

iMARS - Morphing Attack Potential

Matteo Ferrara, Annalisa Franco,
Davide Maltoni, **Christoph Busch**

EAB RPC 2022-09-14

Overview

Agenda

- Introduction - problem description
- The project iMARS
- Morphing attack potential
- Morphing attack detection - evaluation
- Conclusion

Passports and Identity Cards of European Union Citizens

ICAO 9303 Logical Data Structure

Data to be stored in the RFID-Chip

- Alpha-numeric data: 5 Kbyte
- Facial image: ISO/IEC 19794-5:2005
 - ▶ 12 Kbyte (JPEG, JPEG2000)
- Fingerprint images: ISO/IEC 19794-4:2004
 - ▶ 2* 10 Kbyte (JPEG, JPEG2000, WSQ)



Source: ICAO 9303 Part 4, 2021

- Facial image: ISO/IEC 39794-5:2019
<https://www.iso.org/standard/72155.html>
 - Fingerprint images: ISO/IEC 39794-4:2019
<https://www.iso.org/standard/72156.html>
 - ▶ ICAO has adopted its 9303 specification in 2020 and refers now to ISO/IEC 39794 and its Parts 1, 4 and 5.
 - ▶ Passport reader equipment must be able to handle ISO/IEC 39794 data by 2025-01-01 (5 years preparation period).
 - ▶ Between 2025 and 2030, passport issuers can use the old version or the new version of standards (5 years transition period).
- Adopted by
ICAO in 2020**

**Adopted by
ICAO in 2020**

Is the Principle valid on the left Side?

Principle of equality - in our society

- One individual - **one** passport



Principle of **unique link** of ICAO

- **One** individual - one passport
- ICAO 9303 part 2, 2006:



*„**Additional security measures:** inclusion of a machine verifiable biometric feature **linking** the document to its **legitimate holder**“*

Is the Principle valid on the left Side?

Principle of unique link of ICAO

- **One** individual - one passport



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

- **Multiple** individuals - one passport

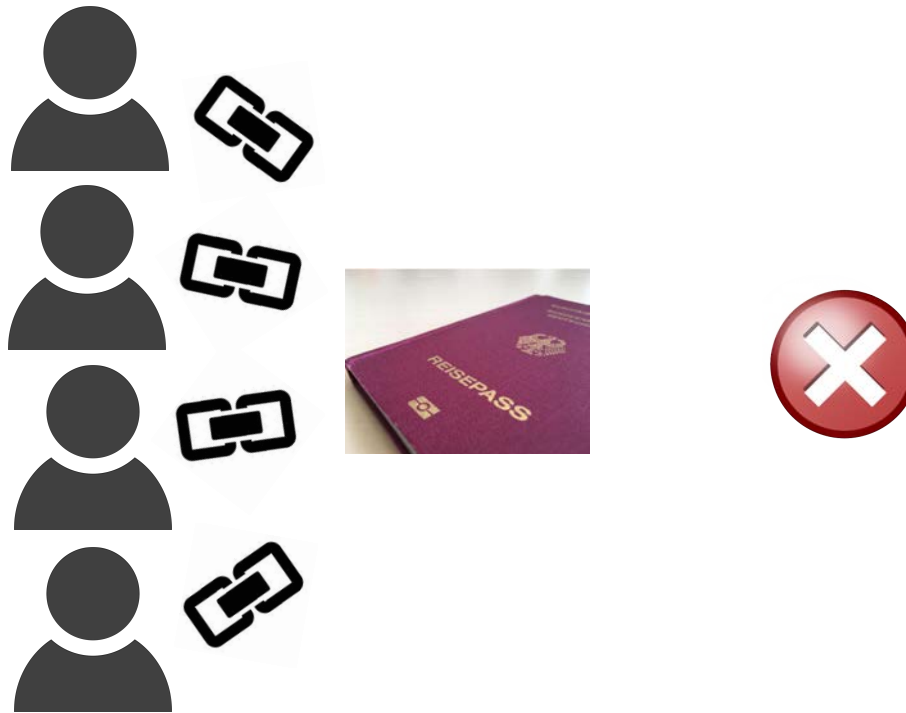


image source: <https://pixabay.com/de/vectors/tick-sternchen-kreuz-rot-gr%C3%BCn-40678/>

What is Morphing?

What is Morphing?

In our real world morphing can become a **threat**

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

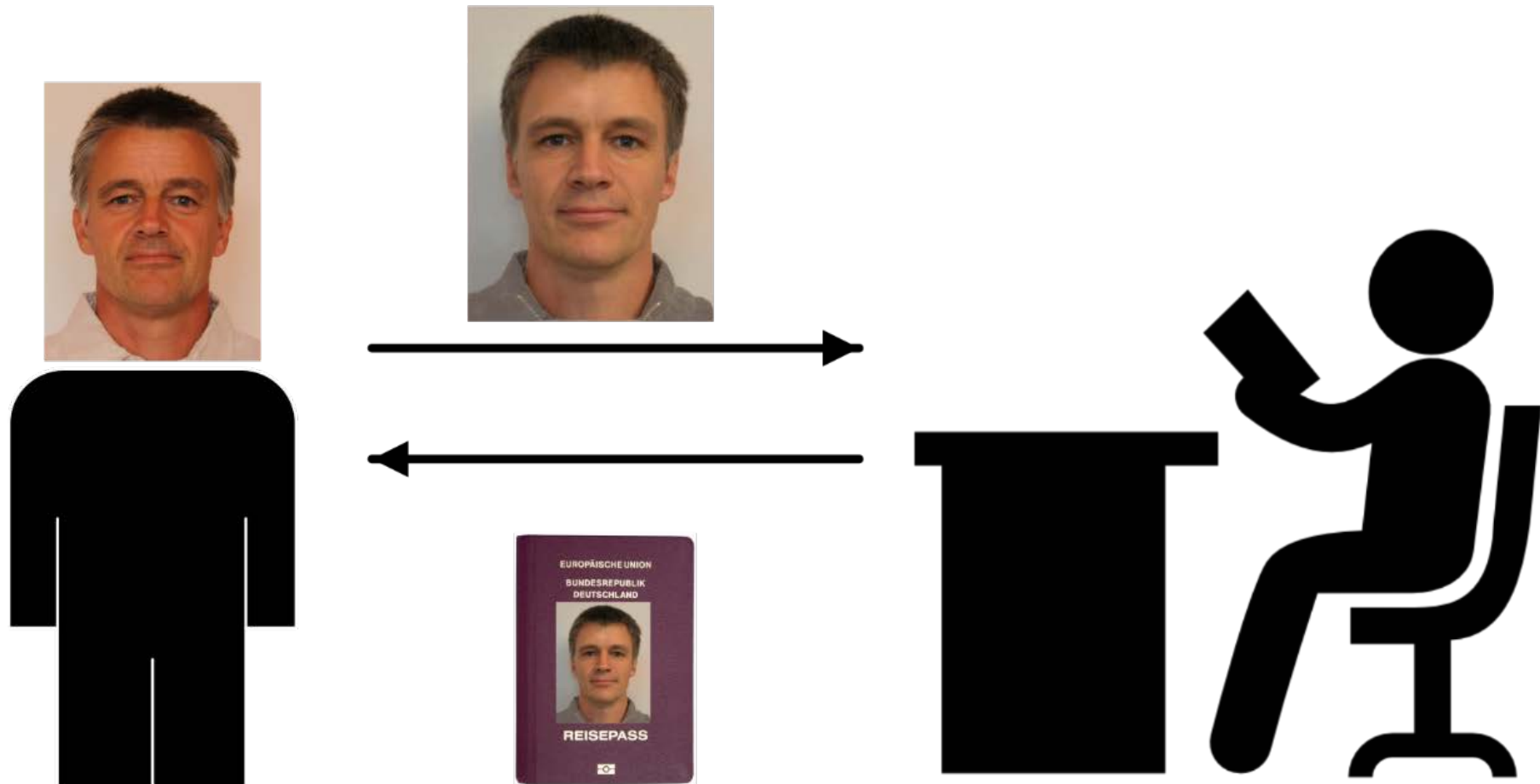


Problem Description

Problem: Morphing Attacks

Morphing attack scenario

- Passport application of the accomplice A



Problem: Morphing Attacks

Morphing attack scenario

- Border control



Problem: Morphing Attacks

Is it a really problem ? - **YES!**

- In September 2018 German **activists**
 - ▶ used a morphed images of Federica Mogherini (High representative of the European Union for Foreign Affairs and Security Policy) and a member of their group
 - ▶ and received an **authentic German passport**.



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

Problem: Morphing Attacks

Is it a really problem ? - **YES!**

Report by the Slovenian Police [Tork2021]

- Reported in September 2021 that in the last 12 month more than 40 morphing cases
 - ▶ were detected at Airport Police in Ljubljana
- Business model:
 - ▶ Albanian citizens, applying for a Slovenian passport
 - ▶ offered as a professional service travel route via Vienna and Warsaw to Canada

[Tork2021] M. Torkar: “Morphing Cases in Slovenia”, German Biometric Working Group, (2021), <https://eab.org/events/program/220>

The iMARS Project Summary

The iMARS Project

Key figures

- Start date: September 2020
- End date: 31 August 2024
- H2020-SU-SEC-2019
- Grant agreement ID: 883356
- Programme(s):
 - ▶ H2020-EU.3.7.3. - Strengthen security through border management
 - ▶ H2020-EU.3.7.8. - Support the Union's external security policies including through conflict prevention and peace-building
- Topic:
 - ▶ SU-BES02-2018-2019-2020 -
Technologies to enhance border and external security
- Overall budget: € 6 988 521,25
- Website: <https://imars-project.eu/>



The iMARS Consortium

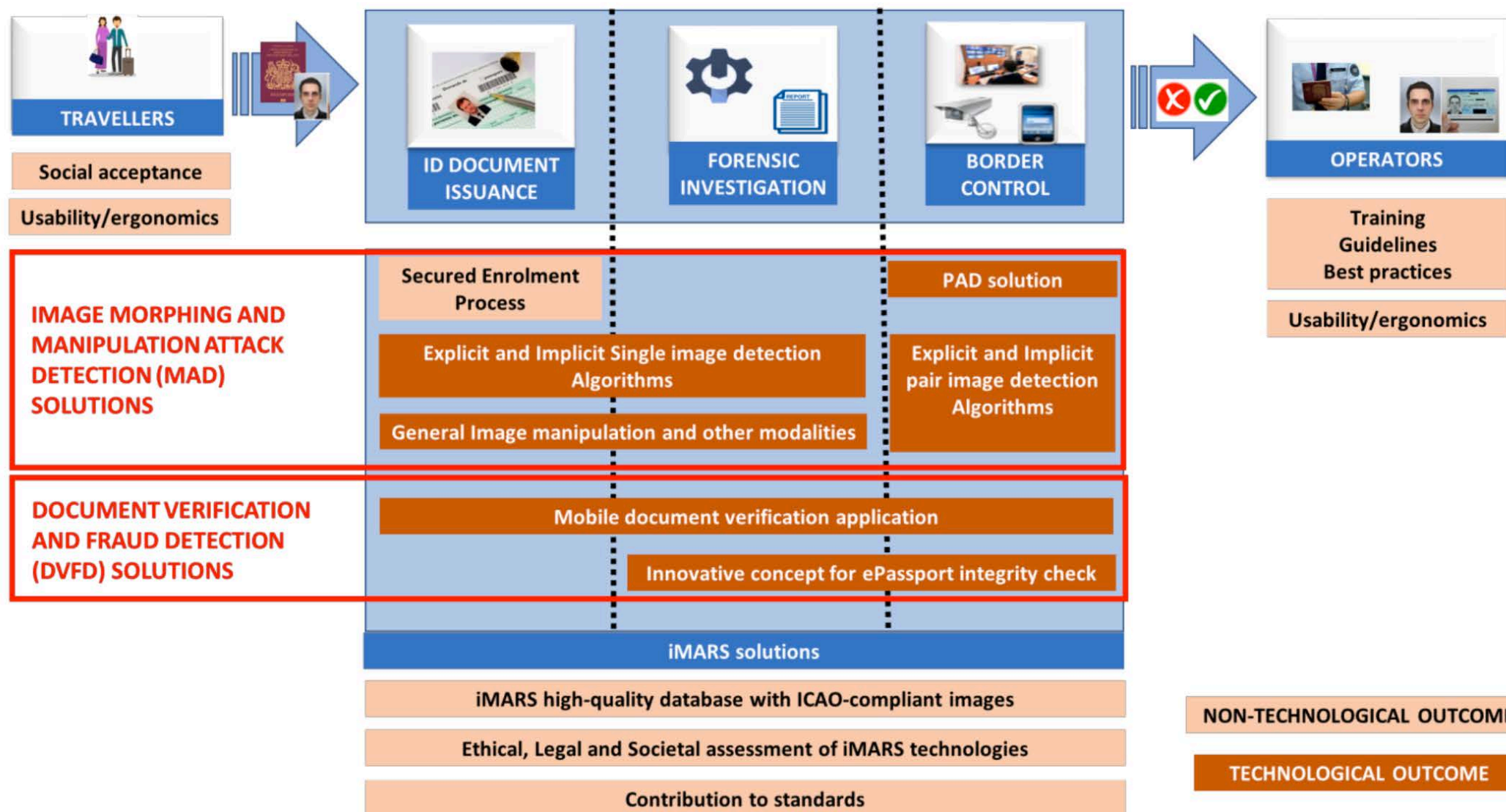
24 Partners

- IDM - IDEMIA IDENTITY & SECURITY FRANCE (FR)
- DG - IDEMIA IDENTITY & SECURITY GERMANY (DE)
- COG - COGNITEC SYSTEMS GMBH (DE)
- VIS - VISION BOX (PT)
- MOB - MOBAI AS (NO)
- ART - ARTTIC (FR)
- SUR - SURYS (FR)
- NTN - NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET (NO)
- UBO - UNIVERSITA DI BOLOGNA (IT)
- UTW - UNIVERSITY OF TWENTE (NL)
- HDA - HOCHSCHULE DARMSTADT (DE)
- KUL - KATHOLIEKE UNIVERSITEIT LEUVEN (BE)
- IBS - INSTITUTE OF BALTIC STUDIES (EE)
- EAB - EUROPEAN ASSOCIATION FOR BIOMETRICS
- KEM - KENTRO MELETON ASFALIAS (EL)
- BKA - BUNDESKRIMINALAMT (DE)
- NOI - MINISTERIE VAN BINNENLANDSE ZAKEN (NL)
- INC - IMPRENSA NACIONAL (PT)
- POD - POLITIDIREKTORATET (NO)
- PBP - PORTUGUESE IMMIGRATION AND BORDERS SERVICES (PT)
- HEP - HELLENIC POLICE (EL)
- CYP - CYPRUS POLICE (CY)
- PBM - BORDER POLICE OF THE REPUBLIC OF MOLDOVA (MD)
- BFP - POLICE FEDERALE BELGE (BE)



The iMARS Research

The iMARS overall concept



What is the vulnerability?

Automatic Border Control

The verification process

- at an Automatic Border Control (ABC) gate
- is **comparing** the **reference image** from the ePass against **multiple** consecutive **frames** acquired **live**.

ABC gates of different manufacturers use different FRSs.

- Different FRSs use a **different number** of live frames during the verification process



Image source: BSI

Measure the Vulnerability

When is a morphing attack considered **successful**?

- Only if **all contributing subjects** reach successfully a **match** when being compared against the morphed reference sample.

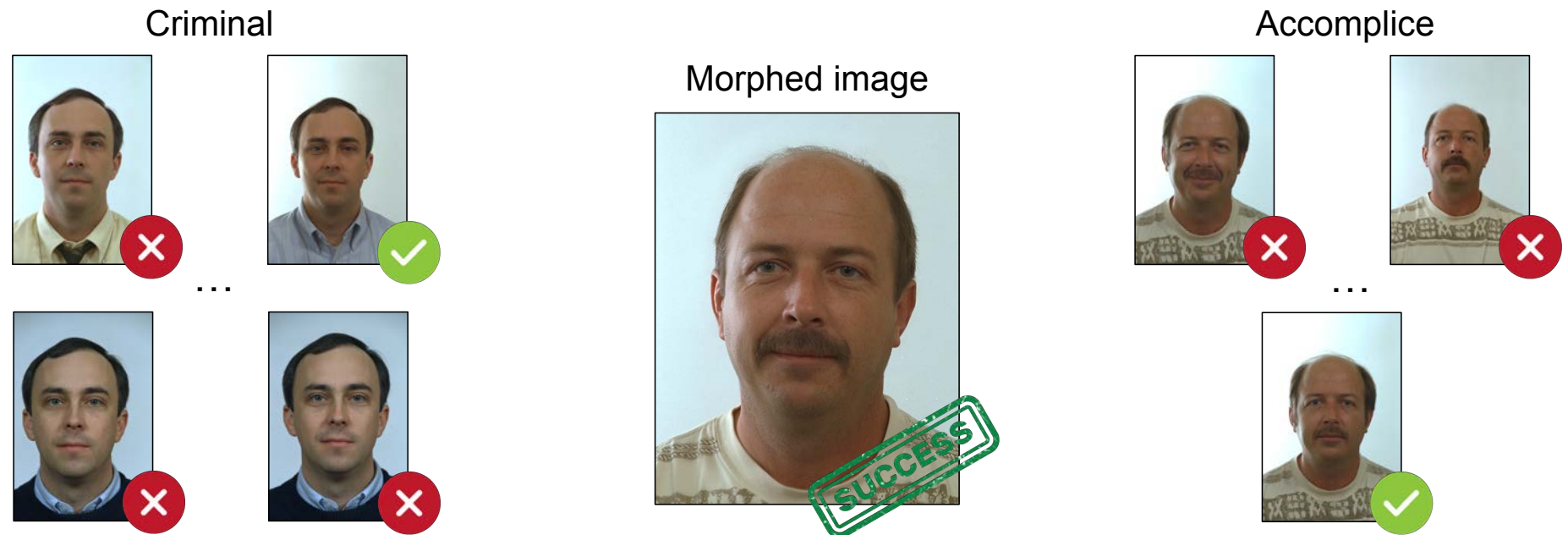
The vulnerability to morphing is usually measured on specific databases of morphed images.

- It is quantified as the **proportion** of **morphed images** that are erroneously **verified** as **bona fide** with **all contributing subjects**.
- Two metrics have been introduced for vulnerability assessment
 - ▶ MMPMR
 - ▶ FMMPMR

Measure the Vulnerability

Mated Morph Presentation Match Rate (MMPMR)

- A morphing attack **succeeds** if the morphed image can be successfully verified against **at least one** of the probe images of **each** subject.



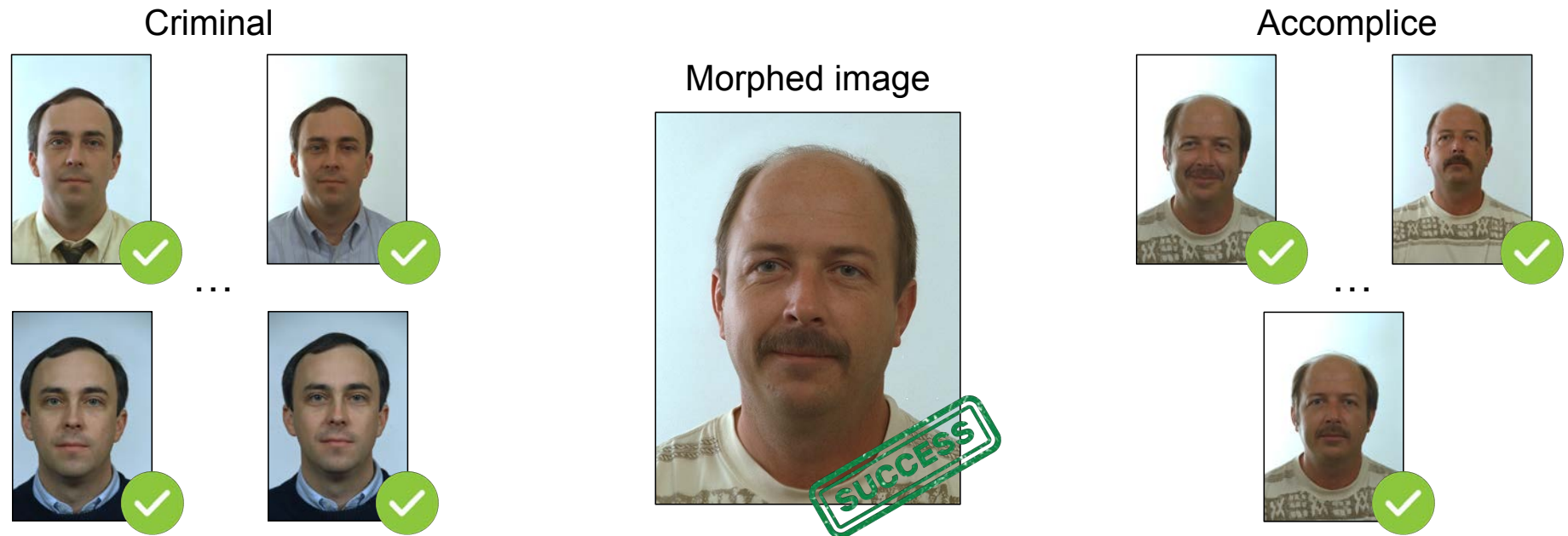
Source: M. Ferrara, IWBF-2022

[SNRG+17] 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 BIOSIG, (2017)

Measure the Vulnerability

Fully Mated Morph Presentation Match Rate (FMMPMR)

- A morphing attack **succeeds** if the morphed image can be successfully verified **against all** probe images of **each** subject.



Source: M. Ferrara, IWBF-2022

[Venk2020] S. Venkatesh, R. Raghavendra, K. Raja, C. Busch. "Face Morphing Attack Generation & Detection: A Comprehensive Survey." IEEE-TTS, (2021)

Morphing Attack Potential

The MMPMR and FMMPMR

- can only **partially** estimate the **attack potential**.

They do not take into account:

- **multiple** FRSs (**generality**);
- a **variable number** of verified **probe** images (robustness).

To extend these concepts [Fera2022]

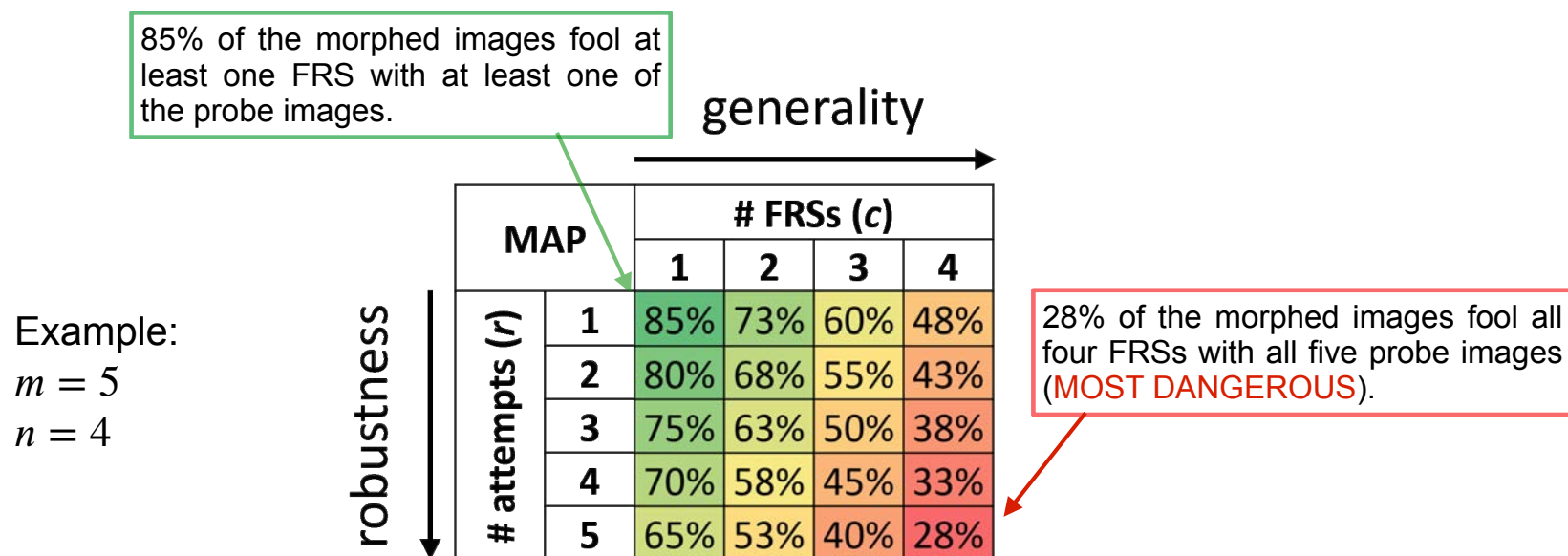
- proposed a new metric called **Morphing Attack Potential (MAP)**
- that considers a variable number of attempts (frames acquired live at the gate) and multiple FRSs.

[Fera2022] M. Ferrara, A. Franco, D. Maltoni, C. Busch: "Morphing Attack Potential", in Proceedings of 10th International Workshop on Biometrics and Forensics (IWBF 2022), Salzburg, AT, April 20-21, (2022)

Morphing Attack Potential

Definition of Morphing Attack Potential (MAP)

- Given a **dataset** of morphed images $\mathbb{M}$, m probe images for each contributing subject and n FRSs to evaluate, **MAP** is defined as a **matrix** of size $m \times n$ whose element $MAP[r, c]$ reports the **proportion** of morphed images **successfully verified** with **both** contributing subjects with at least r probe images by at least c FRSs.



[Fera2022] M. Ferrara, A. Franco, D. Maltoni, C. Busch: "Morphing Attack Potential", in Proceedings of 10th International Workshop on Biometrics and Forensics (IWBF 2022), Salzburg, AT, April 20-21, (2022)

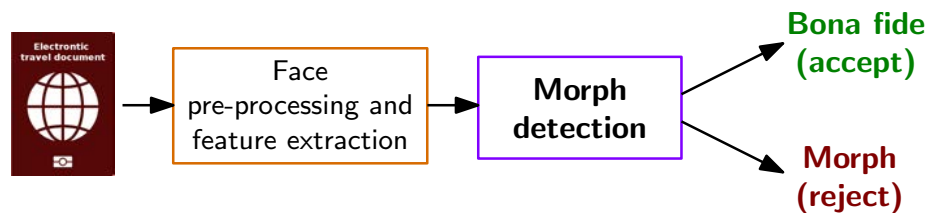
Morphing Attack Detection (MAD)

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)

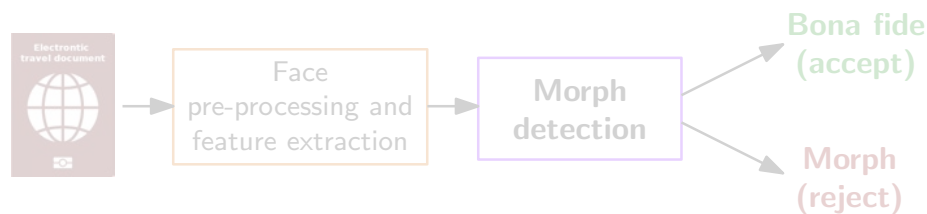


[SRB2018a] U. Scherhag, C. Rathgeb, C. Busch: "Towards Detection of Morphed Face Images in electronic Travel Documents", in Proceedings of the 13th IAPR International Workshop on Document Analysis Systems (DAS), April 24-27, (2018)

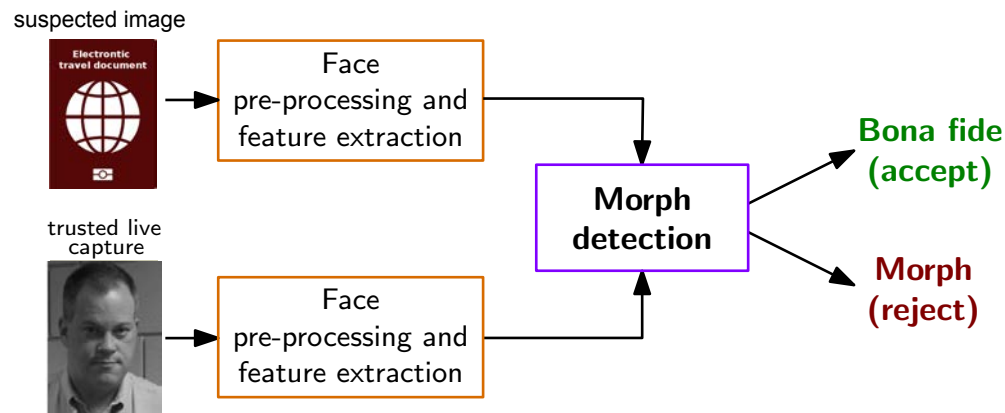
Morphing Attack Detection Scenarios

Real world scenarios

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



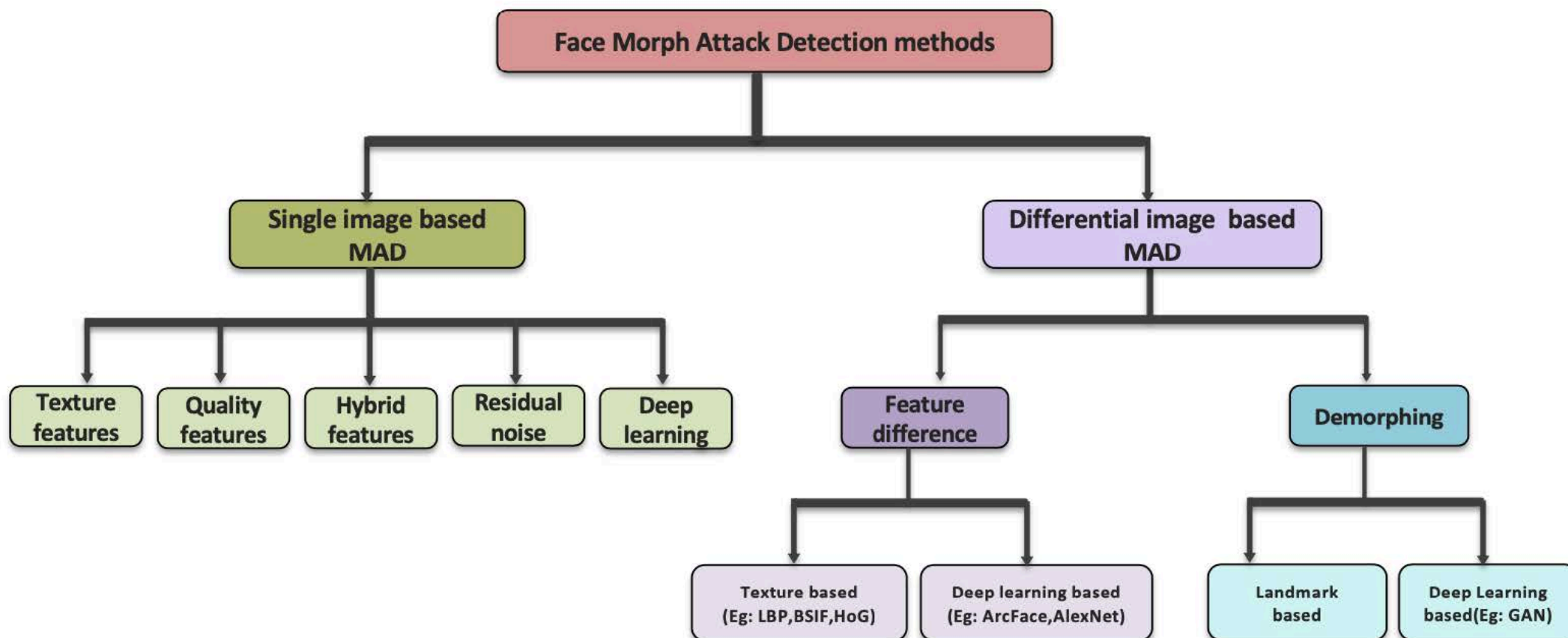
- **Differential** morphing attack detection (D-MAD)
 - ▶ a **pair** of images is analysed - and one is a trusted Bona Fide image
 - ▶ biometric verification (e.g. at the border)



[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)

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

Standardized Testing Metrics

Definition according to ISO/IEC 30107-3

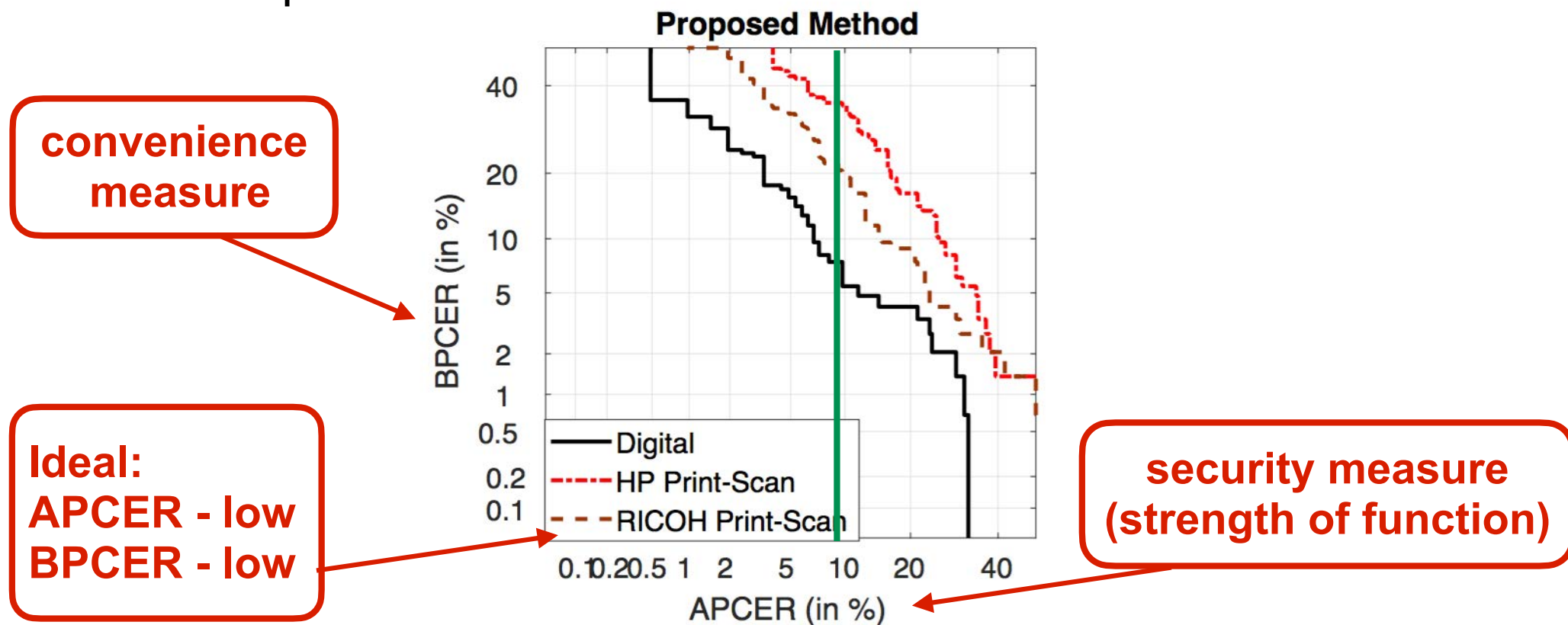
- Testing the false-negative and false-positive errors:
- **Attack presentation classification error rate (APCER)**
*proportion of **attack presentations** using the same PAI species incorrectly **classified as bona fide presentations** in a specific scenario*
- **Bona fide presentation classification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

source: [ISO/IEC 30107-3] SO/IEC 30107-3, “Biometric presentation attack detection - Part 3: Testing and reporting”, (2017)
<https://www.iso.org/standard/67381.html>

Standardized Testing Metrics

Definition of metrics in ISO/IEC 30107-3

- DET curve analyzing operating points for various thresholds and plot **convenience** measures over **security** 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)

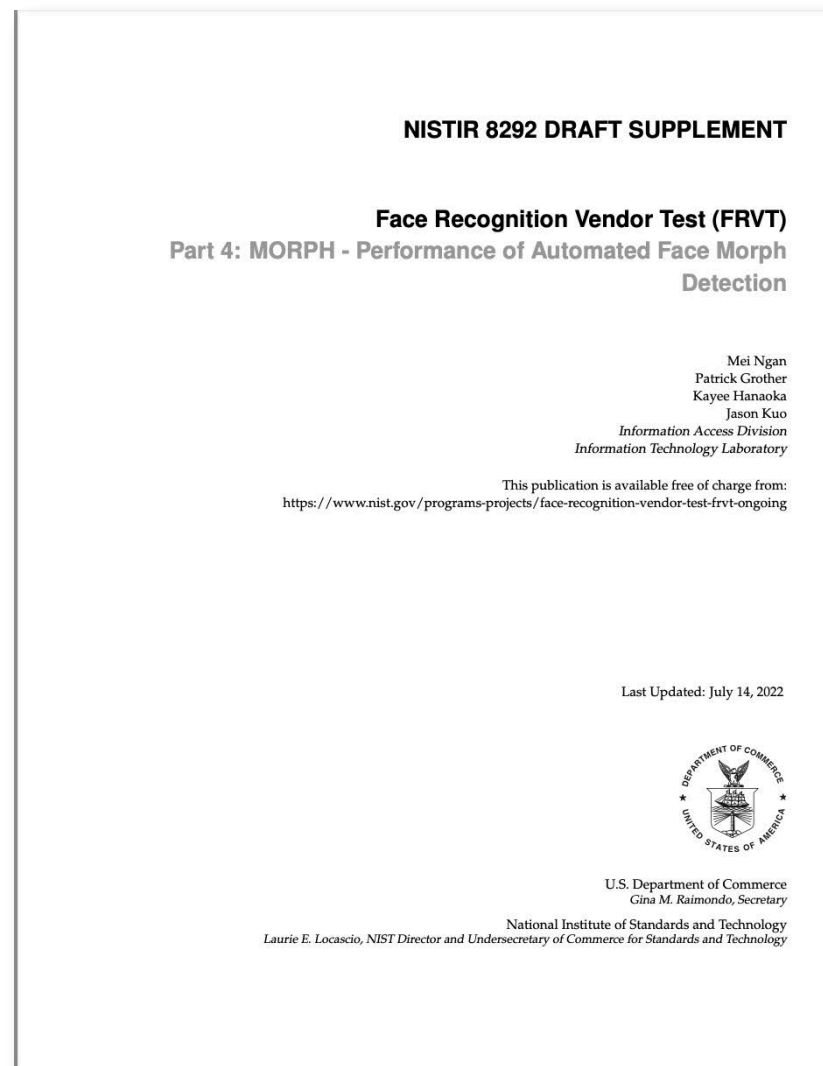
NIST FRVT MORPH

NIST IR 8292 report presented July, 2022

FRVT MORPH

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

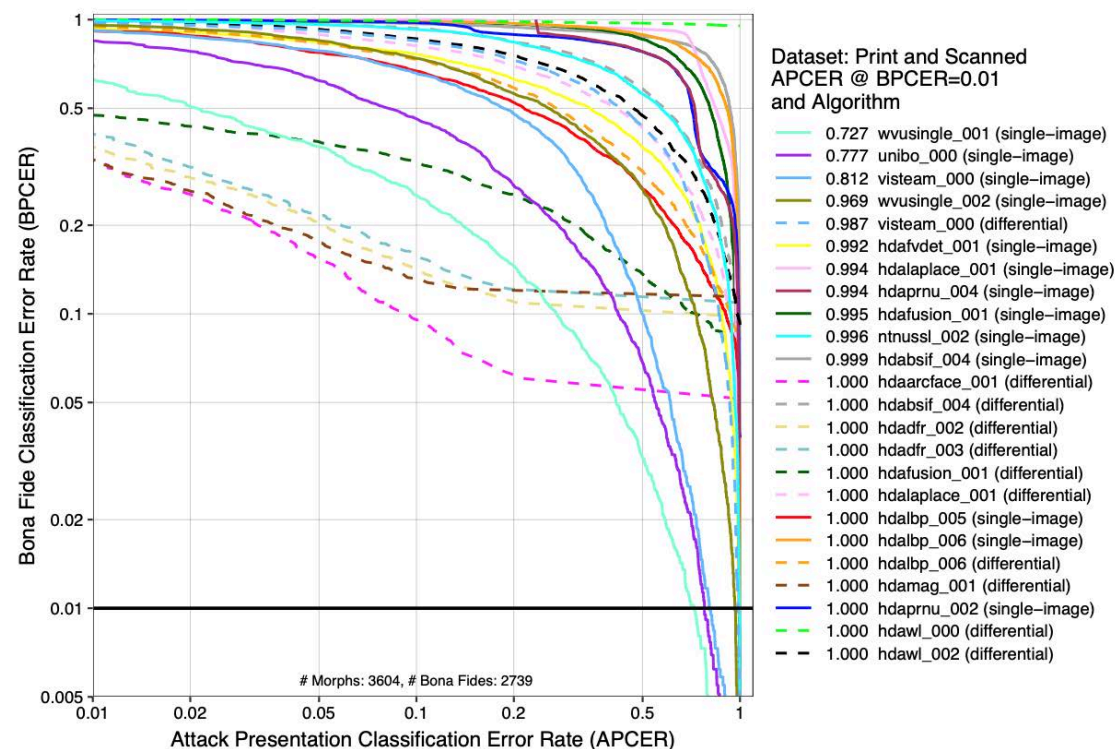
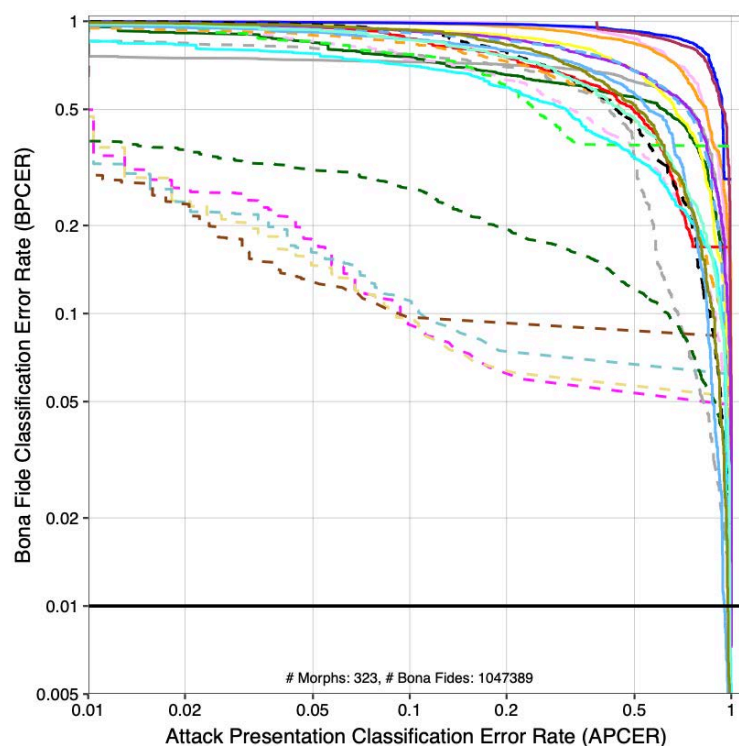
- results for MAD algorithms from six research labs:
 - ▶ Hochschule Darmstadt (HDA)
 - ▶ Norwegian University of Science and Technology (NTNU)
 - ▶ University of Bologna (UBO)
 - ▶ University of Twente (UTW)
 - ▶ Universidade de Coimbra (VIS)
 - ▶ West Virginia University (WVU)



NIST FRVT MORPH

NIST IR 8292 report presented July, 2022

- 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**



New Work Item Proposal for ISO/IEC JTC1 SC37

New Work Item Proposal

Suggested structure

- Scope
 - vulnerability of face recognition - testing and reporting
- Normative references
- Terms and definitions
- Morphing attacks
- Morphing attack potential (MAP)
 - evaluates the comprehensive **attack potential** of a dataset of morphed images **on a set of FRSs** (4 OpenSource reference FRSs in [Fera2022])

[Fera2022] M. Ferrara, A. Franco, D. Maltoni, C. Busch: "Morphing Attack Potential", in Proceedings of 10th International Workshop on Biometrics and Forensics (IWBF 2022), Salzburg, AT, April 20-21, (2022)

New Work Item Proposal

MAP can also be useful to answer the following questions:

- What is the **impact** of **one morphing method** on a set of FRSs?
 - ▶ using a dataset containing morphed images generated by such algorithm
- What is the **vulnerability** of **one (operational) FRS** to morphing?
 - ▶ computing a MAP-matrix with a single column
- What is the **impact** of a specific **factor** (e.g., morphing factor, subject age/gender/ethnicity, JPEG compression, print and scan process, etc.) on the attack potential of morphing?
 - ▶ using a dataset containing only morphed images with the specific factor

Conclusion

We are facing a situation, where

- Passports with morphs are already in **circulation**
 - ▶ 1000+ reported cases
 - ▶ Switch to live enrolment is a good decision, but does not solve the problem
- Passports with morphed face images will have a major impact on border security
 - ▶ introduction of EU's entry/exit system, global migration flows
- In combination with **passport brokers** a dramatic problem
 - ▶ the darknet offers numerous such opportunities ...
- Countermeasures to the problem
 - ▶ researching robust MAD algorithms in iMARS
 - ▶ supporting the research with standardisation of the methodology

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



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>