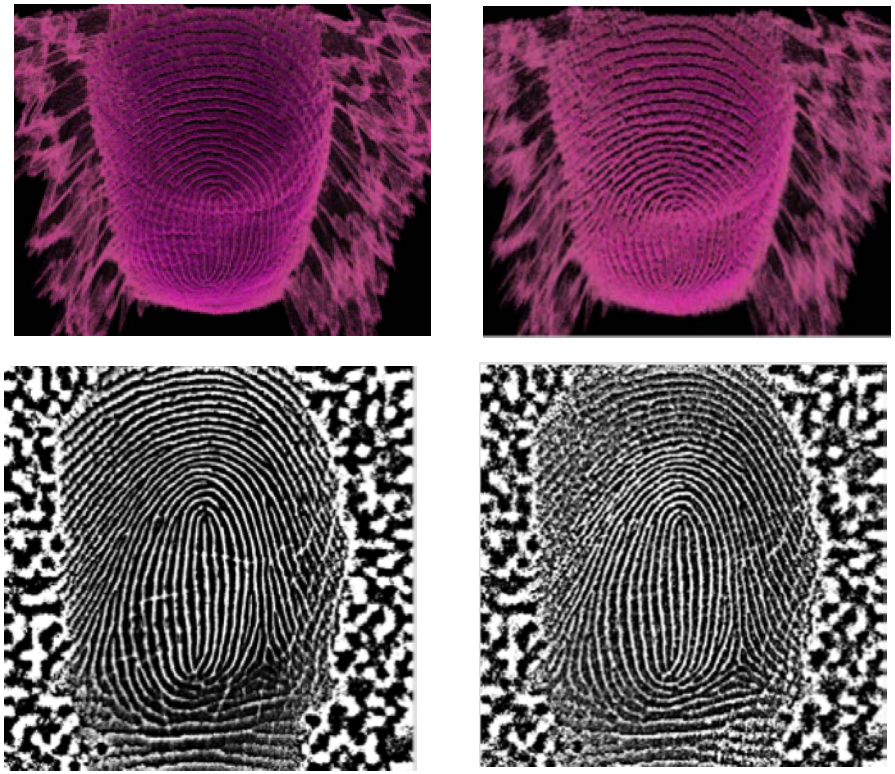




Fingerprint Capture Device Security

Comparing outer and inner fingerprint patterns

- Less than 2s (on GTX980)
  - Detection of surface and internal layer
  - 2D projection



Surface Fingerprint Internal Fingerprint

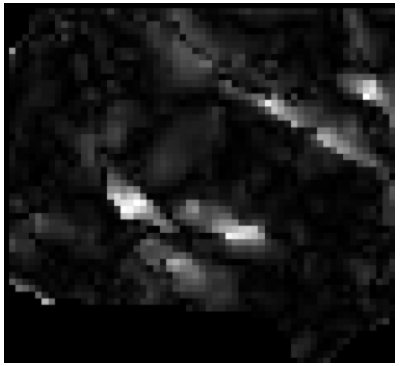
Altered Fingerprint Detection - Algorithms

- Feature: OFA and DOFTS
- Orientation Field Analysis (OFA)
  - Altered areas cause discontinuities in the OF [YoonJain2012]
- Differentials of Orientation Fields by Tensors in Scale (DOFTS)
  - Complex valued structure tensor [MikBig2014]

BonaFide fingerprint

Error map

Altered fingerprint



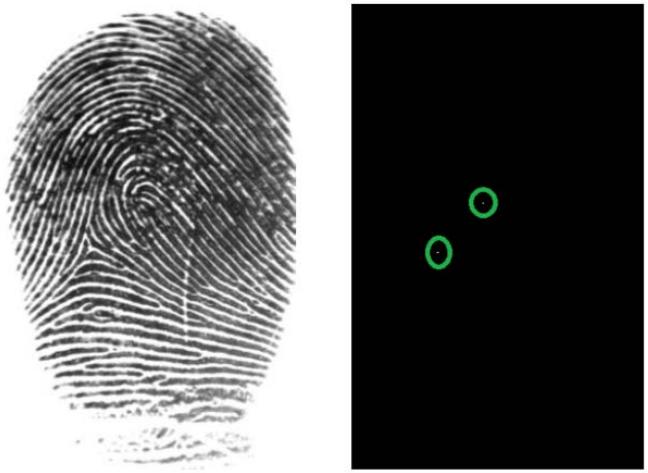
Error map

[YoonJain2012] S. Yoon, J. Feng, and A. Jain, “Altered fingerprints: Analysis and detection,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 34, no. 3, Mar. 2012

[MikBig2014] A. Mikaelyan and J. Bigun, “Symmetry assessment by finite expansion: application to forensic fingerprints,” in Proc. BIOSIG, Darmstadt, Germany, pp. 75–86. , (2014)

Altered Fingerprint Detection - Algorithms

- Feature: SPDA
- Singular Point Density Analysis [Ellingsg2014]
- using the Poincare´ index to detect noisy friction ridge areas



BonaFide fingerprint

altered fingerprint

Poincare´ index response

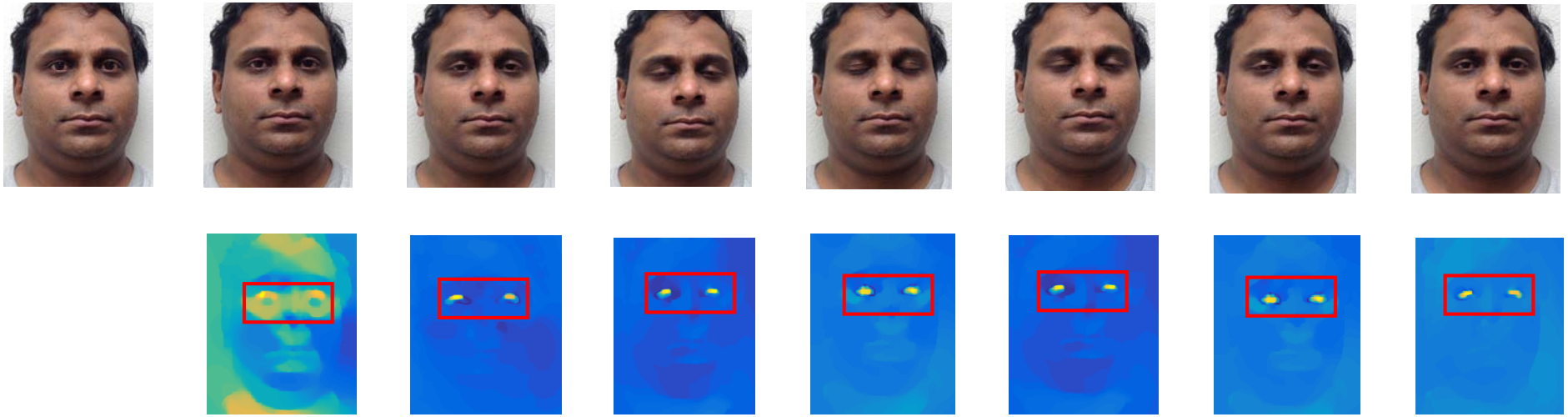
[Ellingsg2014] J. Ellingsgaard, C. Sousedik, and C. Busch, “Detecting fingerprint alterations by orientation field and minutiae orientation analysis,” in Proc. IWBF, Valletta, Malta, (2014)

Face PAD

Face Presentation Attack Detection

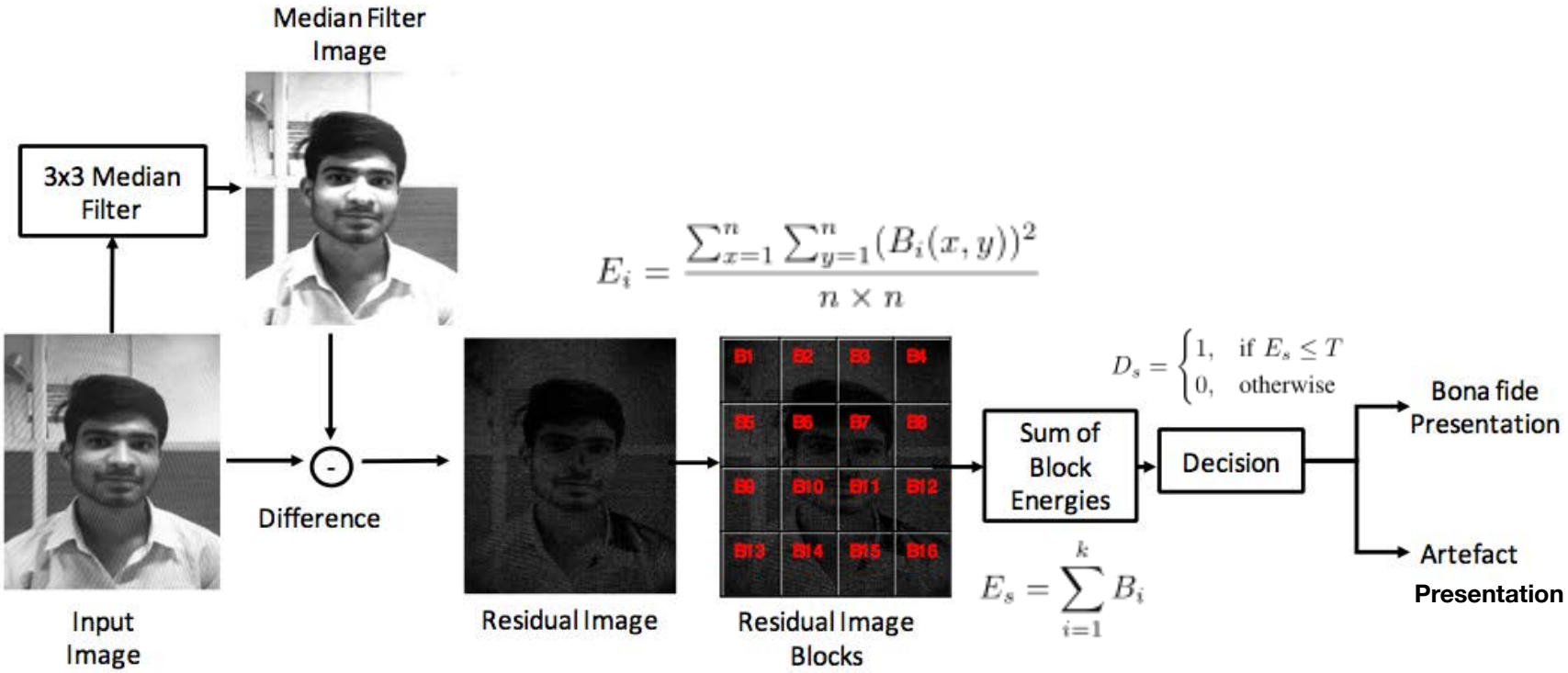
Hardware based

- Challenge Response
  - challenge the subject instructions and then compare the response to reference model for a bona fide behaviour
    - Instructions to the user to change head pose.
    - Reads user's lips after playing audio tracks of words or numbers.
- Blink detection



Smartphone - Face PAD

- Channel based processing



[Wasnik2016] P. Wasnik, K. Raja, R. Raghavendra, and C. Busch. “Presentation attack detection in face biometric systems using raw sensor data from smartphones”. In Proc. 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), (2016)

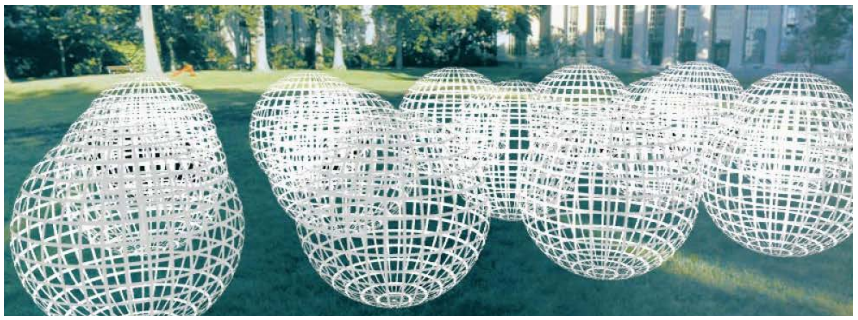
PAD – based on Depth Information

Light-field camera based PA detection

- panoptic or directional camera

Why light-field camera?

- Multiple focus/depth images in one shot.
- No need to adjust the lens to set focus.
- Portable and hand-held, low cost.

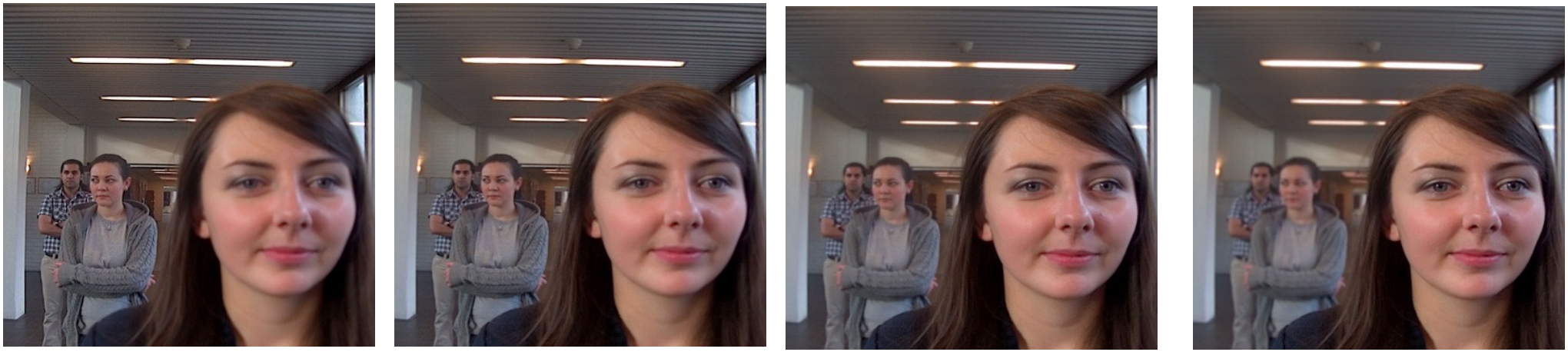


$$P(\theta, \phi, \lambda, t, Vx, Vy, Vz)$$

[Raghu2015] R. Raghavendra, K.B. Raja, and C. Busch: "Presentation Attack Detection for Face Recognition using Light Field Camera", in IEEE Transactions on Image Processing, vol. 24, no. 3, pp. 1060–1075, (2015)

PAD – based on Depth Information

Example of light-field imaging (LYTRO)



[Raghu2015] R. Raghavendra, K.B. Raja, and C. Busch: "Presentation Attack Detection for Face Recognition using Light Field Camera", in IEEE Transactions on Image Processing, vol. 24, no. 3, pp. 1060–1075, (2015)

Skin Detection

Short Wave Infrared Range (SWIR) imaging

- With multiple point sensors proposed by Steiner et al.
- Skin types defined by Fitzpatrick [Fitzpatrick1988]
  - I - Always burn, never tan
  - II - Usually burn, tan less than average
  - III - Sometimes mild burn, tan about average
  - IV - Rarely burn, tan more than average
  - V - brown
  - VI - black

Image Source: HSBRS, (2016)

[Fitzpatrick1988] T. Fitzpatrick: „The validity and practicality of sun-reactive skintypes I through VI“, Archives of Dermatology, (1988)

Skin Detection

Short Wave Infrared Range (SWIR) imaging

- Extraction of spectral remission properties
- Remission spectrum above 1200 nm independent by melanin, but strongly impacted by water

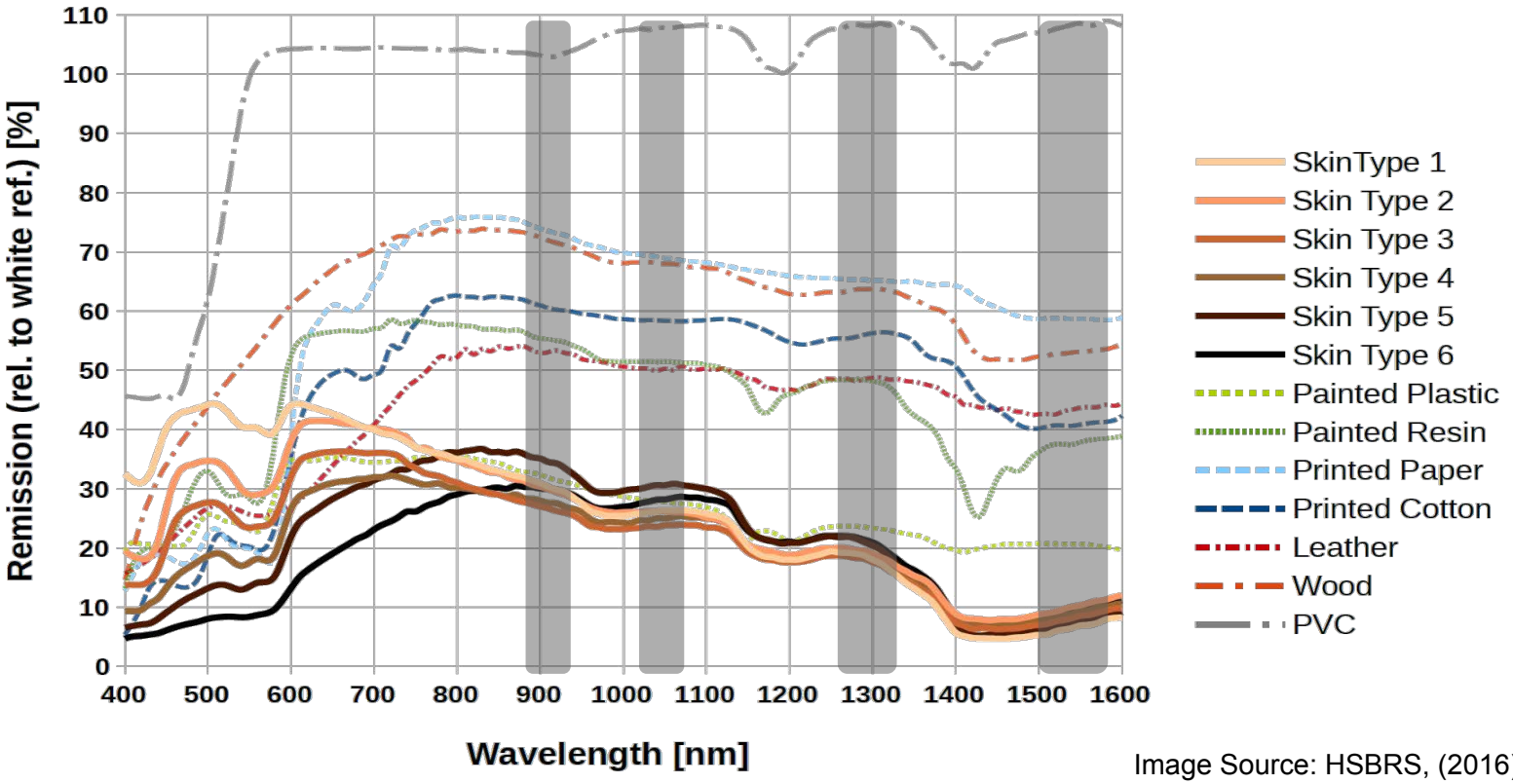


Image Source: HSBRS, (2016)

[Jacquez1955] J. Jacquez: „Spectral reflectance of human skin in the region 0.7-2.6m“,J. of Applied Physiology, (1955)

Skin Detection

Short Wave Infrared Range (SWIR) imaging

- Computing a signature from four wavebands
  - 935nm, 1060nm, 1300nm and 1550nm

$$\vec{s}(x,y) = (i_1, .., i_{n-1})$$

with $i_w, 1 \leq w < n$ being the intensity value of pixel (x, y) for waveband w

  - Classification with a Support Vector Machine (SVM)
  - Makeup, facial cream or tattoos should not be rejected as a presentation attack

[Steiner2016] H. Steiner, A. Kolb, N. Jung: „Reliable Face Anti-Spoofing Using Multispectral SWIR Imaging“, in Proceedings ICB, (2016)

Morphing Attacks - Context

ICAO International Specifications

The idea:

- One citizen - one passport

Principle of unique link

- 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 citizen - one passport

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

- Multiple individuals - one passport

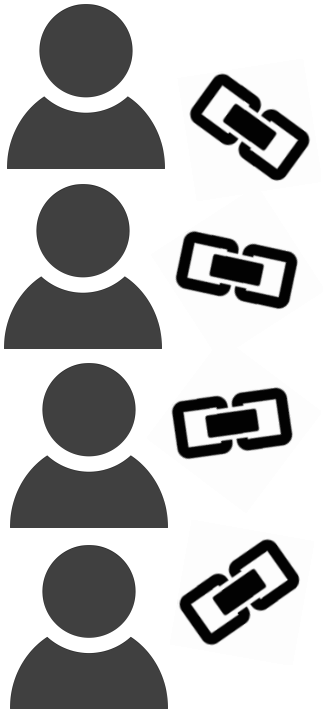


image source: https://pixabay.com/de/vectors/tick-sternchen-kreuz-rot-gr%C3%BCn-40678/

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

What is Morphing?

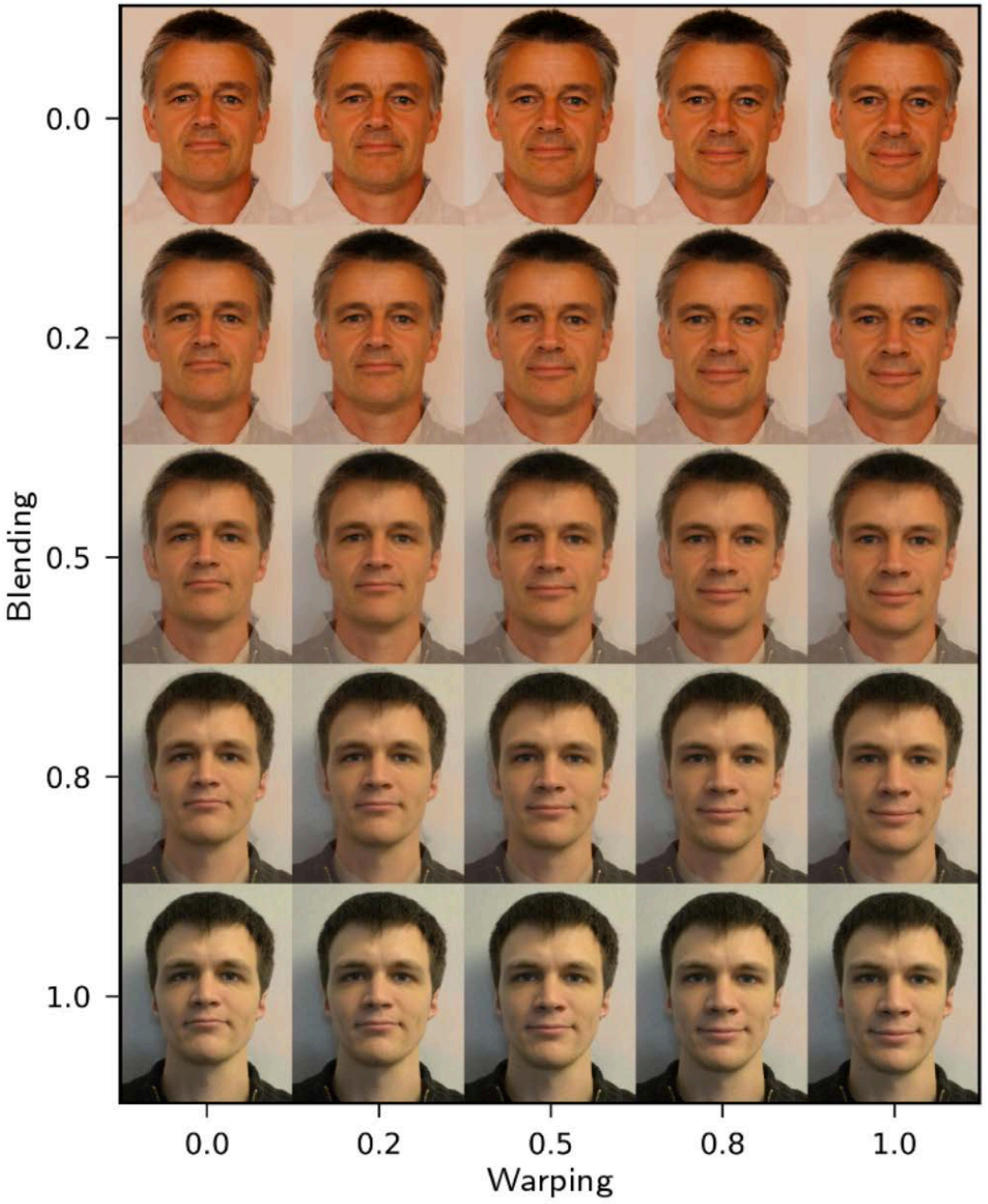
Warping and blending

- 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: Morphing Attacks

Morphing attack scenario

- Passport application of the accomplice A

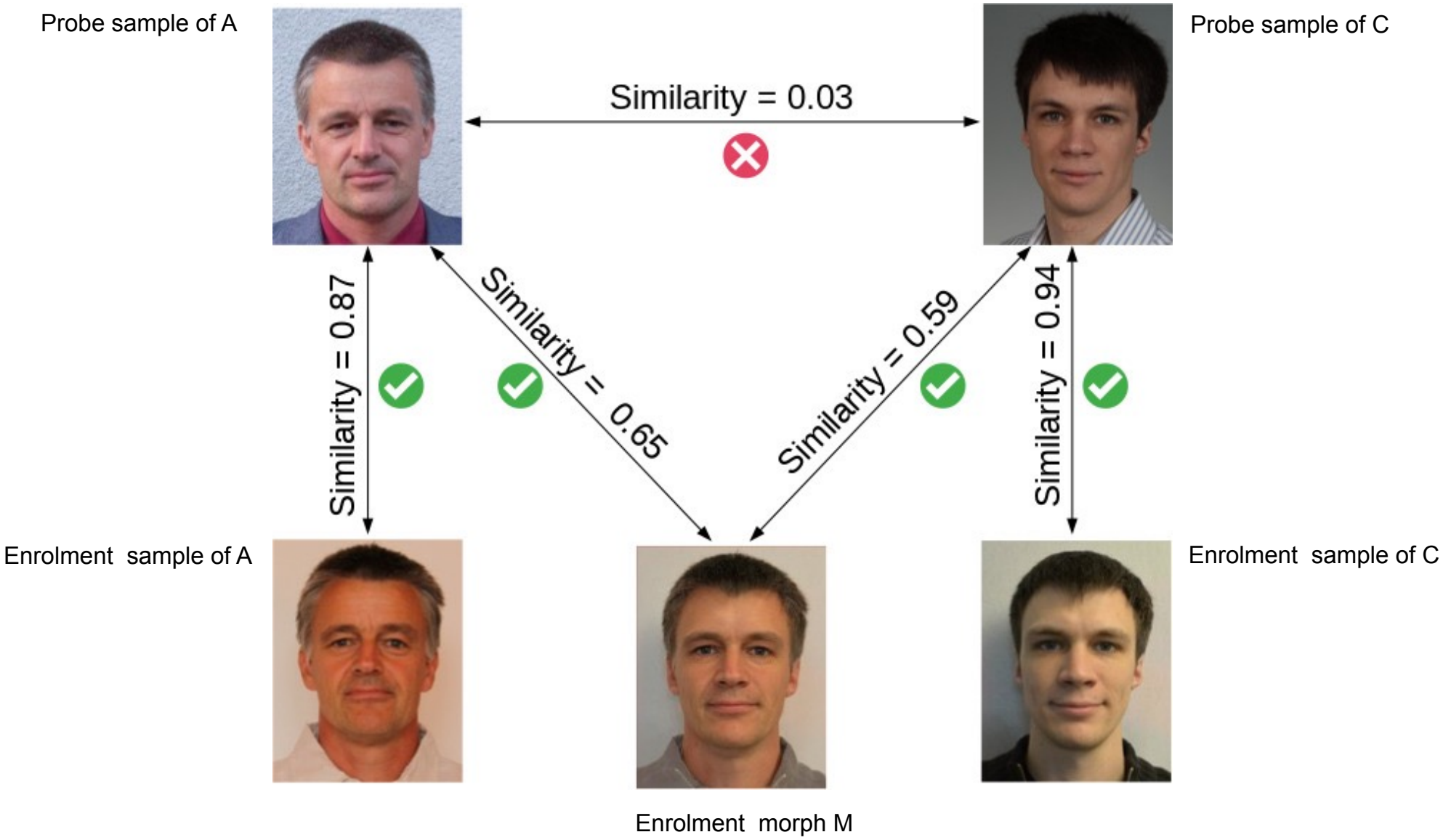
Problem: Morphing Attacks

Morphing attack scenario

- Border control

Problem: Morphing Attacks

Verification against morphed facial images



Problem: Morphing Attacks

Is it a really problem ?

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.

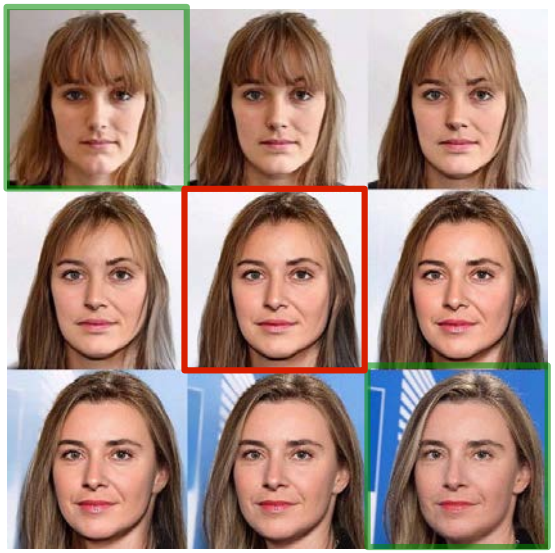
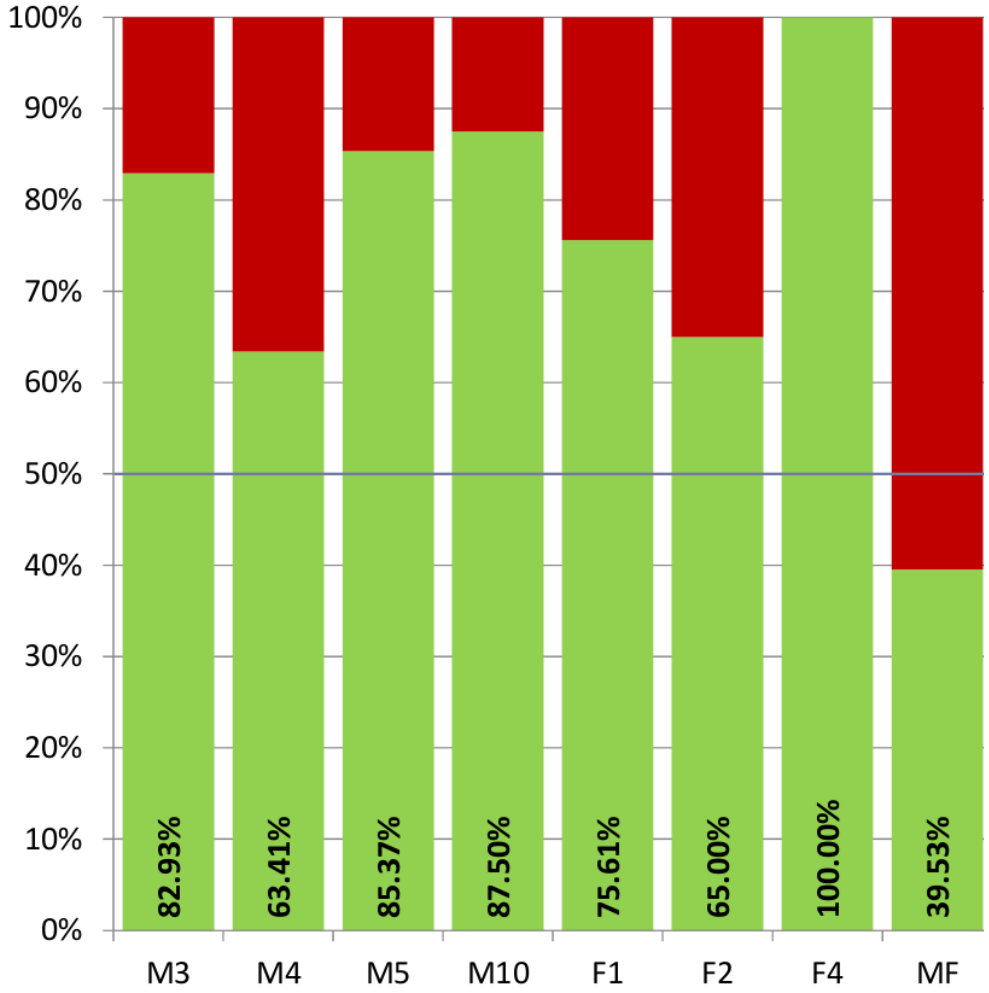


Image source: https://www.spiegel.de/netzwelt/netzpolitik/biometrie-im-reisepass-peng-kollektiv-schmuggelt-fotomontage-in-ausweis-a-1229418.html

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)

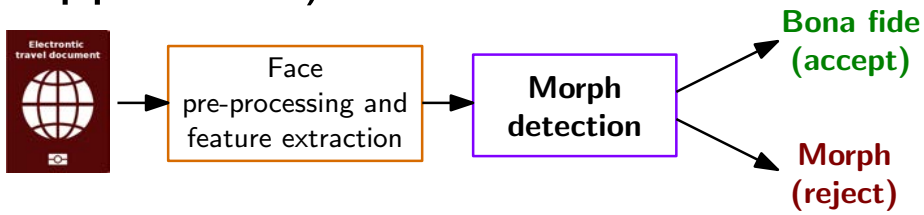
Morphing Attack Detection (MAD)

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)

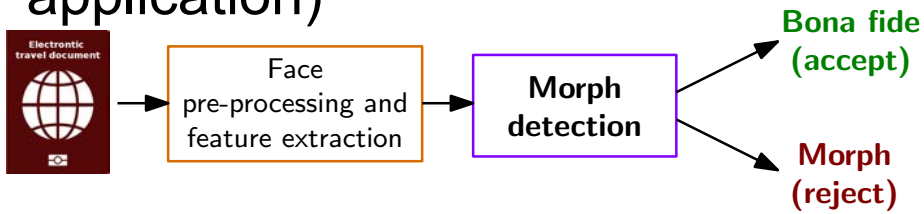


[SRB2018a] U. Scherhag, C. Rathgeb, C. Busch: "Towards Detection of Morphed Face Images in electronic Travel Documents“, in Proceedings of the 13th IAPR International Workshop on Document Analysis Systems (DAS), April 24-27, (2018)

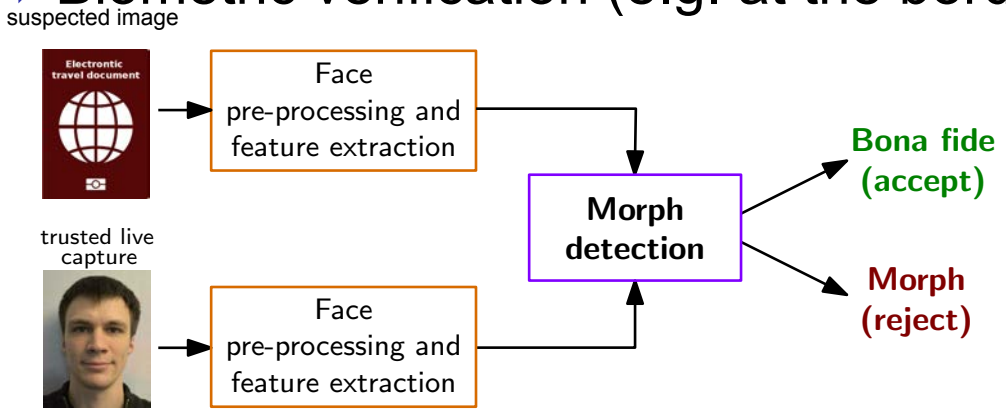
Morphing Attack Detection Scenarios

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)

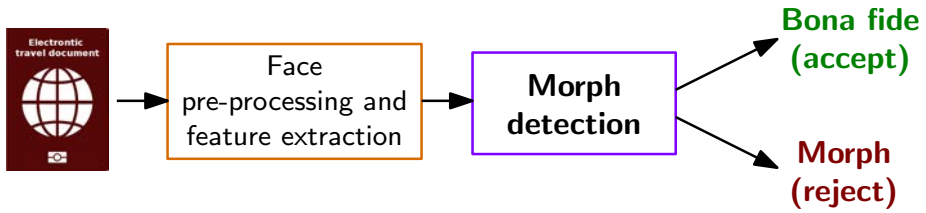


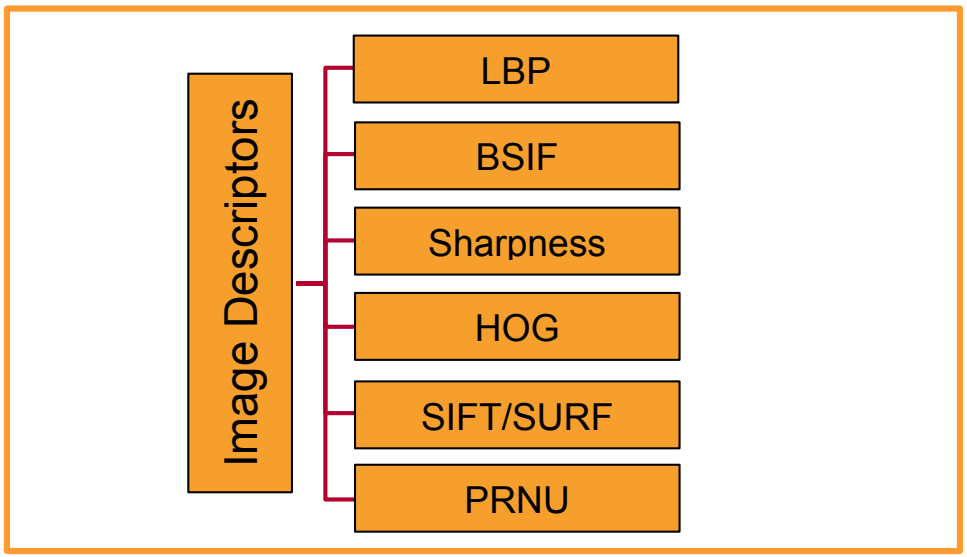
[SRB2018a] U. Scherhag, C. Rathgeb, C. Busch: "Towards Detection of Morphed Face Images in electronic Travel Documents“, in Proceedings of the 13th IAPR International Workshop on Document Analysis Systems (DAS), April 24-27, (2018)

Face Pre-processing and Feature

Morphing Attack Detection (S-MAD) with texture analysis

- Image descriptors as hand-crafted features





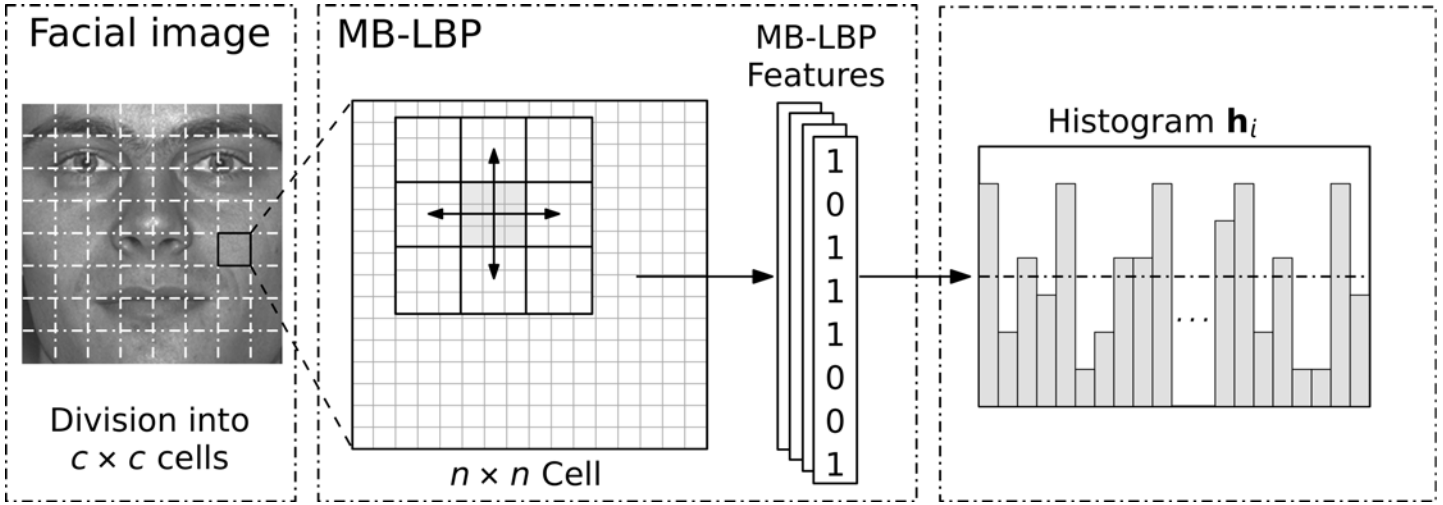
Morph Detection Classifier

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

Face Pre-processing and Feature

S-MAD with image descriptor

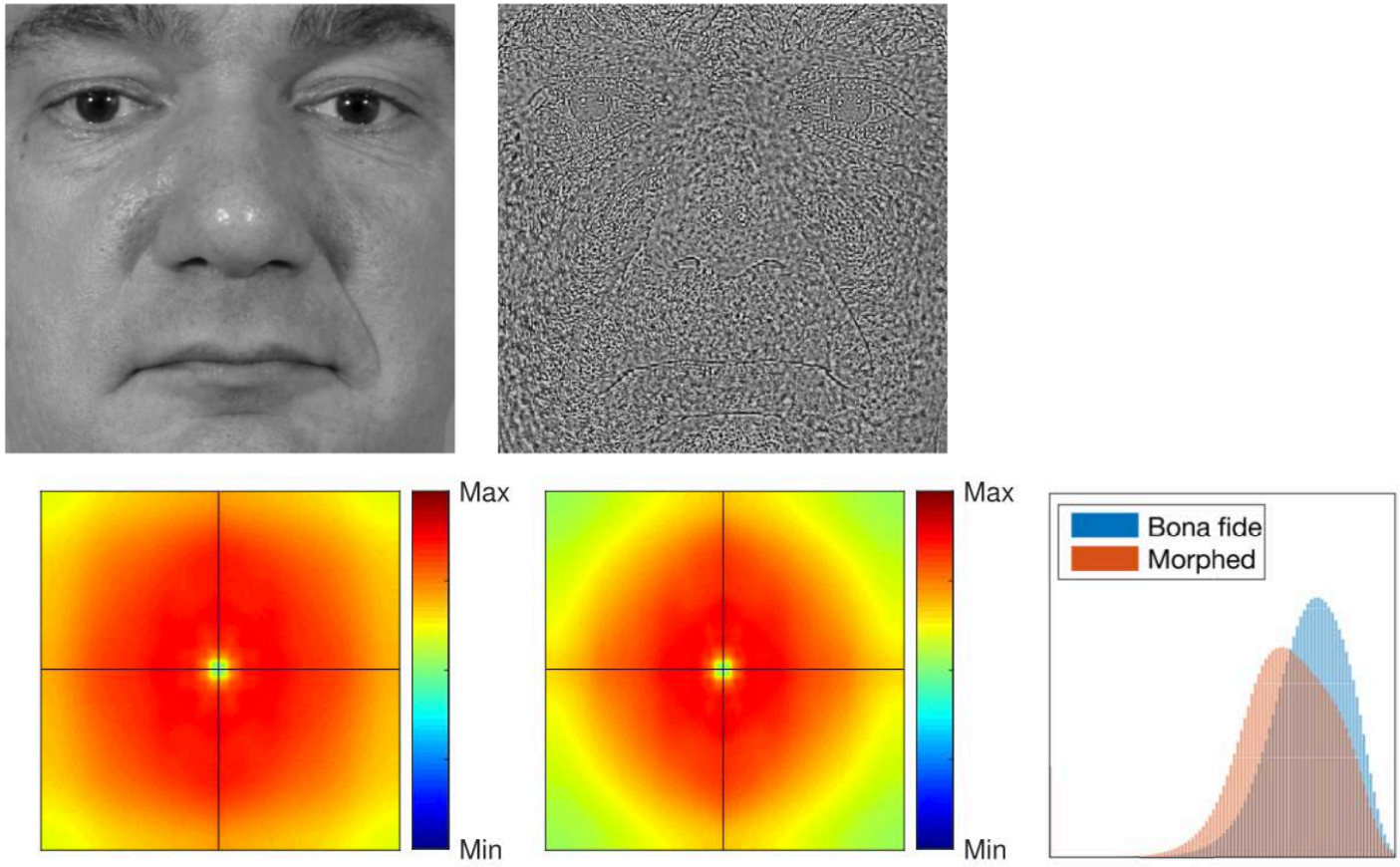
- Local Binary Pattern (LBP)



Face Pre-processing and Feature

S-MAD with image descriptor / forensic approach

- Photo Response Non-Uniformity (PRNU)

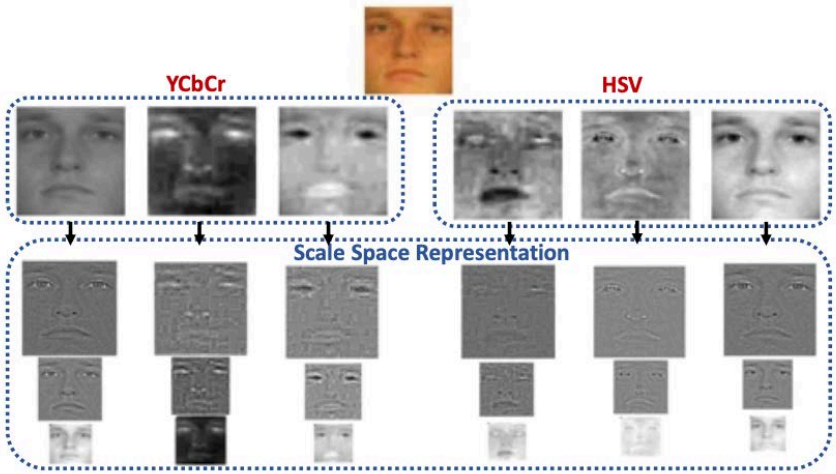


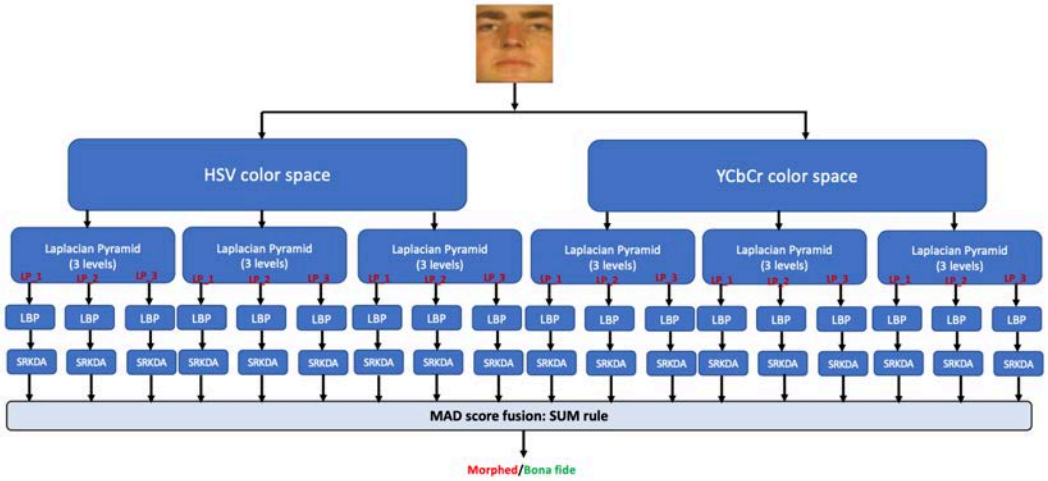
[SDRBU2019] U. Scherhag, L. Debiasi, C. Rathgeb, C. Busch and A. Uhl: "Detection of Face Morphing Attacks based on PRNU Analysis“, in IEEE TBIOM, (2019)

Face Pre-processing and Feature

S-MAD with Scale-Space features

- Transformation to different color spaces
- Laplacian decomposition



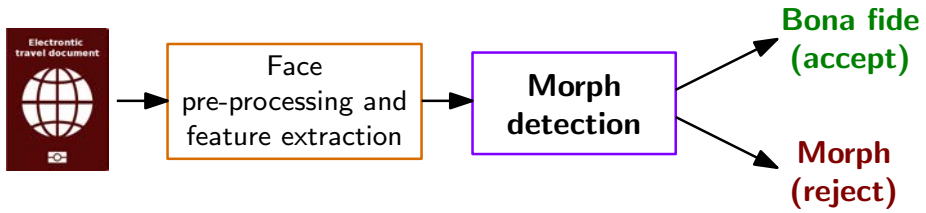


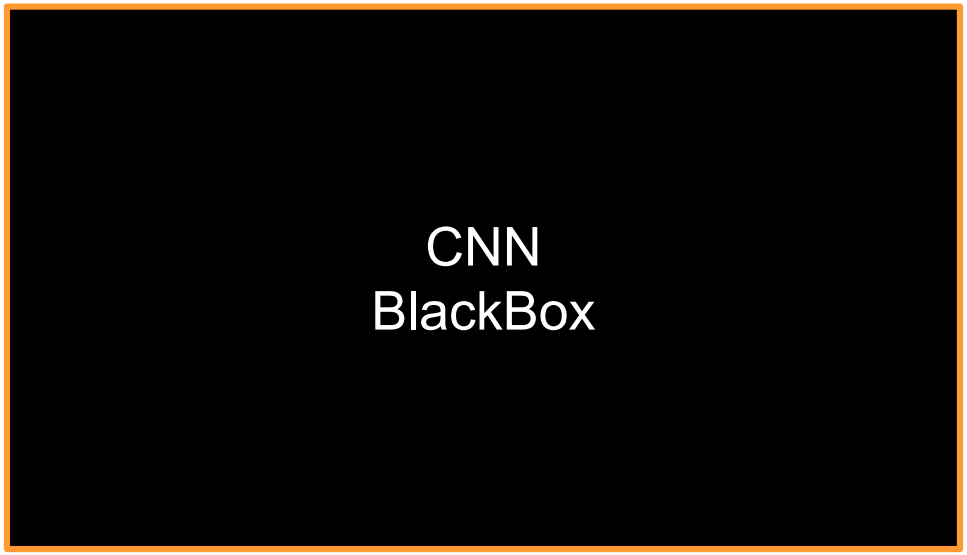
[RVRB2019] R. Raghavendra, S. Venkatesh, K. Raja, C. Busch: "Towards making Morphing Attack Detection robust using hybrid scale-space Colour Texture Features", in Proceedings of the International Conference on Identity, Security and Behavior Analysis (ISBA), (2019)

Face Pre-processing and Feature

Morphing Attack Detection (S-MAD) with texture analysis

- Image descriptors as Deep features



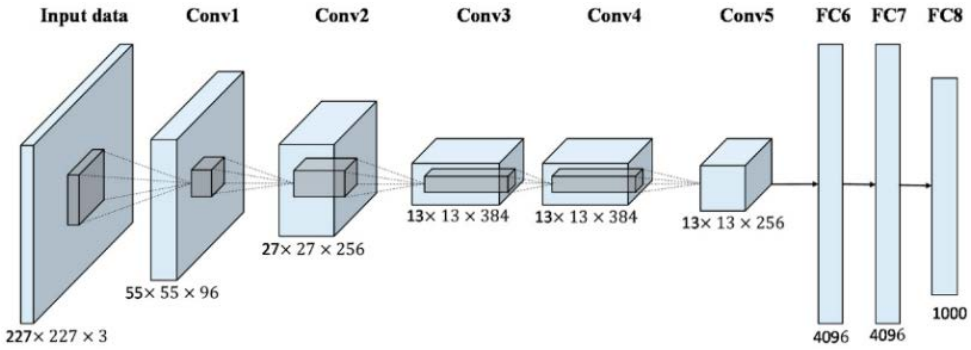


Morph Detection Classifier

Face Pre-processing and Feature

S-MAD with deep learning

- Feature Representations
  - pre-trained Convolutional Neural Network (CNN)

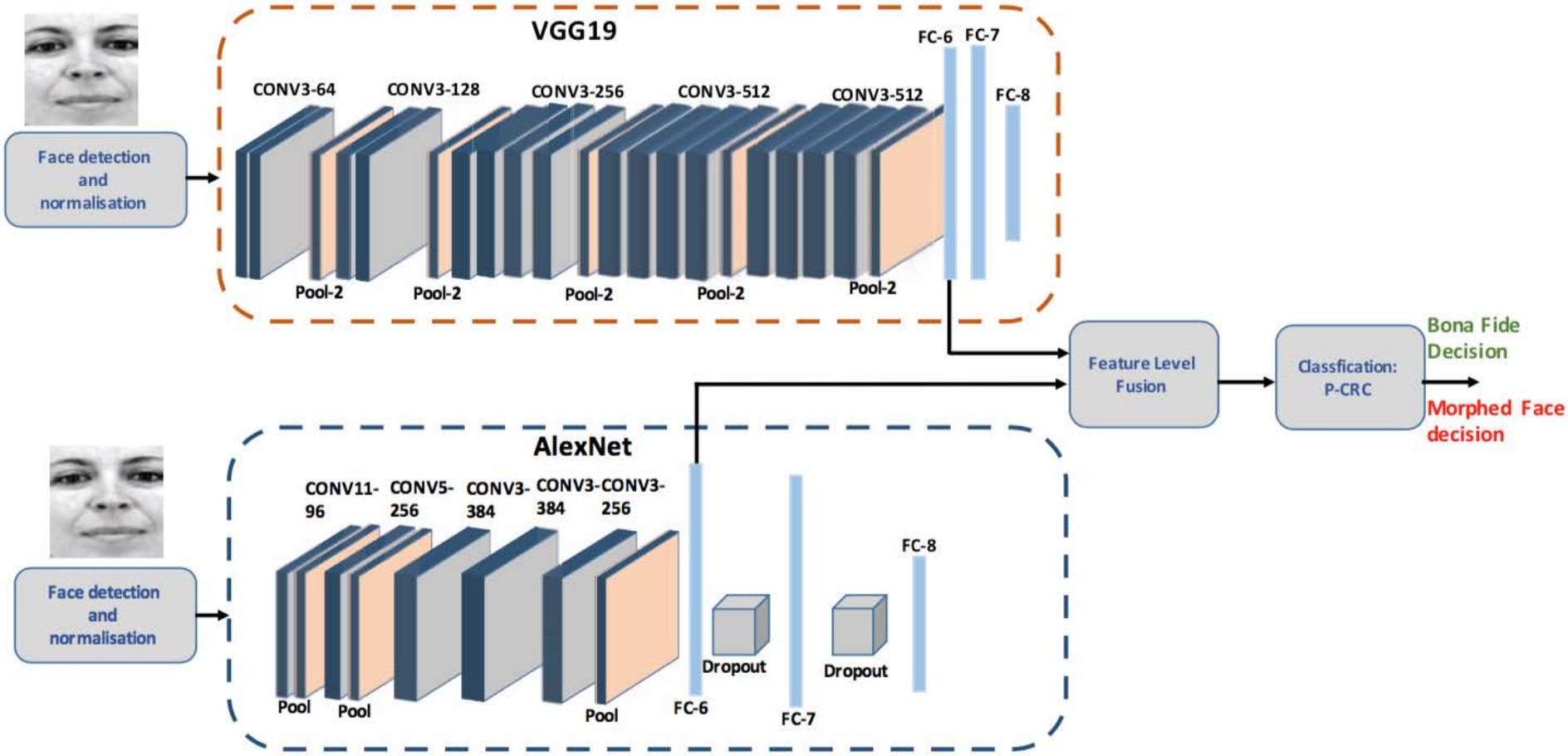


Morph Detection Classifier

Single Image Morphing Attack Detection

S-MAD with deep learning

- Feature level fusion of Deep CNNs

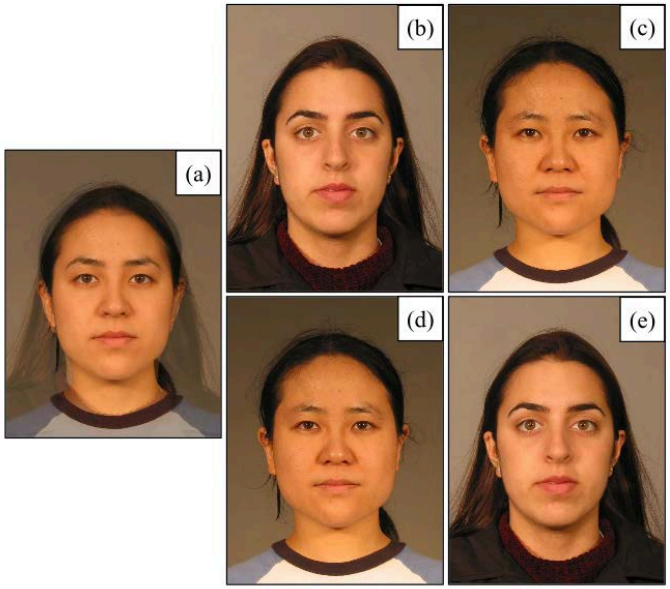


[RRVBu2017] R. Raghavendra, K. Raja, S. Venkatesh, C. Busch: "Transferable Deep-CNN features for detecting digital and print-scanned morphed face images", in Proceedings of 30th International Conference on Computer Vision and Pattern Recognition Workshop (CVPRW), July 21-26, (2017)

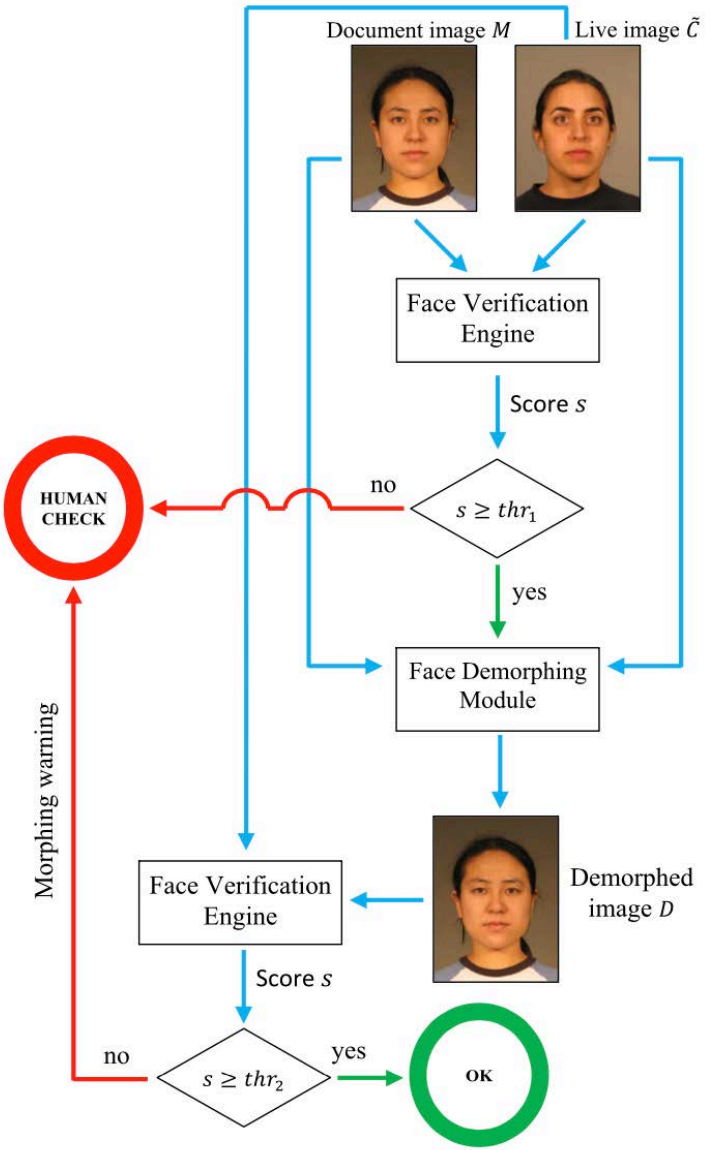
Differential Morphing Attack Detection

D-MAD with Demorphing

- Invert the morphing process
- Then confirm the similarity score



a) suspected image
b) and c): trusted live capture image
d) and e): recovery image

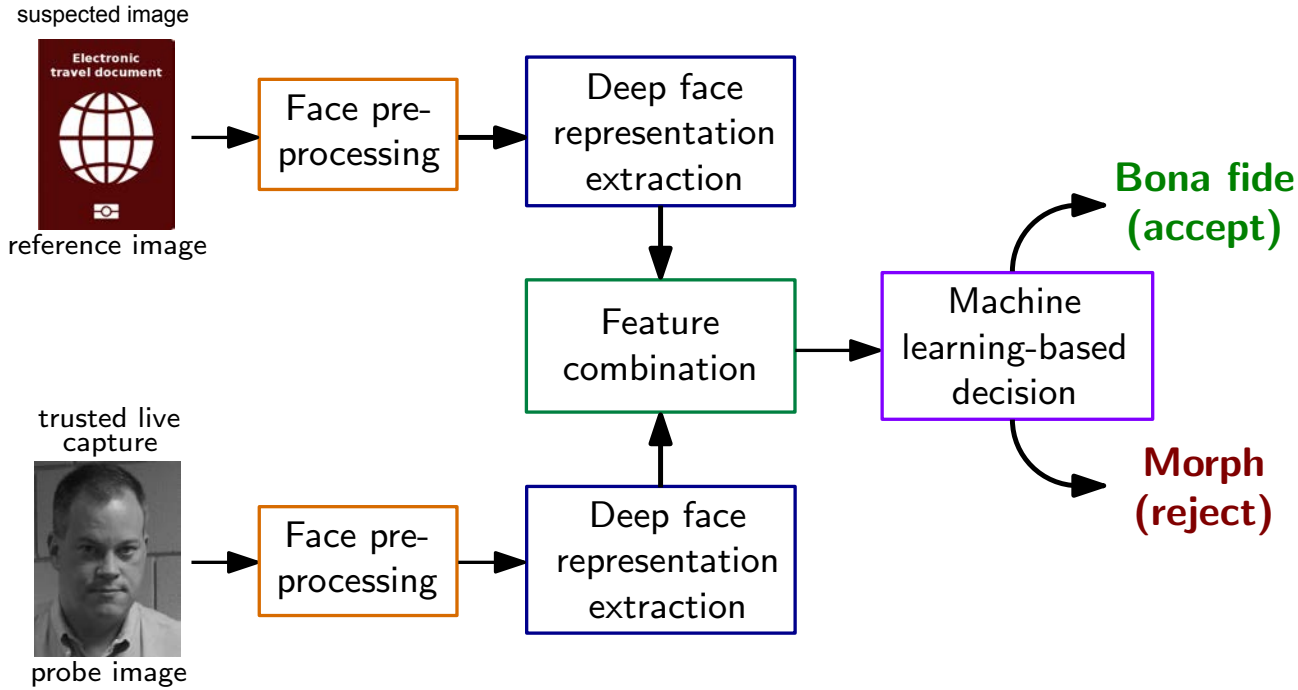


[Ferrara2018] M. Ferrara, A. Franco, D. Maltoni: "Face Demorphing“,
in IEEE Transactions on Information Forencics and Security (TIFS), (2018)

Differential Morphing Attack Detection

D-MAD with deep learning

- Deep Face representations of Deep CNNs

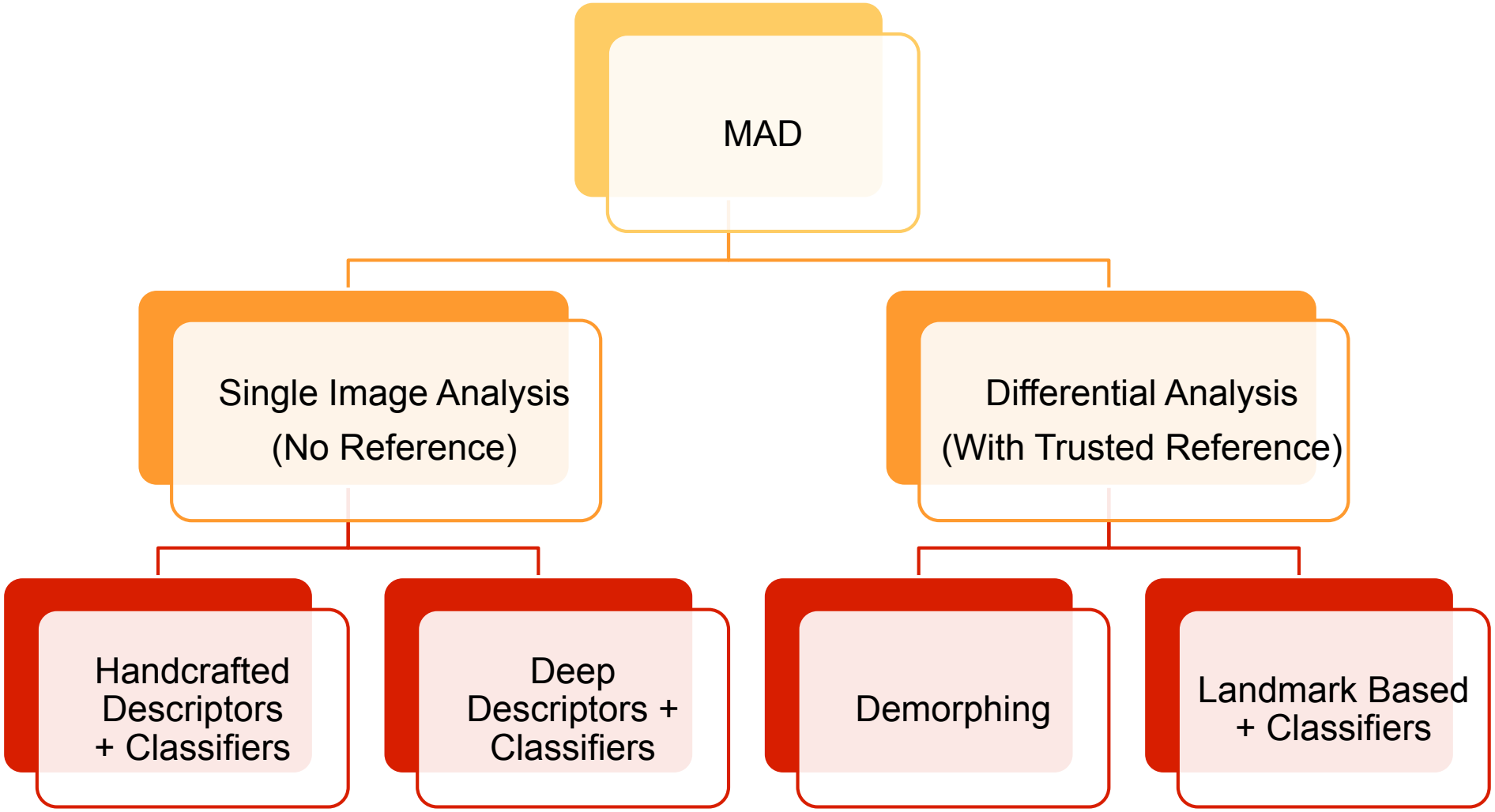


- Deep representations extracted by the neural network (on the lowest layer)
- Feature space with small dimension: 512 (for ArcFace and FaceNet)
- SVM with radial basis function

[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)

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

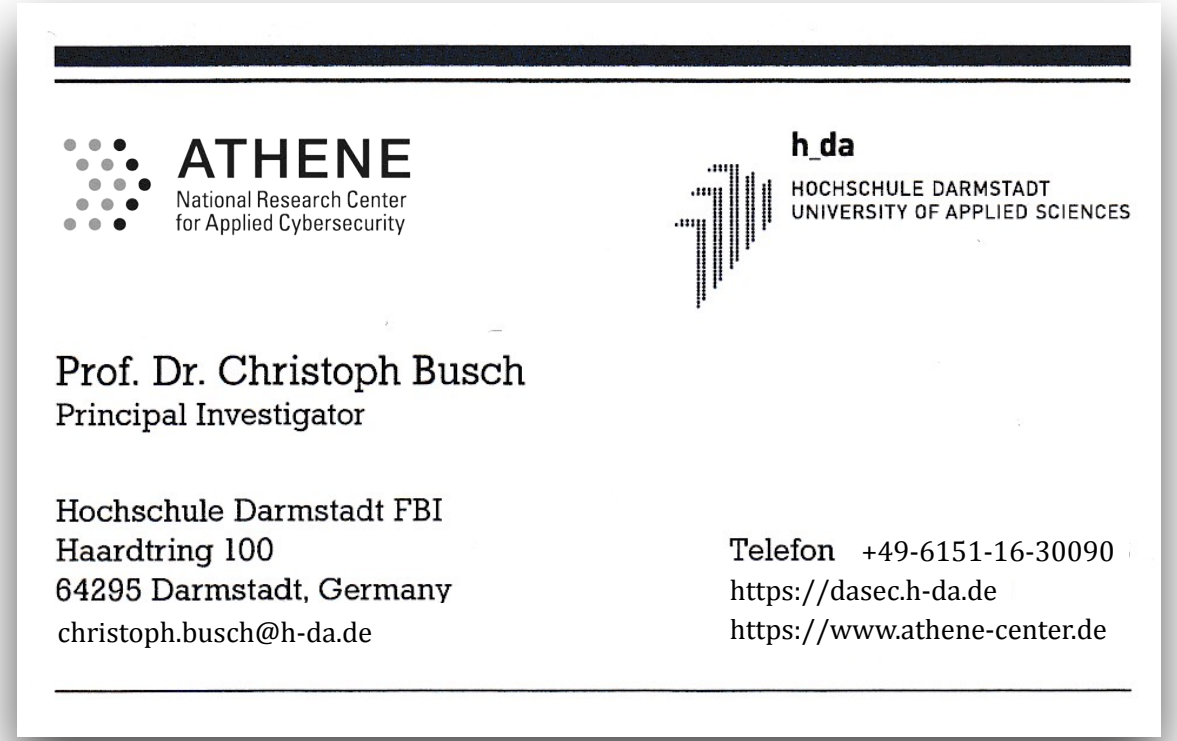
A. FACE MORPHING ATTACK

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


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