2018 BTAS Conference

Conference report on IEEE BTAS 2018

Los Angeles, U.S., 2018-10-26

The 9th edition of the International Conference on Biometrics: Theory, Applications and Systems (BTAS) was hosted from 22 to 26 October 2018 by the University of Southern California's (USC) Information Sciences Institute in cooperation with the IEEE Biometrics Council.

BTAS conference

The conference attracted more than 130 participants from 14 countries. The program committee selected 51 papers with an acceptance rate of 36%. Each paper is presented in both a 12-min oral presentation, and a poster session.

The opening keynote talk was given by Lars Ericson, who is Program manager for the ODIN program at the Intelligence Advanced Research Projects Activity (IARPA) within the Office of the Director of National Intelligence. Lars reported about the IARPA sponsored research on detecting Presentation Attack for face, iris and fingerprint biometrics. The motivation behind this research is that the US Government uses biometrics to identify persons of interest, but biometric presentation attacks can prevent correct identification. The goal of the Odin program is to develop biometric presentation attack detection technologies to ensure biometric security systems can detect when someone is attempting to disguise their biometric identity. The talk provided a summary of the first government-controlled test for the Odin program, which was conducted in early summer 2018.

Lars Ericson

The keynote on the second day was delivered by P. Jonathon Phillips (NIST), the 2018 IEEE Biometrics Council Leadership Award Winner. The title of Jonathon's was *Face Recognition Accuracy of Forensic Examiners, Super-recognizers, and Algorithms*. A forensic facial examiner has two to fours years of extensive training, before she can provide testimony in court. Super-recognizers are people with extraordinary ability to remember faces. In addition to facial examiners and super-recognizers, fingerprint examiners, undergraduate students, and four deep convolutional neural networks (DCNNs) were included in the study. The DCNN based algorithms, which were developed under the IARPA Janus program (VGG-Face, A2016, A2017a, A2017b). The DCNN were trained on 3.7 million images of over 58,000 faces. The analysis shows that facial examiners have a median area under the curve (AUC) of the ROC of 0.93. It is interesting that for the super-recognizers reached a median AUC of 0.85. Naturally, fingerprint examiners and students performed at lower accuracies. The best algorithm was competitive with the best humans. Fusing the opinion of four facial examiners or super-recognizers boosted the performance to a median AUC of 1.0. The corresponding paper can be downloaded at http://www.pnas.org/content/115/24/6171.

Mark Nixon, Jonathon Phillipps and Wael AbdAlmageed

The final day included the keynote of Shantanu Rane, Research Area Manager, Palo Alto Research Center (PARC). The scope of his keynote was a Cyberphysical Systems Perspective on Biometric Security and Privacy, motivated by the wide adoption of fingerprint and face recognition on mobile phones. Many of the usability concerns that plagued biometric recognition systems in the past have been addressed. Moreover the biometric recognition systems on today's mobile devices have generally proved successful in preventing adversaries from extracting reference data, however biometric capture devices are vulnerable to a variety of presentation attacks. While presentation attacks (a.k.a. spoofing) are less successful on biometric recognition systems developed by governments for civilian and law enforcement applications, these pose other concerns. Today, these systems maintain massive biometric databases that are, in turn, parts of much larger cyber-physical infrastructure. To assure the security and privacy of these databases, it is necessary not only to harden the protocols used for biometric recognition, but to securely configure the entirety of the system. This is an extremely challenging problem. Template protection is a promising approach to protect the privacy of enrolled individuals. To drive widespread adoption of template protection schemes, further work is needed to bridge the performance and complexity gap with respect to conventional biometric systems.

Awards

The BTAS awards committee selected the winners of the best paper award, which was granted to the paper titled *DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution* contributed by Philip J Bontrager, Aditi Roy, Julian Togelius, Nasir Memon and Arun Ross from New York University / Michigan State University. The best student paper award was granted to the work titled *ID Preserving Generative Adversarial Network for Partial Latent Fingerprint Reconstruction* by Ali Dabouei, Sobhan Soleymani, Hadi Kazemi, Seyed mehdi Iranmanesh, Jeremy Dawson and Nasser Nasrabadi from West Virginia University.

The papers from the BTAS conference are available at: https://www.isi.edu/events/btas/btas2018-cameraready-final/

The next BTAS conference will take place in Tampa, Florida from 24 to 26 September 2019.

Shantanu Rane

Best paper awards winner Philip Bontrager