Advanced Seminar / Masterseminar WS 2019/20

Term Paper Topics

C. Rathgeb, P. Drozdowski, J. Priesnitz

2019–10–17

1 Bias in Face Recognition

In recent years, the possibility of systemic biases inherent to several automated decisions systems (including biometrics) have been reported and debated. In this context, different outcomes (decisions) for different groups (e.g. based on sex, age, and ethnicity) of individuals are generated by a biased algorithm. The biases can occur and propagate through multiple stages of the data processing pipelines. Often, they are not explicitly designed for, but rather occur implicitly. This matter presents a challenge associated with automated decision systems (including biometrics) at the intersection of technology, ethics, and legislation.

1.1 Task

- Practical
  - Conduct a literature survey on the existence and mitigation/prevention of bias in facial biometrics.
- Paper
  - A comprehensive state-of-the-art survey with bibliography (using primary literature sources) of studies on bias in facial biometrics (including e.g. recognition, classification, and quality estimation algorithms)
  - A survey and discussion (using primary or secondary literature sources) of bias mitigation or avoidance in automated decision systems with focus on biometrics
  - Discussion (using primary or secondary literature sources) of the open problems and future research perspectives in the area, as well as potential consequences of algorithmic biases in operational real-world biometrics applications

1.2 Starting Material

- Literature
  - Klare et al.: "Face Recognition Performance: Role of Demographic Information"
  - Phillips et al: "An other-race effect for face recognition algorithm"
  - Buolamwini and Gebru: "Gender shades: Intersectional accuracy disparities in commercial gender classification"
  - Danks and London: "Algorithmic Bias in Autonomous Systems"

2 Anonymisation in Face Recognition

In recent years, privacy has arisen as a major concern associated with biometric systems. Obscuring or anonymising faces in images and videos is one option, which can be used to protect privacy, while retaining certain level of visual coherence/intelligibility of the image.

2.1 Task

- Practical
  - Conduct a literature survey on anonymisation and de-anonymisation methods for facial images.
- Paper
  - A comprehensive state-of-the-art survey (with bibliography) of methods and existing open-source software for anonymisation and de-anonymisation of facial images
  - Qualitative and quantitative discussion of capabilities, and strengths and weaknesses of the surveyed approaches
  - Discussion of the open problems and future research perspectives in the area

2.2 Starting Material

- Literature
  - Ruchaud and Dugelay: "Automatic Face Anonymization in Visual Data: Are we really well protected?"
  - Ren et al.: "Learning to Anonymize Faces for Privacy Preserving Action Detection"

3 Partial Face Recognition

Partial face images frequently occur in unconstrained (in-the-wild) scenarios, such as video surveillance and mobile devices. The holistic facial recognition methods developed in the recent years achieve impressive recognition results. However, the recognition of arbitrary patches from facial images presents an arguably more difficult challenge, which is highly relevant in certain practical applications.

3.1 Task

- Practical
  - Conduct a literature survey on recognition methods using partial facial images.
- Paper
  - A comprehensive state-of-the-art survey (with bibliography) of methods for partial face recognition
  - Qualitative and quantitative discussion of capabilities, and strengths and weaknesses of the surveyed approaches
  - Discussion of the open problems and future research perspectives in the area

3.2 Starting Material

- Literature
  - He et al. "Dynamic Feature Learning for Partial Face Recognition"
  - Liao et al. "Partial Face Recognition: Alignment-Free Approach"

4 Impact of Facial Tattoos on Face Recognition

These days, many people have tattoos done on various body part including the face. Such tattoos which clearly affect their appearance and are expected to have an impact on face recognition systems. As current state-of-the-art face recognition systems have been show to generalize very well it is of interest whether they are able to compensate for changes in facial appearance caused by tattoos. The goal of this project is to evaluate said scenario by developing an according face database and investigate the effect of facial tattoos on state-of-the-art face recognition systems.

4.1 Task

- Practical
  - Creation of face database of face images before/after tattoos
  - Evaluation of face recognition systems on the created database
- 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

- Code
  - FaceNet, ArcFace face recognition software
  - Face databases
  - 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"

5 Colorisation in Face Recognition

With the advent of DNNs, the performance of face recognition systems has skyrocketed. It has been shown that DNNs can be trained with large amounts of data to learn a face representation that is robust to the variations present in the training data. Further, it has been demonstrated that deep learning can also be used to colorize b/w images. In this work it should be investigated whether such methods could be used to improve the performance of state-of-the-art face recognition systems.

5.1 Task

- Practical
  - Creation of face database of face images before/after colorisation
  - Evaluation of face recognition systems on the created database
- 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
  - FaceNet, ArcFace face recognition software
  - Face databases
  - Colorisation software
  - DET curve software
- Literature
  - DeOldify: Colorizing and Restoring Old Images and Videos with Deep Learning
  - 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”

6 Fingerphoto Presentation Attack Detection

Specifically in unsupervised scenarios it is essential that fingerprint sensors can not be spoofed. Examples for such scenarios are mobile payment protocols. Thus an important aspect for the security of a biometric systems is its robustness to artefacts (e.g. fake fingerprints).

6.1 Task

- Practical
  - Implement at least two selected methods for presentation attacks in smartphone fingerphoto based biometrics
  - Implement at least two presentation attack detection scheme based on a given Android app
  - Capture a little data set of bona fide fingerphotos an presentation attacks
  - Report the APCER and BPCER your data set
- Paper
  - Conduct a survey for presentation attacks on smartphone touchless fingerprint capturing
  - Weight the actual risk of such presentation attacks
  - Evaluate how to prevent presentation attacks

6.2 Starting Material

- Code
  - Android App and smartphone
  - Presentation Attack Instruments (PAIs)
- Literature
  - Stein et al.: "Video-based fingerphoto recognition with anti-spoofing techniques with smartphone cameras"
  - Wasnik et al.: "Presentation Attack Detection for Smartphone Based Fingerphoto Recognition Using Second Order Local Structures"

7 Contrast Research on touchless Fingerprint Recognition under different Illuminants

In touchless fingerprint recognition the biometric performance of a captured sample highly depends on the illumination. In mobile scenarios the sample quality can be improved by a sophisticated illumination which is not achiavable by e.g. a flashlight of a smartphone.

7.1 Task

- Practical
  - Capture a little data set of finger photos under different illuminants
  - Find algorithms and parameters for finger segmentation and fingerphoto contrast enhancement
  - Compute the biometric performance the considered parameters
- Paper
  - Review the literature for suitable illumination colors
  - Evaluation of selected algortithms and parameters regarding segmentation and contrast enhancement
  - Report of biometric performance for different illuminants

7.2 Starting Material

- Code
  - Android App and external illumination
  - Framework for fingerprint feature extraction and comparison
- Literature
  - Wang et al. "Contrast Research on Full Finger Area Extraction Method of Touchless Fingerprint Images Under Different Illuminants"
  - Cheddad. "A new colour space for skin tone detection"