Special Section Guest Editorial

THE INTERNATIONAL Joint Conference on Biometrics (IJCB) combines two major biometrics conferences: the IEEE Biometrics Theory, Applications, and Systems (BTAS) conference and the International Conference on Biometrics (ICB). The blending of these two conferences happened once every 3 years between 2011 and 2017. Since 2020 – thanks to a special agreement between the IEEE Biometrics Council and the IAPR Technical Committee on Biometrics (TC4) – this joint conference has become an annual event. It represents an exciting event for the worldwide biometrics research community. This Special Issue of the IEEE TRANSACTIONS ON BIOMETRICS, BEHAVIOR, AND IDENTITY SCIENCE collects the extended versions of the best papers presented in the 2021 edition.

All papers invited to the Special Issue underwent a new review process to assure a significant addition of relevant content with respect to the conference papers. A summary of the accepted papers is provided below.

The paper [A1] by Song et al. introduces a video understanding based random hand gesture authentication method that eliminates the need to have the probe gesture types to be consistent with the registered ones. Users only need to perform a random hand gesture in front of an RGB camera without memory and hesitation in both the enrollment and verification stage. The random hand gesture can be considered as a promising biometric trait containing both physiological and behavioral characteristics.

The paper [A2] by Yang et al. presents a multi-view, multi-spectral 3D finger imaging system. Through this system the authors scanned numerous fingers obtaining external skin images and internal vein images from 6 different views. These views are used to generate 3D finger models with skin and vein textures. In addition, the paper establishes a benchmark dataset, namely the Large-scale Finger Multi-Biometric database and benchmark for 3D Finger Biometrics (LFMB-3DFB) containing 695 fingers. Each finger is acquired 10 times, yielding 6 finger skin images and 6 finger vein images for a total of 83,400 images and 6,950 3D finger models. The authors finally propose a comprehensive evaluation protocol for extensive experimental research.

The paper [A3] by Jiang et al. proposes a new lightweight framework in which point set data can be directly processed for 3D face recognition. Along this line, two weight-shared encoders are proposed to encode point cloud into two embedded features for identity prediction and similarity measurement. Experimental results show that the proposed method on three publicly available datasets outperforms state-of-the-art 2D face recognition algorithms.

The paper [A4] by Khaertdinov et al. introduces a sensor-based human activity recognition (HAR) method that includes a SimCLR framework and a transformer-like model. The proposed method addresses the problem of negative pairs in SimCLR by using dynamic temperature scaling within a contrastive loss function. Experimental results show that the method is robust and can achieve state-of-the-art performance on three widely used datasets in sensor-based HAR.

In [A5], Vance et al. present a new dataset with 70 subjects for deception detection and physiological monitoring. The data was collected in an interview scenario, and the interviewee attempts to deceive the interviewer on selected responses. The interviewee was recorded in visible, near-infrared, and long-wave infrared light, along with cardiac pulse, blood oxygenation, and audio. For the collected data, the authors estimated subject heart rates (remotely from face videos with a mean absolute error lower than two beats per minute), pupil size, and eye gaze. They also provided experimental results and discovered that a combination of remote plethysmography, pupil size, and thermal data yields the best deception detection results, with an equal error rate of 0.357.

In [A6], Hu et al. describe a face anti-spoofing solution based on neural networks that has three main modules: Multi-scale Representation Extraction Module, Structure Destruction Module, and Content Combination Module. The idea here is to leverage the multi-scale information in the input image in order to glean "spoof cues". Further, the image is broken down into patches thereby directing the network to focus on local details present in the image. The content combination module facilitates cross-domain generalization, where features extracted by the network are somewhat domain independent. The proposed technique is tested on 5 datasets including a non-face dataset. Experimental results convey the benefit of each of the modules developed in this work.

In [A7], Agrawal et al. harness Generative Adversarial Networks (GANs) for the task of continuous authentication of individuals interacting with a smartphone based on their touch and swipe gestures. The authors demonstrate the efficacy of their method under three active adversarial environments: zero-effort, population-effort, and random-input attacks. The main idea here is to use a pair of GANs: the Genuine-GAN generates synthetic swipe patterns similar to Genuine swipes while the Impostor-GAN generates synthetic swipe patterns similar to impostor swipes. The outputs of both Genuine-GAN and Impostor-GAN are then appended to genuine and impostor pairs, respectively. Besides demonstrating the resilience of the proposed authentication approach to adversarial attacks,

Digital Object Identifier 10.1109/TBIOM.2022.3222672

2637-6407 © 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

the authors also evaluate the fairness of their technique across genders.

The paper [A8] by Schuiki et al. investigates the presentation attacks for hand vein recognition systems. An in-depth analysis of threat evaluations for 15 different vein recognition schemes is conducted when presenting attack examples from three attack datasets of finger vein and one of palm vein. For presentation attack detection, experiments are further carried out to combine different similarity scores from the threat evaluation. Results show that score-level strategy together with feature scaling could be used to well detect presentation attacks.

We would like to thank the authors of the Special Issue for their contributions and the diligent reviewers for their valuable comments and suggestions which benefited the authors. We hope you enjoy reading the articles in the Special Issue!

APPENDIX: RELATED ARTICLES

[A1] W. Song, W. Kang, L. Wang, Z. Lin, and M. Gan, "Video understanding based random hand gesture authentication," *IEEE Trans. Biom., Behav., Ident. Sci.*, vol. 4, no. 4, pp. 453-470, Oct. 2022.

[A2] W. Yang, Z. Chen, J. Huang, and W. Kang, "A novel system and experimental study for 3D finger multi-biometrics," *IEEE Trans. Biom., Behav., Ident. Sci.*, vol. 4, no. 4, pp. 471-485, Oct. 2022.

[A3] C. Jiang, S. Lin, W. Chen, F. Liu, and L. Shen, "PointFace: Point cloud encoder based feature embedding for 3D face recognition," *IEEE Trans. Biom., Behav., Ident. Sci.*, vol. 4, no. 4, pp. 486-497, Oct. 2022.

[A4] B. Khaertdinov, S. Asteriadis, and E. Ghaleb, "Dynamic temperature scaling in contrastive self-supervised learning for sensor-based human activity recognition," *IEEE Trans. Biom., Behav., Ident. Sci.*, vol. 4, no. 4, pp. 498-507, Oct. 2022.

[A5] N. Vance et al., "Deception detection and remote physiological monitoring: A dataset and baseline experimental results," *IEEE Trans. Biom., Behav., Ident. Sci.*, vol. 4, no. 4, pp. 522-532, Oct. 2022.

[A6] C. Hu, J. Cao, K.-Y. Zhang, T. Yao, S. Ding, and L. Ma, "Structure destruction and content combination for generalizable anti-spoofing," *IEEE Trans. Biom., Behav., Ident. Sci.*, vol. 4, no. 4, pp. 508-521, Oct. 2022.

[A7] M. Agrawal, P. Mehrotra, R. Kumar, and R. R. Shah, "GANTouch: An attack-resilient framework for touch-based continuous authentication system," *IEEE Trans. Biom., Behav., Ident. Sci.*, vol. 4, no. 4, pp. 533-543, Oct. 2022.

[A8] J. Schuiki, M. Linortner, G. Wimmer, and A. Uhl, "Attack detection for finger and palm vein biometrics by fusion of multiple recognition algorithms," *IEEE Trans. Biom., Behav., Ident. Sci.*, vol. 4, no. 4, pp. 544-555, Oct. 2022.

MARIA DE MARSICO, *Guest Editor*
Sapienza University of Rome
00185 Roma, Italy

JULIAN FIERREZ, *Guest Editor*
Universidad Autonoma de Madrid
28049 Madrid, Spain

ARUN ROSS, *Guest Editor*
Michigan State University
East Lansing, MI 48824 USA

SHIQI YU, *Guest Editor*
Southern University of Science and Technology
Shenzhen 518055, China

P. C. YUEN, *Guest Editor*
Hong Kong Baptist University
Hong Kong

JIANGUO ZHANG, *Guest Editor*
Southern University of Science and Technology
Shenzhen 518055, China