State of the Art:
Morphing Attack Detection

Dinusha Frings, Christoph Busch

copy of slides available at:
https://www.christoph-busch.de/projects-mad.html

SecurityPrinters 2019, October 25

National Office for Identity Data
*Ministry of the Interior and
Kingdom Relations*

NTNU

Overview

Disclaimer

- The work presented in this talk is funded by the European Union’s Internal Security Fund — Borders and Visa
- The content of this presentation represents the views of the authors only and is their sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains

Important Abbreviation

- MAD - Morphing Attack Detection

Overview

State Of The Art of Morphing Detection (SOTAMD)

- Funding: European Commission Direct Award
- Timeframe: February 2019 – January 2020
- Coordinator: National Office for Identity Data, NL
- Partners:
  - Bundeskriminalamt (BKA), DE
  - University of Bologna (UBO), IT
  - Hochschule Darmstadt (HDA), DE
  - The University of Twente (UTW), NL
  - Norwegian University of Science and Technology (NTN), NO

Bundeskriminalamt

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

NTNU

National Office for Identity Data
Ministry of the Interior and
Kingdom Relations

ALMA MATER STUDIORUM A.D. 1088

UNIVERSITY OF TWENTE.

Problem Description

History - 2014

Integrated Project FIDELITY

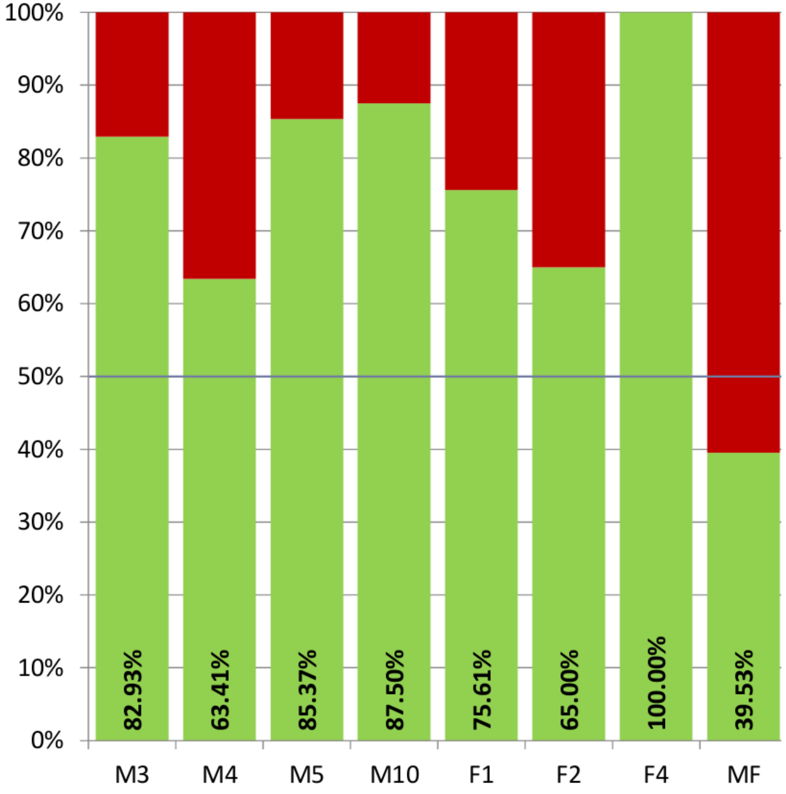
http://www.fidelity-project.eu/

- Fast and trustworthy Identity Delivery and check with ePassports leveraging Traveler privacy
- 4 years project (2012-2016)
  - European 7th Framework Programme
- Key Objective:
  - To improve the ePassport issuing process
    - Security of birth certificates and other evidence of identity
    - Quality of biometric data in the chip
    - One individual one passport (duplicate enrolment check)

[MFM2014] M. Ferrara, A. Franco, D. Maltoni, “The Magic Passport”, in Proceedings IEEE IJCB 2014

Scale of the Problem: Vulnerability

Human Capabilities: Experts (44 border guards)



[MFM2016] M. Ferrara, A. Franco, D. Maltoni: “On the Effects of Image Alterations on Face Recognition Accuracy”, in Face Recognition Across the Imaging Spectrum, Springer Nature, (2016)

Problem: Morphing Attacks

FIDELITY project conclusion (December 2015)

- The current procedure, where a printed face photo can be provided by the citizen, poses serious security risks
- Solutions - suggested in 2015:
  - Switch to live enrolment (that is the case for Norway and Sweden)
  - Software-supported detection of morphed face images

Slido – show us your numbers

This poll is anonymous

Can you tell us the number of passports/ID cards with “morphed face images” your country detected over the past 5 years? This also contains foreign national documents.

- 0 – 5 cases
- 6 – 50 cases
- 51 – 500 cases
- 501 – 50.000 cases

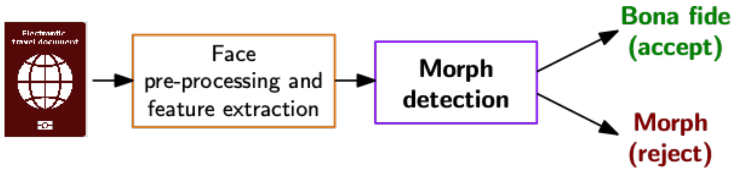
Morphing Attack Detection (MAD)

Scenarios and Methods

Morphing Attack Detection Scenarios

Real world scenarios

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



Face pre-processing and feature extraction

Morph detection

Bona fide (accept)

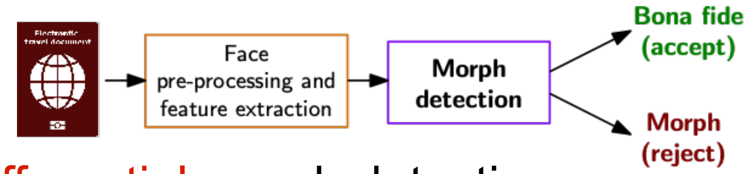
Morph (reject)

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

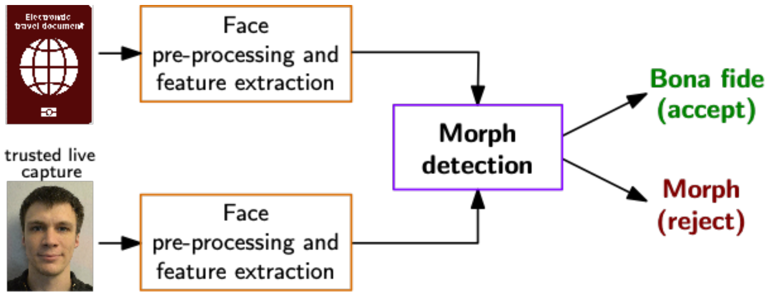
Morphing Attack Detection Scenarios

Real world scenarios

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


Electronic travel document
Face pre-processing and feature extraction
Morph detection
Bona fide (accept)
Morph (reject)

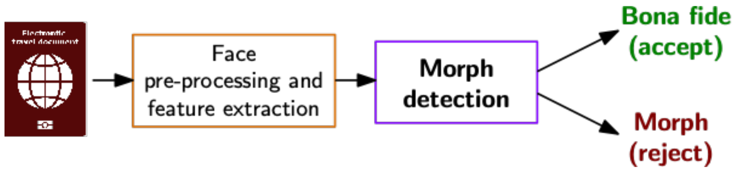
- Differential morph detection
  - A pair of images is analysed - and one is a trusted Bona Fide image
  - Biometric verification (e.g. at the border)

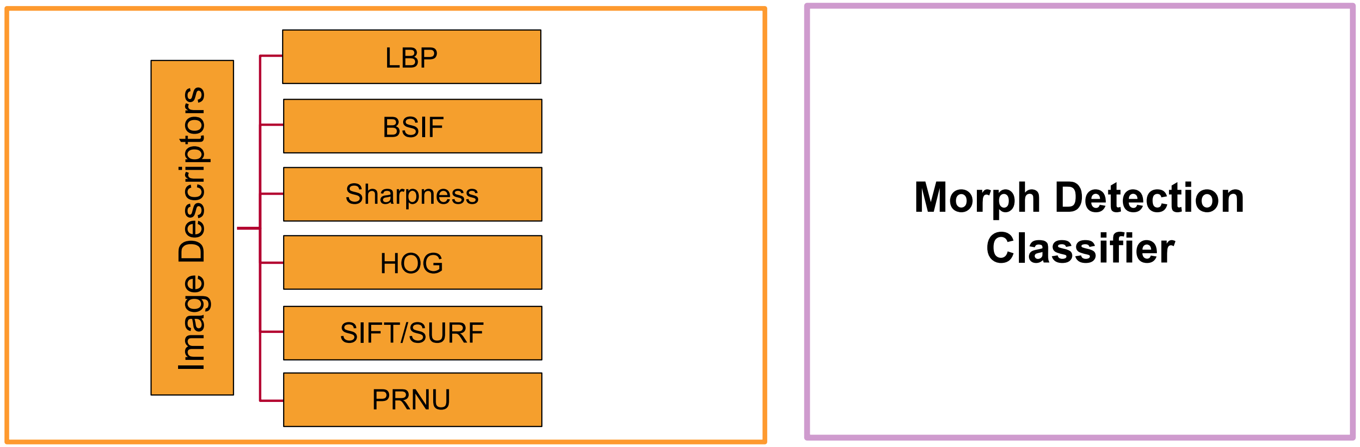

Electronic travel document
trusted live capture
Face pre-processing and feature extraction
Face pre-processing and feature extraction
Morph detection
Bona fide (accept)
Morph (reject)

Face Pre-processing and Feature Extraction

Morphing Attack Detection (MAD) with texture analysis

- Image descriptors as hand-crafted features


Electronic travel document
Face pre-processing and feature extraction
Morph detection
Bona fide (accept)
Morph (reject)

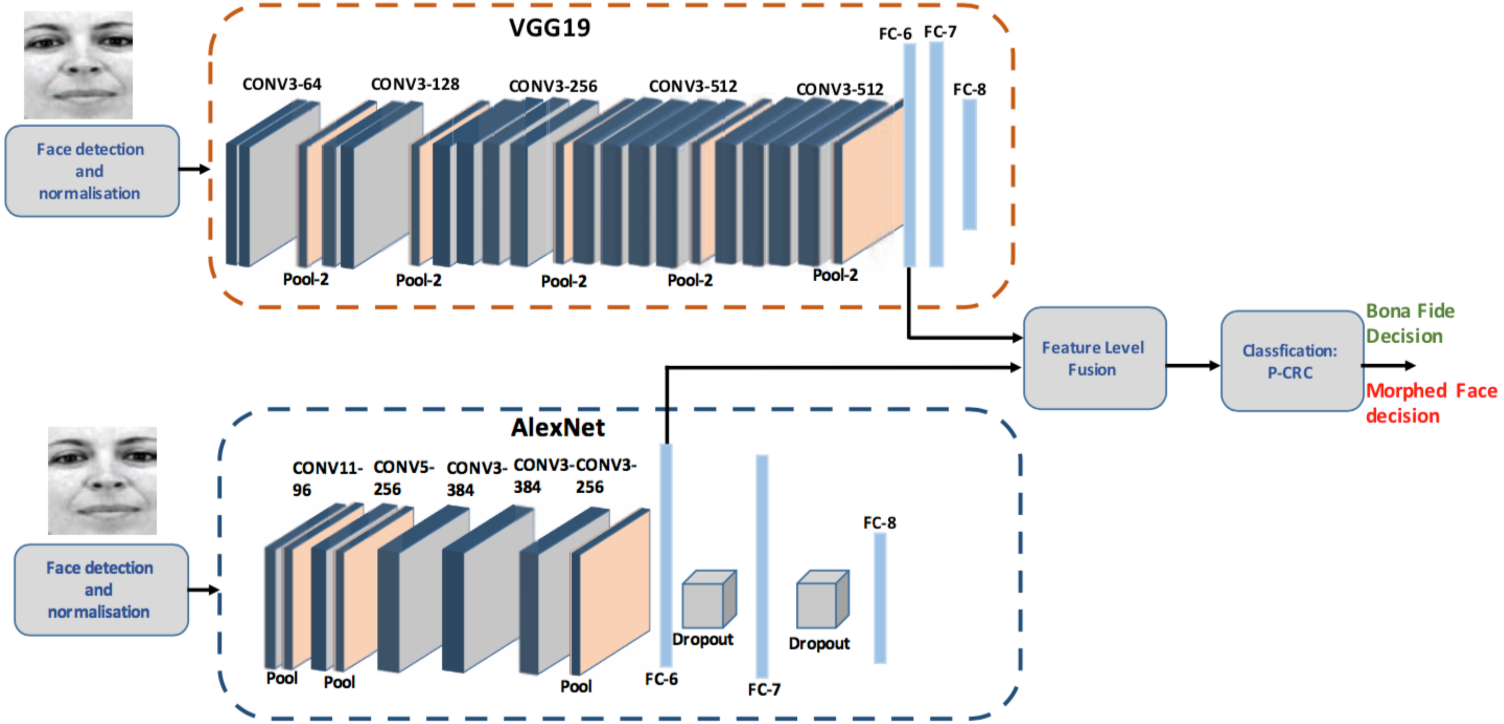


[SRB18b] U. Scherhag, C. Rathgeb, C. Busch: „Detection of Morphed Faces from Single Images: a Multi-Algorithm Fusion Approach“, in Proceedings if of the 2nd International Conference on Biometric Engineering and Applications (ICBEA 2018), Amsterdam, The Netherlands, May 16-18, (2018)

No-Reference Morph Detection

MAD with deep learning

- Feature level fusion of Deep CNNs



[RRVBu17] R. Raghavendra, K. Raja, S. Venkatesh, C. Busch: "Transferable Deep-CNN features for detecting digital and print-scanned morphed face images", in Proceedings of 30th International Conference on Computer Vision and Pattern Recognition Workshop (CVPRW 2017), July 21-26, (2017)

MAD Evaluation Methodology

MAD Evaluation Methodology

Face Morphing Attack evaluations are complex

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

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

[SNR17] U. Scherhag, A. Nautsch, C. Rathgeb, M. Gomez-Barrero, R. Veldhuis, L. 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

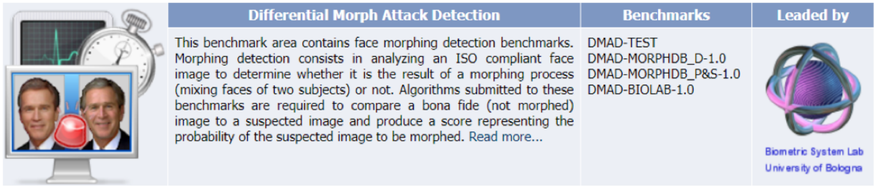
Specific objectives:

- Capture face images from 150 subjects
  - Enrolment images
  - ABC gate images
- Generate morphed face images with at least 3 algorithms
- Validate ICAO compliance
- Post-process automatically and manually
- Print and scan morphed and bona fide face images
- Adapt, integrate and test at least 3 MAD algorithms
- Test the MAD algorithms on the University of Bologna benchmarking server https://biolab.csr.unibo.it/FVConGoing

MAD Evaluation in SOTAMD

Benchmarks

- A new benchmark area for differential morphing detection



Differential Morph Attack Detection	Benchmarks	Leaded by
This benchmark area contains face morphing detection benchmarks. Morphing detection consists in analyzing an ISO compliant face image to determine whether it is the result of a morphing process (mixing faces of two subjects) or not. Algorithms submitted to these benchmarks are required to compare a bona fide (not morphed) image to a suspected image and produce a score representing the probability of the suspected image to be morphed. Read more...	DMAD-TEST DMAD-MORPHDB_D-1.0 DMAD-MORPHDB_P&S-1.0 DMAD-BIOLAB-1.0	Biometric System Lab University of Bologna

- Two benchmarks to evaluate different image types:
  - Digital or Printed/Scanned images

- Possibility of analyse results according to specific factors:
  - Manual or automatic post-processed morphing
  - Morphing approaches and parameters (e.g., morphing factor)
  - Gender, age, etc.

SOTAMD compliance with NIST-FRVT-MORPH

NIST recently realized FRVT MORPH

- an ongoing independent testing of face morph detection technologies. https://www.nist.gov/programs-projects/frvt-morph

The SOTAMD consortium decided to define

- a testing protocol perfectly compatible with the NIST interface,
- in order to minimize the effort for developers and
- promote the submission of algorithms to both evaluation platforms.

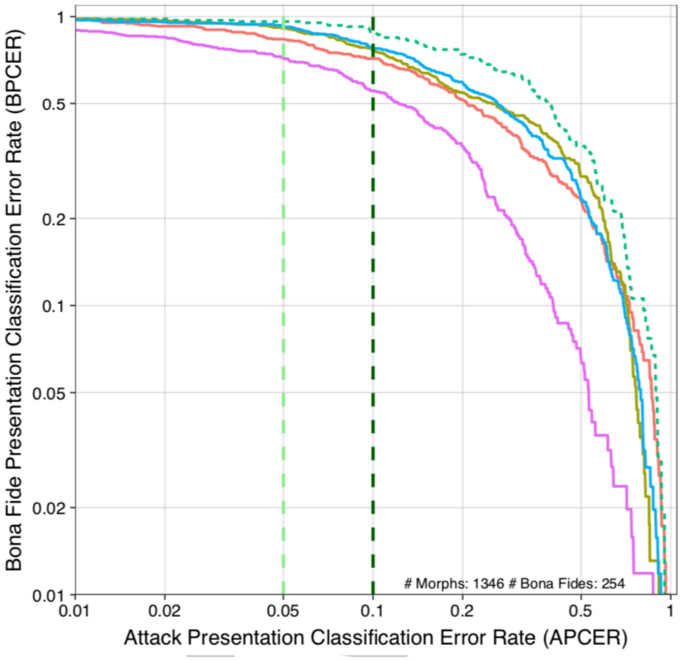
NIST only accepts Linux dynamically-linked library file;

- FVC-onGoing will accept both Windows and Linux executables

NIST-FRVT-MORPH

NIST draft report presented in September 2019

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



Draft NISTIR xxxx
(For Public Comment)

Face Recognition Vendor Test (FRVT) MORPH
Performance of Automated Face Morph Detection

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

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.xxxx

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

Testing Metrics

Definition according to ISO/IEC 30107-3

- **Attack presentation classification error rate (APCER)**
  proportion of attack presentations using the same PAI species incorrectly classified as bona fide presentations
  in a specific scenario

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

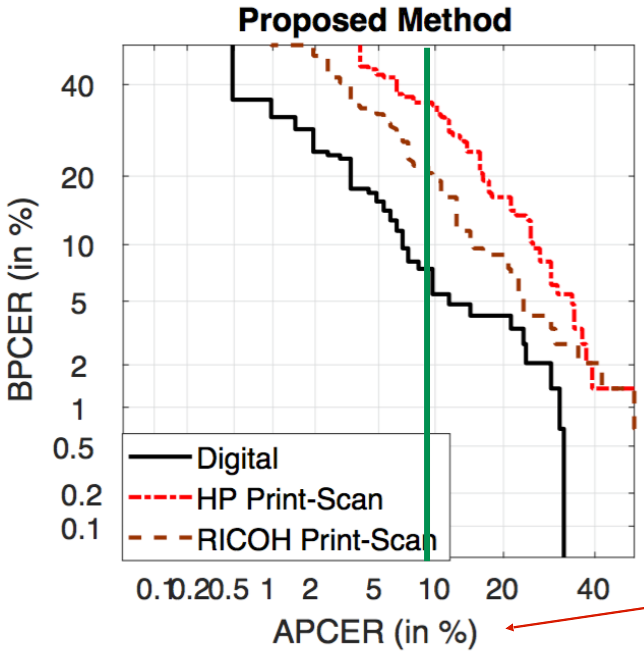
source: [ISO/IEC 30107-3] SO/IEC 30107-3, “Biometric presentation attack detection - Part 3: Testing and reporting”, (2016)
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67381

Testing Metrics

Definition according to ISO/IEC 30107-3

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

convenience measure



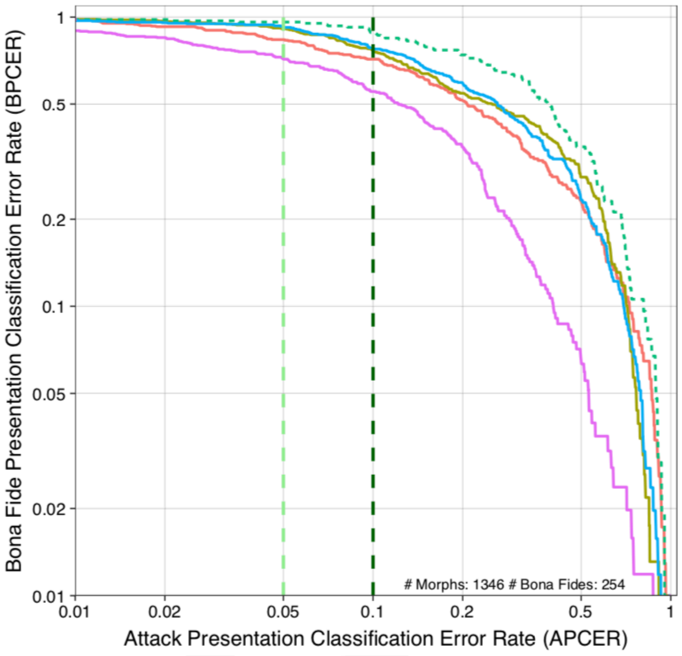
security measure (strength of function)

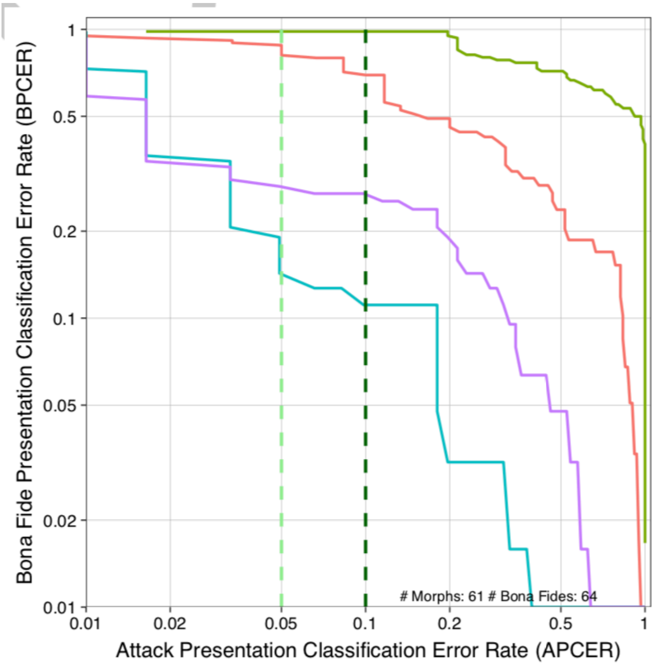
Source: R. Raghavendra, K. Raja, S. Venkatesh, C. Busch: "Transferable Deep-CNN features for detecting digital and print-scanned morphed face images", in Proceedings of 30th International Conference on Computer Vision and Pattern Recognition Workshop (CVPRW 2017), Honolulu, Hawaii, July 21-26, (2017)

NIST-FRVT-MORPH

NIST draft report presented in September 2019

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





What needs to be done?

MAD Action Plan

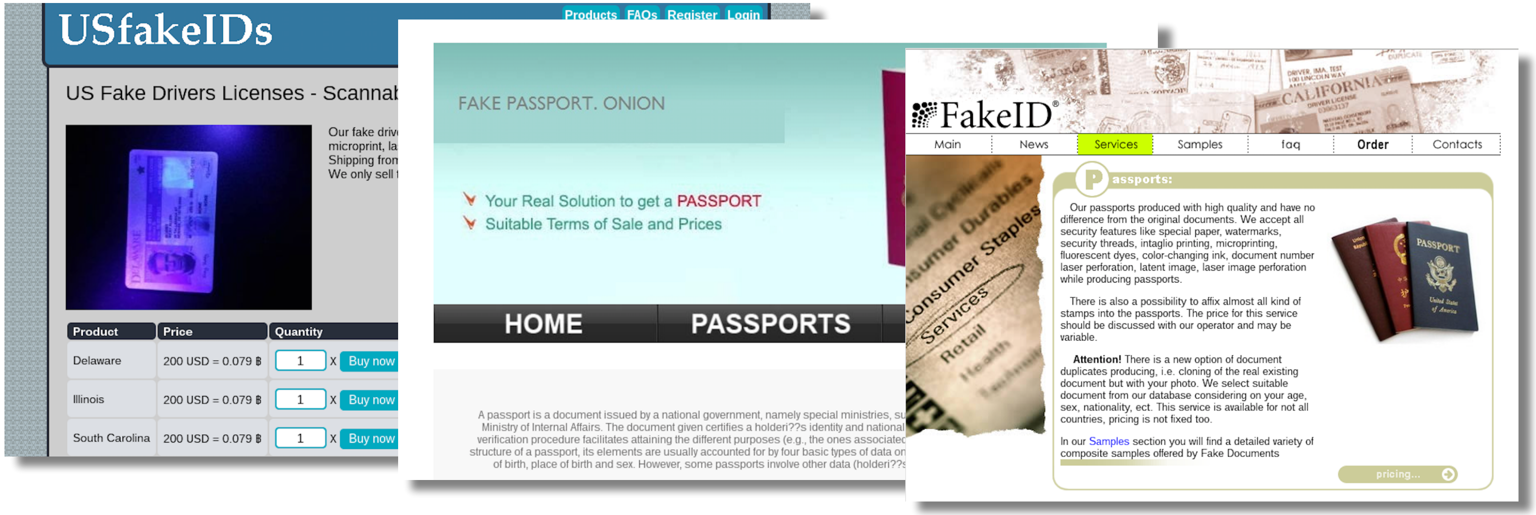
Establish consensus amongst stakeholders

- We should immediately start an action to secure
  - the trusted link between a MRTD and the document holder
  - develop and deploy technical mechanisms
    that can detect a morph passport at borders.

Conclusion

We are facing

- Passports with morphed face images are already in circulation
  - 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 global border security
- In combination with passport brokers a dramatic problem
  - the darknet offers numerous such opportunities:



US Fake Drivers Licenses - Scannab

Our fake driv
microprint, la
Shipping from
We only sell t

Product	Price	Quantity
Delaware	200 USD = 0.079 ฿	1 x Buy now
Illinois	200 USD = 0.079 ฿	1 x Buy now
South Carolina	200 USD = 0.079 ฿	1 x Buy now

- Your Real Solution to get a PASSPORT
- Suitable Terms of Sale and Prices

A passport is a document issued by a national government, namely special ministries, su
Ministry of Internal Affairs. The document given certifies a holderi??s identity and national
verification procedure facilitates attaining the different purposes (e.g., the ones associated
structure of a passport, its elements are usually accounted for by four basic types of data on
of birth, place of birth and sex. However, some passports involve other data (holderi??s

Our passports produced with high quality and have no difference from the original documents. We accept all security features like special paper, watermarks, security threads, intaglio printing, microprinting, fluorescent dyes, color-changing ink, document number laser perforation, latent image, laser image perforation while producing passports.

There is also a possibility to affix almost all kind of stamps into the passports. The price for this service should be discussed with our operator and may be variable.

Attention! There is a new option of document duplicates producing, i.e. cloning of the real existing document but with your photo. We select suitable document from our database considering on your age, sex, nationality, ect. This service is available for not all countries, pricing is not fixed too.

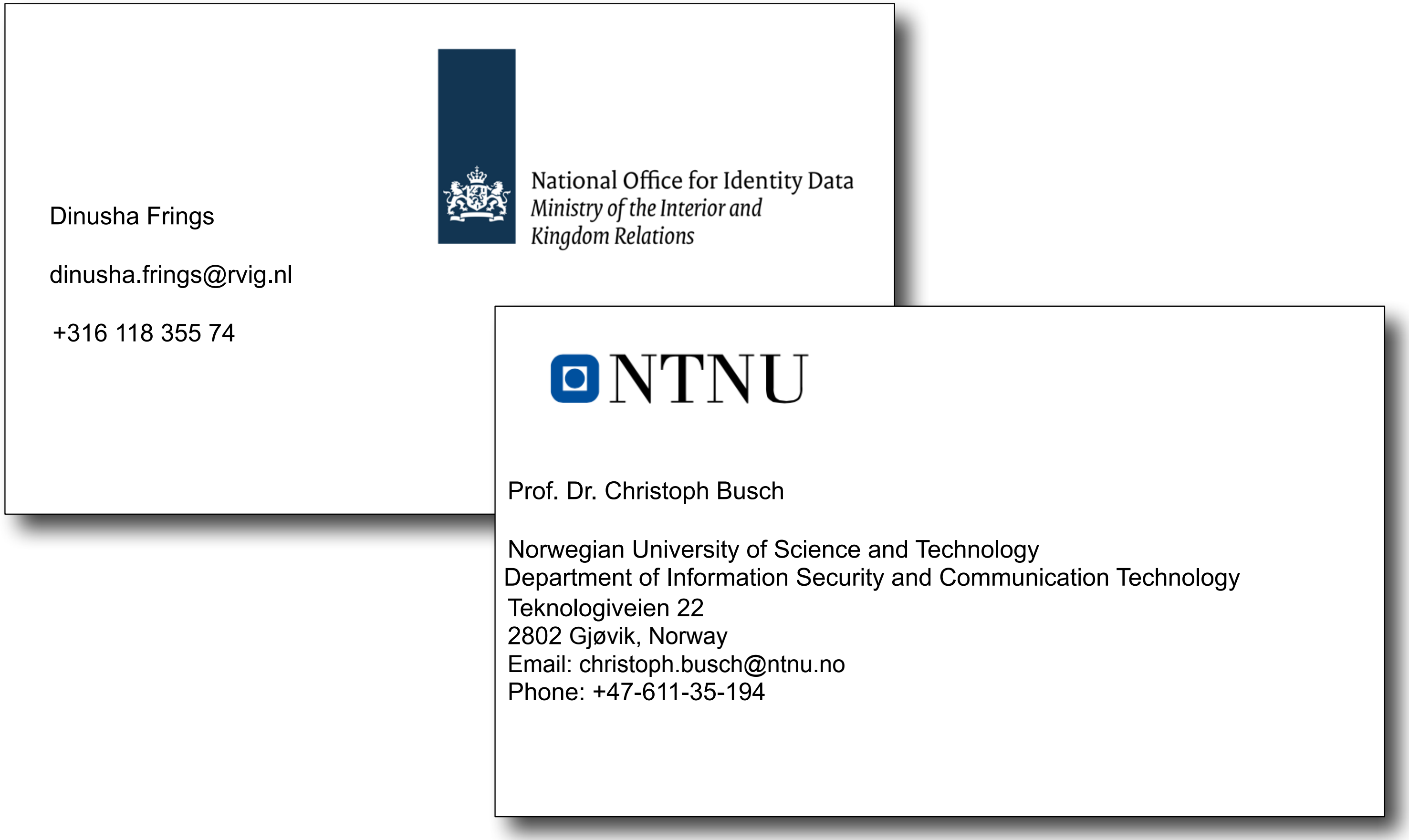
In our Samples section you will find a detailed variety of composite samples offered by Fake Documents

References

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

- S. Venkatesh, R. Raghavendra, K. Raja, L. Spreeuwers, R. Veldhuis, C. Busch: "Morphed Face Detection Based on Deep Color Residual Noise“, in Proceedings of the ninth International Conference on Image Processing Theory, Tools and Applications (IPTA 2019), Istanbul, Turkey, November 6-9, (2019)
- U. Scherhag, L. Debiasi, C. Rathgeb, C. Busch and A. Uhl: "Detection of Face Morphing Attacks based on PRNU Analysis“, in IEEE TBIOM, (2019)
- U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, C. Busch: "Face Recognition Systems und Morphing Attacks: A Survey“, in IEEE Access, (2019)
- R.Raghavendra, S. Venkatesh, K. Raja, C. Busch: "Towards making Morphing Attack Detection robust using hybrid Scale-Space Colour Texture Features“, in Proceedings of 5th International Conference on Identity, Security and Behaviour Analysis (ISBA 2019), Hyderabad, IN, January 22-24, (2019)
- L. Debiasi, C. Rathgeb, U. Scherhag, A. Uhl, C. Busch: "PRNU Variance Analysis for Morphed Face Image Detection“, in Proceedings of 9th International Conference on Biometrics: Theory, Applications and Systems (BTAS 2018), Los Angeles, US, October 22-25, (2018)
- R.Raghavendra, S. Venkatesh, K. Raja, C. Busch: "Detecting Face Morphing Attacks with Collaborative Representation of Steerable Scale-Space Features“, in Proceedings of 3rd International Conference on Computer Vision and Image Processing (CVIP 2018), Japalpur, IN, September 29 - October 1, (2018)
- U. Scherhag, D. Budhrani, M. Gomez-Barrero, C. Busch: "Detecting Morphed Face Images Using Facial Landmarks“, in Proceedings of International Conference on Image and Signal Processing (ICISP 2018), Cherbourg, FR, July 2-4, (2018)
- U. Scherhag, C. Rathgeb, C. Busch: "Performance Variation of Morphed Face Image Detection Algorithms across different Datasets“, in Proceedings of 6th International Workshop on Biometrics and Forensics (IWBF 2018), Sassari, IT, June 7-8, (2018)
- L. Debiasi, U. Scherhag, C. Rathgeb, A. Uhl, C. Busch: "PRNU-based Detection of Morphed Face Images“, in Proceedings of 6th International Workshop on Biometrics and Forensics (IWBF 2018), Sassari, IT, June 7-8, (2018)
- U. Scherhag, C. Rathgeb, C. Busch: „Detection of Morphed Faces from Single Images: a Multi-Algorithm Fusion Approach“, in Proceedings if of the 2nd International Conference on Biometric Engineering and Applications (ICBEA 2018), Amsterdam, The Netherlands, May 16-18, (2018)
- U. Scherhag, C. Rathgeb and C. Busch: „Towards Detection of Morphed Face Images in electronic Travel Documents“, in Proceedings of the 13th IAPR International Workshop on Document Analysis Systems (DAS 2018), Vienna, Austria, April 24-27, (2018)
- M. Gomez-Barrero, C. Rathgeb, U. Scherhag, C. Busch: „Predicting the Vulnerability of Biometric Systems to Attacks based on Morphed Biometric Samples“, in IET Biometrics, (2018)
- C. Rathgeb, C. Busch: "On the Feasibility of Creating Morphed Iris-Codes", in Proceedings of International Joint Conference on Biometrics (IJCB 2017), Denver, Colorado, October 1-4, (2017)
- R. Raghavendra, K. Raja, S. Venkatesh, C. Busch: "Face Morphing Versus Face Averaging: Vulnerability and Detection", in Proceedings of International Joint Conference on Biometrics (IJCB 2017), Denver, Colorado, October 1-4, (2017)
- U. Scherhag, A. Nautsch, C. Rathgeb, M. Gomez-Barrero, R. Veldhuis, L. Spreeuwers, M. Schils, D. Maltoni, P. Grother, S. Marcel, R. Breithaupt, R. Raghavendra, C. Busch: "Biometric Systems under Morphing Attacks: Assessment of Morphing Techniques and Vulnerability Reporting", in Proceedings of the IEEE 16th International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, September 20-22, (2017)
- R. Raghavendra, K. Raja, S. Venkatesh, C. Busch: "Transferable Deep-CNN features for detecting digital and print-scanned morphed face images", in Proceedings of 30th International Conference on Computer Vision and Pattern Recognition Workshop (CVPRW 2017), Honolulu, Hawaii, July 21-26, (2017)
- M. Gomez-Barrero, C. Rathgeb, U. Scherhag, C. Busch: "Is Your Biometric System Robust to Morphing Attacks?", in Proceedings of 5th International Workshop on Biometrics and Forensics (IWBF 2017), Coventry, UK, April 4-5, (2017)
- U. Scherhag, R. Raghavendra, K. Raja, M. Gomez-Barrero, C. Rathgeb, C. Busch: "On The Vulnerability Of Face Recognition Systems Towards Morphed Face Attacks", in Proceedings of 5th International Workshop on Biometrics and Forensics (IWBF 2017), Coventry, UK, April 4-5, (2017)
- R. Raghavendra, K. Raja, C. Busch: "Detecting Morphed Facial Images", in Proceedings of 8th IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS-2016), September 6-9, Niagra Falls, USA, (2016)

Contact



National Office for Identity Data
Ministry of the Interior and
Kingdom Relations

Dinusha Frings

dinusha.frings@rvig.nl

+316 118 355 74

NTNU

Prof. Dr. Christoph Busch

Norwegian University of Science and Technology
Department of Information Security and Communication Technology
Teknologiveien 22
2802 Gjøvik, Norway
Email: christoph.busch@ntnu.no
Phone: +47-611-35-194