DOI: 10.1049/bme2.12051

The Institution of Engineering and Technology WILEY

EDITORIAL

Guest Editorial: WACV 2020—Presentation attacks on biometric systems

Despite recent developments in improving the performance of biometric systems for various applications, the systems are still vulnerable to different kind of attacks. Some such attacks are presentation attacks (PAs), where an adversary presents a fabricated artefact or an altered trait to biometric sensors. The intent is often to obfuscate one's own identity, create a synthetic identity, or spoof another person's identity. Typically observed attacks include but are not limited to printed attack, replay attack, makeup attack and 3D mask attack. To detect or deflect PAs on biometric systems, numerous presentation attack detection (PAD, a.k.a., anti-spoofing) schemes have been developed in the literature, which vary from sensor-based (e.g. RGB, depth and IR) to image-based solutions. With the massive use of techniques such as convolutional neural networks (CNNs) and generative adversarial networks (GANs), sophisticated PAs such as Deepfakes/re-enactment attacks have emerged. Recent advances in computer vision have made it possible to generate realistic morphed images that can compromise biometric systems and attack multiple identities simultaneously.

The need for effective countermeasures to be addressed to make them robust and reliable has been more than ever before. Several EU, national and international projects have started coordinated efforts to address some of the challenges. In addition, many open competitions and independent evaluations are being conducted to push the frontiers of suitable detecting mechanisms against such attacks. This special issue focusses on approaches for detecting PAs and morphing attacks on biometric systems. Four papers in this issue discuss in detail PAD, and three other papers focus on image manipulation attacks such as synthetic manipulation and recently uncovered morphing attacks. The papers discuss various aspects of attacks on biometrics systems, from devising detection approaches to illustrating the challenges of generalisability and explainability.

PAD ON BIOMETRIC SYSTEMS

Four high-quality papers have addressed different aspects of biometric PAs and PAD. Two of the presented papers addressed fingerprint PAD with a focus on the generalisability of the PAD approaches. The other two papers were concerned with face PAD with a focus on two interesting aspects. The first is the explainability of PAD decisions, and the other is the evaluation of the generalisation of PAD decisions.

González-Soler et al. target the issue of detecting fingerprint PAs of unknown (to the PAD) origins. This was perused by combining local and global information of several local feature descriptors, using the Fisher vector (FV) technique. The authors measured the impact of presentation attack instruments (PAIs) and fabrication materials on the PAD performance of a large set of handcrafted descriptors combined with FV. The presented results showed advances in terms of the generalisability of fingerprint PAD.

Kolberg et al. also targeted the generalisation of fingerprint PAD. The authors have evaluated 10 fingerprint PAD solutions in experimental setups specifically designed to assess the generalisability of the PAD performance. The evaluation data included 4339 PA samples of 45 different PAIs captured in the short-wave infrared domain. The results pointed out that the detectability of PAs (as unknown PAs) varies significantly depending on the nature of the PAIs. The authors also point out the variation in the generalisability of the different evaluated PAIs.

Sequeira et al. do not directly focus on the traditional goal of enhancing PAD performance, but rather on providing and studying the interpretability of PAD decisions. Sequeira et al. present an in-depth study of the interpretability of deep learning-based PAD decisions. The authors supported their study by measuring the differences between different explanations. They additionally analysed the stability of the decision explanation under known and unknown PAD experimental setups, stressing the need for diverse PAD training data.

Costa-Pazo et al. address a bridging effort between the academic-driven and the deployability-driven advances in face PAD. The authors analysed the generalisation problem in face PAD along with their evaluation strategies based on the aggregation of publicly available datasets. The authors proposed novel protocols addressing realistic deployment settings that include issues such as demographic bias. The paper presented a detailed categorisation of PAs and PAIs to enable a more realistic generalisation assessment of PADs. This all was presented as a modular framework that enables realistic evaluation of the performance and generalisation of face PAD.

IMAGE MANIPULATION DETECTION

Three papers have devoted their efforts to create manipulation dataset and image manipulation detection techniques. Novozamsky et al. present a large-scale dataset for visual content manipulation detection along with the baseline performance of the state-of-the-art forensic image manipulation detection methods. Batskos et al. and Ferrara et al. focus on face morphing attack detection using legacy passport and ID card face images and off-the-shelf CNNs in the presence of printing/scanning and heterogeneous image sources.

Novozamsky et al. assembled a large-scale annotated dataset, Extended IMD2020, which consists of more than 35,000 real and manipulated images for visual content manipulation detection. The manipulations such as copy–paste, splicing, and re-touching were introduced to the images. Furthermore, a random combination of image processing operations such as blurring, contrast manipulation, interpolation using bilinear and bicubic kernels, along with GANs, were used for image manipulation. The baseline performance of five image forensic manipulation detection methods, namely NOI1, CFA1, BLK, ADQ1 and ManTraNet, is also provided to further research the detection of manipulated visual content detection.

Batskos et al. identify and analyse security vulnerabilities due to morphing attacks. The authors further propose a verification solution that utilises the legacy images from the passport and ID card to prevent successful comparison against morphing attacks. The authors created an in-house dataset of 50 individuals, and commercial Cognitec FaceVACS SDK was used for the experimental evaluations. Results suggest the efficacy of legacy images in preventing morphing attacks.

Ferrara et al. evaluated various state-of-the-art CNNs, namely, AlexNet, VGG19, VGG-Face16, and VGG-Face2 pre-trained on ImageNet and VGG-Face datasets for facial morphing detection in the presence of printing/scanning and heterogeneous image sources. Experimental evaluation on MorphDBD and MorphDBP&S suggested good detection performance on digital images. However, high error rates were generated for image manipulation due to printing and scanning. The models trained on face datasets usually outperformed those pre-trained on the ImageNet dataset. The authors suggest that more sophisticated and face-specific filters are necessary to detect the fine artefacts that survive the printing and scanning process.

Summary/Conclusion

All the papers selected for this special issue discuss the beneficial findings in image manipulation detection and presentation attack detection. The first part consists of four papers that present and discuss the new challenges and solutions for presentation attack detection. The second part consists of three papers that discuss the challenges of face morphing. Altogether, this special issue provides the collection of insightful articles to address the evolving problem of image manipulation and presentation attack detection on biometric systems.

Raghavendra Ramachandra[1]
Naser Damer[2]
Kiran Raja[1]
Ajita Rattani[3]

[1]*IIK, Norwegian University of Science and Technology, Gjøvik, Norway*
[2]*Fraunhofer-Institut für Graphische Datenverarbeitung IGD, Darmstadt, Germany*
[3]*Department of Electrical Engineering and Computer Science, Wichita State University, Wichita, Kansas, USA*

Correspondence
Raghavendra Ramachandra, IIK, Norwegian University of Science and Technology, Teknologivegen, 2815 Gjøvik, Norway.
Email: raghavendra.ramachandra@ntnu.no

ORCID
Raghavendra Ramachandra https://orcid.org/0000-0003-0484-3956
Naser Damer https://orcid.org/0000-0001-7910-7895