IET Biometrics

DOI: 10.1049/bme2.12101

GUEST EDITORIAL

BIOSIG 2021 Special issue on efficient, reliable, and privacy-friendly biometrics

This special issue of IET Biometrics, “BIOSIG 2021 Special Issue on Efficient, Reliable, and Privacy-Friendly Biometrics”, has as starting point the 2021 edition of the Biometric Special Interest Group (BIOSIG) conference. This special issue gathers works focussing on topics of biometric recognition put under the new light of fostering the efficiency, reliability and privacy of biometrics systems and methods.

The “BIOSIG 2021 Special Issue on Efficient, Reliable, and Privacy-Friendly Biometrics” issue contains 12 papers, several of them being extended versions of papers presented at the BIOSIG 2021 conference, dealing with concrete research areas within biometrics such as **Presentation Attack Detection for Face and Iris**, **Biometric Template Protection Schemes** and **Deep Learning techniques for Biometrics**.

1 | PRESENTATION ATTACK DETECTION FOR FACE AND IRIS

Paper “Face Morphing Attacks and Face Image Quality: The Effect of Morphing and the Attack Detectability by Quality” was authored by Biying Fu and Naser Damer. This paper addresses the effect of morphing processes both on the perceptual image quality and the image utility in face recognition (FR) when compared to bona fide samples. This work provides an extensive analysis of the effect of morphing on face image quality, including both general image quality measures and face image utility measures, analysing six different morphing techniques and five different data sources using 10 different quality measures. The consistent separability between the quality scores of morphing attack and bona fide samples measured by certain quality measures sustains the proposal of performing unsupervised morphing attack detection (MAD) based on quality scores. The study looks into intra- and inter-dataset detectability to evaluate the generalisability of such a detection concept on different morphing techniques and bona fide sources. The results obtained point out that a set of quality measures, such as MagFace and CNNNIQA, can be used to perform unsupervised and generalised MAD with a correct classification accuracy of over 70%.

Paper “Pixel-Wise Supervision for Presentation Attack Detection on ID Cards” was authored by Raghavendra Mudgalgundurao, Patrick Schuch, Kiran Raja, Raghavendra Ramachandra, and Naser Damer. This paper addresses the problem of detection of fake ID cards that are printed and then digitally presented for biometric authentication purposes in unsupervised settings. The authors propose a method based on pixel-wise supervision, using DenseNet, to leverage minute cues on various artefacts such as moiré patterns and artefacts left by the printers. To test the proposed system, a new database was obtained from an operational system, consisting of 886 users with 433 bona fide, 67 print and 366 display attacks (not publicly available due to GPDR regulations). The proposed approach achieves better performance compared to handcrafted features and deep learning models, with an Equal Error Rate (EER) of 2.22% and Bona fide Presentation Classification Error Rate (BPCER) of 1.83% and 1.67% @ Attack Presentation Classification Error Rate (APCER) of 5% and 10%, respectively.

Paper “Deep Patch-Wise Supervision for Presentation Attack Detection” was authored by Alperen Kantarcı, Hasan Dertli, and Hazım Ekenel. This paper addresses the generalisation problem in face presentation attack detection (PAD). Specifically, convolutional neural networks (CNN)-based systems have gained significant popularity recently due to their high performance on intra-dataset experiments. However, these systems often fail to generalise to the datasets that they have not been trained on. This indicates that they tend to memorise dataset-specific spoof traces. To mitigate this problem, the authors propose a new presentation attack detection (PAD) approach that combines pixel-wise binary supervision with patch-based CNN. The presented experiments show that the proposed patch-based method forces the model not to memorise the background information or dataset-specific traces. The proposed method was tested on widely used PAD datasets—Replay-Mobile, OULU-NPU— and on a real-world dataset that has been collected for real-world PAD use cases. The results presented show that the proposed approach is found to be superior on challenging experimental setups. Namely, it achieves higher performance on OULU-NPU protocol 3, 4 and on inter-dataset real-world experiments.

Paper “Transferability Analysis of Adversarial Attacks on Gender Classification to Face Recognition: Fixed and Variable Attack Perturbation” was authored by Zohra Rezgui, Amina Bassit, and Raymond Veldhuis. This paper focusses on the challenge of transferability of adversarial attacks. This work is motivated by the fact that it was proved in the literature that these attacks, targeting a specific model, are transferable among models performing the same task, however, the transferability scenarios are not considered in the literature for models performing different tasks but sharing the same input space and model architecture. In this paper, the authors study the above mentioned challenge regarding VGG16-based and ResNet50-based biometric classifiers. The impact of two white-box attacks on a gender classifier is investigated and then their robustness to defence methods is assessed by applying a feature-guided denoising method. Once the effectiveness of these attacks was established in fooling the gender classifier, we tested their transferability from the gender classification task to the facial recognition task with similar architectures in a black-box manner. Two verification comparison settings are employed, in which the authors compare images perturbed with the same and different magnitude of the perturbation. The presented results indicate transferability in the fixed perturbation setting for a Fast Gradient Sign Method (FGSM) attack and non-transferability in a Projected Gradient Descent (PGD) attack setting. The interpretation of this non-transferability can support the use of fast and train-free adversarial attacks targeting soft biometric classifiers as means to achieve soft biometric privacy protection while maintaining facial identity as utility.

Paper “Combining 2D Texture and 3D Geometry Features for Reliable Iris Presentation Attack Detection using Light Field Focal Stack” was authored by Zhengquan Luo, Yunlong Wang, Nianfeng Liu, and Zilei Wang. In this paper, the authors leverage the merits of both light field (LF) imaging and deep learning (DL) to combine 2D texture and 3D geometry features for iris presentation attack detection (PAD). The proposed study explores off-the-shelf deep features of planar-oriented and sequence-oriented deep neural networks (DNNs) on the rendered focal stack. The proposed framework excavates the differences in 3D geometric structure and 2D spatial texture between bona fide and spoofing irises captured by LF cameras. A group of pre-trained DL models are adopted as feature extractor and the parameters of SVM classifiers are optimised on a limited number of samples. Moreover, two branch feature fusion further strengthens the framework's robustness and reliability against severe motion blur, noise, and other degradation factors. The results indicate that variants of the proposed framework significantly surpass the PAD methods that take 2D planar images or LF focal stack as input, even recent state-of-the-art methods fined-tuned on the adopted database. The results of multi-class attack detection experiments also verify the good generalisation ability of the proposed framework on unseen presentation attacks.

2 | BIOMETRIC TEMPLATE PROTECTION SCHEMES

Paper “Hybrid Biometric Template Protection: Resolving the Agony of Choice between Bloom Filters and Homomorphic Encryption” was authored by Amina Bassit, Florian Hahn, Chris Zeinstra, Raymond Veldhuis and Andreas Peter. This paper addresses the development of biometric template protection (BTP) schemes investigating the strengths and weaknesses of Bloom filters (BFs) and homomorphic encryption (HE). The paper notes that the pros and cons of BF-based and HE-based BTPs are not well studied in the literature and these two approaches both seem promising from a theoretical viewpoint. Thus, this work presents a comparative study of the existing BF-based BTPs and HE-based BTPs by examining their advantages and disadvantages from a theoretical standpoint. This comparison was applied to iris recognition as a study case, where the biometric and runtime performances of the BTP approaches were tested on the same setting, dataset, and implementation language. As a synthesis of this study, the authors propose a hybrid BTP scheme that combines the good properties of BFs and HE, ensuring unlinkability and high recognition accuracy, while being about 7 times faster than the traditional HE-based approach. The evaluation of the proposed scheme confirmed its biometric accuracy (an EER of 0:17% over the IITD iris database) and runtime efficiency (104:35 ms, 155:15 ms and 171:70 ms for 128,192, and 256 bits security level, respectively).

Paper “Locality Preserving Binary Face Representations Using Auto-encoders” was authored by Mohamed Amine HMANI, Dijana Petrovska-Delacrétaz and Bernadette Dorizzi. This paper focusses on template protection schemes for face biometrics and introduces a novel approach to binarising biometric data using Deep Neural Networks (DNN) applied to facial data. The authors propose the use of DNN to extract binary embeddings from face images directly. The proposed binary embeddings give a state-of-the-art performance on two well-known databases (MOBIO and the Labelled Faces in the Wild (LFW)) with almost negligible degradation compared to the baseline. Further, as an application, the paper proposes a cancellable system based on the binary embeddings using a shuffling transformation with a randomisation key as a second factor. The cancellable system is analysed according to the ISO/IEC 24745:2011 standardised metrics. The templates generated by the cancellable system are unlinkable without the disclosure of the second factor.

3 | DEEP LEARNING TECHNIQUES FOR BIOMETRICS SYSTEMS

Paper “Reliable Detection of Doppelgängers based on Deep Face Representations” was submitted by Christian Rathgeb, Daniel Fischer, Pawel Drozdowski and Christoph Busch. This paper assesses the impact of doppelgängers (people that look alike) on the *HDA Doppelgänger* and *Disguised Faces in The Wild* databases using a state-of-the-art face recognition system, confirming that the existence of doppelgängers significantly increases false match rates. The paper then presents a method able to distinguish doppelgängers from mated comparison trials, by analysing differences in deep representations obtained from face image pairs. The proposed detection system achieves a state-of-the-art detection equal error rate of approximately

2.7% for the task of separating mated authentication attempts from doppelgängers in the mentioned databases.

Paper "Benchmarking Human Face Similarity Using Identical Twins" was authored by Shoaib Meraj Sami, John McCauley, Sobhan Soleymani, Nasser Nasrabadi, and Jeremy Dawson. This paper addresses the problem of distinguishing identical twins and non-twin look-alikes in automated facial recognition (FR) applications. This work makes use of one of the largest twin datasets compiled to date to address two FR challenges: 1) determining a baseline measure of facial similarity between identical twins and 2) applying this similarity measure to determine the impact of doppelgangers, or look-alikes, on FR performance for large face datasets. The methodology proposed for facial similarity measure is based on a deep convolutional neural network trained on a tailored verification task designed to encourage the network to group together highly similar face pairs in the embedding space and achieves a test AUC of 0.9799. The proposed network provides a quantitative similarity score for any two given faces and has been applied to large-scale face datasets to identify similar face pairs. An additional analysis which correlates the comparison score returned by a facial recognition tool and the similarity score returned by the proposed network has also been performed.

Paper "Discriminative Training of Spiking Neural Networks Organised in Columns for Stream-based Biometric Authentication" was authored by Enrique Argones Rúa, Tim Van hamme, Davy Preuveneers, and Wouter Joosen. In this paper, the authors address stream-based biometric authentication using a novel approach based on spiking neural networks (SNNs). SNNs have proven advantages regarding energy consumption and they are a perfect match with some proposed neuromorphic hardware chips, which can lead to a broader adoption of user device applications of artificial intelligence technologies. One of the challenges when using SNNs is the discriminative training of the network, since it is not straightforward to apply the well-known error backpropagation (EBP), massively used in traditional artificial neural networks (ANNs). Thus, the authors propose to use a network structure based on neuron columns, resembling cortical columns in the human cortex, and a new derivation of error backpropagation for the spiking neural networks that integrates the lateral inhibition in these structures. In the experiments presented, the potential of the proposed approach is tested in the task of inertial gait authentication, where gait is quantified as signals from Inertial Measurement Units (IMU). The proposed approach is compared to state-of-the-art ANNs being shown that SNNs provide competitive results, obtaining a difference of around 1% in Half Total Error Rate when compared to state-of-the-art ANNs in the context of IMU-based gait authentication.

Paper "Towards Understanding the Character of Quality Sampling in Deep Learning Face Recognition" was authored by Iurii Medvedev, João Tremoço, Luís Espírito Santo, Beatriz Mano, and Nuno Gonçalves. This paper addresses the problem of the inconsistency between the training data and the deployment scenario in face-based biometric systems, which are developed specifically for dealing with ID document compliant images. This inconsistency is often caused by the choice of unconstrained face images of celebrities for training, motivated by its public availability opposed to the fact that existing document compliant face image collections are hardly accessible due to security and privacy issues. To mitigate the addressed problem, the authors propose to regularise the training of the deep face recognition network with a specific sample mining strategy, which penalises the samples by their estimated quality. This deep learning strategy is expanded to seek for the penalty (sampling character) that better satisfies the purpose of adapting deep learning face recognition for images of ID and travel documents. The presented experiments demonstrate the efficiency of the approach for ID document compliant face images.

Paper "Masked Face Recognition: Human versus Machine" was authored by Naser Damer, Fadi Boutros, Marius Süßmilch, Meiling Fang, Florian Kirchbuchner and Arjan Kuijper. This paper focusses on the assessment of the effect of wearing a mask on face recognition (FR) in a collaborative environment. This work provides a joint evaluation and in-depth analyses of the face verification performance of human experts in comparison to state-of-the-art automatic FR solutions. In this paper, an extensive evaluation by human experts is presented along with four automatic recognition solutions. An analysis was made of the correlations between the verification behaviours of human experts and automatic FR solutions under different settings, such as involved unmasked pairs, masked probes and unmasked references, and masked pairs, with real and synthetic masks. The study concludes with a set of take-home messages on different aspects of the correlation between the verification behaviour of humans and machines.

ACKNOWLEDGEMENTS

The Guest Editorial Board would like to thank all of the authors for their contributions to this Special Issue: "BIOSIG 2021 Special Issue on Efficient, Reliable, and Privacy-Friendly Biometrics". We would also like to express our appreciation to the reviewers, who have provided insightful comments and suggestions contributing to improving the quality of the manuscripts.

Ana F. Sequeira[1]
Marta Gomez-Barrero[2]
Naser Damer[3]
Paulo Lobato Correia[4]

[1]*CTM, INESC TEC, Porto, Portugal*
[2]*Hochschule Ansbach, Residenzstr, Ansbach, Germany*
[3]*Fraunhofer-Institut für Graphische Datenverarbeitung IGD, Darmstadt, Germany*
[4]*Instituto de Telecomunicações, Instituto Superior Técnico - Universidade de Lisboa, Lisbon, Portugal*

Correspondence
Ana F. Sequeira, CTM, INESC TEC, INESC TEC Campus da FEUP, Rua Dr Roberto Frias, Porto, Portugal.
Email: ana.f.sequeira@inesctec.pt

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no new data were created or analysed in this study.

ORCID

Ana F. Sequeira https://orcid.org/0000-0002-6685-2033
Naser Damer https://orcid.org/0000-0001-7910-7895

AUTHOR BIOGRAPHIES

Ana F. Sequeira holds a PhD in Electrical and Computer Engineering and a Degree and a Master in Mathematics. Sequeira's research is focussed on fundamental computer vision and machine learning topics and comprises anti-spoofing techniques (for iris, face and fingerprint); biometric recognition for border control; as well as facial analysis topics, such as emotion recognition, image compliance with standardisation requirements; and more recently, the study of interpretability of AI for biometrics. In particular, her research has focussed on biometric applications in challenging scenarios in use cases such as border control or transactions on mobile devices. Currently, Sequeira is a researcher at INESC TEC and, in the past, was a postdoctoral research assistant at the University of Reading, UK, collaborating in two European projects on biometrics for border control (FASTPASS—FP7 312583 and PROTECT—H2020 700259). In addition, Sequeira collaborated with the company IrisGuard UK to evaluate the iris recognition-based technology for monetary transactions on mobile devices—EyePay Technology. Sequeira led the construction of several biometric databases; managed biometric competitions focussing on iris spoofing, multimodal recognition and iris/periocular cross-spectral recognition and has co-authored several research publications recognised by the peers with citations.

Marta Gomez-Barrero is a Professor for IT-Security and technical data privacy at the Hochschule Ansbach, in Germany. Between 2016 and 2020, she was a postdoctoral researcher at the National Research Center for Applied Cybersecurity (ATHENE)—Hochschule Darmstadt, Germany. Before that, she received her MSc degree in Computer Science and Mathematics (2011), and her PhD degree in Electrical Engineering (2016), all from *Universidad Autonoma de Madrid*, Spain. Her current research focusses on security and privacy evaluations of biometric systems, Presentation Attack Detection (PAD) methodologies, and biometric template protection (BTP) schemes. She has co-authored more than 70 publications, chaired special sessions and competitions at international conferences; she is associate editor for the EURASIP Journal on Information Security and represents the German Institute for Standardisation (DIN) in ISO/IEC SC37 JTC1 SC37 on biometrics.

Naser Damer is a senior researcher at the Fraunhofer IGD, performing research management, applied research, scientific consulting, and system evaluation. He received his Ph.D. in computer science from TU Darmstadt (2018). His main research interests lie in the fields of biometrics, machine learning, and information fusion. Naser is a research area co-coordinator and a principal investigator at the National Research Center for Applied Cybersecurity ATHENE, Germany. He lectures on Human and Identity-centric Machine Learning, as well as on Ambient Intelligence at TU Darmstadt. Naser is a member of the organising teams of several conferences, workshops, and special sessions, including being a program co-chair of BIOSIG. He serves as an associate editor for Pattern Recognition (Elsevier) and the Visual Computer (Springer). He represents the German Institute for Standardization (DIN) in the ISO/IEC SC37 international biometrics standardization committee. He is a member of the IEEE Biometrics Council serving on its Technical Activities Committee.

Paulo Lobato Correia is Associate Professor at the Department of Electrical and Computer Engineering, Instituto Superior Técnico, Universidade de Lisboa, Portugal. He is a Senior Researcher of the Multimedia Signal Processing research group of Instituto de Telecomunicações. He is Senior Member of the IEEE. Paulo Correia coordinated the participation in several national and international research projects, dealing with image and video analysis and processing. He is Editor in Chief of IET Biometrics for the term 2020–2022. He was Subject Editor (for Multimedia papers) of the Elsevier Signal Processing Journal (2018–2020). He was Associate Editor of the IEEE Transactions on Circuits and Systems for Video Technology (2006–2014), of the Elsevier Signal Processing Journal (2005–2017), and of IET Biometrics (2013–2019). He has been Guest Editor of several special issues for scientific journals and cooperated in many conference organising committees. He is a founding member of the Advisory Board of the European Signal Processing Association (EURASIP) and was the elected chairman of EURASIP's Technical Area Committee on "Biometrics, Data Forensics and Security" for the term 2018–2020. He has co-authored more than 140 journal and conference papers. The main research interests are about video analysis and processing, with emphasis on biometrical signal analysis, targeting recognition, sports, medical and forensic applications.