Advanced Seminar / Masterseminar WS 2020/21

Term Paper Topics

C. Rathgeb, P. Drozdowski, J. Priesnitz

2020–30–10

1 Face recognition for Doppelgängers

Lookalikes may cause false positives in face recognition system. However, this has not yet been investigated in depth in the scientific literature. The goal of this project is to collect a face image database of subjects and their doppelgängers and to evaluate how face recognition systems are impacted by them.

1.1 Task

- Practical
  - Create a database with face image pairs of subjects and their doppelgängers.
  - Perform evaluation using different face recognition systems.
  - Compute score distribution histograms, equal error rate (EER) and detection error tradeoff (DET) curves.
- Paper
  - Report the results from the practical part
  - The paper ought to be self-contained, i.e. in addition to the above, ought to contain sections such as: general topic introduction, related work, experimental setup description and results, discussion, conclusions, etc., but the focus should be on the experimental evaluation.

1.2 Starting Material

- Code
  - Face recognition systems
  - DET curve software
- Literature

- ISO/IEC 19795-1:2006 “Information technology – Biometric performance testing and reporting – Part 1: Principles and framework”
- ISO/IEC 2382-37:2017 “Information technology – Vocabulary – Part 37: Biometrics”

This topic is als suitable for a survey paper.

2 Face spoofing with masks

Medical masks have been shown to affect the performance of face recognition systems as they hide parts of the face. The goal of this project is to investigate whether masks could be used to spoof face recognition systems. The idea would be to test the impact of face images with synthetically generated face masks on face recognition systems. Generated masks should contain patterns which are created to fool the face recognition system.

2.1 Task

- Practical
  - Create a database with synthetic face masks for spoofing.
  - Perform evaluation using different face recognition systems.
  - Compute score distribution histograms, conduct vulnerability analysis.
- Paper
  - Report the results from the practical part
  - The paper ought to be self-contained, i.e. in addition to the above, ought to contain sections such as: general topic introduction, related work, experimental setup description and results, discussion, conclusions, etc., but the focus should be on the experimental evaluation.

2.2 Starting Material

- Code
  - Face recognition systems
  - DET curve software
- Literature
  - Damer *et al.* “The Effect of Wearing a Mask on Face Recognition Performance: an Exploratory Study”
  - NISTIR 8311 - Ongoing FRVT Part 6A: Face recognition accuracy with face masks using pre-COVID-19 algorithms
  - ISO/IEC 2382-37:2017 “Information technology – Vocabulary – Part 37: Biometrics”

3 Face spoofing in eLearning platforms

In an eLearning system a user may present an identity proof containing biometric data, e.g. identity document, at enrolment. The presented identity proof may be verified and its biometric reference data is captured remotely. During authentication identity verification is performed by comparing the reference against a simultaneously captured probe. The goal of this work would be to test whether a face recognition could be fooled by presenting a fake identity document containing a morphed face image.

3.1 Task

- Practical
    - Create a database with morphing attacks in elearning systems.
    - Perform evaluation using different face recognition systems.
    - Compute score distribution histograms, conduct vulnerability analysis.
- Paper
    - Report the results from the practical part
    - The paper ought to be self-contained, i.e. in addition to the above, ought to contain sections such as: general topic introduction, related work, experimental setup description and results, discussion, conclusions, etc., but the focus should be on the experimental evaluation.

3.2 Starting Material

- Code
    - Face recognition systems
    - Morphing software
    - DET curve software
- Literature
    - Scherhag *et al.* “Face Recognition Systems Under Morphing Attacks: A Survey”
    - ISO/IEC 30107-1:2016 “Information Technology – Biometric presentation attack detection – Part 1: Framework”
    - ISO/IEC 2382-37:2017 “Information technology – Vocabulary – Part 37: Biometrics”

4 Attacking privacy-preserving face recognition

Different research groups have proposed privacy-preserving face representations. Usually, simple machine learning-based classifiers for demographic attributes are incorporated in the learning process. The resulting face representation are claimed to hide demographic attributes, e.g. gender. However, such schemes might be attacked by analysing score distributions as false positive usually appear for subjects with same demographics. The goal of this work would be to launch attacks on such schemes for which feature vectors are available.

4.1 Task

- Practical
  - Conceptual design of attack methods.
  - Perform attack on different existing privacy-enhancing face representations.
  - Compute score distribution histograms, conduct vulnerability analysis.
- Paper
  - Report the results from the practical part
  - The paper ought to be self-contained, i.e. in addition to the above, ought to contain sections such as: general topic introduction, related work, experimental setup description and results, discussion, conclusions, etc., but the focus should be on the experimental evaluation.

4.2 Starting Material

- Biometric data
  - Protected templates of different algorithms
- Literature
  - Morales *et al.* "SensitiveNets: Learning Agnostic Representations with Application to Face Images"
  - Terhrst *et al.* "PE-MIU: A Training-Free Privacy-Enhancing Face Recognition Approach Based on Minimum Information Units"
  - ISO/IEC 19795-1:2006 "Information technology – Biometric performance testing and reporting – Part 1: Principles and framework"
  - ISO/IEC 2382-37:2017 "Information technology – Vocabulary – Part 37: Biometrics"

5 Demographic bias in face morphing attacks

Systemic biases inherent to several facial biometrics systems have recently been reported. In this context, a biased algorithm produces statistically different outcomes for different demographic groups of individuals. Morphing techniques can be used to create artificial biometric samples, which resemble the biometric information of two (or more) individuals in image and feature domain, thus having significant implications for the security of operational biometric systems. This project combines the two areas described above with the goal of investigating the impact of demographic factors on the efficacy of facial morphing attacks.

5.1 Task

- Practical
  - Create several databases with morphing attacks where the data subjects to be morphed are selected based on demographic criteria.
  - Perform evaluation using different face recognition systems.
  - Compute score distribution histograms, conduct vulnerability assessment, and analyse statistically the impact of demographics.
- Paper
  - Report the results from the practical part.
  - The paper ought to be self-contained, i.e. in addition to the above, ought to contain sections such as: general topic introduction, related work, experimental setup description and results, discussion, conclusions, etc., but the focus should be on the experimental evaluation.

5.2 Starting Material

- Code and images
  - Facial images with demographic annotations
  - Face recognition systems
  - Morphing software
- Literature
  - Scherhag *et al.* “Face Recognition Systems Under Morphing Attacks: A Survey”
  - Drozdowski *et al.* “Demographic Bias in Biometrics: A Survey on an Emerging Challenge”
  - ISO/IEC 30107-1:2016 “Information Technology – Biometric presentation attack detection – Part 1: Framework”
  - ISO/IEC 2382-37:2017 “Information technology – Vocabulary – Part 37: Biometrics”

6 Make-up attacks on facial recognition systems

Facial cosmetics have the ability to substantially alter the facial appearance, which can negatively affect the decisions of face recognition systems. In addition, it was recently shown that the application of make-up can be abused to launch so-called make-up presentation attacks. In such attacks, the attacker might apply heavy make-up in order to conceal their identity or even to achieve the facial appearance of a target subject for the purpose of impersonation.

6.1 Task

- Practical
  - Collect a dataset of specific types of make-up images (concealment and impersonation) by extracting images from high resolution online sources (e.g. artists' websites, YouTube videos, Instagram feeds).
  - Perform evaluation using different face recognition systems.
  - Compute score distribution histograms, equal error rate (EER), and detection error tradeoff (DET) curves.
- Paper
  - Report the results from the practical part.
  - The paper ought to be self-contained, i.e. in addition to the above, ought to contain sections such as: general topic introduction, related work, experimental setup description and results, discussion, conclusions, etc., but the focus should be on the experimental evaluation.

6.2 Starting Material

- Code
  - Face recognition systems
  - DET curve software
- Literature
  - Rathgeb *et al.* "Impact and Detection of Facial Beautification in Face Recognition: An Overview"
  - Rathgeb *et al.* "Detection of Makeup Presentation Attacks based on Deep Face Representations" (sections 1 and 2)
  - ISO/IEC 30107-1:2016 "Information Technology – Biometric presentation attack detection – Part 1: Framework"
  - ISO/IEC 2382-37:2017 "Information technology – Vocabulary – Part 37: Biometrics"

7 Mobile Touchless Fingerprint Presentation Attack Detection

Presentation attack detection refers to the detection of spoofed fingerprints e.g. with fake fingers or overlays. Touchless acquisition technologies are vulnerable to other presentation attacks, e.g. printed images, too. The goal of this topic is to propose and test new Presentation Attack Instruments especially for touchless sensors and to find countermeasures against them. In addition the implemented algorithms should be tested on a publicly available database.

7.1 Task

- Practical
  - Define presentation attack scenarios especial for touchless sensors
  - Implement countermeasures for the defined attacks
  - Test your countermeasures on your oen data and on a given database
- Paper
  - Description of your own dataset
  - Detailed description of the proposed implementation
  - Report the Bona fide Presentation Classification Error Rate (BPCER) and Attack Presentation Classification Error Rate (APCER)

7.2 Starting Material

- Biometric data
  - Touchless Sensor (Android smartphone + demonstrator app)
  - Biometric Database
- Literature
  - C. Stein *et al.*: ”Video-based fingerphoto recognition with anti-spoofing techniques with smartphone cameras.” 2013 International Conference of the BIOSIG Special Interest Group (BIOSIG). IEEE, 2013.
  - A. Taneja *et al.* ”Fingerphoto spoofing in mobile devices: a preliminary study.” 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS). IEEE, 2016.
  - ISO/IEC 2382-37:2017 “Information technology – Vocabulary – Part 37: Biometrics”

This topic is also suitable for a survey paper.

8 Unknown Presentation Attack Detection for Touchless Fingerprint Recognition

Presentation attack detection refers to the detection of spoofed fingerprints e.g. with fake fingers or overlays. In a real world scenario presentation attacks shown to the sensor are not necessarily known. Kolberg et al. proposed a method to detect unknown presentation attacks on touch based fingerprints using covolutional autoencoders. The goal is to transfer this approach into the touchless domain.

8.1 Task

- Practical
  - Implement and refine a given convolutional autoencoders
  - Apply the refined algorithm to a touchless fingerprint database
  - Capture a new dataset of touchless presentation attacks using fake fingers and overlays
  - Test your implementation on your own dataset
- Paper
  - Describe your adaptations of the convolutional autoencode
  - Report the capturing process of presentation attack database
  - Report the presentation attack detection performance in terms of APCER and BPCER

8.2 Starting Material

- Biometric data
  - Biometric Database
  - Autoencoder resources
- Literature
  - J. Kolberg *et al.* "Anomaly Detection with Convolutional Autoencoders for Fingerprint Presentation Attack Detection" arXiv preprint 2020
  - A. Taneja *et al.* "Fingerphoto spoofing in mobile devices: a preliminary study." 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS). IEEE, 2016
  - ISO/IEC 2382-37:2017 "Information technology – Vocabulary – Part 37: Biometrics"

9 Touchless Fingerprint Enhancement in the Gabor Spectrum

The processing for touchless finger images is much more critical compared to touch based technologies because of environmental influences. Sisodia, et al. proposed a post-processing of segmented fingerprint images using the Gabor spectrum. The goal of this topic is to implement a Gabor Filter based enhancement scheme for a given database and to test this method.

9.1 Task

- Practical
  - Implement a fingerprint enhancement scheme using the Gabor spectrum
  - Test different enhancement parameters (e.g. block size) on a given database
- Paper
  - Detailed description of the implemented method
  - Report the biometric performance compared to a baseline approach

9.2 Starting Material

- Biometric data
  - Pre-segmented touchless fingerprint database
  - Baseline approach
  - Test framework (Python)
  - DET curve software
- Literature
  - Sisodia *et al.*: "A conglomerate technique for finger print recognition using phone camera captured images" IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI). 2017.
  - ISO/IEC 2382-37:2017 "Information technology – Vocabulary – Part 37: Biometrics"

10 Deformation Correction for Touchless Fingerprints

Interoperability between touchless and touch based fingerprints is crucial for the success of touchless fingerprint technologies. Lin and Kumar suggest and deformation correction method based on Robust thin-plate spline (RTPS). This topic focuses on the re-evaluation of this approach on different databases.

10.1 Task

- Practical
  - Implement and adapt the deformation correction scheme of Lin and Kumar
  - Apply the implementation to touchless fingerprint databases
- Paper
  - Report your deformation correction method
  - Report the biometric performance before and after the deformation correction

10.2 Starting Material

- Biometric data
  - Two touchless fingerprint data sets
  - DET curve software
- Literature
  - Lin and Kumar: "Matching Contactless and Contact-Based Conventional Fingerprint Images for Biometrics Identification". 2018
  - ISO/IEC 2382-37:2017 "Information technology – Vocabulary – Part 37: Biometrics"

This topic is also suitable for a survey paper.