This newsletter is issued by the European Association for Biometrics (EAB). Its content is contributed by the members of the EAB. If you feel an important news from your biometric sector or from your Region missing – do not hesitate to submit a news item to the secretariat before the next newsletter is issued (October 2016).
1. News from the EAB

EAB Workshop: Performance and Evaluation of Mobile Biometrics

On 22 July 2016, 13:30 – 17:00 CET, the EAB will host a workshop on the Performance and Evaluation for Mobile Biometrics. The workshop takes place at AFNOR in Paris. During the workshop it will be discussed how standards and evaluation capabilities can be set up in order to independently assess the performance of biometric authentication and identification applications on mobile devices, such as smart phones and tablets.

There will be presentations from ING Bank, UL, IDEX, FPC, Safran Identity & Security and the University of Kent. The objectives of the workshop are to get more insight in the needs and requirements from the financial industry, as well as to come to a draft proposal for a new ISO/IEC work item on standardization and testing of mobile biometrics. The workshop will discuss performance and testing requirements of biometrics on mobile devices, including topics such as:

- Requirements for embedded sensors to allow quality biometric sample acquisition
- Accuracy requirements for biometric verification on mobile devices
- Presentation Attack Detection evaluation on mobile devices
- Performance assessment of biometric systems embedded in mobile devices

You can find the full program here: [http://eab.org/events/upcoming_events.html](http://eab.org/events/upcoming_events.html)

EAB members get free access!

Registration is required and can be done here: [http://eab.org/events/registration/129](http://eab.org/events/registration/129)

EAB General Assembly takes place in Darmstadt on 20th September

EAB members are cordially invited to participate to the 2016 General Assembly of the European Association for Biometrics. On the agenda will be the financial report for 2015 and the plans for 2016-2017. In addition we will have a discussion on a letter of recommendation to the European Commission and the European Parliament regarding the establishment and use of biometrics databases in Europe for research and testing purposes. Your opinion on that will be highly appreciated.

You will find the agenda here: [http://eab.org/events/program/117](http://eab.org/events/program/117)

Registration is required and will be for free (EAB members only, diner included).
EAB Workshop: Preserving Privacy in an Age of Increased Surveillance – A Biometrics Perspective

This one-day workshop will focus on privacy issues surrounding biometric technologies and applications. We will together reflect upon the many new threats and opportunities arising from the rapid increase in the channels of biometric data capture (e.g. sensors on mobile devices) and processing capabilities. The workshop will bring together various stakeholders from amongst end users, technology developers, researchers and legal experts to discuss the serious challenges that these developments present and explore together ways for addressing them. Location: IBM SouthBank, London. EAB members get free access!

Registration is required and can be done here: http://eab.org/events/program/128

EAB-CITeR

On 5 April 2016 a workshop on the European Cooperative Identification Technology Research Consortium (EAB-CITeR) took place in Amsterdam Airport. There were 25 registrations. The workshop was organized by IDIAP and EAB. The workshop was targeted to those who are interested in new research and development opportunities in the area of biometrics and other identification technologies in Europe. The objective of the workshop was for participants to learn:

- How does the EAB-CITeR work and how can an EAB member participate
- What are the benefits and opportunities of joining the EAB CITeR
- When will the first research projects start

The EAB-CITeR initiative and the Amsterdam workshop have been presented to Interpol in Lyon. The participants unanimously agreed that the workshop was very informative and that the EAB-CITeR initiative fills a gap in the current research landscape. The presentation by James Loudermilk clearly indicated that the CITeR cooperative model can be very effective in achieving a fruitful and dynamic cooperation between the stakeholders, resulting in many useful research projects. He also emphasized that the CITeR projects are a stepping stone towards larger projects, which take place outside the CITeR environment. He made clear that the CITeR cooperative model enables end users (governments) to interact with industry and research partners, without going into formal tendering procedures or legal obstacles. The EAB-CITeR is generally considered as a promising initiative.

Read more: http://eab.org/expertise/com/eab-citer.html

http://eab.org/events/program/119
## EDPS: Privacy Shield is not good enough

The European Data Protection Supervisor (EDPS) has issued an Opinion in which he says that the proposed EU-US Privacy Shield is not robust enough.

Giovanni Buttarelli, EDPS, said: "I appreciate the efforts made to develop a solution to replace Safe Harbour but the Privacy Shield as it stands is not robust enough to withstand future legal scrutiny before the Court [of Justice of the European Union]. Significant improvements are needed should the European Commission wish to adopt an adequacy decision, to respect the essence of key data protection principles with particular regard to necessity, proportionality and redress mechanisms. Moreover, it’s time to develop a longer term solution in the transatlantic dialogue."

Recognising that organisations should not be expected to constantly change compliance models, the EDPS proposes some improvement to Privacy Shield. These include integrating all main data protection principles, limiting derogations and improving redress and oversight mechanisms.

*Read more: [http://www.privacylaws.com/int_enews_08_06_16](http://www.privacylaws.com/int_enews_08_06_16)*

## EC Smart Borders Package: Questions & Answers

The Smart Borders package includes: a Communication on 'Stronger and Smarter Information Systems for Borders and Security'; a Regulation for the establishment of an Entry-Exit System; a proposed amendment to the Schengen Borders Code to integrate the technical changes needed for the Entry-Exit System.

The Smart Borders package will modernise the Schengen area's external border management by improving the quality and efficiency of border crossing processes. It aims to help Member States deal with increasing traveller flows, without necessarily increasing the number of border guards, and to promote mobility between the Schengen zone and third countries in a secure environment, while contributing to the fight against terrorism and serious crimes.

A fact sheet including question and answers regarding the smart borders package has been published by the European Commission.

New electronic ID cards to be issued in Italy

Last December it was published a decree containing the technical procedures for the issuance of the new Italian electronic identity card. The technical specifications for the new electronic ID card have been published on the Digital Italy Agency (AGID) website:


The new ID card will be equipped with a contactless chip with two applications:

- **MRTD** for physical identity verification, with personal and biometric data (facial image and two fingerprints) in ICAO standard format, protected with protocols SAC, PA, EAC
- **IAS** for online authentication, with authentication certificate.

The procedures for the acquisition of biometrics data and the characteristics of acquisition devices, defined by AGID in technical guidelines, are similar to those adopted for the issuance of the passport and residence permit card.

The tenders for the supply of data acquisition stations to be installed at the municipalities and of the central systems for issuing ID cards are being evaluated.

By Alessandro Alessandroni

German competition policy agency investigates Facebook

The German Bundeskartellamt has initiated proceedings against Facebook on suspicion of the company having abused its dominant market position by infringing data protection rules. The German competition policy agency is investigating Facebook Inc., US, the Irish subsidiary of the company and Facebook Germany GmbH, Hamburg. The Bundeskartellamt is investigating suspicions that Facebook could be imposing unfair conditions on users.

Andreas Mundt, President of the Bundeskartellamt said: "Dominant companies are subject to special obligations. These include the use of adequate terms of service as far as these are relevant to the market. For advertising-financed internet services such as Facebook, user data are hugely important. For this reason it is essential to also examine under the aspect of abuse of market power whether the consumers are sufficiently informed about the type and extent of data collected."

The Bundeskartellamt says that by creating user profiles the company enables its advertising customers to better target their advertising activities. In order to access the social network, users must first agree to the company’s collection and use of their data by accepting the terms of service. It is difficult for users to understand and assess the scope of the agreement accepted by them. There is considerable doubt as to the admissibility of this procedure, in particular under applicable national data protection law. If there is a connection between such an infringement and market dominance, this could also constitute an abusive practice under competition law.

Read more: http://www.privacylaws.com/Int_enews_1_4_16
Automatic Border Control systems are spreading in Italian airports

Automatic Border Control (ABC) systems for checking electronic passports are spreading in Italian airports.

Several e-gates have been installed at Rome Fiumicino Airport (FCO), Rome Ciampino Airport (CIA), Naples Capodichino Airport (NAP) and Venice Marco Polo Airport (VCE).

The Italian Ministry of the Interior fixed the minimum requirements of ABC systems and performance monitoring arrangements to ensure the security of borders in accordance with the Frontex guidelines.

By Alessandro Alessandroni

European Court of Justice: Decision about the Collection and Storage of Fingerprints for ePassports

About two years after its decision in Schwarz, the European Court rendered another decision about the scope of Regulation No 2252/2004 on standards for security features and biometrics in passports and travel documents.

Willems v. Burgemeester van Nuth e.a. combined various cases in which the applicants refused to provide fingerprints for the ePassport and eID in the Netherlands, as a result whereof they got their application rejected and possibly underwent additional negative consequences. The referring court Raad van State asked the European Court of Justice (ECJ) two questions.

On the first question whether the Regulation does not apply to identity cards issued by a Member State to its nationals, such as the Netherlands identity cards (...), the Court replied that according to the wording of Article 1(3) of the Regulation, the Regulation does not apply to identity cards issued by Member States to their nationals, whatever the period of their validity. Moreover, the fact that identity cards such as the Netherlands identity cards may be used for the purposes of travel within the European Union and to certain non-Member States does not bring it within the scope of Regulation No 2252/2004.

As to the second question for preliminary ruling, the Raad van State asked whether Article 4(3) of Regulation No 2252/2004, read together with Articles 6 and 7 of Directive 95/46 and Articles 7 and 8 of the Charter, must be interpreted as meaning that it requires Member States to guarantee that the biometric data collected and stored pursuant to that regulation will not be collected, processed and used for purposes other than the issue of passports or other travel documents. Article 4(3) of Regulation No 2252/2004 states that, for the purposes of that regulation, the biometric data ‘collected’ and ‘stored’ on the storage medium are to be used only for (1) verifying the authenticity of the document or (2) the identity of the holder when the passport or other travel documents are required to be produced by law.

In the Schwarz decision, and interesting for the national debate in several EU Member States, was the statement of the ECJ that the Regulation No 2252/2004 “cannot in and of itself (...) be interpreted as providing a legal basis for the centralised storage of data collected thereunder or
for the use of such data for purposes other than that of preventing illegal entry into the European Union.”

Referring to Schwarz, in which the court stated that setting up and maintaining databases for storage of biometric data is an exclusive competence of the Member States, the ECJ decided that Regulation No 2252/2004 does not require a Member State to guarantee in its legislation that biometric data will not be used or stored by that State for purposes other than those mentioned in Article 4(3) of that regulation.

The ECJ hereby did not take the opportunity to provide guidance for the compatibility of the fundamental rights to privacy and data protections, laid out in the Charter, and the Directive 95/46/EC, with the plans of several Member States to set up central biometric databases, and the need to provide adequate safeguards. The reasoning of the Court is that the fundamental rights guaranteed by the Charter must in its view be respected where national legislation falls within the scope of EU law. In other words, according to the ECJ, (only) the applicability of EU law would entail the applicability of the fundamental rights guaranteed by the Charter, according and referring hereby to some of its own case law.

This seems quite restrictive. Member States do collect biometric data precisely because of Regulation No 2252/2004 which is EU law. Without this Regulation, the issues may never have been risen. Moreover, the European Directive 95/46/EC does apply to this processing of personal data, and any implementing national laws could therefore be considered as falling within the scope of EU law, including the Charter. Finally, the ECJ has in previous case law stated that the requirements of the fundamental rights had to be considered upon the processing of personal data (Österreichischer Rundfunk and others, C-465/00, C-138/01 and C-139/01).

The result on this second question was that the Court stated that Regulation No 2252/2004, as amended by Regulation No 444/2009, must be interpreted as meaning that it does not require the Member States to guarantee, in their legislation, that biometric data collected and stored in accordance with that regulation will not be collected, processed and used for purposes other than the issue of the passport or travel document, since that is not a matter which falls within the scope of that regulation.

This could be misunderstood in that Member States would not have to provide adequate safeguards. This is in our view clearly not the case. This case only means that the Court did not assess this matter as it is in the view of the Court a national matter. In the view of the Court, it had not to review it, also not under the fundamental rights of the Charter. In other words, the Court missed a chance to provide guidance in this clearly important and heavily debated topic of the legality and conditions for national central biometric databases set up by governments in many Member States.

For more information, you can contact els.kindt@law.leuven.be, EAB member.
An AFIS for SIS-II: Workshop on Fingerprint Quality Metrics

In 2015 DG-JRC conducted a study on the readiness of the AFIS technology to be incorporated to the Schengen Information System (SIS) and the feasibility for such integration. The study, published in the form of a “JRC Science for Policy Report”, was presented to the European Parliament in February 2016.

The DG-JRC study concludes with a series of recommendations for a successful deployment of the AFIS technology in SIS. One of the key aspects identified is the use and appropriate management of fingerprint quality metrics. The study pointed out that further in depth analysis was required regarding the potential uses of biometric quality in order to optimize the performance of the future SIS-II AFIS.

Following with this activity, DG-JRC organized a two-day technical Workshop in Ispra that took place on the 30th and 31st of May 2016. The title and main focus of the Workshop was: "Workshop on Fingerprint Quality in the Context of SIS-II". The workshop was exclusively focused on the scientific and technical dimensions of fingerprint quality metrics. Two major fields of fingerprint quality were explored during the sessions: 10-prints (day 1) and fingermarks (day 2).

The workshop counted with the participation of representatives from all the main stakeholders dealing with implementation and future use of an AFIS functionality in SIS-II. This included: researchers in the field of fingerprint quality, vendors, law-enforcers from EU Member States, US NIST representative as well as representatives from different EU institutions and bodies involved in the integration process (DG-HOME, DG-JRC, EU-LISA).

Read more: http://publications.jrc.ec.europa.eu/repository/handle/JRC97779
3. Outside Europe

Standardisation of Presentation Attack Detection

Over the last years the International Standardisation committee on Biometrics (ISO/IEC JTC1 SC37) has generated a number of relevant standards that are now widely in use. Examples are:


In the upcoming meeting of SC37 in Paris on July 20 and 21 the committee will discuss and decide another very relevant topic for the biometric community, which is the definition of standardized performance assessment for Presentation Attack Detection (PAD). This standard ISO/IEC 30107-3 will build on top of the already published framework (ISO/IEC 30107-1) and will pave the road for future system evaluations and certifications of biometric capture devices.

If you are working in the field of PAD (a.k.a. anti-spoofing) please take a look at the current committee draft:
http://isotc.iso.org/livelink/livelink?func=ll&objId=17578675&objAction=Open&viewType=3

Please consider to contribute to the upcoming SC37 meeting and participate in the discussion about this committee draft. If you are interested, then please join your national standardisation body (and the respective mirror-committee of SC37) and register as soon as possible with the local host of the Paris meeting by contacting: <amelle.mouradi@afnor.org>

Please note that the published standard ISO/IEC 30107-1 "Biometric Presentation Attack Detection - Part 1: Framework" is freely accessible at:

Face Recognition Vendor Test 2016

The Face Recognition Vendor Test (FRVT) 2016 will continue NIST’s two-decade old programs of face recognition evaluations. It will measure performance of verification algorithms running on massive sequestered data, and will then, for the first time at NIST, be open to developers on an ongoing basis aligning the frequency of independent evaluation more closely with research and development schedules. This will allow a supplier to submit algorithms to NIST at any time, with a frequency not to exceed two algorithms once every 120 days. This mechanism is
intended to attract both mature FR providers and new entrants focusing on new markets. The verification test will be followed by an evaluation of one-to-many identification algorithms using enrolled populations in the low millions. The evaluation extends recent one to many evaluations (e.g. megaface) by characterizing accuracy at very low false positive identification rates and, can thereby, assess the discriminative power of new CNN-based approaches. NIST anticipates using operational collections of visa images, mugshot captures, photojournalism images, and others collected for dedicated studies. FRVT 2016 will also measure accuracy of age and gender estimation algorithms.

Read more: http://www.nist.gov/itl/iad/ig/frvt-home.cfm

IREX - Iris Recognition

The ninth activity under NIST’s Iris Exchange (IREX) umbrella program supporting interoperable iris recognition will start in September 2016. It will extend the one-to-many iris evaluations of the IREX III and IREX IV evaluations of 2010 - 2012 by using expanded and higher quality operational datasets to refine iris recognition accuracy at low false positive identification rates. IREX IX will additionally run two novel one-to-one verification trials. The first will quantify accuracy for non-frontal-gaze iris images; this, we hope, will approximately represent the challenges associated with relaxed acquisition, highly usable, rapid authentication on portable devices such as smart phones. Second, the test will characterize accuracy of algorithms capable of matching near infrared images against visible light images.

Read more: http://www.nist.gov/itl/iad/ig/irex.cfm

On-Card Comparison

NIST will resume its evaluation of on-card comparison (OCC) implementations later in 2011. In three phases running from 2007 to 2011, the MINEX II program showed some algorithms implemented on ISO/IEC 7816 conformance smart cards could compare ISO/IEC 19794-2 compact templates with accuracy approaching that of off-card analogues, and do so within a few tenths of a second. The new evaluation MINEX IV supports the US Government’s PIV identity credential which optionally includes OCC, and upcoming payment applications based on OCC. The now running MINEX III tests supports off-card comparison and has added more image samples, new more stringent performance targets and a new semantic conformance test to the original MINEX assessment NIST published in 2006.

Read more: http://www.nist.gov/itl/iad/ig/minex.cfm

Fingerprints: Giving Child an Identity

There is a growing demand for biometrics-based recognition of children for a number of applications (e.g. tracking child vaccination schedules, identifying missing children, preventing
fraud in food subsidies), particularly in developing countries where children, as well as their parents, lack any form of identification. Our objective is to develop a fingerprint-based ID system for children (0-48 months). This ongoing research is addressing following issues: (i) design of a compact, ergonomic, high-resolution (1000ppi) fingerprint reader; (ii) image enhancement algorithms to improve quality of child fingerprint images; and (iii) collection of longitudinal fingerprint data to evaluate recognition accuracy over time. This collaborative research project involving four partners (Michigan State University, Dayalbagh Educational Institute, Saran Ashram Hospital, Agra, India and NEC Corporation), funded by the Gates Foundation and VaxTrac, has resulted in following findings: (i) 500ppi fingerprint resolution is adequate for recognizing children over 12 months of age, (ii) fingerprint resolution close to 1000ppi is needed to recognize children in 6+ months age group, and (iii) newborns and infants in 0-6 months age group are difficult to recognize with state of the art fingerprint technology. These findings are based on longitudinal fingerprint data (left and right thumbs) of about 200 children, collected at four different time instants over a 12 month period. High quality fingerprint image capture is the single most important challenge for recognizing children. For details, see the following publications and presentations. By Anil Jain.

Read more:

http://biometrics.cse.msu.edu/Presentations/NIST_IBPC_May4_2016_short_updated_Final.pdf


4. Industry

Advent makes a bid for Safran’s biometric identification unit

Reuters is reporting that private equity fund Advent has made a bid for Safran’s biometric identification unit Morpho with the aim to merge it with Advent-owned Oberthur Technologies. In an interview with French newspaper Le Figaro, the head of Advent France, Cedric Chateau, said that the merger of the two firms could create a France-based world leader in secure authentication. A Safran spokesman declined to comment on Advent’s offer.

In April, Safran agreed to sell its U.S.-based Morpho Detection business and related activities to UK engineering firm Smiths Group (SMIN.L) for $710 million. At the time, Chief Executive Philippe Petitcolin said Safran continues to assess the future of another security business that makes identity cards and biometric systems and that those units also could be put up for sale, according to a Wall Street Journal report.


Privacy Multistakeholder Process: Facial Recognition Technology

The National Telecommunications and Information Administration announced that the goal of the multistakeholder process is to develop a voluntary, enforceable code of conduct that specifies how the Consumer Privacy Bill of Rights applies to facial recognition technology in the commercial context. Over the past two years, stakeholders involved in the process have discussed how best to ensure that consumers’ rights to control, transparency, security, access and accuracy, focused collection and accountability are respected within the context of current and emerging commercial uses of facial recognition technology. In the summer of 2015 however, after 16 months of discussion, all of the privacy advocates who participated in the process, which included: the American Civil Liberties Union, the Electronic Frontier Foundation, the Center for Digital Democracy, and the Consumer Federation of America, decided to withdraw from further negotiations. Stakeholders at the June 15, 2016 meeting agreed to conclude the process, and a group of stakeholders came to consensus on a best practices document.

Read more: https://www.ntia.doc.gov/other-publication/2016/privacy-multistakeholder-process-facial-recognition-technology
Samsung sees biometrics as a pillar of Samsung Pay security

Samsung representatives have given an update on Samsung’s major payments platform at the Money20/20 Europe conference.

Samsung sees biometrics as an important part of Samsung Pay, when it comes to strengthen the security in payments. The major consumer use case for mobile biometrics is payments. What has not been clear is how the OEMs like Samsung and Apple see biometrics in terms of the mcommerce value proposition. With mobile wallets, the name of the game is most often convenience, with security regularly going unmentioned in any announcements about the services.

Elle Kim, Vice President, Samsung Pay, highlighted Samsung Pay’s biometric security as one of the mpayment solution’s foundations, along with KNOX and tokenization. She said they are currently using fingerprint authentication and they are developing biometric sensors so that Samsung phones and Samsung Pay can be more secure.

5. Offerings

PostDoc Positions at Univ. Autonoma de Madrid, Spain

Univ. Autonoma de Madrid has opened a public call for postdocs in similar conditions to the prestigious EU Marie Curie Fellowships.

More information is available here: [http://media.fuam.es/intertalentum](http://media.fuam.es/intertalentum)

The Biometric Recognition Group - ATVS ([http://atvs.ii.uam.es](http://atvs.ii.uam.es)) will be happy to help proposers and host them to develop projects focused on biometrics.

Please contact [mailto:atvs@uam.es](mailto:atvs@uam.es) for further details.
6. Software, Databases and Journals

Biometrics Evaluation and Testing (BEAT)

After 4 years of development Open Source the BEAT Platform has been released:
https://www.beat-eu.org/platform

Call for Papers - IEEE Journal of Selected Topics in Signal Processing

Special Issue on Spoofing and Countermeasures for Automatic Speaker Verification

Automatic speaker verification (ASV) offers a low-cost and flexible biometric solution to person authentication. While the reliability of ASV systems is now considered sufficient to support mass-market adoption, there are concerns that the technology is vulnerable to spoofing, also referred to as presentation attacks. Replayed, synthesized and converted speech spoofing attacks can all project convincing, high-quality speech signals that are representative of other, specific speakers and thus present a genuine threat to the reliability of ASV systems.

Recent years have witnessed a movement in the community to develop spoofing countermeasures, or presentation attack detection (PAD) technology to help protect ASV systems from fraud. These efforts culminated in the first standard evaluation platform for the assessment of spoofing and countermeasures of automatic speaker verification - the Automatic Speaker Verification Spoofing and Countermeasures Challenge (ASVspoof) - which was held as a special session at Interspeech 2015.

This special issue is expected to present original papers describing the very latest developments in spoofing and countermeasures for ASV. The focus of the special issue includes, but is not limited to the following topics related to spoofing and countermeasures for ASV:

- vulnerability analysis of previously unconsidered spoofing methods;
- advanced methods for standalone countermeasures;
- advanced methods for joint ASV and countermeasure modelling;
- information theoretic approaches for the assessment of spoofing and countermeasures;
- spoofing and countermeasures in adverse acoustic and channel conditions;
• generalized and speaker-dependent countermeasures;
• speaker obfuscation, impersonation, de-identification, disguise, evasion and adapted countermeasures;
• analysis and comparison of human performance in the face of spoofing;
• new evaluation protocols, datasets, and performance metrics for the assessment of spoofing and countermeasures for ASV;
• countermeasure methods using other modality or multimodality that are applicable to speaker verification.

Also invited are submissions of exceptional quality with a tutorial or overview nature. Creative papers outside the areas listed above but related to the overall scope of the special issue are also welcome. Prospective authors can contact the Guest Editors to ascertain interest on such topics.

Prospective authors should visit http://www.signalprocessingsociety.org/publications/periodicals/jstsp/ for submission information. Manuscripts should be submitted at http://mc.manuscriptcentral.com/jstsp-ieee and will be peer reviewed according to standard IEEE processes.

Important Dates:
Manuscript submission due: August 1, 2016
Publication date: June, 2017
7. Events

Calendar

<table>
<thead>
<tr>
<th>Event</th>
<th>Where</th>
<th>When</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAB Workshop Performance and Evaluation of Mobile Biometrics</td>
<td>Paris, France</td>
<td>22.07.16</td>
</tr>
<tr>
<td>8th IEEE International Conference on Biometrics: Theory, Applications, and Systems</td>
<td>Niagara Falls, NY, USA</td>
<td>06.09.16 – 09.09.16</td>
</tr>
<tr>
<td>EAB Research Projects Conference</td>
<td>Darmstadt, Germany</td>
<td>19.09.16 – 20.09.16</td>
</tr>
<tr>
<td>EAB Biometrics Research and Industry Awards</td>
<td>Darmstadt, Germany</td>
<td>21.09.16</td>
</tr>
<tr>
<td>15th International Conference of the Biometrics Special Interest Group</td>
<td>Darmstadt, Germany</td>
<td>21.09.16 – 23.09.16</td>
</tr>
<tr>
<td>23rd International Conference on Pattern Recognition</td>
<td>Cancun, Mexico</td>
<td>04.12.16 – 08.12.16</td>
</tr>
</tbody>
</table>


The IEEE Eighth International Conference on Biometrics: Theory, Applications, and Systems (BTAS 2016), a continuation of the highly successful BTAS conference series started in 2007, will be held in the September 6 - 9, 2016 time period in Niagara Falls, Buffalo, New York (USA). BTAS 2016 is a premier research conference focused on all aspects of biometrics. It is intended to have a broad scope, including advances in fundamental signal processing, image processing, pattern recognition, and statistical and mathematical techniques relevant to biometrics.

Areas of coverage include biometrics based on voice, fingerprint, iris, periocular, face, handwriting, gait and other modalities, as well as multi-modal biometrics and new biometrics based on novel sensing technologies. Submissions will be rigorously reviewed, and should clearly make the case for a documented improvement over existing state-of-art. Experimental
results for contributions in established areas such as voice, face, iris, fingerprint, and gait are encouraged to use the largest and most challenging existing publicly available datasets.

The Swiss Centre for Biometrics Research and Testing and the Biometric group at Idiap Research Institute organize the Speaker Anti-spoofing competition at BTAS 2016.


**EAB Research Projects Conference – EAB-RPC’16, Darmstadt, Germany 19-20 September 2016**

On 19 and 20 September 2016 Europe’s largest conference on research in the area of Biometrics and Identity Management funded by the European Commission will take place at the premises of Fraunhofer IGD in Darmstadt, Germany. The third EAB Research Projects Conference 2016 will be co-located with the IEEE BIOSIG conference that will take place later that same week. The European Association for Biometrics (EAB) and numerous EU research projects, namely FIDELITY, FastPass, BEAT, FutureID, MobilePass, Eksistenz, PCAS, PIDaaS, ORIGINS, ABC4EU, INGRESS, HECTOS, BODEGA, OCTAVE and PROTECT are jointly organizing the 3rd EAB Research Projects Conference (EAB-RPC) to present research results and to discuss the benefits of this research for our European society. This third conference will present updates of the projects introduced in the first and second conference. New projects in the fields of border control, speaker identification, template protection and more will be presented. Experts from the biometric community will report about their results.

The European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) and also the Directorate-General of Migration and Home affairs (DG Home) will be supporting the event by contributing keynote talks. Moreover both institutions as well as the European Agency for the Management of External Borders (Frontex) will discuss current and future research objectives in a panel discussion "Mind the gap - what research is needed for current and future operational biometric systems". DG Home will also provide an overview of current research projects and the future work programme in the field as supported by the Horizon 2020 "secure Societies" challenge.

Motivation: Biometrics and Identity Management are key research topics that are currently investigated in a variety of EU projects running under the seventh Framework Programme (FP7) and in the Horizon 2020 research program. International research is dealing with innovative solutions for secure and privacy compliant biometrics and federated identity management. For the third time all major European research projects in the area of Biometrics and Identity Management will be provided with a single platform for information exchange and discussion. This will contribute to a stronger research community at European level and a stronger position for European R&D in an international context.

Read more: [http://eab.org/events/program/104](http://eab.org/events/program/104)
EAB Biometrics Research and Industry Awards 2016, Darmstadt, Germany 21 September 2016

EAB is launching the tenth European Biometrics Research and Industry Awards 2016. These prestigious awards are granted annually to individuals who have been judged by a panel of internationally respected experts to be making a significant contribution to the field of biometrics research in Europe.

Attendance is free of charge, Registration is required!

Read more: http://eab.org/events/program/106

15th International Conference of the Biometrics Special Interest Group – BIOSIG’16, Darmstadt, Germany 21-23 September 2016

Biometrics provides efficient and reliable solutions to recognize individuals. With increasing number of identity theft and miscues incidents we do observe a significant fraud in e-commerce and thus growing interests on trustworthiness of person authentication. Nowadays we find biometric applications in areas like border control, national ID cards, e-banking, e-commerce, e-health etc. Large-scale applications such as the European Union Visa Information System (VIS) and Unique Identification (UID) in India require high accuracy and also reliability, interoperability, scalability, system reliability and usability. Many of these are joint requirements also for forensic applications.

Multimodal biometrics combined with fusion techniques can improve recognition performance. Efficient searching or indexing methods can accelerate identification efficiency. Additionally, quality of captured biometric samples can strongly influence the performance. Moreover mobile biometrics is an emerging area and biometrics based smartphone can support deployment and acceptance of biometric systems.

However concerns about security and privacy cannot be neglected. The relevant techniques in the area of presentation attack detection (liveness detection) and template protection are about to supplement biometric systems, in order to improve fake resistance, prevent potential attacks such as cross matching, identity theft etc. The BIOSIG 2016 conference addresses these issues and will present innovations and best practices that can be transferred into future applications.

Read more: http://fg-biosig.gi.de/biosig-2016.html
Hosted by the Mexican Association for Computer Vision, Neurocomputing and Robotics (MACVNR) 23rd International Conference on Pattern Recognition will be an international forum for discussions on recent advances in the fields of Pattern Recognition, Machine Learning and Computer Vision, and on applications of these technologies in various fields. The Scientific Program is organized in five tracks, addressing several Pattern Recognition topics where one track focuses on biometrics: “Document Analysis, Biometrics and Pattern Recognition Applications”.

Read more: http://www.icpr2016.org
Norwegian Biometric Laboratory (NBL) Annual Workshop, Gjøvik, Norway, MD, USA, 25 February 2016

The theme of this workshop was “The future of biometrics” and speakers from Canada, the Netherlands, Norway, India and Switzerland presented their vision on this future. The event was opened by the director of CCIS, Sofie Nystrøm, immediately followed by the director of the NBL, Prof. Christoph Busch who presented the Norwegian Biometric Laboratory.

In the morning session Prof. Issa Traore from the University of Victoria in Canada presented Myths and Reality of biometrics. In his presentation he stressed the differences between biological and behavioural biometrics and he gave his own perspective on the future of biometrics. The second presentation was from Pawel Dworzecki from the Oslo based company Zwipe. The company is involved in biometric smartcard solutions that make identification and authentication much more user friendly and faster. The morning session was concluded by Frøy Løvåsdal, a senior adviser in the area of biometrics and identities at the National ID Centre of Norway. She stressed the need for biometrics for refugee registration, but included also the need for soft biometrics, where individuals are not identified as such, but classified as belonging to a specific group, e.g. based on gender or age. Such a soft biometric solution could be used to refute the claim of adult refugees that want a refugee status as a minor. Current procedures are expensive and time consuming and soft biometric facial recognition might be an actual advantage in both time and costs.

The first presentation after the lunch was by Sébastien Marcel from Idiap in Switzerland. His presentation was on reproducibility of research. Published biometric research is often hard to check because of availability of data and/or evaluation software. At his institute a platform was developed (BEAT) that could solve this issue and make biometric results more trustworthy. Dr. Soumik Mondal from NTNU was the next to present. Dr. Mondal had done his research in behavioural biometrics and in his presentation predicted a future where behavioural biometrics would gain a more prominent place in the research community. The final presentation of the day was by Assistant Professor Luuk Spreeuwers from the University of Twente in the Netherlands. His cry for help was aimed at telling the audience that the academic research was in danger because major companies like Google, Apple and Facebook were getting involved also in the area of biometrics. Such companies have more research available, in terms or staff, money and databases. He gave an example of a face database of 260 million images and a research budget of 350 M US dollar. Besides pointing out the dangers for the academic biometric community he also suggested a number of tasks for this community to take upon themselves to cope with the situation of the big players in the field of biometrics.
At the end of the workshop a panel discussion was held. Questions had been collected and rated by the audience during the day and given to the panel. The panel discussion was very lively with a good interaction from the public.

The future of biometrics might not be completely clear after this workshop, but the various viewpoints of the speakers and panel can be taken into consideration by all the participants of the workshop.

The slides of the workshop are available at: [http://eab.org/events/program/115](http://eab.org/events/program/115)

The 7th NBL Annual Workshop is scheduled for 23rd of February 2017

---

**German TTT Biometrics Working Group Meeting, Darmstadt, Germany, 22nd March 2016**

The spring meeting of the German Biometrics Working Group was hosted in Darmstadt by CASED ([www.cased.de](http://www.cased.de)) and took place on March 22nd, 2016. The meeting with 48 participants featured numerous reports on biometric applications and most recent research results.

Volker Kozok from the German Ministry of Defense reported about use cases of the German army and the compliance of biometric applications with national and international regulations. Major applications are serving access control for armed areas and IT-infrastructure. Moreover person identification plays an important role, which is applied in crisis areas, migrant’s streams analysis as well as of disaster victim identification. Also in focus are open source intelligence (OSINT) use cases of face recognition comparing facial images at border crossings with public social media sources. This application is also linked with image intelligence (IMINT). Handheld Interagency Identification Detection Equipment (HIDE), concerns capture methods such as live-scan, standoff and forensic captures. Field capture scenarios do require robustness for various weather conditions. Biometric Enabled Watch List (BEWL) is shared between international forces and is provided on mobile capture devices. Biometric Enabled Intelligence (BEI) complements the situation analysis. In an increasing number of situations biometric will replace knowledge-based access control. Open issues are presentation attacks and attacks against reference datasets.
Micha Kraus (Bundesdruckerei) reported about a Biometrics-on-Card project. The evolution of the development includes Storage-on-Card, Comparison-on-Card up to full System-on-Card. The new System-on-Card is realized as a no battery solution as energy supply is realized with energy harvesting at 25mW. The multi-functional smart card is equipped with a capacitive fingerprint sensor, a PIN pad and a user-friendly LED display. The card is compliant to the new card standards ISO/IEC 18328-2 (ICC-managed devices) and ISO/IEC 17839 (biometric system on card). The MINEX-II biometric algorithms, which are ISO/IEC 19794-2 compliant, were chosen as master algorithms and are requesting 16 minutia as minimum. Presentation attack detection functionality is shifted to the background system. On the card a BioManager is separating applet functionality from sensitive biometric data. The Yes-Card attack, which is not a biometric-only problem, is handled with a chip-authentication protocol. User convenience was also in focus of the development and high usability was achieved with early user experience feedback workshops. The initially selected bi-stabile display was considered as too contrasted and has been replaced with a LED display.

Eckardt Mohr (Behaviosec) discussed keystroke dynamics under the new European PSDII regulation. Two factor authentication was already requested in the US area by Federal Financial Institutions Examination Council (FFIEC) and is now also enforced in Europe through PSDII since January, 2016. With the new regulation, enter into force on Jan 13, 2018, strong customer authentication is requested for any remote access, which is related to a payment transaction. Strong customer authentication does require two out of three possible elements, knowledge, possession and inherence. The Behaviosec technology works by observing how the user interacts with a device or browser, analyzing the rhythm of typing, the deftness of touch, the unique combination pressure, swipe speed, finger positioning and velocity as the user navigates within an app. The recorded keystroke timing data is then processed through a unique neural algorithm, which determines a primary pattern for future comparison. The real-time solution has a response time of 25 milliseconds. Evaluation of username, password and unique ID shows an accuracy of 98%, while 8-digit transaction authentication reached 94%.

Martin Olsen (Hochschule Darmstadt) presented the NFIQ2.0 project, which has been released in April 2016 after 5 years of development and extensive testing. The intention of NFIQ2.0 is to quantify characteristics in the biometric fingerprint
image and to relate them to biometric performance, while handling temporary conditions as well as permanent factors. NFIQ2.0 has identified 69 features, which were selected based on their contribution to prediction accuracy and the time consumption that an individual feature requires. Features are representing both global and local properties of the fingerprint pattern. Evaluation was performed on operational data from the U.S. NIST and the German Federal Criminal Police Office. Evaluation was done on operational data from the U.S. NIST and the German Federal Criminal Police Office. Evaluation was done with correlation analysis, error versus reject curves, and ranked detection error tradeoff curves.

Josif Grabocka (University Hildesheim) presented a general Machine Learning approach for computing invariant features derived from time-series data. The approach is outperforming neural network or support vector machine classification and is specifically suited, if a signal contains noise and if probe and reference data are shifted to each other. The strategy is a reconstructive factorization mechanism using a sliding window segments and a numerical optimization. The method is exploiting time-series shapelets, which are used in a minimum distance measure between shapelets and all segments of the time series.

Speaker recognition was presented by Robin Bortz (Nuance). He showed how voice biometrics is entering the mainstream with a growing list of deployments in the financial space. The evolution of voice recognition was presented highlighting technology and accuracy improvements such as advanced algorithms using Deep Neural Networks, Super Background Models and voiceprint adaptation. New advancements also include Risk based decision which will generate specific thresholds for every single user. Recordings are addressed in two ways by footprint detection and playback channel detection that detects signal attributes that are introduced during the playback process. The technology also includes both liveness detection as well as synthetic speech detection. The products today support active and passive verification over all channels, telephone, mobile and web as well as solutions for fraud detection.

Slides of the meeting are available at: http://eab.org/events/program/109

The next meeting will take place in Darmstadt on September 21st, 2016.

The agenda will be announced at: http://www.eab.org/events/program/105

**Norwegian Biometrics Forum, Oslo, Norway, 29th April 2016**

The spring edition of the Norwegian Biometrics Forum was organized on April 29th at the National ID Center in Oslo. More than 40 participants representing government agencies, industry and research organizations from Norway, Sweden, Denmark and other non-Scandinavian countries were represented. The Norwegian Biometrics Forum is an informal meeting place for presentation and discussion in the field of the use of biometrics. The following speakers presented their projects.
Annar Bohlin-Hansen reported on the status of the IDeALL program. The target date for launching of the new enrolment is delayed until the autumn of 2017. The planning includes a central ABIS system, a new management system for Passport and National ID cards as well as mobile units to be used in person control, amongst others. The fingerprint search time, within the database, has now been reduced from several hours to a few seconds. The possible use of mobile devices should make it possible to reduce the transaction time even more. In addition to the fingerprint system, the ABIS contains face recognition and will optionally include iris. The Norwegian government has now decided that the national eID will be rolled out, based on the enrolment and carried by the National ID card.

Justus Heuzeveldt (WCC) presented the work that was done for the registration of refugees in charge of the United Nations High Commissioner for Refugees (UNCHR). The system is fusing biometric and alpha-numeric information for the purpose of de-duplication. The system is operated in the UNCHR headquarter in Geneva. The biometric functionality is based on face, iris and fingerprint, where sequential biometric algorithm fusion is done for fingerprints. The UNCHR is in charge of 30 million refugees in 125 countries. Equipment is required to resist difficult environmental conditions such as heat, dust and humidity.

Stephan Hackenberg and Geir Bredholt (IDEX) discussed biometrics on card and credentials. Based on a reflection on the adoption of biometrics on mobile phones, challenges for a wider adoption of biometrics on cards, credentials and embedded systems have been highlighted. Three main areas are to be considered - power consumption, limited system calculation power and system ruggedness. In 2015, according to the SMART PAYMENT Alliance, a volume of 2 billion conventional, non-biometric banking cards have been issued. IDEX presented flexible fingerprint sensor solutions to comply with ISO mechanical test standards (ISO 10 373). Cards as well as the embedded sensor must cope with bending and torsion tests, which require a fully flexible sensor. To achieve lowest cost of
ownership, standard card manufacturing processes need to be supported. IDEX is building upon its experience in off-chip polymer sensing and provides this technology into a wide field of applications.

Pawel Dworzecki (Zwipe) discussed with the Forum the market expectations for the biometric market. He outlined the challenges that are related to remote communication, which caused a significant increase of use of authentication form factors. Fingerprints are favored due its rich biometric entropy. Biometric identification is considered in forensic investigations and refugee enrolment. For biometric verification convenient authentication schemes are in focus, in order to eliminate seals and password pins. The Zwipe card is operating with harvested energy from 13.56 mHz readers and such can communicate via NFC with Smartphone.

Guoqiang Li (NTNU) reported about his PhD project, which is relevant for large scale applications such as the UIA of India (over 1 billion subjects), US-Visit (90 million), FBI-IAFIS (over 100 million) and the EU-VIS (20 million). He illustrated the need to subdivide databases in identification scenarios, in order to keep the response time in reasonable constraints. An efficient approach to reduce the search space is based on fingerprint indexing. Such indexing methods can operate on local minutia ridge information, which in turn is derived from minutiae points. Derived features are geometric features of minutia vicinities (triangles), ridge curvatures and ridge densities. He also presented a binarisation method, which is based on a clustering method. Another part of the presentation concentrated on indexing methods for encrypted fingerprint databases. Evaluation of the presented methods was done based on the international standard for biometric performance measurements in terms of penetration rate and the pre-selection error rate. Experimental results show good performance of the proposed approaches.

Atle Arnes informed about the General Data Protection Regulation (GDPR), which was adopted by the Members of the European Parliament on April 14, 2016. Parliament’s vote ends more than four years of work on a complete overhaul of EU data protection rules. The reform will replace the current data protection directive, dating back to 1995. The new rules provide for special safeguards for children in some areas, as they may be less aware of risks and consequences related to sharing their personal data. For instance, they will have a clearer right to be forgotten. Fines of up 20 million euros or up to 4% of firms' total worldwide turnover should constitute a real deterrent to breaking the rules. Of interest is also the new obligation to be informed to when personal data has been hacked. Article 9 handles sensitive data, which addresses biometric data. The regulation also includes a directive on data transfer for policing and jurisdictional purposes.

Ctirad Sousedik (NTNU) introduced fingerprint imaging with Optical Coherence Tomography (OCT), which is robust against presentation attacks, e.g. executed with artefacts such as silicon fingers. The essential principle is not to learn properties of artefacts that may be varied with no limitation, but rather to develop a presentation attack detection technique, that can learn a
Bona Fide finger (a.k.a. real finger). The OCT scanning looks inside the finger and visualizes the reflection from internal layers and enables one to spot sweat glands.

Bjoern Syvertsen (Kripos) reported about the Prüm system, which was established to prevent and combat serious crime. The system is intended to support the to exchange fingerprint data. The main purpose of the project is to enforce cooperation of European countries in DNA, fingerprint and vehicle information. Kripos is serving as the Norwegian contact point (NCP). Currently Norway has 70,000 DNA profiles, while in the entire EU there are 6 million profiles stored. In the Norway there are approx. 50,000 cases involving non-norwegian citizens each year, and by increasing the use of the Prüm system there is a potential to solve a larger number of these cases.

More information and slides are available at: http://eab.org/events/program/125

The next NBF meeting is scheduled for October 28th, 2016.

International Biometric Performance Testing Conference (IBPC’16), Gaithersburg, MD, USA, 3-5 May 2016

Presentation Attack Detection (PAD) and specifically fingerprint alteration detection was mentioned in the keynote talks of Nick Megna (FBI) and Jim Cole (DHS) in the opening session of the conference.

It was observable that biometrics on mobile systems is a major trend in 2016. Jonas Anderson (Fingerprint Cards) opened that discussion and raised the request for standards on security testing of mobile devices – incorporating biometric performance testing (false accept rate and presentation attack detection accuracy). He also raised the issue that certification of biometrics on mobile devices must adjust to the short live-cycles of smartphones, which are typically 12 month development period and approximately 18 month use period before replacement by the next generation.

The same set of metrics was also requested by Elaine Newton and Colin Soutar, who presented the NIST activity on determining the strength of biometric authentication. The intention of this project is to balance biometric strength with knowledge based authentication strength. Hopefully this activity will be continued as a ISO/IEC standardisation project.

Christopher Boenen (IARPA) presented the ODIN program, which is focused on face,
finger and iris modalities. In the ODIN program known and unknown presentation attacks and detection methods shall be researched.

Ines Goicechea-Telleeria (UC3M) presented the application of ISO/IEC 30107-3 metrics to an evaluation of artefacts on various live scan sensors. The presentation reported about the Attack Presentation Non-Response Rate (APNRR), Attack Presentation Non Capture Rate (APNCR) Attack Presentation Non-Match Rate (APNMR) and Attack Presentation Match Rate (APMR).

Elaine Newton (NIST) and Stephanie Schuckers (Clarkson University) recommended on for levels of risk in a testing framework, which are applied to fingerprint, face, iris, voice. This contribution incorporates the experience from the 5 previous LivDet competitions and specifically the knowledge or absence of knowledge of artefact species that are tested.

Akira Ostuka (AIST) reported about security evaluation of vascular biometrics. He highlighted the relationship between attack potential (AP) and the Attack Presentation Classification Error Rate (APCER) and illustrated the potential gap between a best effort test conducted in a test lab and an exhaustive test conducted by an attacker. He illustrated his approach using a simulated sensor, which is re-engineering the University of Twente vein sensor (introduced at IJCB 2014).

Anil Jain (MSU) reported on Fingerprint Recognition for newborns and young kids. With high resolution sensors (1000 ppi and 1270 ppi) it was shown that ridge patterns are visible in good quality and can be used for recognition.

Elham Tabassi (NIST) presented the new Fingerprint Image Quality algorithm (NFIQ2.0), which was released end of April, 2016. She presented the approach, the machine learning concept and the evaluation on the NIST operational dataset. An independent evaluation was conducted by Timo Ruland (BKA) concluding that NFIQ2.0 is indeed outperforming NIFQ1.0. Martin Olsen (NTNU) explained the 69 features that were identified as valuable contributive measures in the NFIQ2.0 project.

Fares Rahmun (BVA) reported about the German pilot for the Smart Border System, which was conducted to realize an Entry-Exist-System (EES). Pilot sites were Frankfurt Airport and the seaport in Warnemünde. De-Duplication was tested with a simulated dataset of 300 million records. Dan Bachenheimer (Accenture) talked about the pilot at the airport in Helsinki. The Smart Border System pilot results are reported in the Eu-LISA Pilot Report (http://www.eulisa.europa.eu/Publications/Reports/Smart%20Borders%20-%20Technical%20Report.pdf). The experience from these pilots was incorporated in the European strategy paper, which was published in April.
The conference was attended by 176 participants from 10 countries. 49 speakers covered a very rich program over three days. The slides are online as PDFs:

http://www.nist.gov/itl/iad/ig/ibpc2016_presentations.cfm

Videos are available at:

http://www.nist.gov/itl/iad/ig/international-biometric-performance-testing-recording.cfm

Technical Colloquium Quantifying the weight of forensic evidence at IBPC’16, Gaithersburg, MD, USA, 5-6 May 2016

During the past decade, paradigm shifts in forensic science have introduced a variety of emerging decision frameworks to established fields of practice, which concern likelihood ratios, Bayes factors, and evidence analyses. In the NIST IBPC’16 technical colloquium, the latest advances in the forensic field as well as statistical challenges in forensic evaluation and reporting were presented on May 5th & 6th, 2016. Thereby, three open discussion and two panel discussions were held, in which questions of the web-stream audience were included as well. 60 people attended the event in-person and about 100 web-followers attended the technical colloquium.

Currently, Bayesian decision frameworks are strongly recommended by the European Network of Forensic Science Institutes (ENFSI) and are part of an emerging ISO/IEC 19795 standardization project. However, in the past decade, forensic scientists were exhaustively arguing about, whether to use Bayesian methods at all. Nowadays, implementation-related discussions of Bayesian methods take place, for which the technical colloquium provided space. In forensics, decision process roles are well-disjoint: the forensic scientist transfers legal questions into scientific questions, examines the weight of the evidence represented by a questioned mark and some reference specimen of known origin. Thereby, the decision stage is utterly province of court, i.e. the forensic scientist provides the weight of the evidence in the form of a likelihood ratio, which shall lead to good juristic decisions from prosecution and defense perspectives, respectively. The likelihood ratio provides (Bayesian) support considering similarity among the questioned and reference materials, as well as typicality of those materials in a relevant population defined by the relevant propositions in the case. Compared to biometric systems, this role-relationship can be thought of algorithm vendors and system operator decision policies, where the underlying mated and non-mated models are selected on a case-by-case basis.

During the IBPC’16 technical colloquium, the first discussion held concerned validity aspects of different Bayes-based approaches and how/whether verbal representation tagging for
likelihood ratio values are sensible. Therefore, the first talks provided an introduction to related topics from different aspects of court cases, forensic and statistic conceptions to variants of communicating evidence weights between forensic scientists and courts as well as statistical challenges for evaluating and reporting forensic evidence using the likelihood ratio framework. The second discussion involved various fundamental perspectives in mathematical reasoning from the broad range of forensic disciplines with biometric and non-biometric background. In advance of the second discussion, different evidence quantization approaches were compared, and the need for probabilistic logic in US army practice was stated for latent fingerprint examinations.

On the second day, the third discussion session followed presentations of best practices in DNA, firearms, toolmark, and speaker recognition, reassessing combined questions to the presenters. Two panel discussions concluded the technical colloquium emphasizing types of likelihood ratio models, and intervals measuring so-called likelihood ratio uncertainty in terms of credibility rather than certainty. Thereby, panelists were asked to answer three related questions in 10 minutes and to oppose other panelists having 5 minutes, respectively, before auditorium question of about 30 minutes were raised. The discussions included a wide range of topics from (forensic) practitioners, statisticians, academics, and judicial system perspectives. Also, analyses were provided regarding the inclusion of forensic witness reports into (legal) decision simulations, where the test persons utilized likelihood ratios in decision making not as intended by the likelihood ratio framework, i.e. different magnitudes of evidence weight resulted in effectively similar decisions, motivating more appropriate communication designs between forensic scientist and the court.

The first IBPC’16 forensic satellite is a great success for the working progress within the widespread forensic community: paradigm conceptions were discussed, verbal tagging of likelihood ratios was issued to revision, probabilistic methodologies were consolidated, and calibration incorporating underlying probabilistic principles, which was previously perceived as a pure score transformation, is also considered as a desirable property for likelihood ratios. Overall, the technical colloquium took benefit of well-placed introductions, tense and respectful discussions as well as audience-interactive panel discussions.


Nearly 100 participants from 27 different countries attended ICB 2016 held at Halmstad University Campus, Sweden, from 13rd to 16th June.

The conference was technically co-sponsored by both IAPR TC4 (Technical Committee on Biometrics) and the IEEE Biometrics Council, and it also counted with the support of the European Association for Biometrics (EAB), and the Center for Applied Intelligent Systems Research (CAISR) of Halmstad University.
ICB-2016 received 151 submissions, of which 22 were selected for oral presentation and 30 for poster presentation. The review process was managed by four Program Committee Chairs, with the assistance of 31 Area Chairs and 120 Program Committee Members. The whole process was conducted double blind in Microsoft CMT with at least three reviewers per paper. The papers accepted cover a wide range of topics – from Optical Coherence Tomography for fingerprint sensing to Deep Learning for iris segmentation. “Face Recognition” attracted the highest number of submissions followed by “Other Biometrics and Fusion”. Traditionally, “Fingerprint and Palmprint” has attracted the second highest number of submissions, but not so in 2016. This indicates the growing interest in other modalities like vein patterns, signature, gait, and novel traits based on electrophysiological signals. The papers will be made available in IEEE Xplore.

The program was enriched by four invited talks by eminent speakers from industry and academia. The invited keynote speakers included David Burnett, VP for Global Ecosystem Development at Fingerprint Cards AB. While the last two years have seen significant adoption of biometrics in mobile devices, much work remains to realize their benefits and firmly cement their convenience and security benefits into every-day consumer use. In his talk, Mr. Burnett shared his unique insights and experience from an industry perspective, explaining the adoption pattern for biometric solutions at internet-scale, outlining the missing pieces of infrastructure needed to make biometric authentication truly pervasive, and providing a multi-year forward look into biometric adoption trends for a wide range of device types, ecosystems and major milestones/industry turning points.
The second keynote by James Loudermilk, Senior Level Technologist at the FBI Science and Technology Branch, USA, explained the four successive technology insertion programs conducted over the decades by the FBI Fingerprint Program. Since 1924, the FBI has been the United States national repository for fingerprints and related criminal history data and today, the FBI's master criminal fingerprint file contains the records of about 71.2 million individuals, while the civil file represents about an additional 39.5 million individuals. An average of 220+ thousand tenprints is processed daily, with an average response time of 8 minutes for criminal answer required transactions during FY2015, 91 minutes for civil transactions, and 9 seconds for rapid fingerprint searches.

The third keynote speaker was Didier Meuwly, Principal Scientist of the Netherlands Forensic Institute and Chair of Forensic Biometrics, University of Twente, The Netherlands. In his talk, Prof. Meuwly concentrated on the definition of forensic biometrics, the description of the informative value of the different biometric modalities in a forensic context, and covered the different forensic applications of biometric technology using operational examples. The validation of forensic evaluation methods used to assess the strength of evidence was also presented in detail.

ICB 2016 also featured a distinguished talk by the recipient of the 2016 IAPR Senior Biometrics Investigator Award (SBIA). With the first edition presented in 2014, this award is given once every two years to outstanding scientists in the biometrics field. In this second edition, the prize has been awarded to Prof. John Daugman, University of Cambridge, UK, who delighted the audience with the talk “Biometric Entropy: searching for Doppelgängers and the rare Entropod Uniquorns”. Prof. Daugman explored the biometric entropy within the face and iris modalities, meeting along the way Doppelgängers and the rare, newly discovered creatures, Entropod Uniquorns.

A panel session “Relation/Implications of Forensic Biometrics and Multimedia Forensics” sponsored by the EU-Horizon 2020 Project IDENTITY was chaired by Massimo Tistarelli (University di Sassari). Panelists included Chang-Tsun Li (University of Warwick), James Loudermilk (FBI Science and Technology) and Didier Meuwly (Netherlands Forensic Institute and University of Twente). The panel was successful in extending the discussion to actively involve the audience such that a productive brainstorming could take place.

During the first day, the conference offered four invited tutorials conducted by experts in the field on timely topics that represent promising research directions in biometrics, and resulted in useful discussions between tutors and participants. Five highly motivated PhD students also participated in the Doctoral Consortium, where they presented their research during a regular poster session at the conference, together with a luncheon where ten participants from industry and academia met and provided career advise in a very interactive session with the
students. The conference supported too the organization of four biometric competitions, with papers reporting their results spread throughout different sessions of the conference.

ICB is an annual conference that once in every three years it is celebrated in the USA, merging for such occasions with the BTAS conference (Biometrics: Theory, Applications, Systems) into the International Joint Conference on Biometrics (IJCB). As announced during the gala dinner, next year, IJCB 2017 will take place in Denver, Colorado.

Conference and Workshop ‘Biometrics for Civil ID’ Report, Bunnik, the Netherlands, 15th June 2016

Conference and workshop “Biometrics for Civil ID” was held on June 15th 2016, at the Postillion Hotel in Bunnik, the Netherlands. Speakers were Jasper Mutsaers, Victoria Saue, Max Snijder, Reinier van der Drift, Maarten Wegdam, and others. The conference was opened by Max Snijder, Secretary of European Association for Biometrics.

The first presentation was “Identity Management in 2030 and the role of biometrics” by Jasper Mutsaers. Jasper presented the vision of biometrics usage in Identity Management in 2030 as the result of meeting of international experts in the field of ID management. Two brief video animations with key points were also presented.

The next presentation was “e-Residency and e-Business” by Victoria Saue. Victoria presented ID-card and Digi-ID as convenient and secure methods for using internet banking and e-services in Estonia. The main focus of the presentation was on e-Residency – a secure digital identity intended for everybody in the world interested in running location-independent business online. Target markets for 2016 are USA, Singapore, and India.

The next presentation was about innovative and fast authentication created by iProov company. iProov authentication may be done on PCs, tablets, and smartphones. It consists of several steps: Click, Look, Wait 5 seconds, Done. iProov authentication provides resistance against replay attacks. iProov authentication was demonstrated in live.

During the workshop three scenarios were selected from the ‘Identity Management in 2030’ paper and three groups of participants were created. Scenarios were: 1) fingerprint MOC (Match on Card), 2) voice verification over phone, and 3) remote e-passport verification by using face recognition and a mobile phone. Max Snijder explained the Quick Scan Checklist method to all participants. After that, participants in each group shared ideas, knowledge and opinions. Each group analysed
characteristics of a specified biometric method and discussed feasibility of corresponding biometric applications. The results of workshop were presented to all participants by group representatives.

During the plenary session Reinier van der Drift from MicroFocus presented a very interested comprehensive presentation titled "Authentication Technologies: trends and developments". He gave predictions for the possible successors to fingerprint: vein technology, heartbeat, and/or behavioral methods.

Arnold Roosendaal from Privacy Company presented presentation titled “Opportunities in the eID Market”. Topics such as Security, Privacy, and User experience were dominant during the presentation.

The next presentation was titled "Mobile authentication with e-passport and smartphone” by Maarten Wegdam from Innovalor. The concept of online self-registration, consisting of ID document verification and Holder verification, was promoted. The solution uses ePassport and smartphone. Various use cases were presented.

The next presentation was titled “Biometric ID in Consumer Markets” by Joost van Prooijen from Morpho. It was stated that 8.5 billion people will be in the world by 2030 and 2.4 billion people lack an official ID today. Case studies of National database in Pakistan, Republic of Mali, India, and Europe were presented.

Before the end of the Conference, a Panel Discussion was organized with all presenters. The Panel was moderated by Max Snijder. The subject was the following statement: "It is inevitable that governments will store biometrics of all citizens in order to support national identity management". Panel Discussion was dynamic, contemporary, and professional. Some important questions like “Who is the owner of biometric data?” have been initiated.

The conference and workshop were impressive and presenters have succeeded to present the state of the art in the field of biometrics for Civil ID.

By Professor Dejan Simic

Odyssey: The Speaker and Language Recognition Workshop, Bilbao, Spain, 21-24 June 2016

Odyssey 2016 was hosted by the University of the Basque Country (UPV/EHU) in Bilbao, Spain, from June 21 to June 24, 2016 by the University of the Basque Country (UPV/EHU) and the University of Zaragoza. The ninth Odyssey, a biennial event organized by the ISCA SIG on Speaker and Language Characterization (SpLC), brings together researchers from worldwide, who present their latest findings and insights on a wide range of topics, covering speaker and language characterization, modelling, evaluation, and applications. In this edition, with the help of an international Scientific Committee composed of 96 experts from 20 countries, out of
77 submissions, 59 papers have been accepted for presentation, after not less than 3 and up to 5 reviews per paper.

The 4-day technical program included 3 keynotes, 5 oral sessions, 3 poster sessions and 2 special sessions — chaired by NIST and the ISCA SIG on Speech and Language in Multimedia (SLiM). Besides, a Forensics & Industry track and a Show & Tell session had been allocated to give companies, R&D labs, government agencies and other interested parties (e.g. forensic experts and labs) the opportunity to actively participate in the event. Odyssey 2016 featured 3 invited speakers: Dr. Haizhou Li (Institute for Infocomm Research, Singapore) discussed speech liveness detection in the context of speaker verification, the vulnerability of speaker verification to speech synthesis and voice conversion, and the findings from ASVspoof 2015: the First Automatic Speaker Verification Spoofing and Countermeasures Challenge; Dr. Shrikanth (Shri) S. Narayanan (University of Southern California, USA) put focus on steps toward advancing scientific understanding of how vocal tract morphology and speech articulation interact and explain the variant and invariant aspects of speech signal properties across talkers; finally, Dr. Najim Dehak (Johns Hopkins University, USA) showed how Non-negative Factor Analysis (NFA) and Subspace Multinomial Model (SMM), or other similar subspace approaches, can be used to model the hidden layer neuron activations on the deep neural network model for sequential data recognition tasks such as language and dialect recognition. As previous Odyssey proceedings, all papers are freely online available in the ISCA Archive, and superlectures will provide oral presentation recordings.
Publisher: European Association for Biometrics
Editors: Christian Rathgeb, Max Snijder
Production: European Association for Biometrics
Contact: m.snijder@eubioticsgroup.eu / secretariat@eab.org
Phone: +31 624 603809
Web: www.eab.org