Selected Chapters of IT-Security [ITSEC]:
Digital Image Forensics with the focus on Face Morphing Attack

Winter Term 2019/2020

Part 2: Topics

Prof. Dr. Jana Dittmann
Dipl.-Inf. Stefan Kiltz
supported by Dr. Andrey Makrushin (andrey.makrushin@ovgu.de)

Advanced Multimedia and Security Lab (AMSL)
Fakultät für Informatik
Otto-von-Guericke Universität Magdeburg
Magdeburg, Germany

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

AMSL Advanced Multimedia and Security Lab

Outline

(1) Face morphing detection as a one-class classification problem

(2) Face morphing detection based on dictionary learning

(3) Security analysis of the ANANAS infrastructure incl. the network of distributed face morphing detectors

(4) Improvement of the Android-App for verification of persons based on electronic documents (e.g. travel passport) incl. face morphing detection

(5) Analysis of the human experiment results focusing on the question: Does training improve an accuracy of manual face morphing detection?

(6) „Handcrafted“ features vs. features learned by an autoencoder with regard to face morphing detection

(7) Face morphing detection with and without a reference face image

(8) An integral approach (fusion) for identity verification based on document face images incl. compliance with the ICAO portrait quality standard and morphing detection

(9) Analysis of the DEFACTO morphing database

(10) Visual analysis of morphing detection features based on t-SNE projection onto a two-dimensional space

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

AMSL Advanced Multimedia and Security Lab

Topic 1: Face morphing detection as a one-class classification problem

- Consider face morphing detection as an anomaly detection problem with the only known class e.g. morphed face images
- Start literature research with the paper: P. Schlachter, Y. Liao, B. Yang „One-Class Feature Learning Using Intra-Class Splitting“, in Proc. EUSIPCO’19, Sept. 2-6, 2019, A Coruña, Spain
- 3 ETCS:
  - Propose an approach for splitting data to typical and atypical samples
  - Propose a suitable loss function for an autoencoder
  - Demonstrate the effectiveness of your approach based on a small set of given facial morphs
- 6 ETCS:
  + Quantitatively evaluate the proposed approach based on a large set of self-collected facial morphs (min. 1000 samples)

- Team: 2 Students
- Supervisor: Andrey Makrushin

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

AMSL Advanced Multimedia and Security Lab

Topic 2: Face morphing detection based on dictionary learning

- Apply dictionary learning for representing morphed face images enabling adaptive learning of new unknown types of facial morphing
- Start literature research with the paper: P. Irofti, A. Baltoiu „Malware Identification with Dictionary Learning“, in Proc. EUSIPCO’19, Sept. 2-6, 2019, A Coruña, Spain
- 3 ETCS:
  - Mapping from malware identification to morphing identification
  - Discuss possible features to distinguish genuine and morphed face images
  - Compare SVD and PCA based decomposition
  - Demonstrate the effectiveness of your approach based on a small set of given facial morphs
- 6 ETCS:
  + Quantitatively evaluate the proposed approach based on a large set of self-collected facial morphs (min. 1000 samples)

- Team: 2 Students
- Supervisor: Andrey Makrushin

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

AMSL Advanced Multimedia and Security Lab

Topic 3: Security analysis of the ANANAS infrastructure

- Check the ANANAS infrastructure for potential vulnerabilities
- Describe components using the entity model developed in R. Fischer, R. Clausing, J. Dittmann, Y. Ding “Industrie 4.0 Schwachstellen: Basisangriffe und Szenarien,” in Proc. D-A-CH Security 2016, Klagenfurt, Germany, pp. 350-362, 2016
- Apply measures of information security from the “BSI IT-Grundschutz” standard
- 3 ETCS:
  - Structure analysis, software inventory + revealing potential vulnerabilities
  - Security of RESTful webservices in general
  - Security of communication within the ANANAS infrastructure, assessment of the IT-Security-Aspects
  - Privacy within the entire architecture, residual risks
  - Objectives for logging and assessment whether the implemented logging facilities suffice for these goals
- 6 ETCS:
  - \+ Source code analysis
  - \+ Develop a strategy for the maintenance and sustainable operation of the ANANAS infrastructure

- Team: 2 Students
- Supervisors: Andrey Makrushin, Mario Hildebrandt

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

AMSL Advanced Multimedia and Security Lab

Topic 4: Improvement of the Android-App

- Study the identity verification process at Automated Border Control (ABC) gates
- Study the requirements to biometric portraits (ICAO standard) stored in electronic documents (e.g. travel passport)
- Reveal the vulnerabilities and potential attacks on ABC, start a literature research with the paper: M. Ferrara et al. “The magic passport”, in Proc. IJCB’14, Clearwater, FL, 2014, pp. 1-7
- Improve an Android App for simulation of ABC incl. face morphing detection
- The functionality should be similar to the InnoValor ReadID – NFC Passport Reader
- 3 ETCS:
  - Analyze the existing App and list the advantages and disadvantages
  - Improve the user interface
- 6 ETCS:
  + Re-implement
    - Taking and processing a photograph
    - Reading data from a chip (NFC), see http://www.jmrtd.org/
    - Request webservices for face matching and morphing detection

- Team: 2 Students
- Supervisor: Andrey Makrushin

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

AMSL Advanced Multimedia and Security Lab

Topic 5: Analysis of the human experiment results

- Evaluate the results of a human experiment to answer the question: Does training improve an accuracy of manual face morphing detection?
- Start literature research with the paper: R. Kramer et al. “Face morphing attacks: Investigating detection with humans and computers”, Cognitive Research: Principles and Implications (2019) 4:28
- 3 ETCS:
  - Study records of the experiment and collect relevant data
  - Discuss decision process time
  - Discuss error rates
  - Compare the results with studies conducted by psychologists e.g. in D.J. Robertson et al. “Detecting morphed passport photos: a training and individual differences approach”, Cognitive Research: Principles and Implications (2018) 3:27
- 6 ETCS:
  + Create new images/videos for the experiment
  + Run an experiment with a new data, collect, analyze and discuss test results

- Team: 2 Students
- Supervisor: Andrey Makrushin

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

AMSL Advanced Multimedia and Security Lab

Topic 6: „Handcrafted“ features vs. features learned by an autoencoder

- Study whether features learned by an autoencoder perform better than „Handcrafted“ features applied to face morphing detection
- Start literature research with the paper: A. Bhattad, J. Rock, D. Forsyth „Detecting Anomalous Faces with 'No Peeking' Autoencoders“, arXiv:1802.05798 [cs.CV]
- 3 ETCS:
  - Compare autoencoder to other dimensionality reduction approaches
  - Study and discuss possible loss functions
  - Study and discuss image similarity metrics
- 6 ETCS:
  + Implement and evaluate an autoencoder with a self-collected data (min. 1000 genuine/morphed samples)

- Team: 2 Students
- Supervisor: Andrey Makrushin

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

AMSL Advanced Multimedia and Security Lab

Topic 7: Face morphing detection with and without a reference face image

- Describe the limits of the blind morphing detection and investigate the morphing detection techniques with a reference face image; discuss pros and cons of both approaches
- Start literature research with the paper: Fei Peng, Le-Bing Zhang, Min Long „FD-GAN: Face De-Morphing Generative Adversarial Network for Restoring Accomplice's Facial Image", IEEE Access 2019
- 3 ETCS:
  - Compare a GAN-based approach with the approach of Ferrara et al. "Face Demorphing" IEEE Trans. on Information Forensics and Security 13 (2018): 1008-1017.
  - Evaluate an existing implementation (python/keras) with a given data
- 6 ETCS:
  - \+ Improve an existing implementation and evaluate it with a self-collected data (min. 1000 genuine/morphed samples)

- Team: 2 Students
- Supervisor: Andrey Makrushin

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

AMSL Advanced Multimedia and Security Lab

Topic 8: Fusion of identity verification and morphing detection

- Discuss scenarios and procedures which include identity verification based on a document face image
- Discuss how identity verification can be coupled with morphing detection
- Start literature research with the paper: C. Kraetzer, A. Makrushin, T. Neubert, M. Hildebrandt, J. Dittmann „Modeling Attacks on Photo-ID Documents and Applying Media Forensics for the Detection of Facial Morphing“, in Proc. IH&MMSec'17, June 20-22, 2017, Philadelphia, PA, USA
- 3 ETCS:
  - Propose a fusion approach for face morphing detection with and without a reference image and identity verification
  - Evaluate trivial fusion strategies based on the given detectors (ANANAS web services) and image data
- 6 ETCS:
  + Implement some selected components of the proposed fusion approach and evaluate it with a self-collected data (min. 1000 genuine/morphed samples)

- Team: 2 Students
- Supervisor: Andrey Makrushin

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

AMSL Advanced Multimedia and Security Lab

Topic 9: DEFACTO morphing database

- Analysis and classification of the existing approaches for generation of morphed face images
- Analysis of the DEFACTO morphing database described in G. Mahfoudi et al. “DEFACTO: Image and Face Manipulation Data”, in Proc. EUSIPCO’19, Sept. 2-6, 2019, A Coruña, Spain
- 3 ETCS:
  - Generate morphed face images using the ANANAS web service based on the genuine images included in the DEFACTO database
  - Subjective visual comparison of the morphed images from the DEFACTO and ANANAS web service
- 6 ETCS:
  + Quantitative comparison of the morphed face images from the DEFACTO and ANANAS web service (min. 200 morphed samples)
    - Biometric quality
    - Forensic quality

- Team: 2 Students
- Supervisor: Andrey Makrushin

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

AMSL Advanced Multimedia and Security Lab

Topic 10: Visual analysis of morphing detection features

- Visualization of high-dimensional feature vectors in a two-dimensional space for qualitative evaluation of potential separability of genuine and morphed face images
- Start literature research with the paper: C. Seibold et al. “Visual Feature Space Analyses of Face Morphing Detectors” to appear in Proc. WIFS’19, December 9-12, 2019, Delft, Netherlands
- 3 ETCS:
  - Compare different visualization approaches with each other
  - Compare visualization approaches with dimensionality reduction approaches
  - Apply t-SNE visualization to the given feature vectors
- 6 ETCS:
  + Generate feature vectors using ANANAS web services from a self-collected face images (min. 1000 genuine/morphed samples) and apply t-SNE visualization to the generated feature vectors

- Team: 2 Students
- Supervisor: Andrey Makrushin