Conference report on IEEE BIOSIG 2016

The 15th edition of the International Conference of the Biometrics Special Interest Group (BIOSIG) took place at Fraunhofer IGD in Darmstadt, Germany from September 21 to 23 and attracted registered more than 100 participants. This year participants even travelled all the way from Japan, Korea, Argentina, Uruquay and the US to Darmstadt in order to join the BIOSIG community.

The program was composed of scientific research contributions on the one hand and reports about large-scale applications on the other hand. The opening keynote talk was given by Richard Rinkens (EC, DG Home), who presented the new proposal for the Entry Exit System (EES), adopted by the European Commission after an intense period of analysis and real-world testing (eu-LISA has tested 13 entries - sea, rail, air - with different options). The new proposal is based on multi-modal biometrics combining 4-fingerprints and a good quality facial-image taken live. In particular, new procedures for EU citizens, 3rd country nationals with visa and 3rd country without visa are considered. One of the main objectives is the identification of overstayers and to enable subsequent evidence based visa policy making. To tackle these issues, the EES will substitute manual procedures with electronic stamps in an electronic database. In addition, a new link has been made between EES and VIS, and a common AFIS should be deployed for the three systems. Future features include a webservice to check credentials and authorized time left, which will be the first consultable service for an EU system of this kind through internet. Finally, it was highlighted that the EES will seriously reinforce internal security and fight against terrorism.

Accepted conference contributions included 16 presentations and covering soft biometrics for face or iris, fingerprint, vein, face, iris, voice, gait and keystroke recognition. Other challenges addressed included facial forensics use cases, voice activity segmentation, 3D gloves for contactless verification, new biometric template protection schemes or the generation of synthetic fingerprint alteration database to allow the further development of algorithms to detect them. Another relevant topic covered in the conference was Presentation Attack Detection (PAD) for characteristics such as face and iris. The poster session with 25 contributions was a good mix of research results from academic and industrial research labs and visitors did spend a long time in the

poster exhibition before the start of the social event with the traditional late summer barbeque – providing lots of opportunities for networking.

On the last day of the conference, Arun Ross addressed the issue of personal privacy in biometric systems. In particular, he considered several questions such as (a) Can additional information about an individual be automatically gleaned from biometric data? (b) Can biometrics be used to surreptitiously track an individual? (c) Can multiple biometric databases be linked to develop a more complete profile of an individual? (d) Who owns the biometric data collected from an individual, and how long should the biometric data be retained in an identity management system? He started the keynote with a definition stemming from 1890: "privacy is the right to be left alone". However, in contemporary society it is easy for someone to take a picture of you and find out who you are by harnessing the power of automated face recognition and cloud computing. In the first part of the talk, he discussed methods by which biographical (e.g., gender from fingerprints), anatomical (e.g., crypts in iris), sensorial (e.g., type of device used to image a certain fingerprint), and environmental (e.g., intensity of ambient lighting during iris image acquisition) information can be gleaned from biometric data. While the resultant information can be used to improve person recognition performance in the framework of "soft" biometrics or forensics, the extraction of such information can be deemed to violate privacy. He gave the example where face or iris data can be surreptitiously used to divulge pathological information about an individual.

In the second part of the talk, he discussed ways by which privacy can be accorded to stored biometric data. The proposed methods rely on the principles of visual cryptography and signal mixing to generate biometric templates that can suppress some of the additional information about a person that is resident in the biometric data. He reported experimental results discussing the efficacy of these methods. The talk concluded by pointing out that privacy enhancing technologies can be judiciously used by biometric systems to ensure that the benefits of biometrics are not undermined by privacy concerns.

The last conference day concluded with a keynote by Davide Maltoni addressing the issue of large-scale verification within projects such as UIDAI, BMS, ePassports or SIS-II: predicting accuracy of biometric systems is a very difficult problem. Statistical modelling techniques often require to make assumptions on data distributions that we cannot validate in practice. A different approach is running fingerprint recognition algorithms on large datasets of synthetic data. However, we have to face two problems: i) ensure that synthetic data well approximate real data; ii) running huge amount of fingerprint comparisons in a reasonable time. In particular, the SFinGe software developed at the University of Bologna within the EU FIDELITY project can mitigate this lack of large databases, where not only one but several samples of a given synthetic fingerprint can be generated modelling distortion. For the empirical evaluation and comparison with real data, verification was run using Minutiae Cilynder Codes (MCC), which model spatial and directional contributions. The software has been optimized for GPUs, needing only 5.6 ms for a single identification on 250K subjects (44.6 millions of comparisons per seconds). The empirical evaluation on synthetic data yielded predictions similar to those found in a real case study: IUDAI. As future actions an analysis with NFIQ2.0 will be considered and scaling up to a database modelling the world population (7 billion), which will need about 3 months for generation and a few weeks for identification.

As in previous BIOSIG conferences participants of the conference themselves voted for the best paper and the best poster that was presented at the conference. The winner of the BIOSIG 2016 best paper award is Sunpreet S. Arora (Michigan State University) for his presentation “3D Whole Hand Target: Evaluating Slap and Contactless Fingerprint Readers“, which convinced the majority of the participants.

While the poster session showed many impressive research results that stimulated long discussions, there was one contribution, which was chosen by the participants as best and it received thus the BIOSIG 2016 best poster award. It was the poster of Yoshinori Koda (NEC Corporation) with the title: “Advances in Capturing Child Fingerprints: A High Resolution CMOS Image Sensor

with SLDR Method“.

The BIOSIG conference was preceded by the 3rd EAB Research Project Conference and was further co-located with two satellite workshops:
The meeting of the TeleTrusT Biometric Working Group and joint meeting of the ethical committee of the European Association of Biometrics.

The 2016 BIOSIG conference was jointly organized by the Competence Center for Applied Security Technology (CAST) and the special interest group BIOSIG of the Gesellschaft für Informatik e.V. (GI).
The conference was technically co-sponsored by IEEE Biometric Council and the papers will be added to IEEE Xplore.

Next year the BIOSIG conference will take place between
September 20 to 22, 2017 in Darmstadt, Germany.
See: www.biosig.org