Biometric Attack Detection

Christoph Busch

more information at:
https://christoph-busch.de
latest news at:
https://twitter.com/busch_christoph

EAB Training on September 17, 2021

ATHENE

European Association for Biometrics
eab
Human Identity in Europe

NTNU

Overview

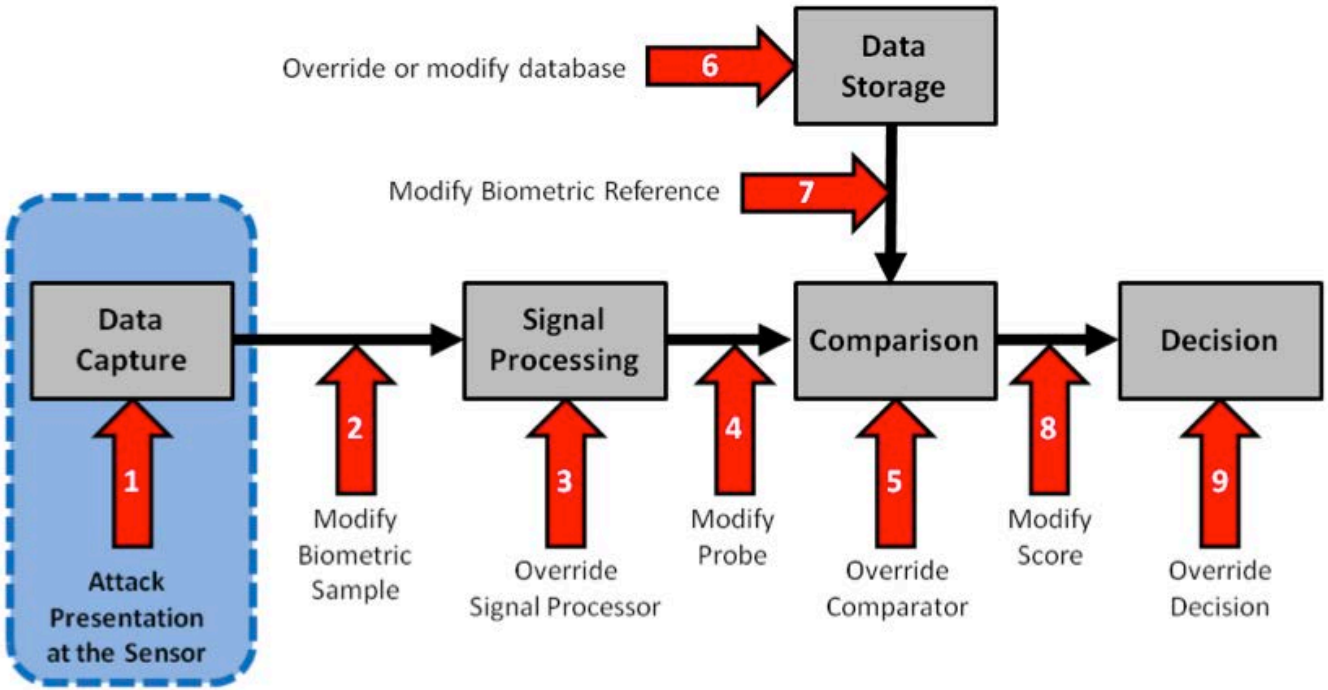
Agenda

- Attacks on facial systems
- Attack types
  - presentation attacks (a.k.a spoofing)
  - morphing
  - deep fakes

Weakness of Biometric Systems

Three main points for a targeted attack

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



Source: ISO/IEC 30107-1:2016

Capture Device - Replicates of Biometric Characteristics and Fake Finger Attacks

Fingerprint Capture Device Security

Artificial Finger

- Generated replicated biometric characteristic should have similar properties compared to a real finger
  - Flexibility
  - Humidity
- Silicone
  - An initiated chemical reaction will harden the silicone

Security Fingerprint Sensor - Attack 1

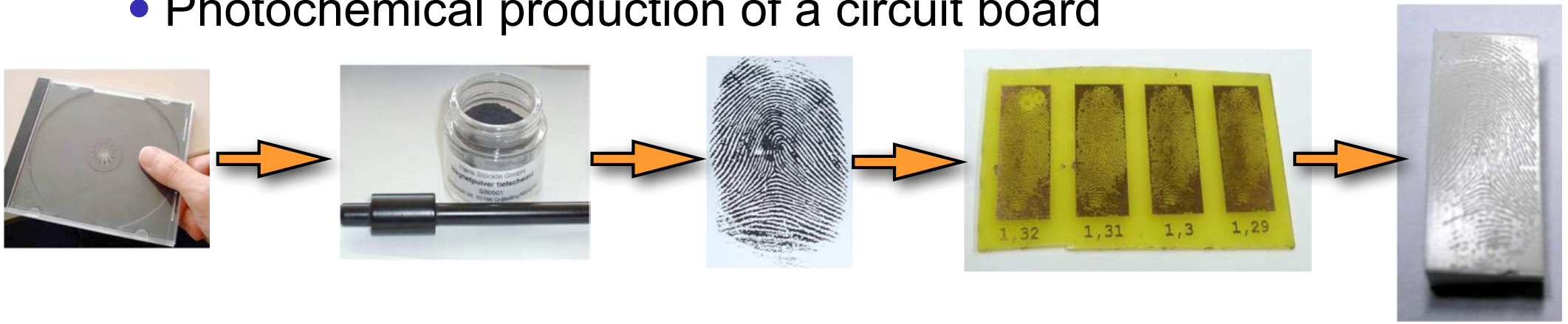
Attack with support of an enrolled individual

- Generation of a negative fingerprint
  as the finger is pressed in modeling mass
- Modeling mass is filled with silicone

Security Fingerprint Sensor - Attack 2

Attack without support of an enrolled individual

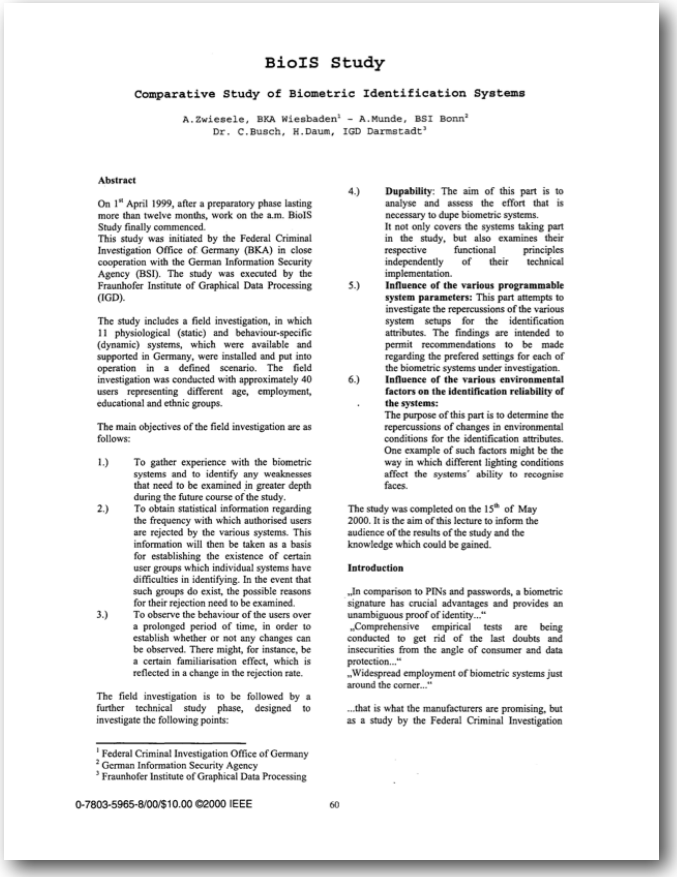
- Recording of a latent fingerprint from flat surface material
  - e.g. glass, CD-cover, etc.
    with iron powder and tape
- Scanning and post processing:
  - Correction of scanning errors
  - Closing of ridge lines (as needed)
  - Image inversion
- Print on transparent slide
- Photochemical production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



Gummy Finger Production in 2000 !

Reported in a publication by the German Federal Police

- 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)



BioIS Study

Comparative Study of Biometric Identification Systems

A.Zwiesele, BKA Wiesbaden[1] - A.Munde, BSI Bonn[2]
Dr. C.Busch, H.Daum, IGD Darmstadt[3]

Abstract

On 1st April 1999, after a preparatory phase lasting more than twelve months, work on the a.m. BioIS Study finally commenced.
This study was initiated by the Federal Criminal Investigation Office of Germany (BKA) in close cooperation with the German Information Security Agency (BSI). The study was executed by the Fraunhofer Institute of Graphical Data Processing (IGD).

The study includes a field investigation, in which 11 physiological (static) and behaviour-specific (dynamic) systems, which were available and supported in Germany, were installed and put into operation in a defined scenario. The field investigation was conducted with appoximately 40 users representing different age, employment, educational and ethnic groups.

The main objectives of the field investigation are as follows:

1.) To gather experience with the biometric systems and to identify any weaknesses that need to be examined in greater depth during the future course of the study.
2.) To obtain statistical information regarding the frequency with which authorised users are rejected by the various systems. This information will then be taken as a basis for establishing the existence of certain user groups which individual systems have difficulties in identifying. In the event that such groups do exist, the possible reasons for their rejection need to be examined.
3.) To observe the behaviour of the users over a prolonged period of time, in order to establish whether or not any changes can be observed. There might, for instance, be a certain familiarisation effect, which is reflected in a change in the rejection rate.

The field investigation is to be followed by a further technical study phase, designed to investigate the following points:

4.) **Dupability**: The aim of this part is to analyse and assess the effort that is necessary to dupe biometric systems.
It not only covers the systems taking part in the study, but also examines their respective functional principles independently of their technical implementation.
5.) **Influence of the various programmable system parameters:** This part attempts to investigate the repercussions of the various system setups for the identification attributes. The findings are intended to permit recommendations to be made regarding the prefered settings for each of the biometric systems under investigation.
6.) **Influence of the various environmental factors on the identification reliability of the systems:**
The purpose of this part is to determine the repercussions of changes in environmental conditions for the identification attributes. One example of such factors might be the way in which different lighting conditions affect the systems' ability to recognise faces.

The study was completed on the 15th of May 2000. It is the aim of this lecture to inform the audience of the results of the study and the knowledge which could be gained.

Introduction

„In comparison to PINs and passwords, a biometric signature has crucial advantages and provides an unambiguous proof of identity..."
„Comprehensive empirical tests are being conducted to get rid of the last doubts and insecurities from the angle of consumer and data protection..."
„Widespread employment of biometric systems just around the corner..."

...that is what the manufacturers are promising, but as a study by the Federal Criminal Investigation

[1] Federal Criminal Investigation Office of Germany
[2] German Information Security Agency
[3] Fraunhofer Institute of Graphical Data Processing

0-7803-5965-8/00/$10.00 ©2000 IEEE

Security Fingerprint Sensor - Attack 2

Artefact preparation

- Overlay artefact: thin latex glue imprinted with fingerprint pattern taken from the target victim
  - collecting for instance a latent print from a surface

Security Fingerprint Sensor - Attack 3

Latent fingerprint

- The latent print that is left behind on the flat surface of the sensor is directly exploited for an attack
- Repeat activation with:
  - Warm temperature
  - Humidity

Security Fingerprint Sensor - Attack 3

- 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

Presentation Attack Detection

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

Concealer

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

- evade face detection

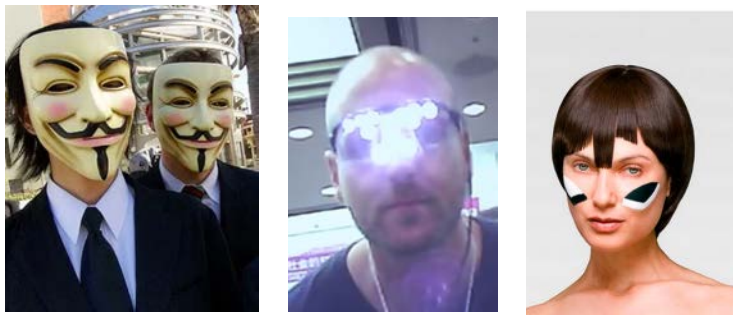


Image Source: https://www.youtube.com/watch?v=LRj8whKmN1M

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

ISO/IEC 30107-1 - Definitions

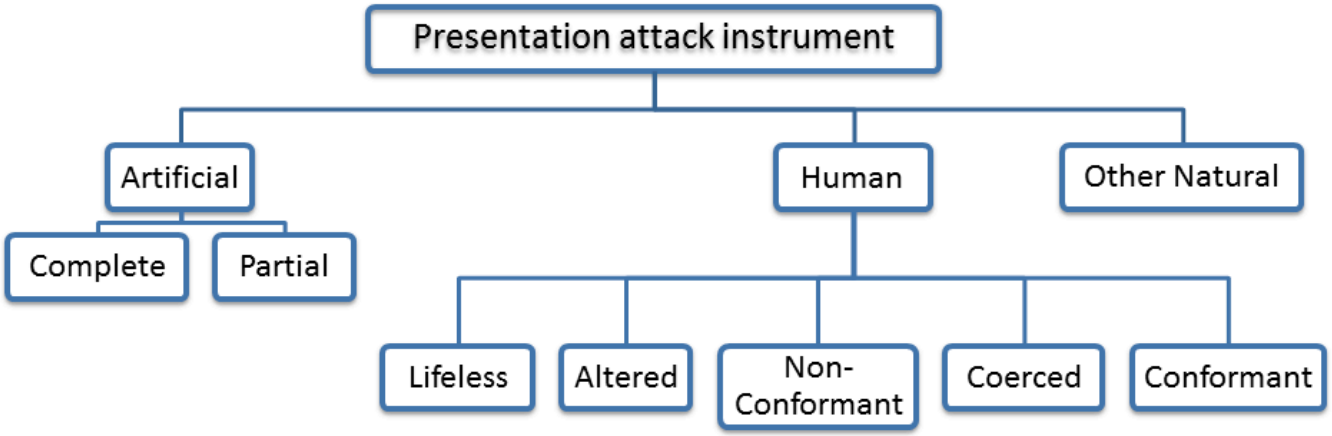
- **presentation attack instrument (PAI)**
  biometric characteristic or object used in a presentation attack
- **artefact**
  artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns

Types of presentation attacks

(General Noun)

(Adjectives describing categories)

(Qualifying adjectives)



Source: ISO/IEC 30107-1

Testing Standards

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

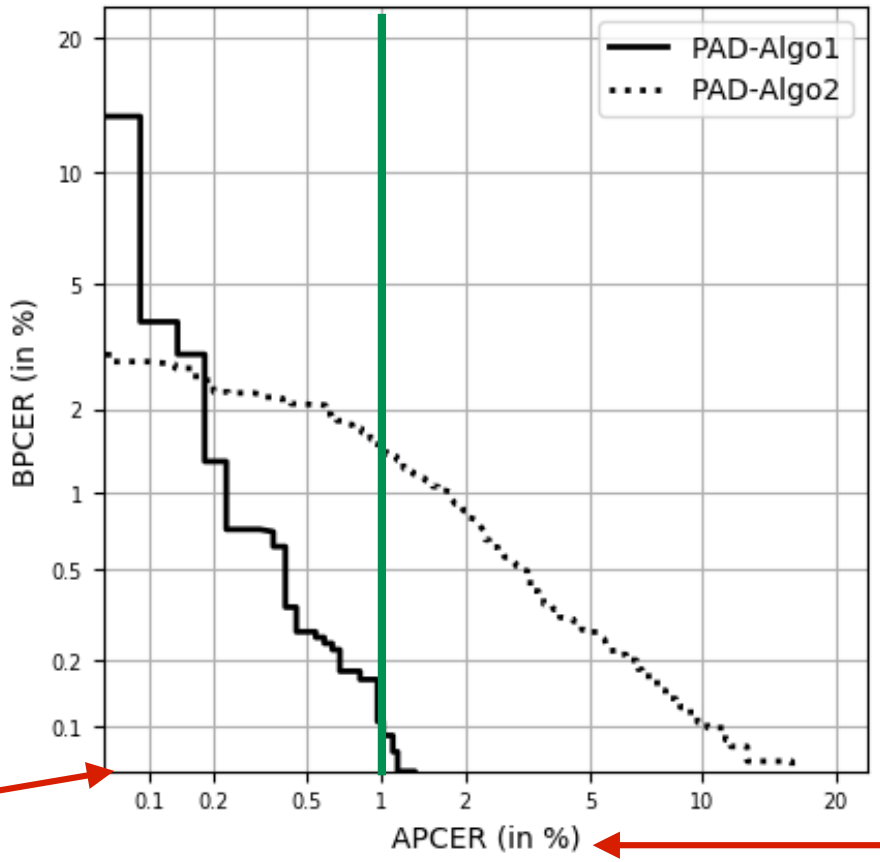
- **Bona fide presentation classification error rate (BPCER)**
  proportion of bona fide presentations incorrectly classified as attack presentations in a specific scenario

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:



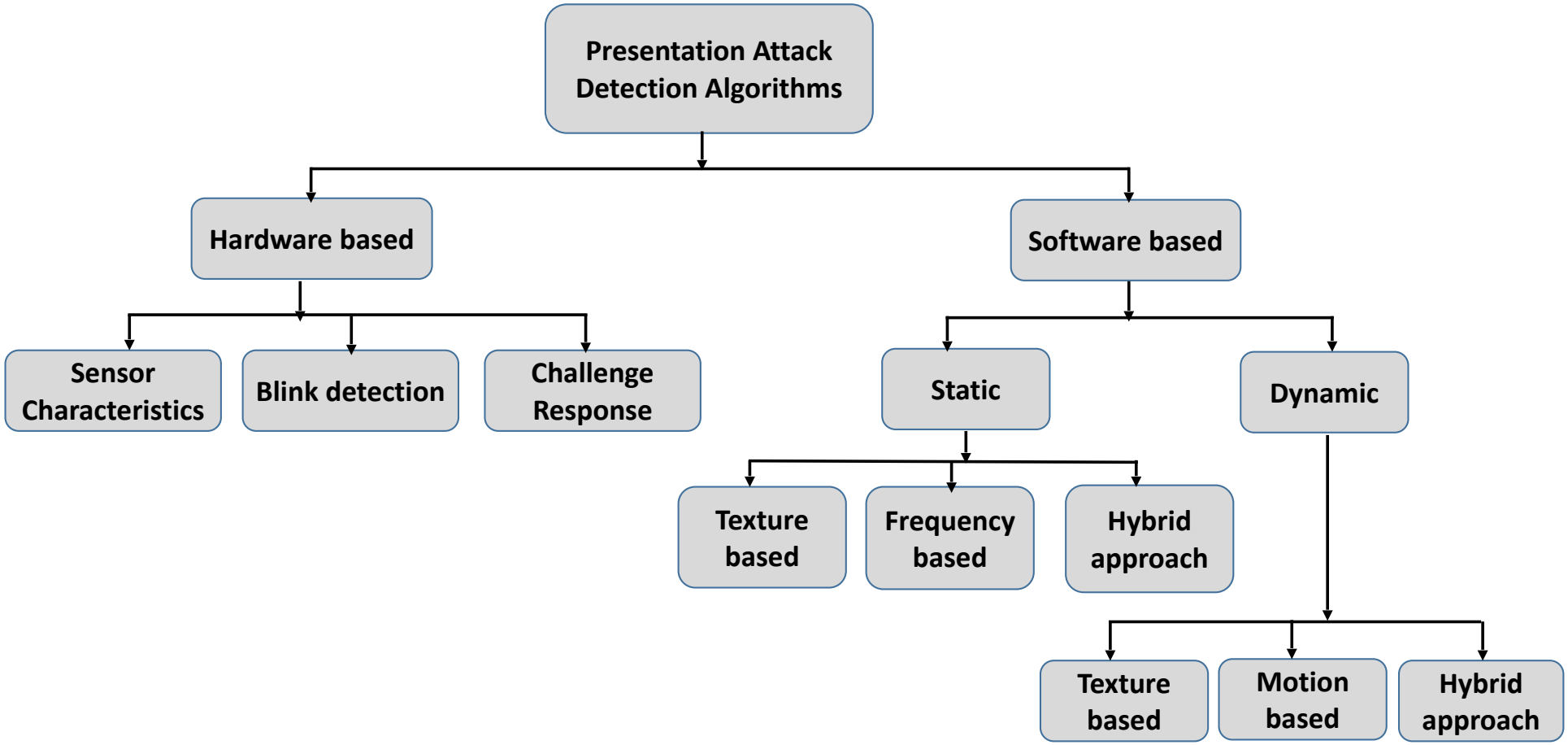
convenience measure

Ideal:
APCER - low
BPCER - low

security measure (strength of function)

Countermeasures:
Presentation Attack Detection

Taxonomy Presentation Attack Detection



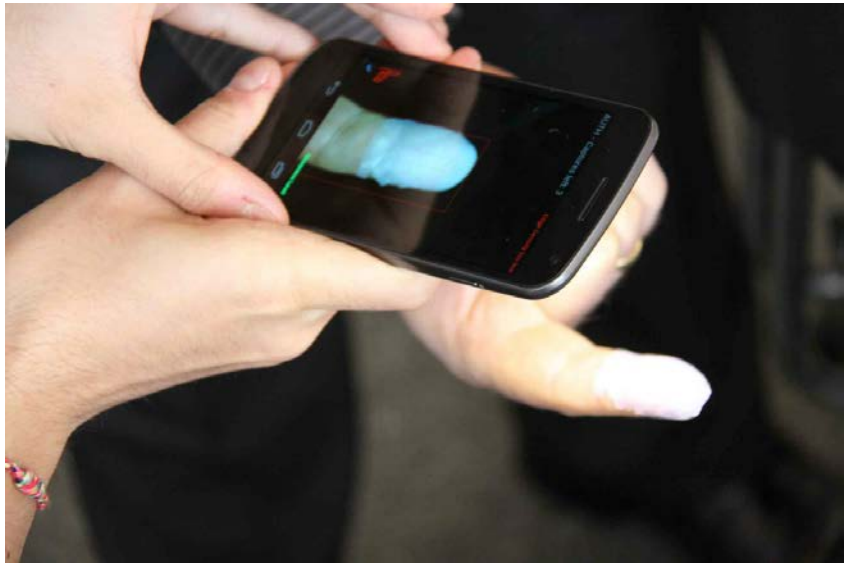
PAD for Fingerprint Capture Devices

Fingerprint Capture Device Security

German Federal Agency of IT-security
www.bsi.bund.de

- collecting and evaluating publicly known fakes
- development of new artefact types
  - BSI-artefact-collection

Source: BSI



Smartphone Access Control

Finger recognition study - 2012/2013

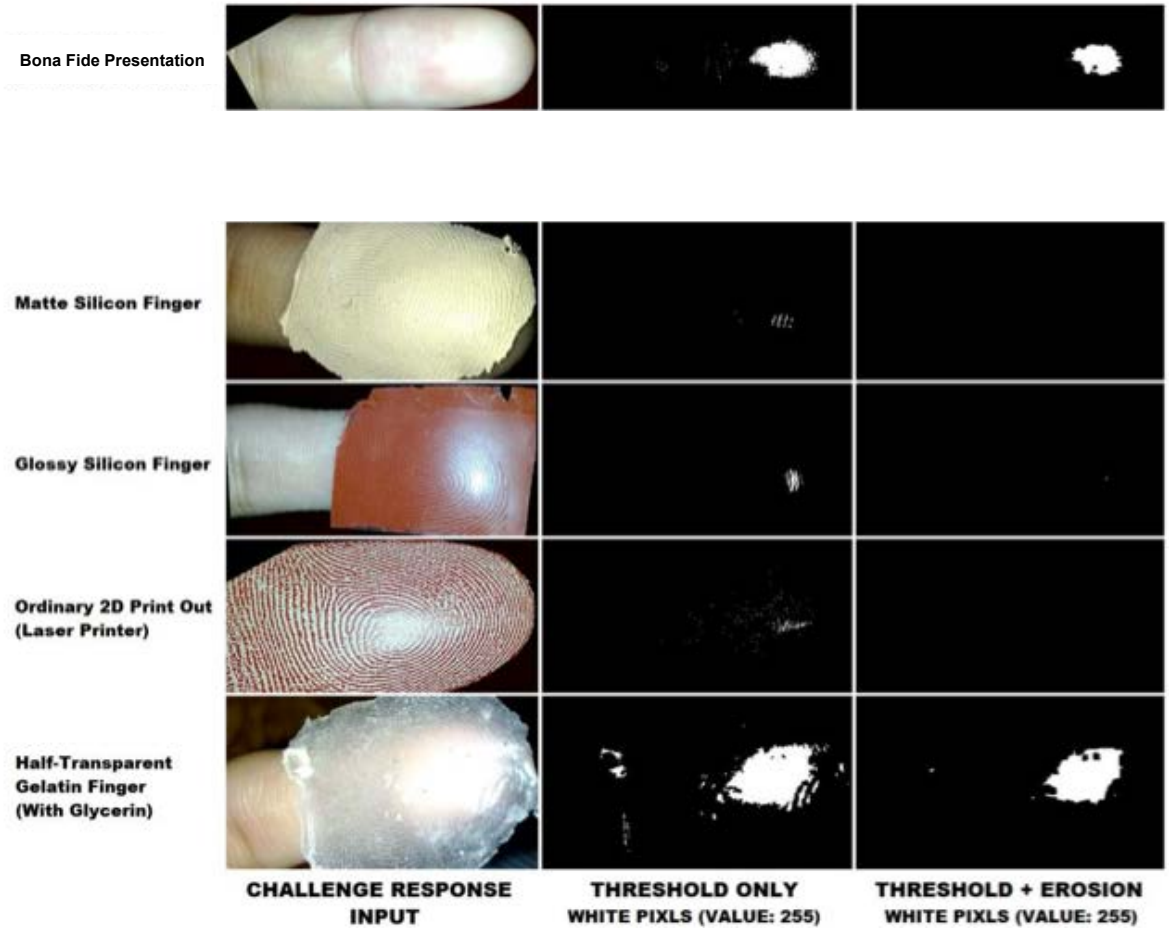
- Observation
  - significant strong light reflection near the fingertip
  - from the cameras LED
- Reflection depends on
  - Shape of the finger
  - Consistency of the finger
  - Angle of the finger to the camera
- Attack detection, as light reflection differs from artefacts to Bona Fide fingers

[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)

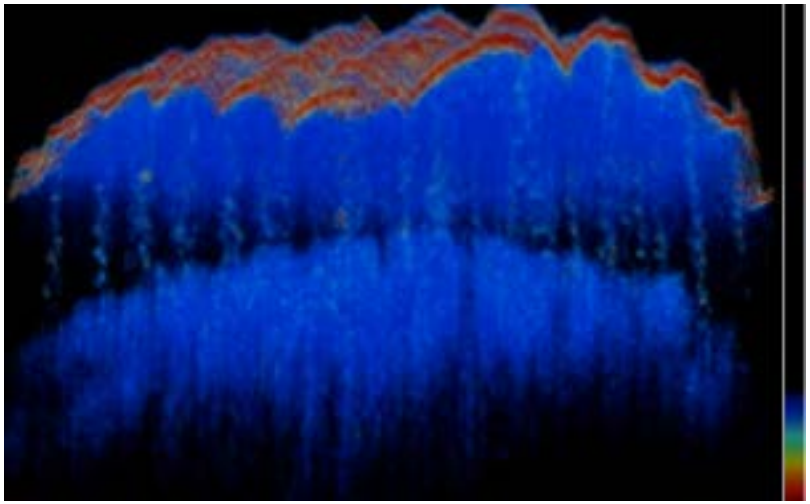


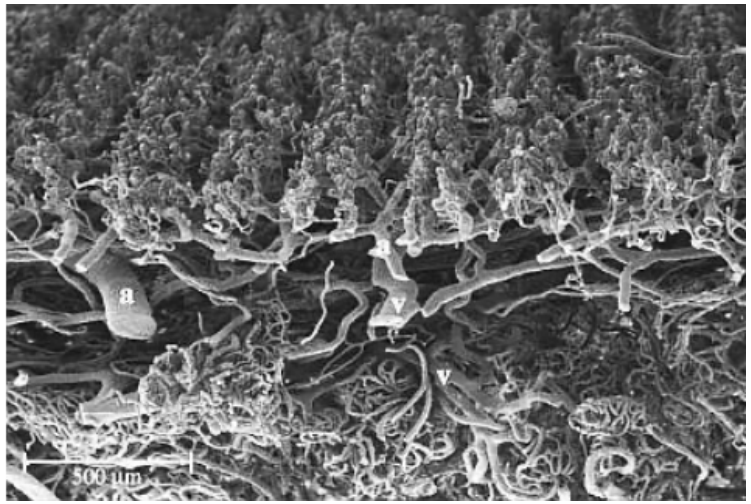
- Conclusion:
  better Presentation Attack Detection than capacitive sensors

Fingerprint Capture Device Security

Countermeasures

- Observation of the live skin properties
  - Dermis and subcutis
  - Dermal-epidermal junction zone (inner fingerprint)
  - Observation of the sweat glandes and sweat ducts
- Sensors
  - Optical Coherence Tomography (OCT)

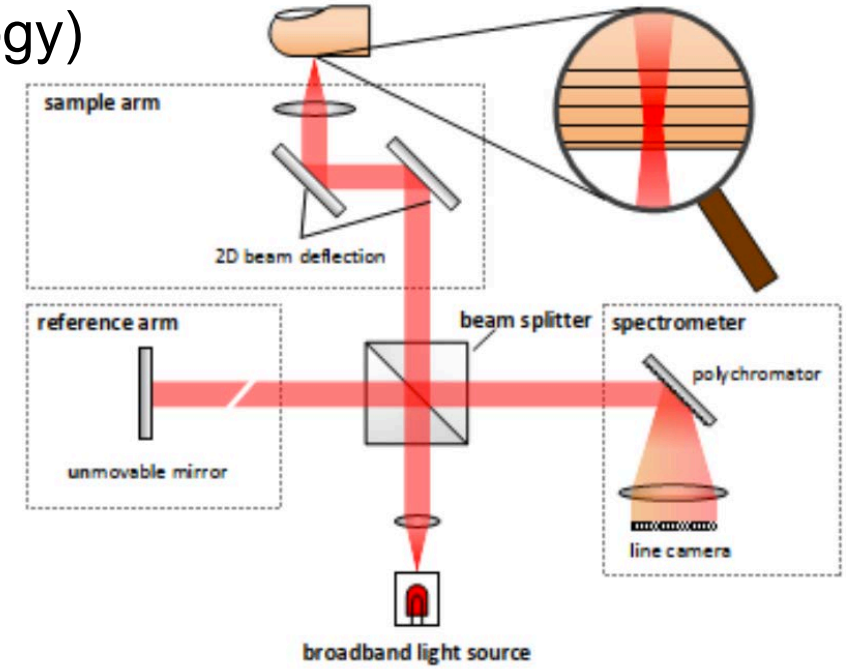




Fingerprint Capture Device Security

OCT - Principle

- Non-invasive imaging technique
  - Micrometer-resolution images from within scattering media (e.g. biological tissue)
- Considered the optical equivalent of ultrasound imaging
- Applications
  - Medical (ophthalmology & dermatology)
  - Nondestructive testing
- Two major functional principles
  - Time domain OCT
  - Fourier domain OCT (for PAD)



Fingerprint Capture Device Security

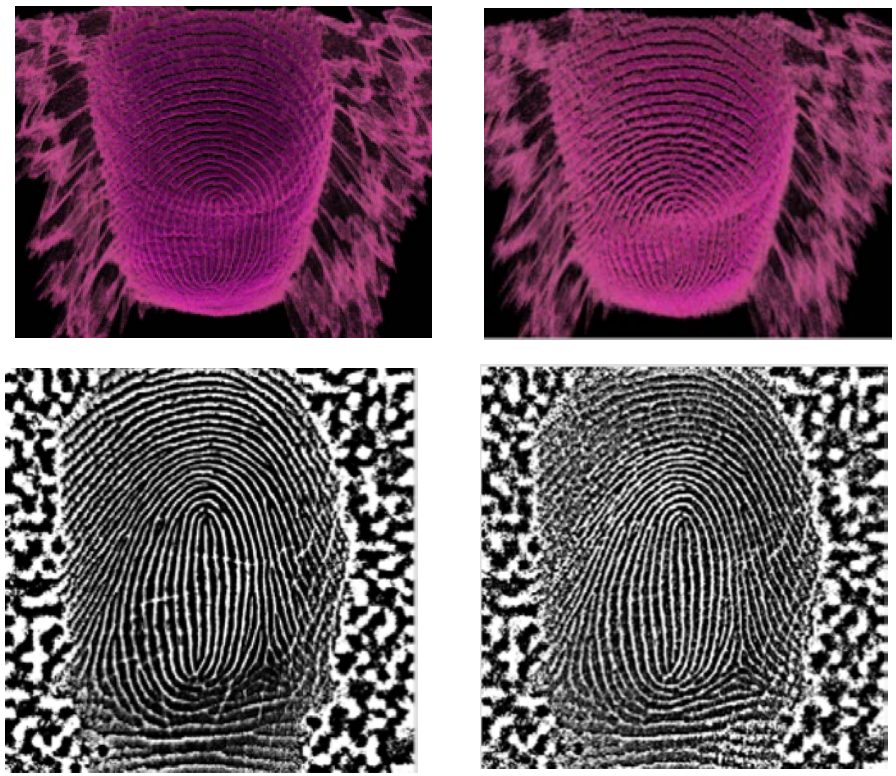
OCT

- Product of Thorlabs (Telesto-III)
  - Base-Unit Tel320
    - Light Source: 1300nm NIR SLD
    - Axial Range: 3.5mm / 2.6mm (Air / Water)
    - Lateral Resolution: 5,5µm / 4,2µm (Air / Water)
    - A-Scan-Rate: 146kSPS
  - Galvo Scan Head
    - OCTG-1300 (Standard Scanner)
  - Lense Kit LK4
    - Field of View: 16×16mm
    - Optical Resolution: 20µm (≙ 1270 PPI)

Fingerprint Capture Device Security

Comparing outer and inner fingerprint patterns

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

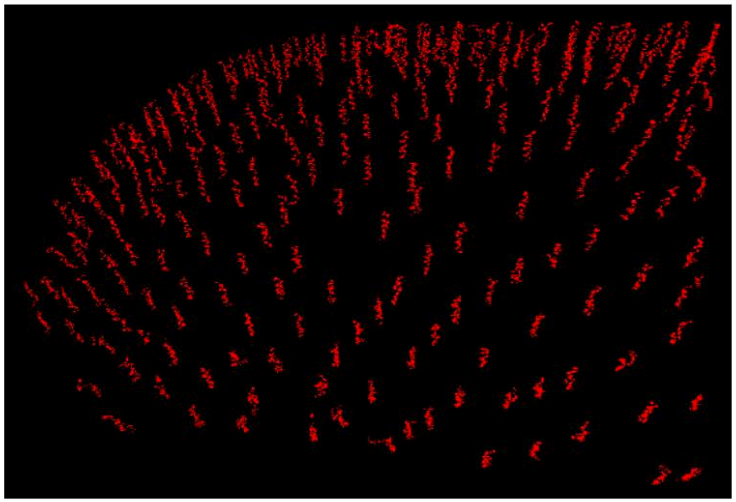
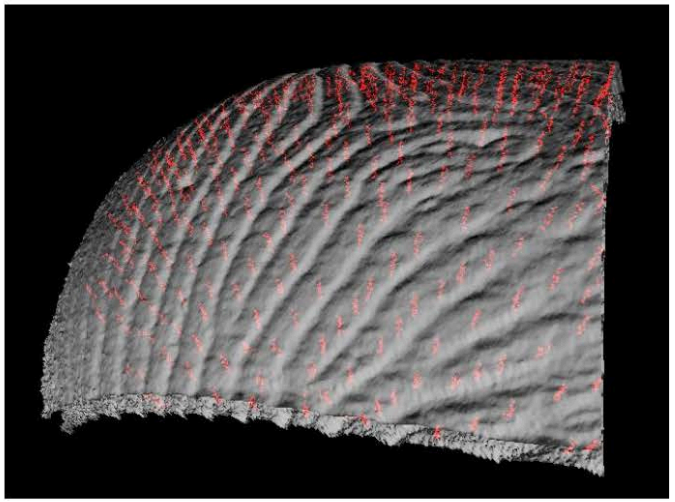
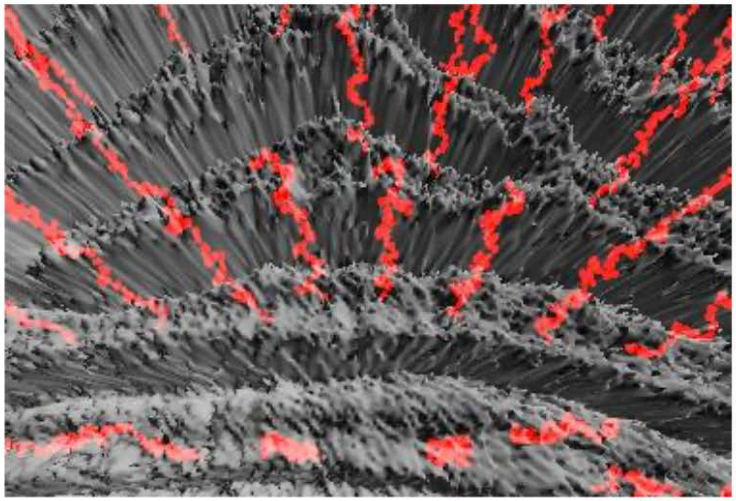
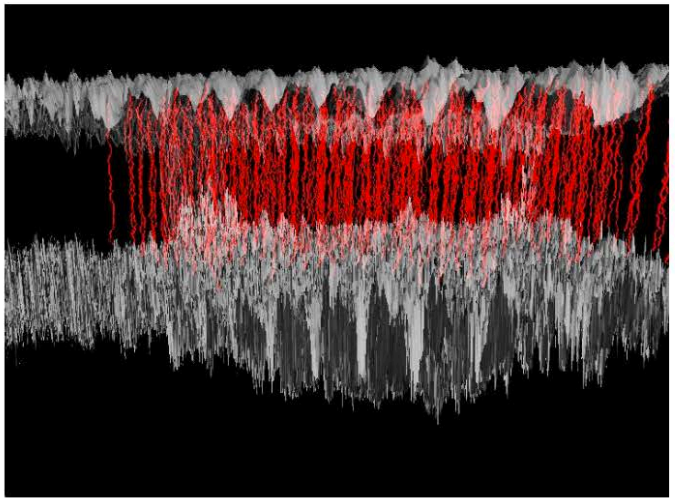


Surface Fingerprint Internal Fingerprint

Fingerprint Capture Device Security

OCT

- Visualizing the sweat ducts

Presentation Attack Detection

PAD Application area - Identity Concealer

Altered Fingerprint Detection - Testing

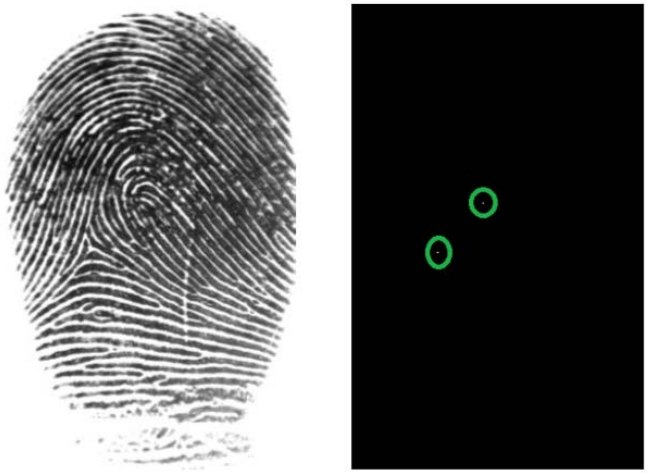
Example for fingerprint alterations

- Z-shaped alteration (Finger of Jose Izquierdo, 1995)

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

Altered Fingerprint Detection - Algorithms

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



BonaFide fingerprint

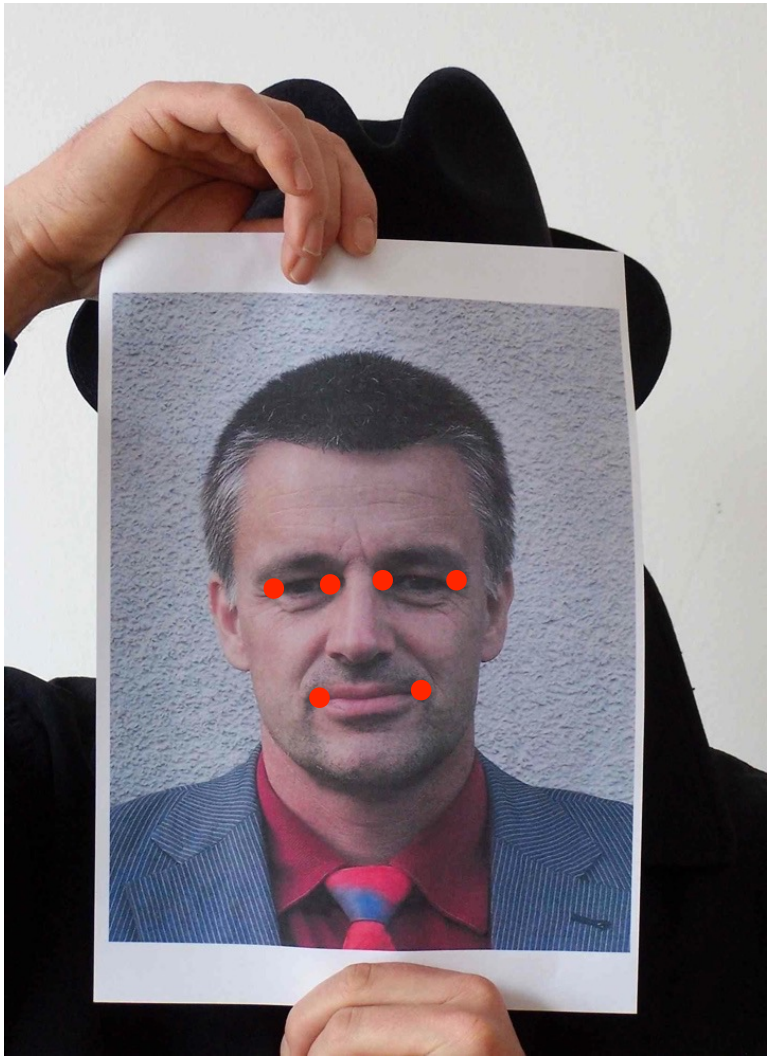
altered fingerprint

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 Presentation Attacks

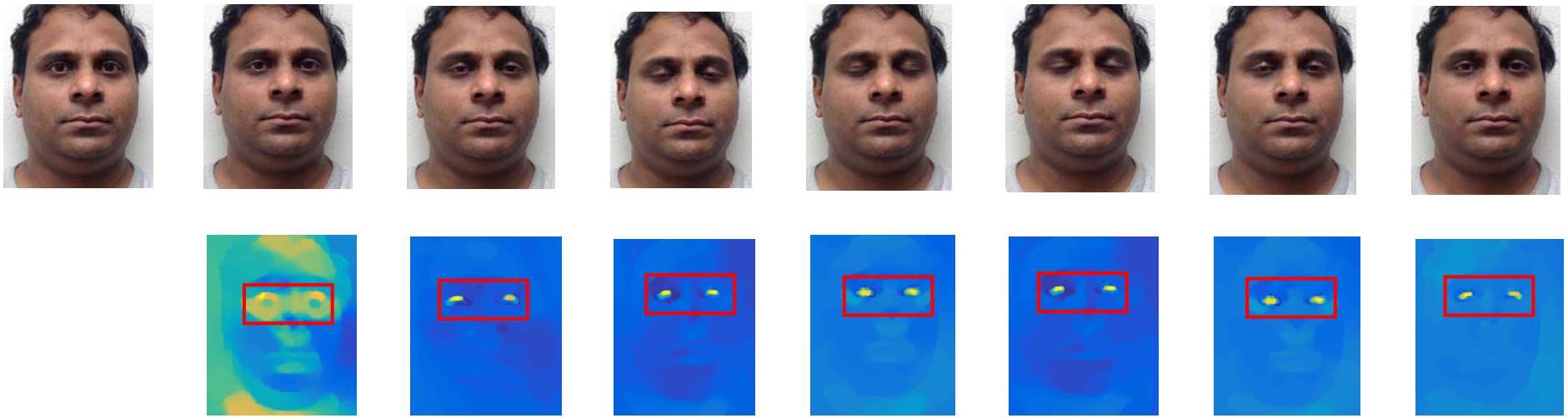
Face Presentation Attacks



Face Presentation Attack Detection

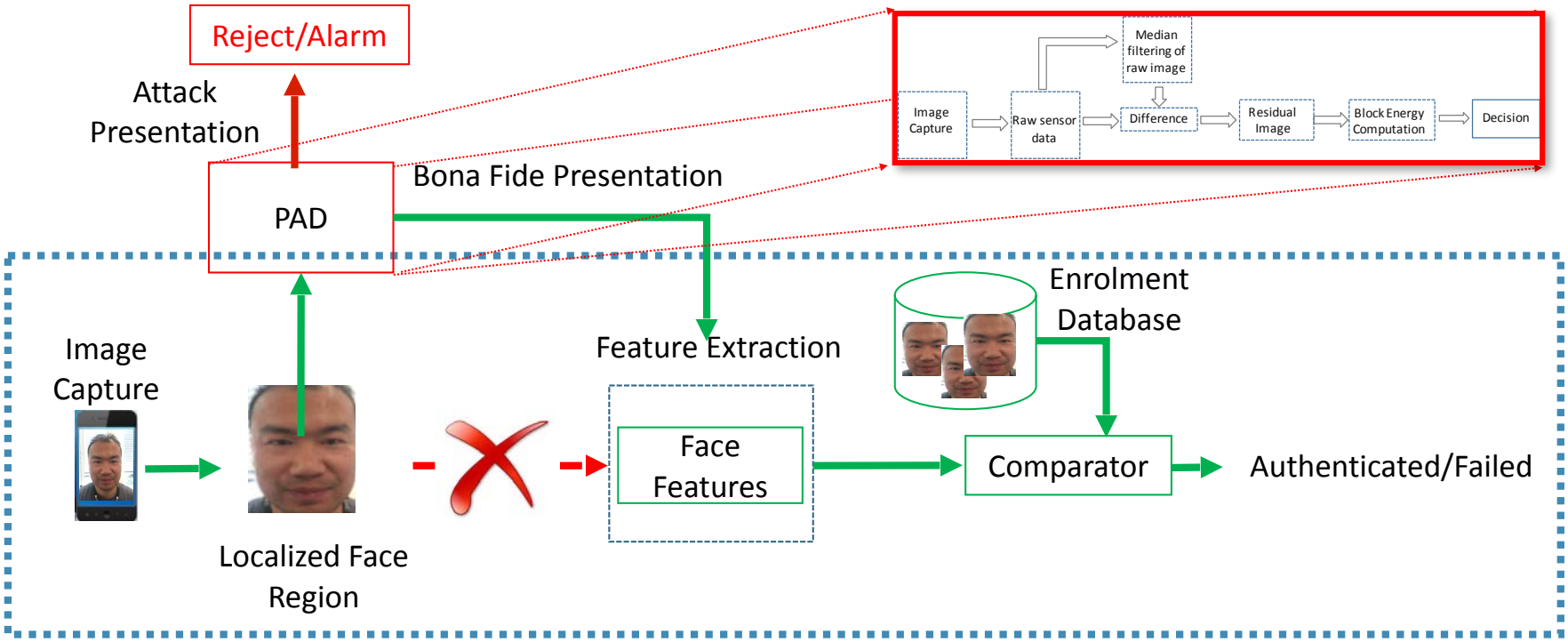
Hardware based

- 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

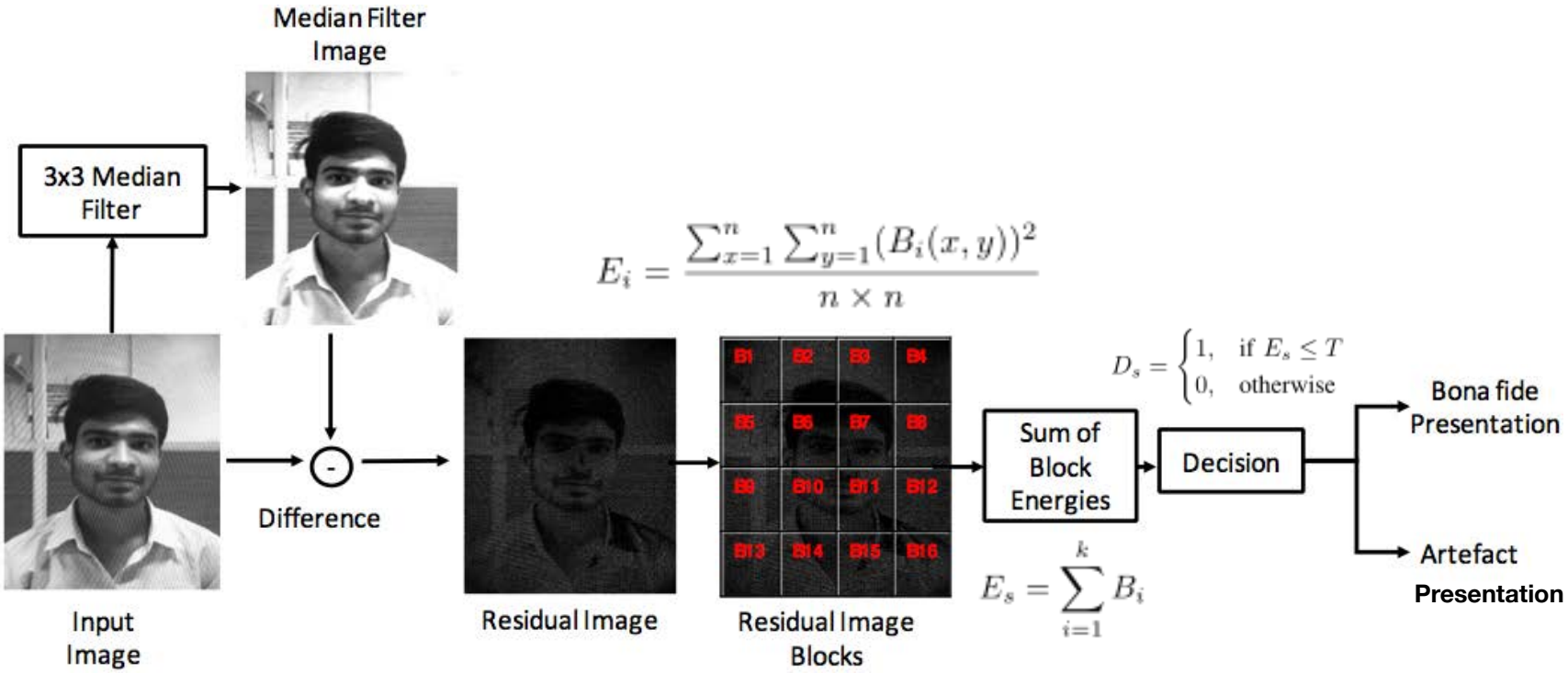
- Augmenting the processing pipeline



[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)

Smartphone - Face PAD

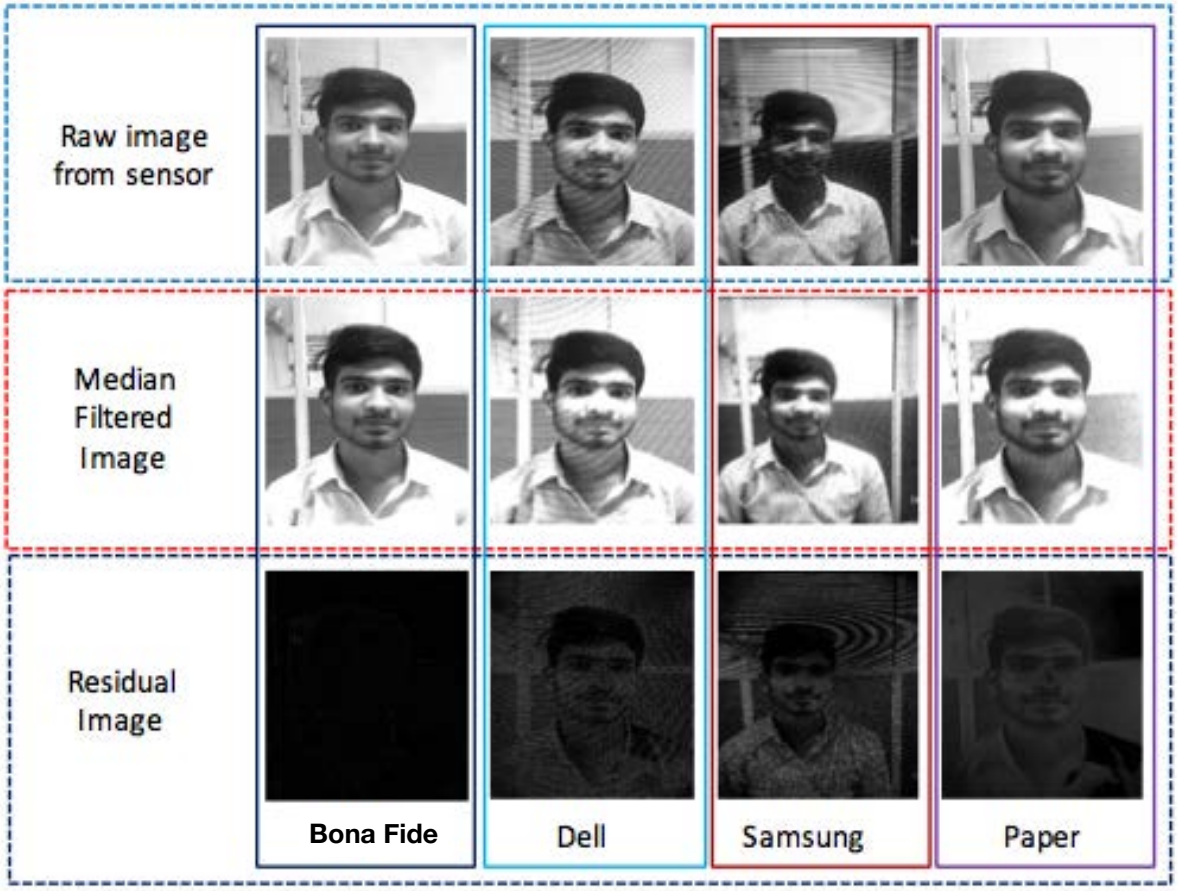
- Channel based processing



[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)

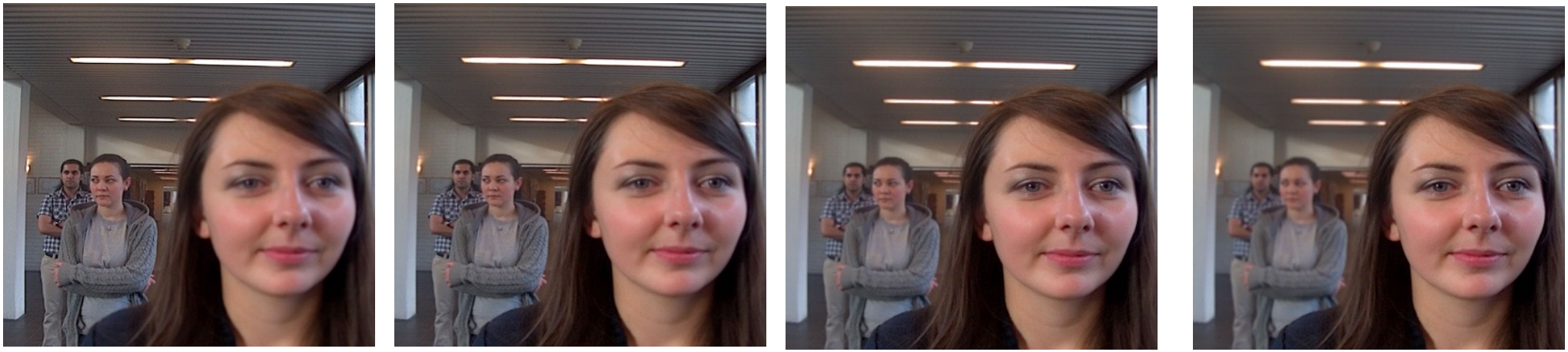
Smartphone - Face PAD

- Residual image computation



PAD – based on Depth Information

Example of light-field imaging (LYTRO)

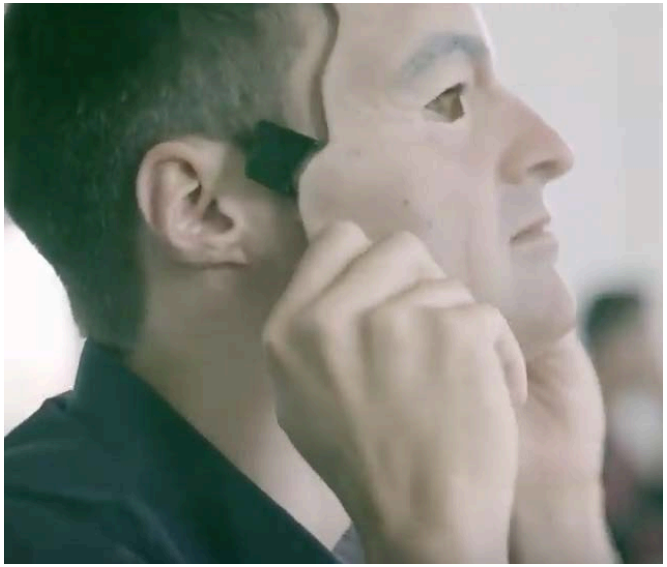


[Raghu2015] R. Raghavendra, K.B. Raja, and C. Busch: "Presentation Attack Detection for Face Recognition using Light Field Camera", in IEEE Transactions on Image Processing, vol. 24, no. 3, pp. 1060–1075, (2015)

Impostor Presentation Attack

3D silicone mask

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

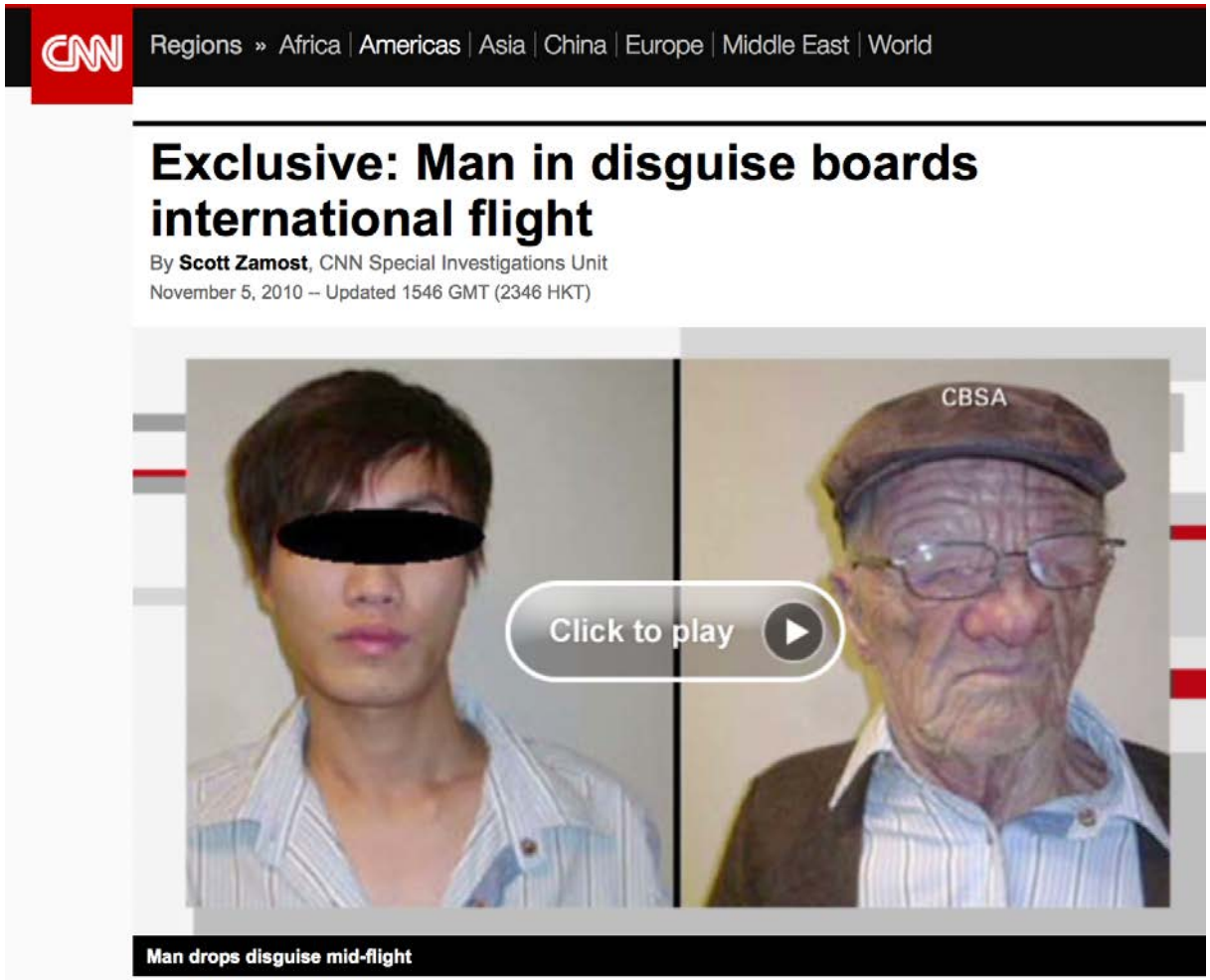


Impostor Presentation Attack

Impostor Presentation Attack

3D silicone mask

http://edition.cnn.com/2010/WORLD/americas/11/04/canada.disguised.passenger



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

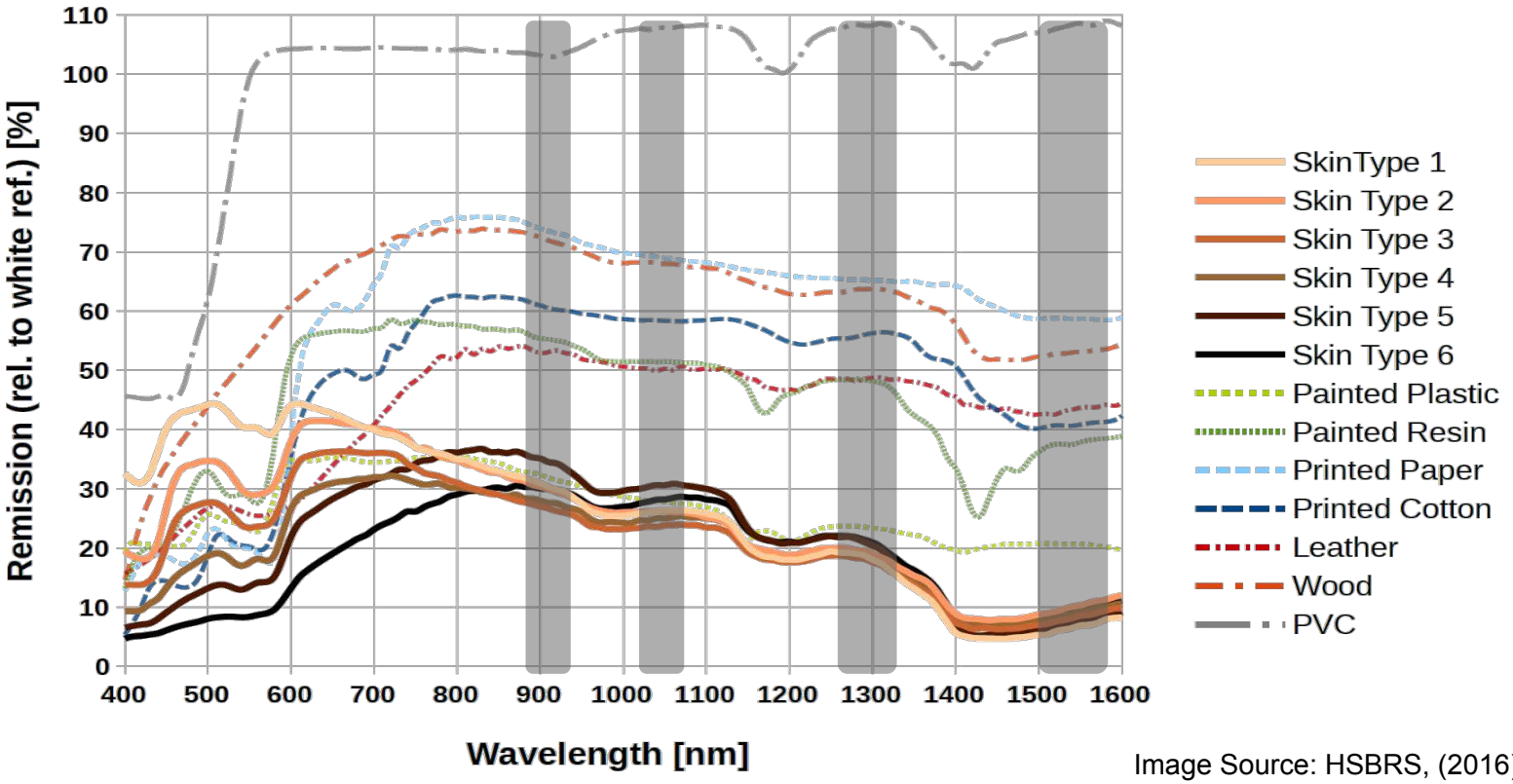


Image Source: HSBRS, (2016)

[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 spectral bands
  - Transform spectral remission to normalized differences
  - False color images based on three channel differences

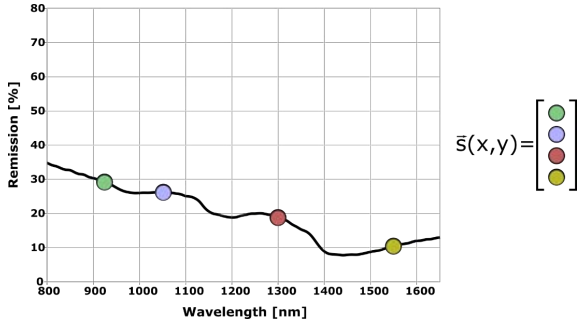


Image Source: HSBRS, (2016)

Concealer Presentation Attack

Face disguise for organized crime (June 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.

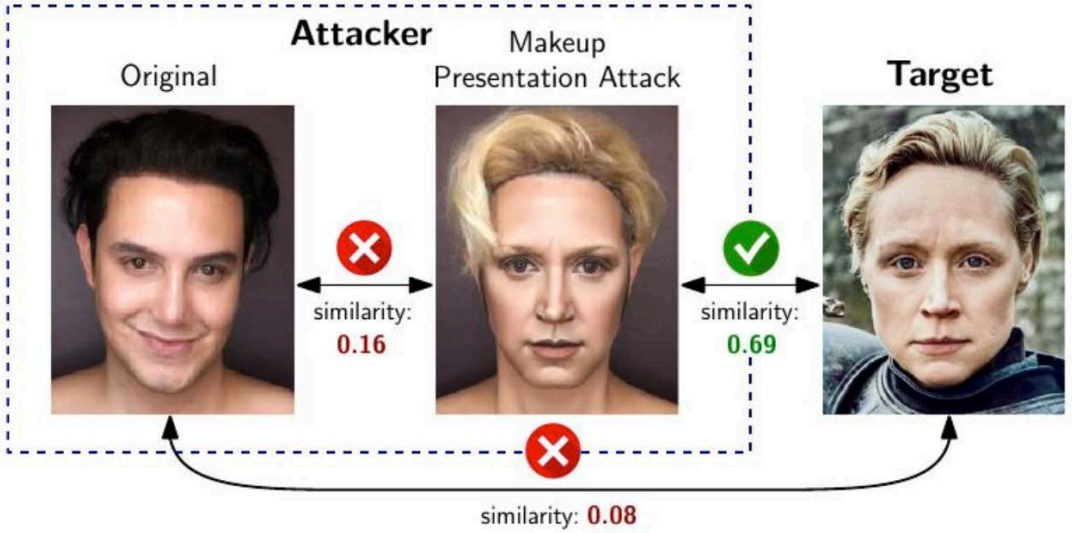
Not this one. Henley Stephenson, 41, eluded police for more than ten years thanks to an extraordinarily lifelike latex mask, which turned him into a white skinhead.

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.

Makeup Presentation Attacks

Severe alterations

- Makeup for impersonation
- Liveness detection is not sufficient
- Detection difficult since bona fide users may also apply



[RDB2020] C. Rathgeb, P. Drozdowski, C. Busch: "Detection of Makeup Presentation Attacks based on Deep Face Representations“, in Proceedings of 25th International Conference on Pattern Recognition (ICPR), (2020)

The Morphing Problem

What is Morphing?

In our real world morphing can become a threat

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

What is Morphing?

In our real world morphing can become a threat

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

What is Morphing?

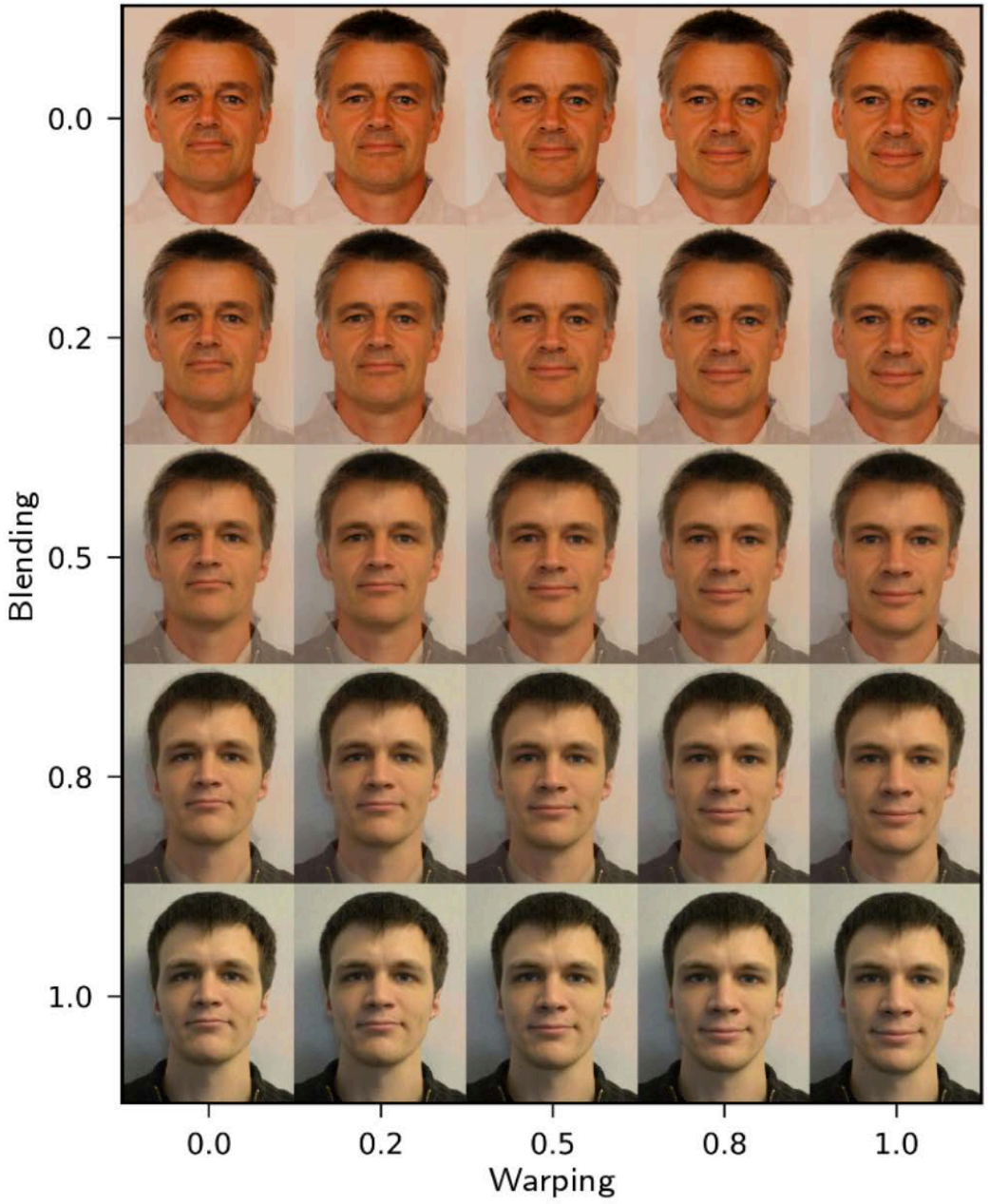
Warping and blending

- controlled by the alpha factor
- Landmark positions

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

- Colour

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



Problem Description

Problem: Morphing Attacks

Morphing attack scenario

- Passport application of the accomplice A

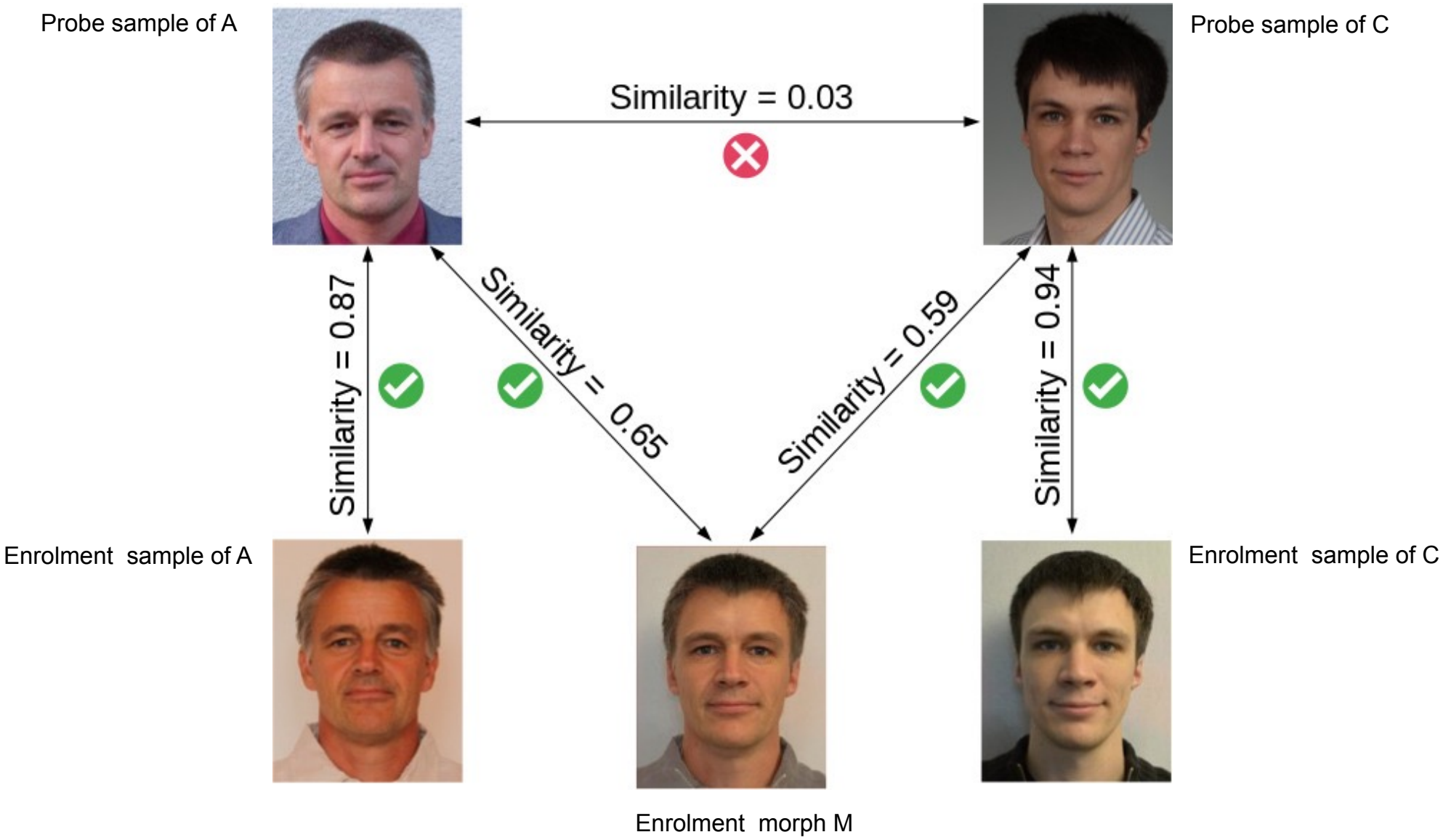
Problem: Morphing Attacks

Morphing attack scenario

- Border control

Problem: Morphing Attacks

Verification against morphed facial images



Problem: Morphing Attacks

Is it a really problem ?

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.

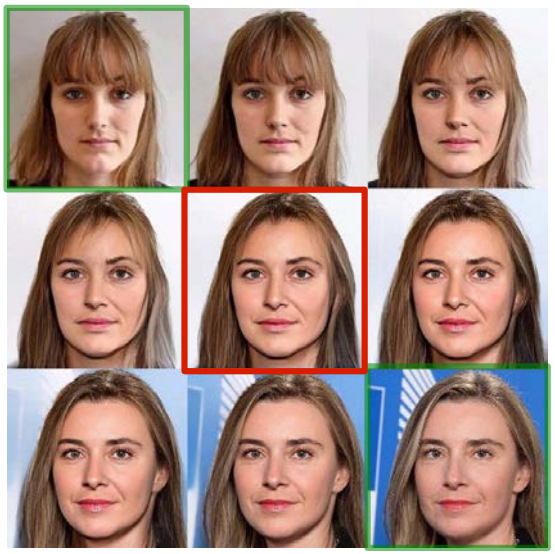
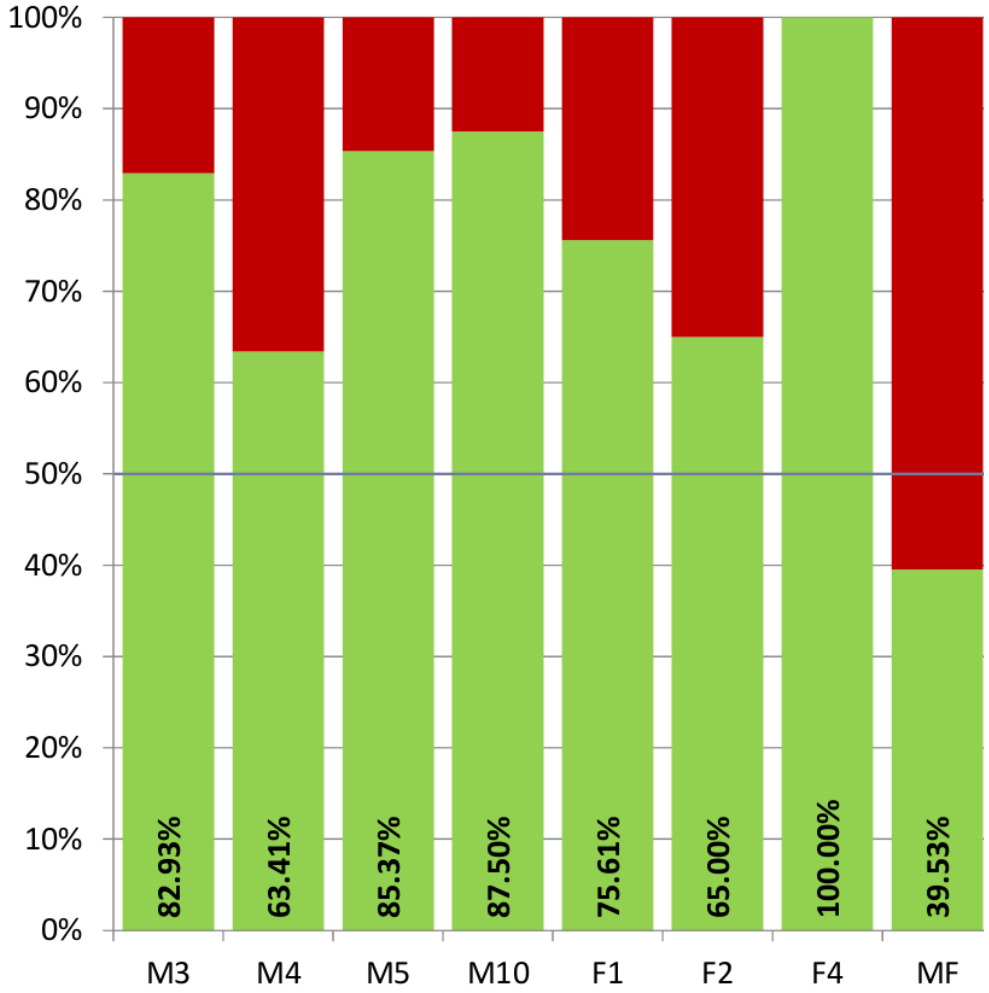


Image source: https://www.spiegel.de/netzwelt/netzpolitik/biometrie-im-reisepass-peng-kollektiv-schmuggelt-fotomontage-in-ausweis-a-1229418.html

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)

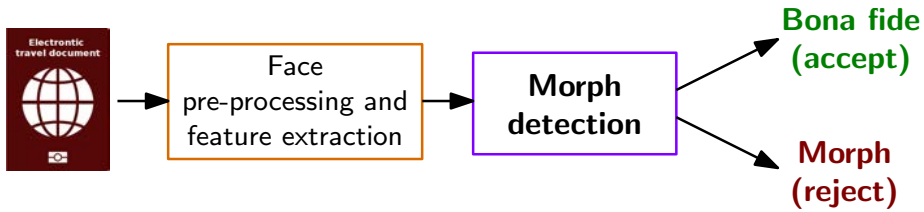
Morphing Attack Detection (MAD)

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)

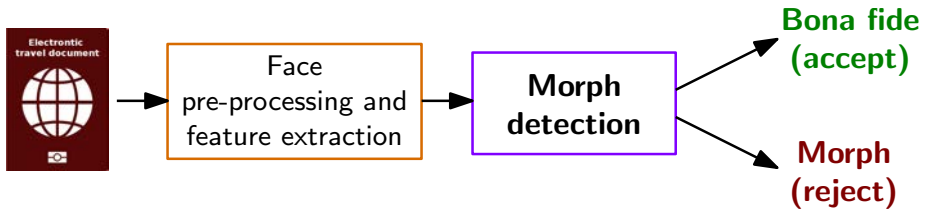


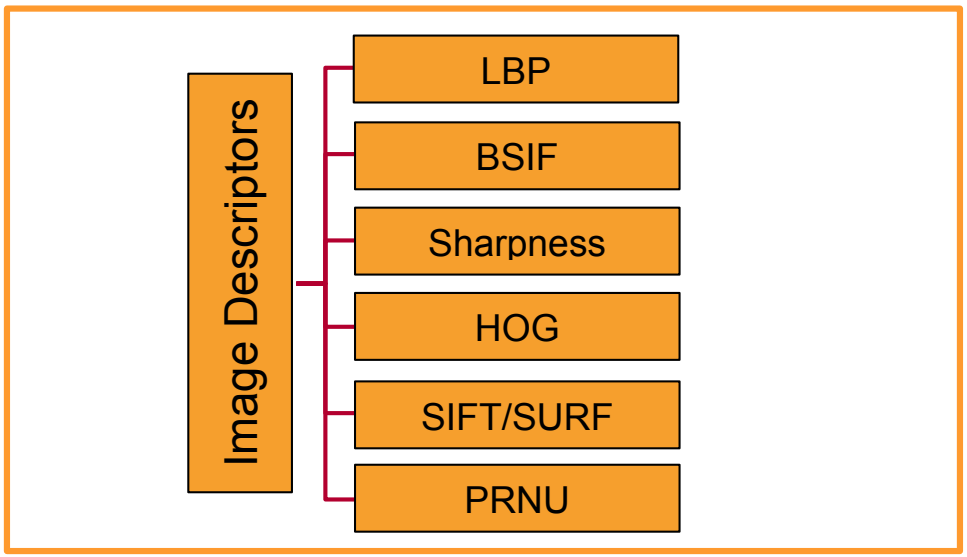
[SRB2018a] U. Scherhag, C. Rathgeb, C. Busch: "Towards Detection of Morphed Face Images in electronic Travel Documents“, in Proceedings of the 13th IAPR International Workshop on Document Analysis Systems (DAS), April 24-27, (2018)

Face Pre-processing and Feature Extraction

Morphing Attack Detection (S-MAD) with texture analysis

- Image descriptors as hand-crafted features





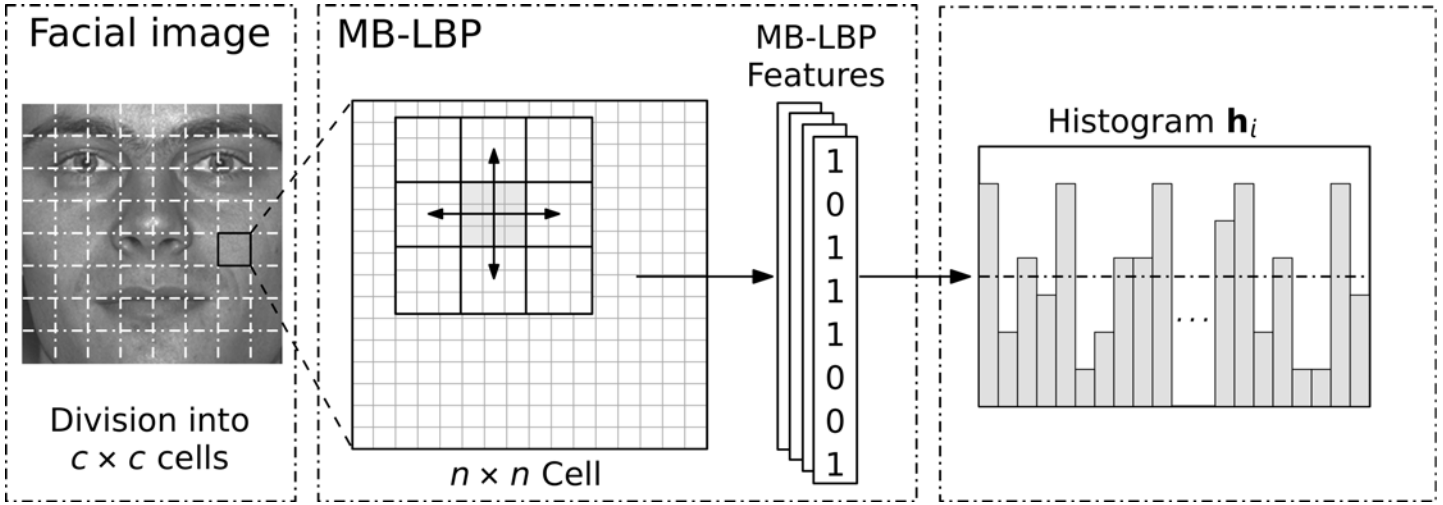
Morph Detection Classifier

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

Face Pre-processing and Feature Extraction

S-MAD with image descriptor

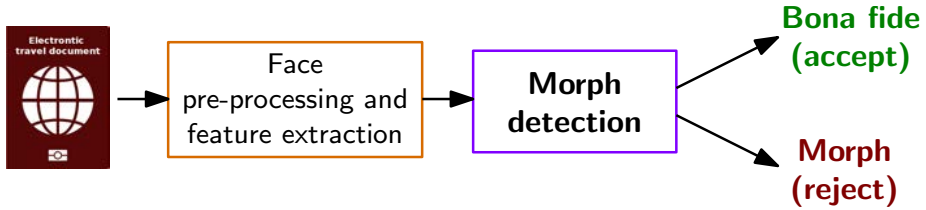
- Local Binary Pattern (LBP)



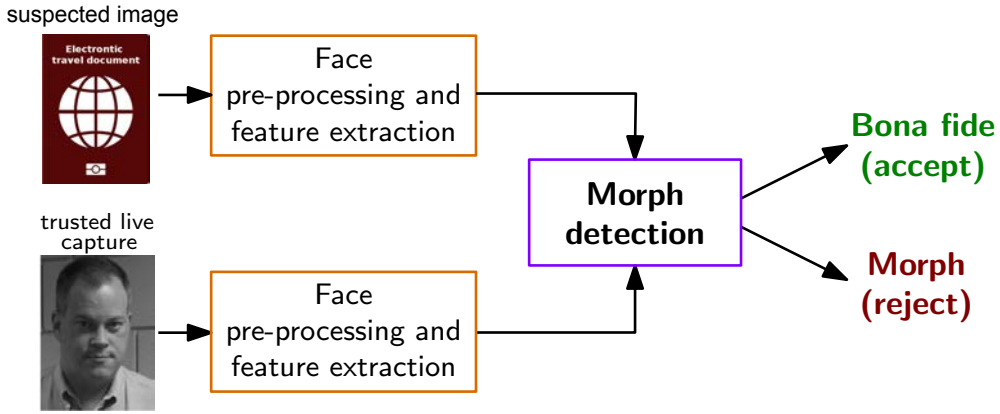
Morphing Attack Detection Scenarios

Real world scenarios

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



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

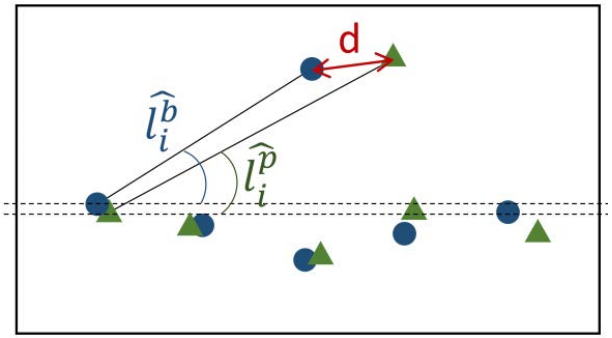


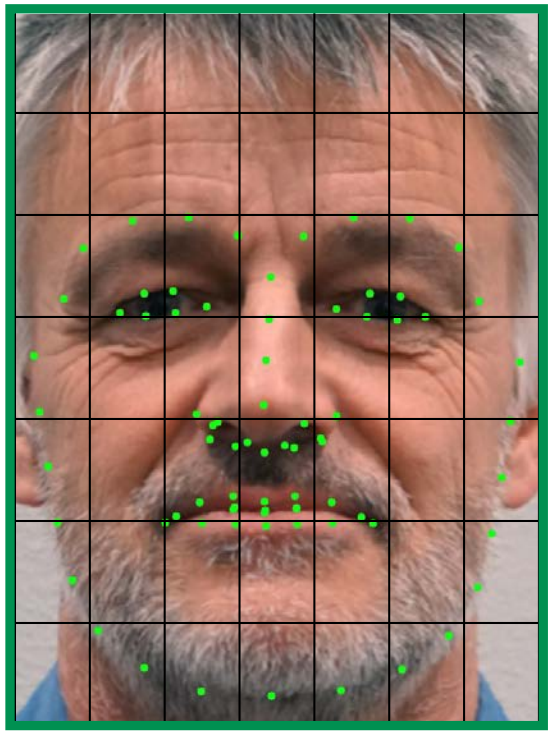
[SRB2018a] U. Scherhag, C. Rathgeb, C. Busch: "Towards Detection of Morphed Face Images in electronic Travel Documents“, in Proceedings of the 13th IAPR International Workshop on Document Analysis Systems (DAS), April 24-27, (2018)

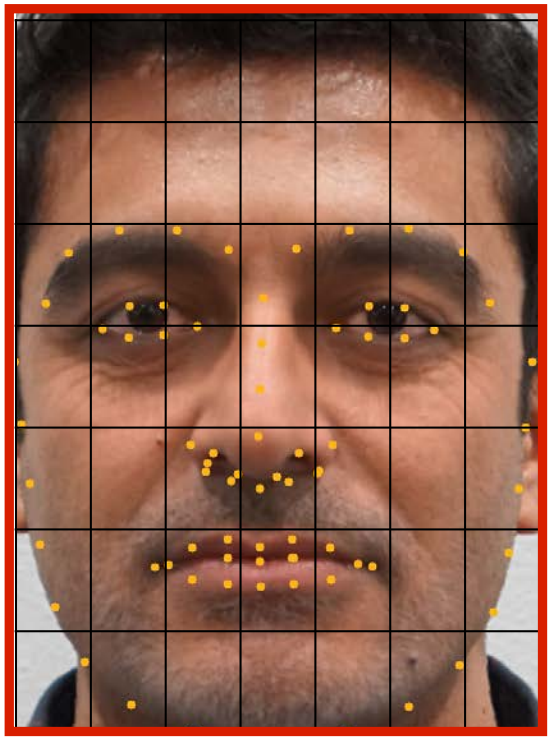
Differential Morphing Attack Detection

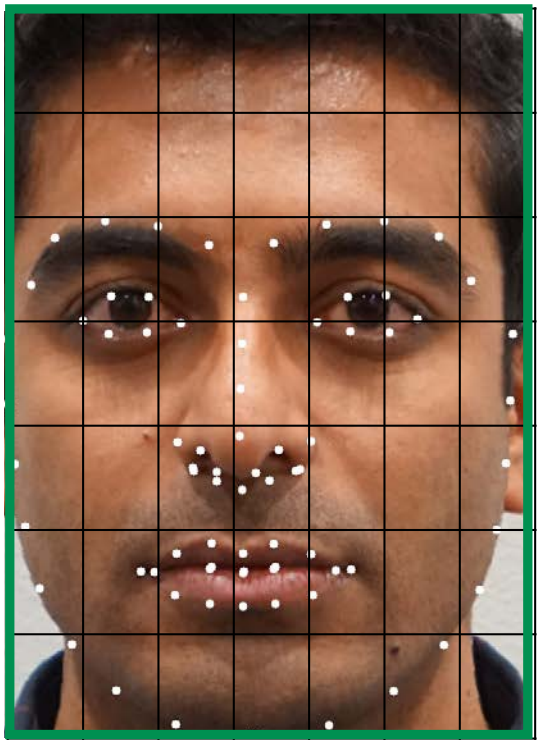
D-MAD with landmark analysis

- Angle based features
- Distance based features







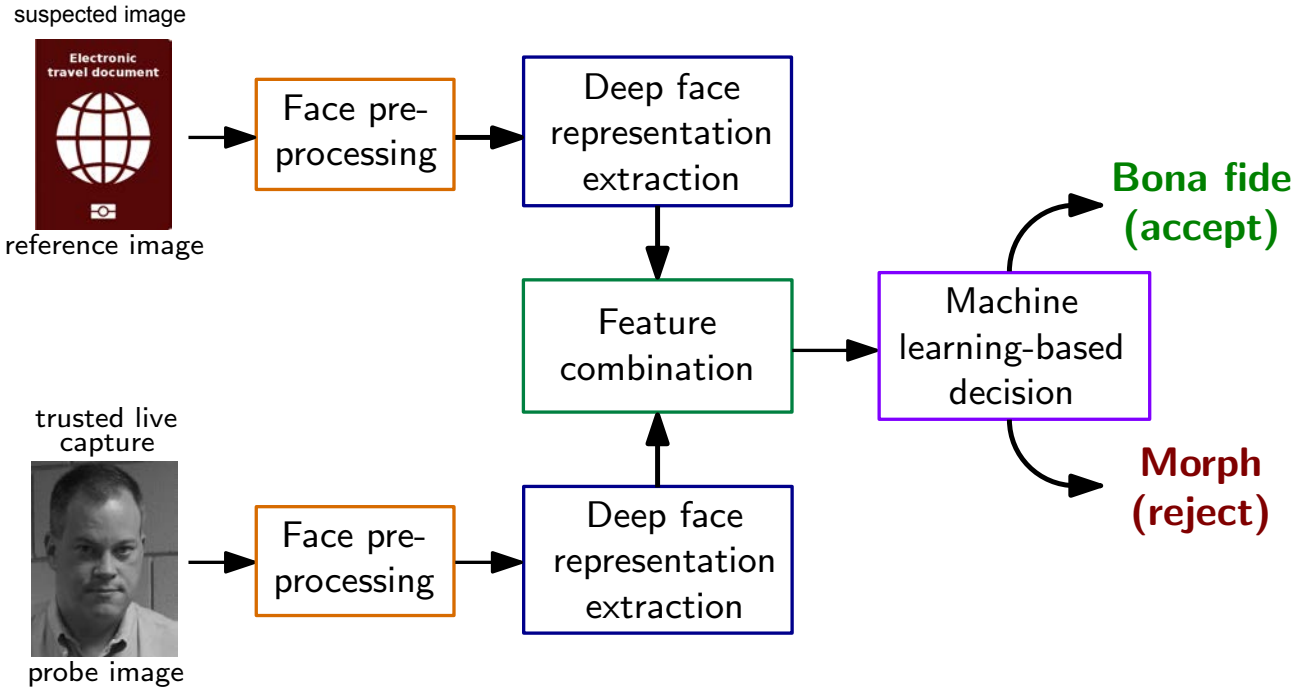


[SDGB2018] U. Scherhag, D. Budhrani, M. Gomez-Barrero, C. Busch: "Detecting Morphed Face Images Using Facial Landmarks“, in Proceedings of International Conference on Image and Signal Processing (ICISP), (2018)

Differential Morphing Attack Detection

D-MAD with deep learning

- Deep Face representations of Deep CNNs



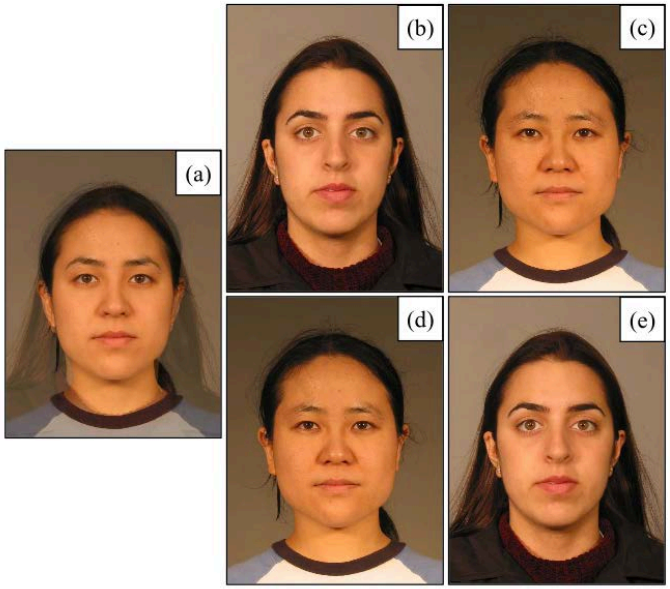
- Deep representations extracted by the neural network (on the lowest layer)
- Feature space with small dimension: 512 (for ArcFace)
- SVM with radial basis function

[SRMB2020] U. Scherhag, C. Rathgeb, J. Merkle, C. Busch: "Deep Face Representations for Differential Morphing Attack Detection", in IEEE Transactions on Information Forensics and Security (TIFS), (2020)

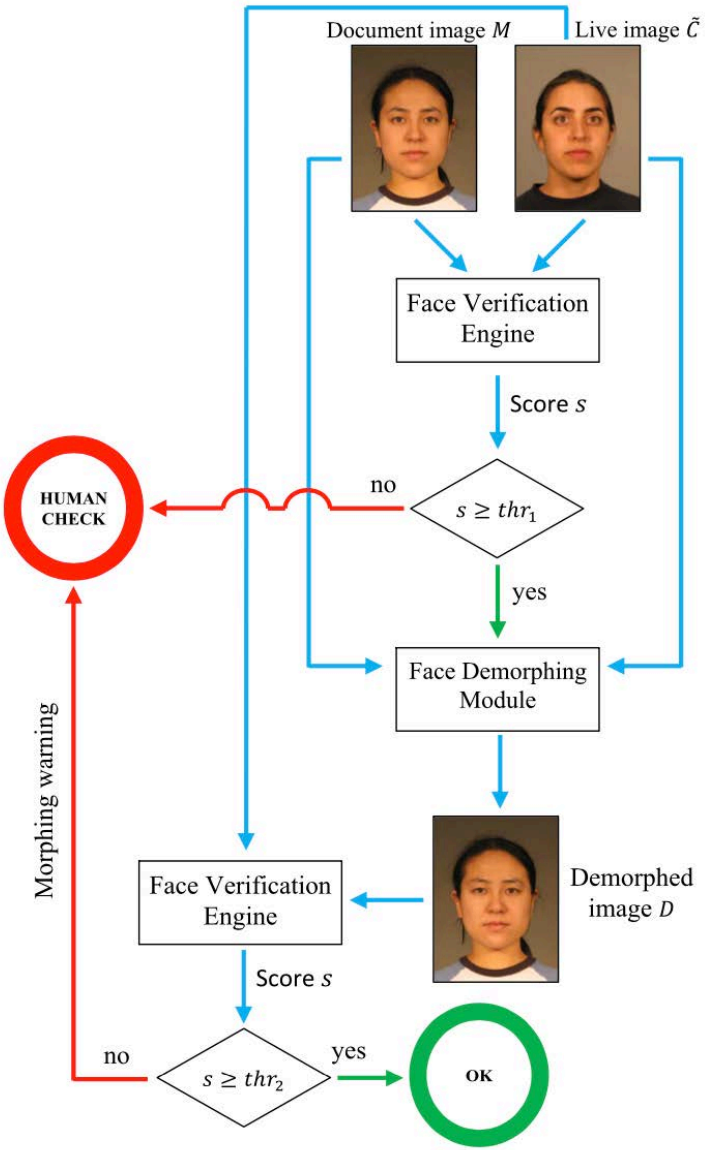
Differential Morphing Attack Detection

D-MAD with Demorphing

- Invert the morphing process
- Then confirm the similarity score



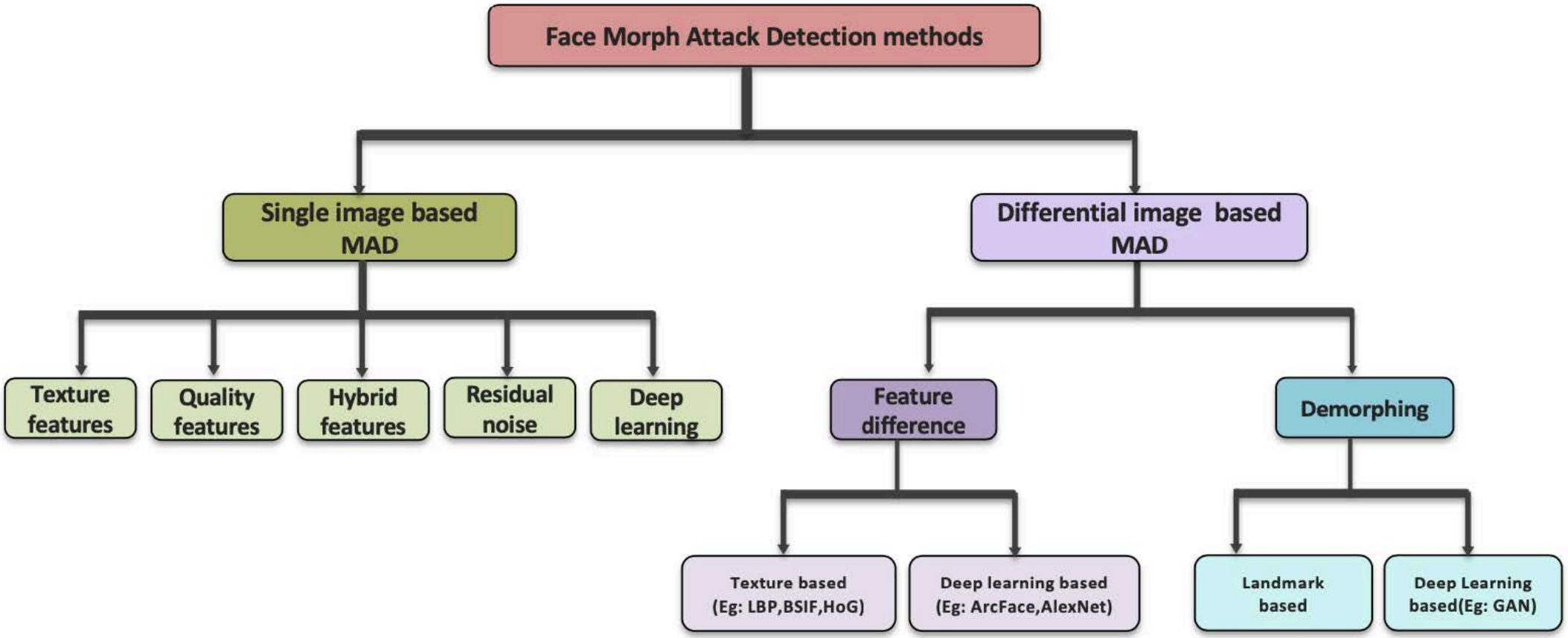
a) suspected image
b) and c): trusted live capture image
d) and e): recovery image



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

State of the Art - MAD Algorithms

Taxonomy of Morphing Attack Detection



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

MAD Evaluation

MAD Evaluation Methodology

Face Morphing Attack evaluations are complex

- Evaluations must consider a dedicated methodology [SNR2017]
- Evaluations must consider many parameters

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

[SNR2017] U. Scherhag, A. Nautsch, C. Rathgeb, M. Gomez-Barrero, R. Veldhuis, L. Spreeuwers, M. Schils, D. Maltoni, P. Grother, S. Marcel, R. Breithaupt, R. Raghavendra, C. Busch: "Biometric Systems under Morphing Attacks: Assessment of Morphing Techniques and Vulnerability Reporting", in Proceedings of the IEEE 16th International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, September 20-22, (2017)

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



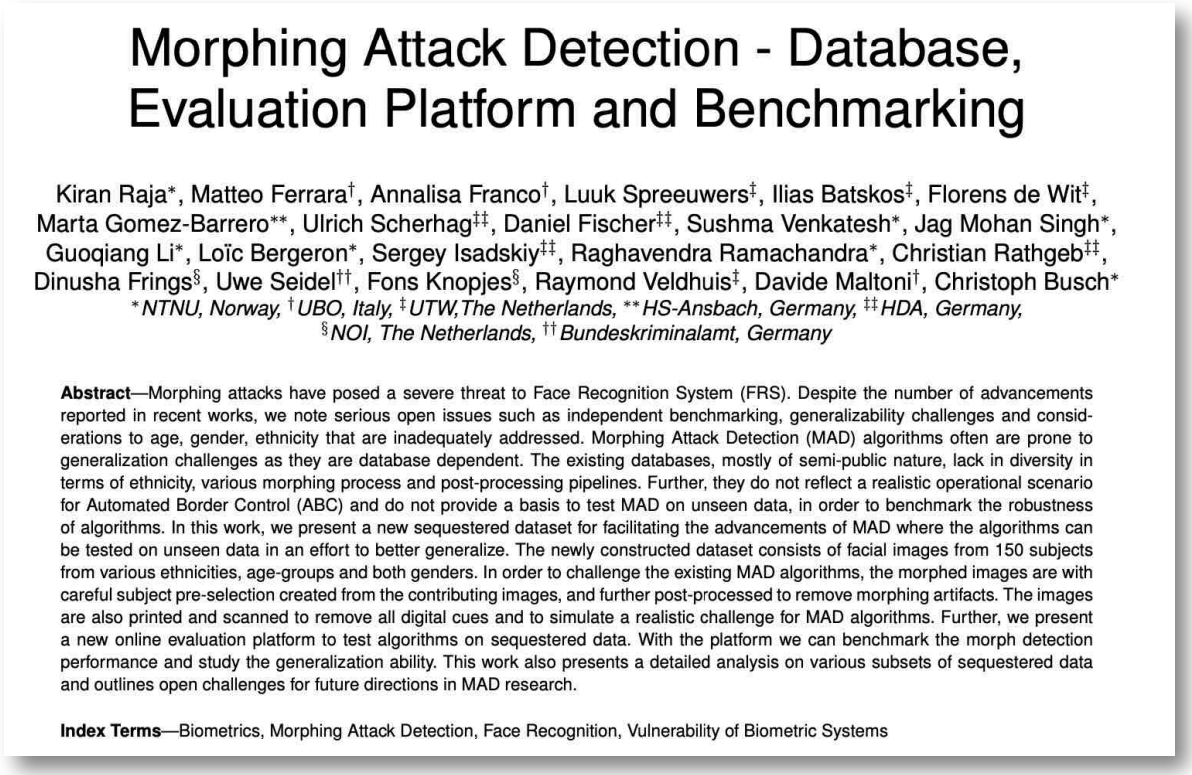

Specific objectives:

- 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
- Test the MAD algorithms on the Bologna server
  https://biolab.csr.unibo.it/FVConGoing

Research on Morphing Attack Detection

MAD Evaluation in SOTAMD

- SOTAMD dataset and testing platform
  https://ieeexplore.ieee.org/document/9246583



Morphing Attack Detection - Database, Evaluation Platform and Benchmarking

Kiran Raja*, Matteo Ferrara†, Annalisa Franco†, Luuk Spreeuwers‡, Ilias Batskos‡, Florens de Wit‡, Marta Gomez-Barrero**, Ulrich Scherhag‡‡, Daniel Fischer‡‡, Sushma Venkatesh*, Jag Mohan Singh*, Guoqiang Li*, Loïc Bergeron*, Sergey Isadskiy‡‡, Raghavendra Ramachandra*, Christian Rathgeb‡‡, Dinusha Frings§, Uwe Seidel††, Fons Knopjes§, Raymond Veldhuis‡, Davide Maltoni†, Christoph Busch*
*NTNU, Norway, †UBO, Italy, ‡UTW,The Netherlands, **HS-Ansbach, Germany, ‡‡HDA, Germany, §NOI, The Netherlands, ††Bundeskriminalamt, Germany

Abstract—Morphing attacks have posed a severe threat to Face Recognition System (FRS). Despite the number of advancements reported in recent works, we note serious open issues such as independent benchmarking, generalizability challenges and considerations to age, gender, ethnicity that are inadequately addressed. Morphing Attack Detection (MAD) algorithms often are prone to generalization challenges as they are database dependent. The existing databases, mostly of semi-public nature, lack in diversity in terms of ethnicity, various morphing process and post-processing pipelines. Further, they do not reflect a realistic operational scenario for Automated Border Control (ABC) and do not provide a basis to test MAD on unseen data, in order to benchmark the robustness of algorithms. In this work, we present a new sequestered dataset for facilitating the advancements of MAD where the algorithms can be tested on unseen data in an effort to better generalize. The newly constructed dataset consists of facial images from 150 subjects from various ethnicities, age-groups and both genders. In order to challenge the existing MAD algorithms, the morphed images are with careful subject pre-selection created from the contributing images, and further post-processed to remove morphing artifacts. The images are also printed and scanned to remove all digital cues and to simulate a realistic challenge for MAD algorithms. Further, we present a new online evaluation platform to test algorithms on sequestered data. With the platform we can benchmark the morph detection performance and study the generalization ability. This work also presents a detailed analysis on various subsets of sequestered data and outlines open challenges for future directions in MAD research.

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

[Raja2020] K. Raja, M. Ferrara, A. Franco, L. Spreeuwers, I. Batskos, F. Wit, M. Gomez-Barrero, U. Scherhag, D. Fischer, S. Venkatesh, J. Singh, G. Li, L. Bergeron, S. Isadskiy, R. Raghavendra, C. Rathgeb, D. Frings, U. Seidel, F. Knopjes, R. Veldhuis, D. Maltoni, C. Busch: "Morphing Attack Detection - Database, Evaluation Platform and Benchmarking", in IEEE Transactions on Information Forensics and Security (TIFS), (2020)

NIST-FRVT-MORPH

NIST IR 8292 report presented September, 2021

FRVT-MORPH

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

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

NISTIR 8292 DRAFT SUPPLEMENT

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

Mei Ngan
Patrick Grother
Kayee Hanaoka
Jason Kuo
Information Access Division
Information Technology Laboratory

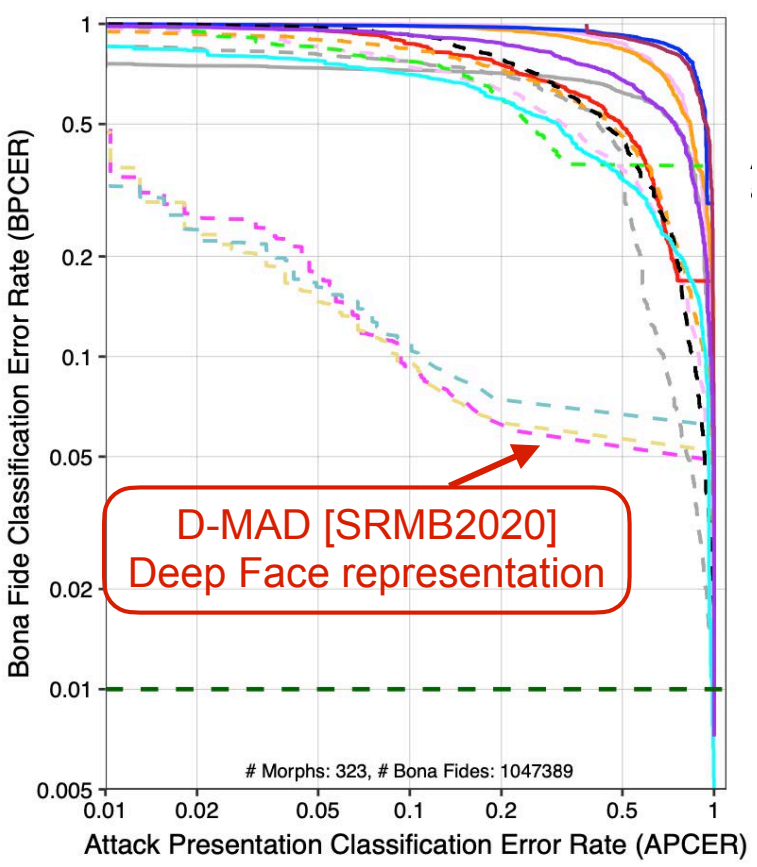
This publication is available free of charge from:
https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

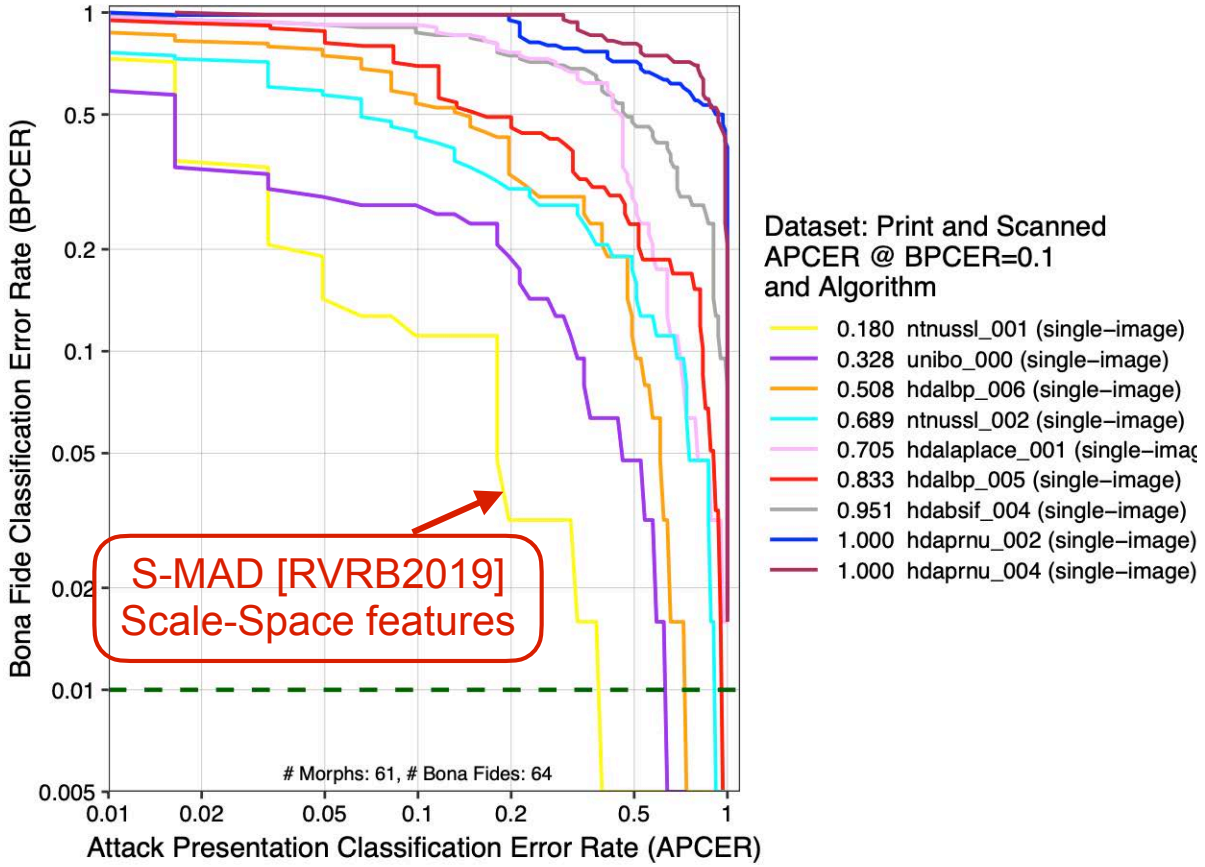
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST-FRVT-MORPH

NIST IR 8292 report presented April, 2021

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





More information

The MAD website

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

The MAD survey papers

- U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, C. Busch: "Face Recognition Systems under Morphing Attacks: A Survey“, in IEEE Access, (2019) https://ieeexplore.ieee.org/document/8642312


IEEE Access

Face Recognition Systems Under Morphing Attacks: A Survey

- S. Venkatesh, R. Raghavendra, K. Raja, C. Busch: "Face Morphing Attack Generation & Detection: A Comprehensive Survey", in IEEE Transactions on Technology and Society (TTS), (2021) https://ieeexplore.ieee.org/document/9380153


Face Morphing Attack Generation & Detection: A Comprehensive Survey

More information

The MAD workshop

https://eab.org/events/program/229

- Luuk Spreeuwers (University of Twente) - recorded talk
  - Morphing Attacks on Face Recognition Systems
- David Robertson (University of Strathclyde) - recorded talk
  - Psychological Experiments on Morphed Faces
- Kiran Raja (NTNU) - recorded talk
  - Morphing Attack Detection Approaches
- Matteo Ferrara (University of Bologna) - recorded talk
  - Bologna Online Evaluation Platform
- Frøy Løvåsdal (Norwegian Police) - recorded talk
  - Morphing Attack Detection Capabilities of Human Examiners
- Mei Ngan (NIST) - recorded talk
  - Face Morphing Detection Evaluation
- Naser Damer (Fraunhofer IGD) - recorded talk
  - Generating Morphs with Generative Adversarial Networks
- Christian Rathgeb (Hochschule Darmstadt) - recorded talk
  - Detection of Face Beautification Manipulations
- Uwe Seidel (BKA)
  - Research Needs for Morphing Attack Detection

Deep Fakes

Generative Adversarial Networks

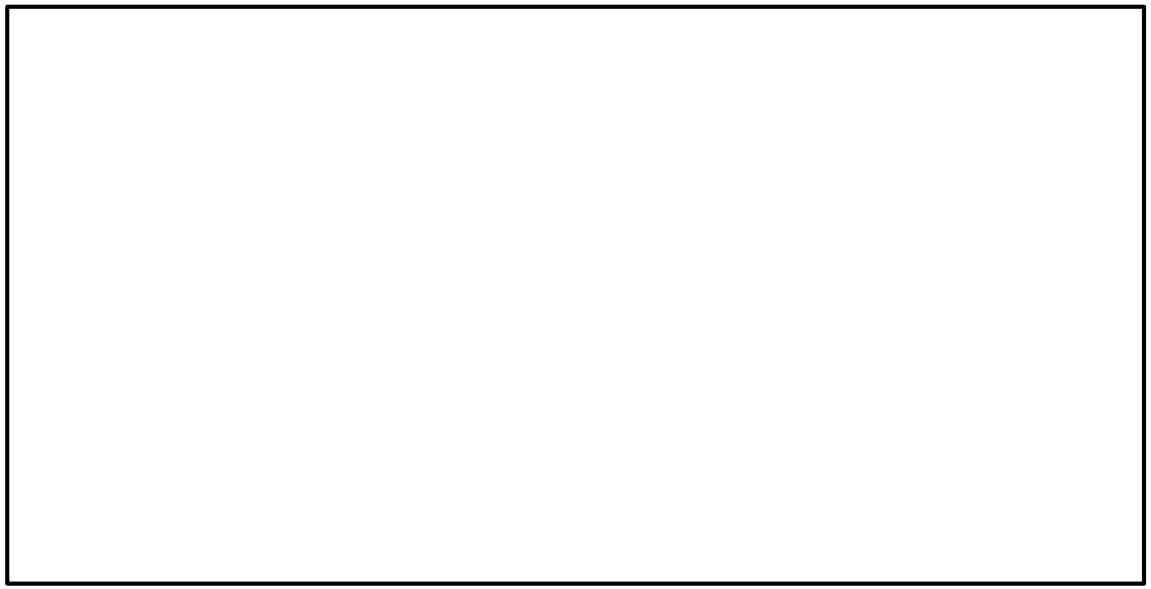
StyleGAN

- Published in 2019 by Karras et al. (NVIDIA Development)
- Synthetic face image generation based on Style Transfer
- Style Transfer = Transfer style of image A to image B via Adaptive Instance Normalization (AdaIN)
- AdaIN: Rescale feature maps of image B (Content) with statistics of image A (mean, standard deviation)

Generative Adversarial Networks

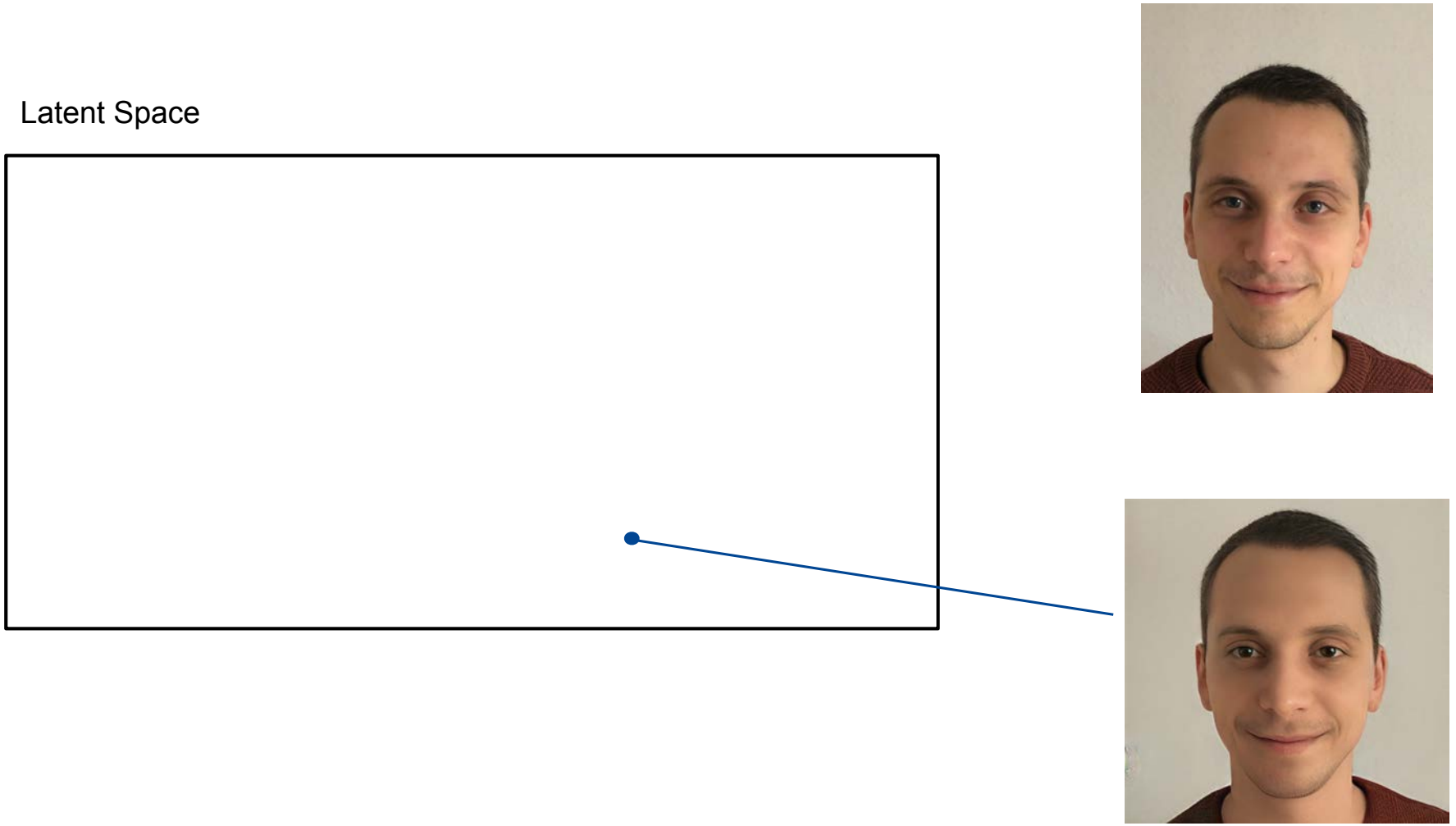
StyleGAN - latent space projection

Latent Space



Generative Adversarial Networks

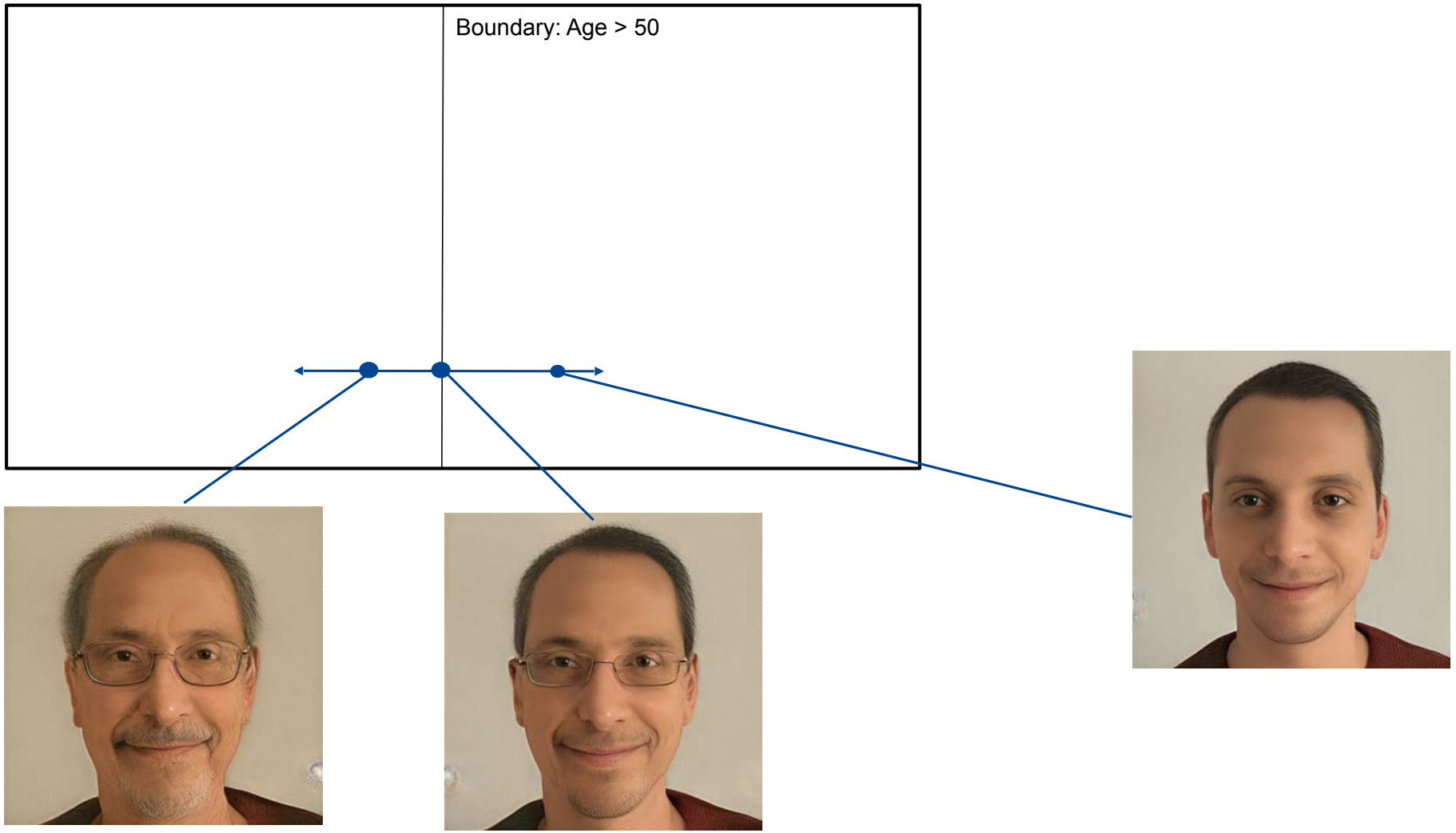
StyleGAN - latent space projection



Generative Adversarial Networks

InterFaceGAN - semantic face edition

- Mated sample generation (e.g. with aging)



Contact

Research opportunities

- Darmstadt (Germany) https://dasec.h-da.de/
- Gjøvik (Norway) https://www.ntnu.edu/nbl
- Internships for Msc and PhD students with possibility of a grant
- Collaboration with governmental and industrial partners