The Challenge of Morphing for Border Control

[redacted]

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

Frontex, October 9, 2019

CRISP
Center for Research in Security and Privacy

European Association for Biometrics
eab
Human Identity in Europe

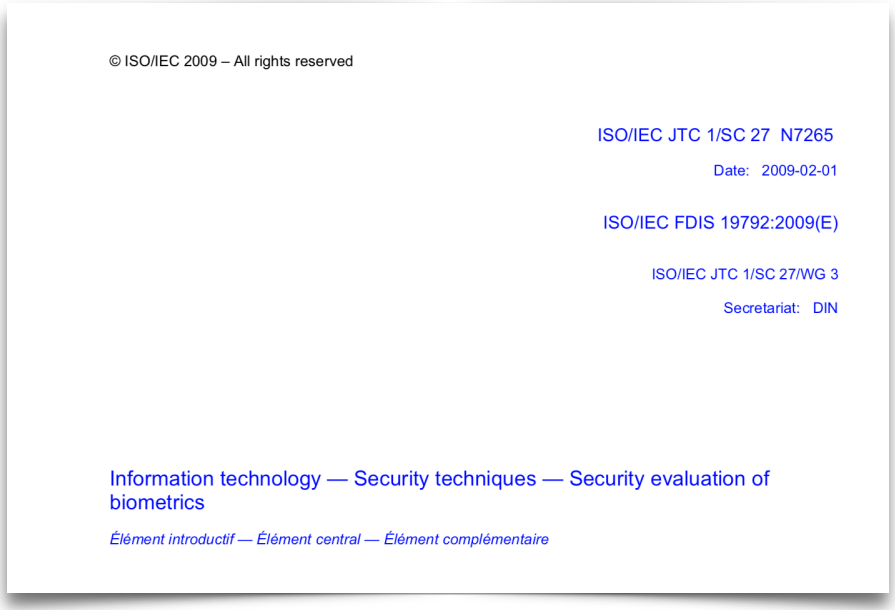
History - 2009

Face Morphing

- The morphing attack was named and classified as vulnerability of a biometric system in Clause 8.3.8.1 of ISO/IEC FDIS 19792:
  - *"… Examples of abnormal characteristics could include those with unusually large or small numbers of features. Such characteristics may not be representative of any human biometric characteristic but could be synthesised and copied to an artefact. Alternatively a synthesised characteristic could be injected electrically during a replay attack or planted in the reference database.*

    ….

    - feature sets comprising amalgamations of biometric features from 2 or more individuals, e.g. morphed facial images"



ISO/IEC JTC 1/SC 27 N7265

Date: 2009-02-01

ISO/IEC FDIS 19792:2009(E)

ISO/IEC JTC 1/SC 27/WG 3

Secretariat: DIN

Information technology — Security techniques — Security evaluation of biometrics

Élément introductif — Élément central — Élément complémentaire

History - 2014

Integrated Project FIDELITY

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

- Fast and trustworthy Identity Delivery and check with ePassports leveraging Traveler privacy
- 4 years project (2012-2016)
  - European 7th Framework Programme
- Objectives:
  - To improve the ePassport issuing process
    - Security of birth certificates and other evidence of identity
    - Quality of biometric data in the chip
    - One individual one passport (duplicate enrolment check)
  - To demonstrate solutions that enable faster and more secure and efficient real-time authentication of individuals at border crossing
  - To protect privacy of the travel document holders with a privacy-by-design approach.

Problem: Morphing Attacks

FIDELITY 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:
  - Photo studio should digitally sign the picture and send it to the passport application office (this is in progress for Finland)
  - Switch to live enrolment (that is the case for Norway and Sweden)
  - Software-supported detection of morphed face images

What needs to be done?

MAD Action Plan

1.) Establish consensus amongst stakeholders

- Europe should immediately start an action to secure
  - the trusted link between a MRTD and the document holder
  - and to develop and deploy technical mechanisms that can detect a morph passport at borders.
- Support the iMARS-consortium, that is ready to jointly work on the morphing challenges
  - iMARS = image Manipulation Attack Resolving Solutions (H2020 proposal)
  - The iMARS consortium consists of Idemia, NTNU, University Bologna, University Twente, Hochschule Darmstadt, University Leuven, Dutch National Office for Identity Data, German Bundeskriminalamt, Vision-Box, Cognitec, IBS, EAB and various end users (border control agencies)
  - iMARS is a pan-European approach that is supported by the European Association for Biometrics

MAD Action Plan

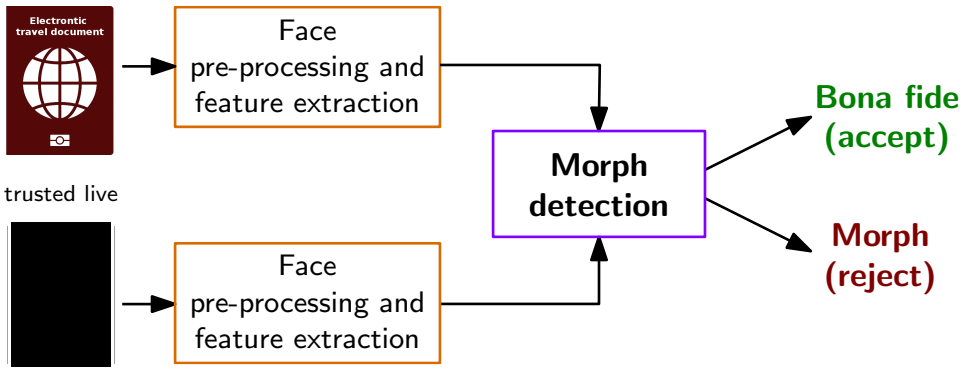
2.) Standardise the passport application process

- A European regulation should enforce that all Member States switch to live enrolment, as it is already operational e.g. in Norway and Sweden.
  - Only then, with full control of the biometric capture process by a civil servant in the passport application office, trust in the link of passport holder to reference data can be assured.
- The iMARS consortium has proposed to define a secure ID Document application process:
  - Make it difficult to apply for an ID document with a photograph that has been morphed or manipulated otherwise (e.g. data subjects want to look younger)
  - Take precautions to detect a case that someone tries to enrol with a well-crafted facemask (avoid a presentation attack with a morphed face image on the mask)
  - The capture device certification scheme will be recorded in the data record, as defined in the new extensible interchange format ISO/IEC 39794-5

MAD Action Plan

3.) Detect automatically Morph Passports at Borders

- After the completed transition to live enrolment in all MS we must anticipate that European passports - potentially containing a morphed image - are presented at least for the next 10 years.
  - iMARS consortium proposed efficient Morphing Attack Detection (MAD) solutions for border control points
  - Border control process based on a differential analysis, where the images stored on the ID document are compared with a trusted live image of the ID document holder, while the capture process is run under supervision.



- Explicit and implicit image pair detection algorithms

MAD Action Plan

4.) Detect Morph Passports in Forensic Investigations

- A forensic investigator has a single image only
- In support of forensic investigations, we need single image MAD
  - also known as no-reference MAD or forensic MAD
  - explicit MAD and implicit MAD with transfer learning
  - trained with large-scale face morph databases.
  - based on the relatively low-resolution digital image stored in the passport,
  - print and scan MAD robustness
  - fusion of multiple MAD subsystems.

MAD Action Plan

5.) Compose Test Data and Online Evaluation Platform

- Testing of MAD solution can't be done without appropriate data.
- Extend the SOTAMD database of 150 individuals and diversify
  - more subjects
  - more enrolment processes / print and scan equipment
  - more morphing tools
  - high AND controlled degrading quality
- Need for an iMARS mixed quality dataset
  - Minimizing image artefacts generated by morphing
  - Diversity in the morphing factor (also known as α factor)
- Augment the Bologna-Online-Evaluation-Platform (BOEP)
  - Provide open access benchmark tests.
  - Thus Frontex and the national border control agencies will be able to evaluate if the MAD State-of-the Art meets the operational requirements.
  - The technical interfaces are by design equivalent to the benchmark portal of the NIST Face Recognition Vendor Test (FRVT) MORPH Competition

MAD Action Plan

6.) Standardise Testing of MAD Solutions

- Find consensus, how we test
  - Measures for vulnerability and detection accuracy
- Morphing vulnerability metric based on the Mated-Morph-Presentation-Match-Rate (MMPMR)
  - anchor the MAD evaluation methodology in the ISO/IEC 30107 multipart standard
  - Find consensus in the MAD research community
- Standardise metrics to evaluate the performance of MAD methods
  - APCER and BPCER (and corresponding DET-Plots)
    - APCER - Attack Presentation Classification Error Rate
    - BPCER - Bona Fide Presentation Classification Error Rate
- Border control agencies of EU Member State shall be motivated by Frontex to participate in this standardisation process

MAD Action Plan

7.) Develop Face Image Quality Metrics

- We need the equivalent to NFIQ2.0 for facial images
- Ensure to capture samples that are sufficiently good in term of illumination, sharpness, or pose
- Align with the framework for biometric sample quality described in ISO/IEC 29794-1:2016
  - align with ISO/IEC NP 24357 and-or ISO/IEC 29794-5
- Develop an automatic face image quality assessment software,
  - which can predict recognition accuracy
  - provide actionable feedback to the data capture subject and/or to the operational personnel.
- Once predictive face quality software is available, MAD evaluation can be adapted to the three relevant scenarios (ID Document issuance, border control, and forensic investigation)
  - observe the impact of face image quality on morphing attack detection

MAD Action Plan

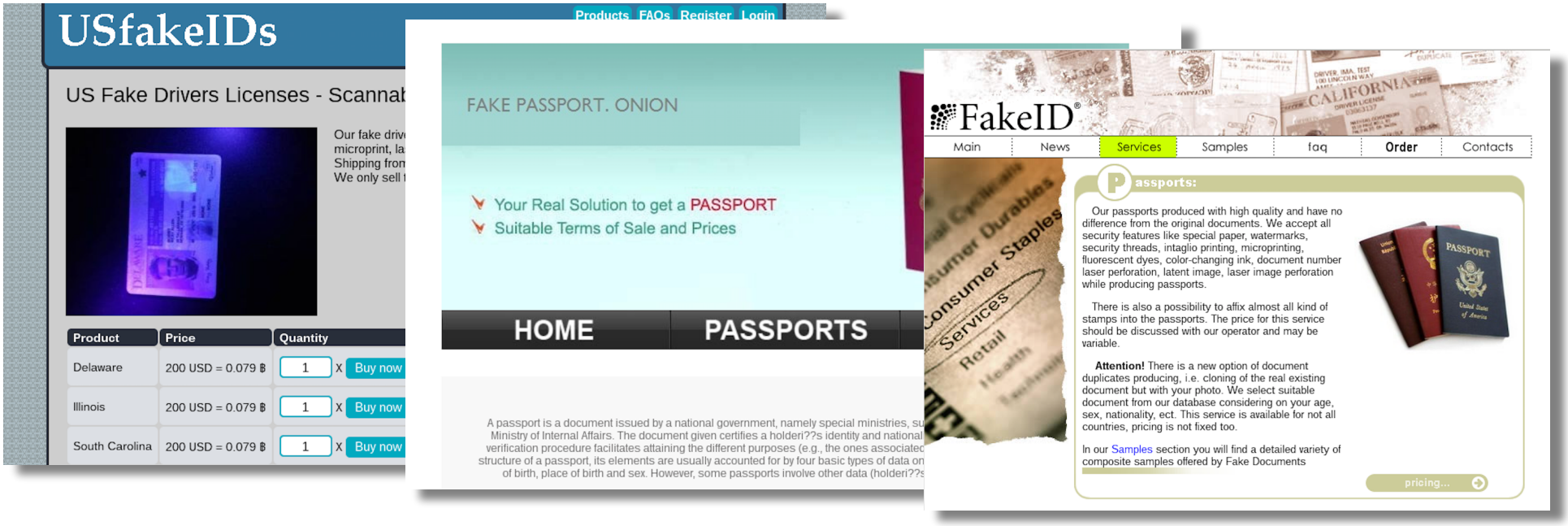
8.) Train operating Border Officers and Communication Personnel

- Train the agencies staff, how to react
- Develop best practices for improving the officers' skills on manipulated/morphed image and document fraud detection
  - design a training curriculum in interaction of Frontex and active researchers
  - show to border guards that the MAD tools will not replace, but complement, their expertise.
- Training of operators' communication personnel
  - to mitigate public excitement and explain attack resolving solutions against morphing attacks,
  - once the threat is reported in the media.

Conclusion

We are facing

- One of the most challenging research tasks
  - we have to assign this task to our best researchers,
    in order to get a decent solution for robust morphing attack detection algorithms
- Passports with morphs are already in circulation
  - Switch to live enrolment is a good decision, but does not solve the problem
- In combination with passport brokers a dramatic problem
  - the darknet offers numerous such opportunities:



Upcoming Events

Standardisation Week in January 2020

Upcoming ISO/IEC SC37 Working Group 3 meeting

- 20-24 July, 2020 in New Orleans, US
- Terms of Reference:
  - "To consider the standardisation of the content, meaning, and representation of biometric data formats. …"
- On the agenda:
  - The third generation:
    ISO/IEC IS CD 39794-5 Extensible biometric data interchange formats – Part 5: Face image data
  - Face Sample Quality: New standardization project
    - ISO/IEC NP 24357 and-or ISO/IEC 29794-5
- see: https://isotc.iso.org/livelink/livelink/open/jtc1sc37wg3

Darmstadt Biometric Week in September 2020

- 7th EAB research projects conference (EAB-RPC)
  - September 14-16, 2020 in Darmstadt, Germany
  - https://www.eab.org/events/program/151
- 19th IEEE BIOSIG conference
  - September 16-18, 2020 in Darmstadt, Germany
  - www.biosig.org/biosig-2020

Call for Papers

BIOSIG 2020

19th International Conference
of the Biometrics Special Interest Group

16.-18.09.2020, Darmstadt, Germany

http://www.biosig.de

Biometrics Special Interest Group in cooperation with IEEE

Fraunhofer IGD, CRISP

Biometrics provides efficient and reliable solutions to recognize individuals. With increasing number of identity theft and miss-use incidents we do observe a significant fraud in e-commerce and thus growing interests on trustworthiness of person authentication. Nowadays we find biometric applications in areas like border control, national ID cards, e-banking, e-commerce, e-health etc. Large-scale applications such as the European Union SmartBorder Concept, the Visa Information System (VIS) and Unique Identification (UID) in India require high accuracy and also reliability, interoperability, scalability and usability. Many of these are joint requirements also for forensic applications.
Multimodal biometrics combined with fusion techniques can improve recognition performance. Efficient searching or indexing methods can accelerate identification efficiency. Additionally, quality of captured biometric samples can strongly influence the performance. Moreover, mobile biometrics is an emerging area and biometrics based smartphones can support deployment and acceptance of biometric systems.
However, concerns about security and privacy cannot be neglected. The relevant techniques in the area of presentation attack detection (liveness detection) and template protection are about to supplement biometric systems, in order to improve fake resistance, prevent potential attacks such as cross matching, identity theft etc.
The BIOSIG 2019 conference addresses these issues and will present innovations and best practices that can be transferred into future applications. The conference is jointly organized by the Competence Center for Applied Security Technology (CAST), the German Federal Office for Information Security (BSI), the European Association for Biometrics (EAB), the Joint Research Centre of the European Commission (JRC), the TeleTrusT-Association, the Norwegian Biometrics Laboratory (NBL), the Center for Research in Security and Privacy (CRSIP), the Fraunhofer Institute for Computer Graphics Research IGD, IET Biometrics Journal and the special interest group BIOSIG of the Gesellschaft für Informatik e.V. (GI). The conference will be technically co-sponsored by IEEE and papers will be added to IEEE Xplore (approval pending).

We invite stakeholders and technical experts to submit original research papers. Industrial contributions presenting lessons learnt from practical usage, case study, recent results of prototypes, are also welcomed.

Important Dates

30.05.2020	Deadline for submissions
20.07.2020	Notification of authors via e-mail
20.08.2020	Deadline for final papers (ready for press)
14.09.2020	Satellite Workshop TTT Working Group
14.-16.09.2020	EAB-Research Project Conference
16.09.2020	EAB European Research and Industry Award
17./18.09.2020	Main Conference: Talks and Presentations

Invited Talks

T.B.A.

Special Interest Group BIOSIG

The BIOSIG Group is dedicated to the foundations of biometrics. Its objective is to to link practical experience with academic innovations. Thus the Special Interest Group BIOSIG together with its co-organizers is providing with its annual conference a suitable platform to work on these issues.

Topics of Interest

Topics of the conference include but are not limited to: Biometric standards and interoperability, multimodal and multi-biometrics, security analysis of biometric components or systems, on-card comparison, fake resistance, liveness detection, aging of reference data, template protection, de-identification, user interface design for biometric systems, biometric performance measurement, sample quality, best practices, usability, continuous authentication, forensics and other emerging applications, ethical, legal and socio-technological aspects, biometrics for public administrations.

Organizing Committee

General Chair: Christoph Busch
Program Chairs: Antitza Dantcheva, Christian Rathgeb, Kiran Raja, Andreas Uhl
Publication Chair: Arslan Brömme
Publicity Chair: Victor Philipp Busch
Local Chairs: Alexander Nouak, Claudia Prediger

EAB-RPC Conference 2020

European Association for Biometrics eab

European Association for Biometrics invites to the
7th Research Project Conference, September 14 to 16

Darmstadt, Germany

European Commission through DG Joint Research Centre teams-up again with the European Association for Biometrics (EAB) to organize the 7th edition of the EAB Research Projects Conference (EAB-RPC) focused on presenting the results of European biometric related projects. The conference is part of the Darmstadt Biometric Week running from September 14 to 18, 2020.

Based on the experiences from earlier conference editions you can expect the following:

- Learn about research currently conducted in approx. 20 European projects
- Find partners for you next research consortium
- Meet industry and start technology transfer
- Listen to operators and understand their needs for future research
- Discuss with stakeholders
- Meet with more than 200 biometricians attending the Darmstadt Biometric Week

For more information on EAB-RPC visit: https://www.eab.org/events/program/195
or contact the chairman: javier.galbally@ec.europa.eu

A **biometrician** is defined as: "individual being interested in biometrics either from a researchers, developers or operator's point of view"

@euro_biometrics

References

Publications available https://www. .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

Contact