WELCOME MESSAGE

MARK S. NIXON

It is my great pleasure to be elected to serve the IEEE Biometrics Council as its president, from January 2017. I feel truly privileged to have this opportunity to serve the biometrics community and continue to build upon the strong foundations laid out by my predecessors. I have seen biometrics grow from a loose network of academic researchers, before the word biometrics was even coined for our use. Now we are more professional, more organised and reflect better the importance of this new technology. I see the Biometrics Council as an important part of the standards, quality, the future and the proliferation of biometrics technology. I am indeed fortunate to have the support of an experienced and motivated Executive Council (ExCom) that has already been working tirelessly to realize the visions of the council. I would like to thank my predecessor Prof. Venu Govindaraju for his many excellent contributions in promoting the Council in its activities and across the various IEEE societies whilst navigating the IEEE procedures.

Our technology continues to permeate society more and more, and we can observe an increase in deployments due to the many advantages conferred by the use of biometrics. It is also consistent with the developments in society: we need secure access, secure society and secure transactions. As such we can see the proliferation of biometrics in cybersecurity, in forensics and in mobile devices. There are challenges still for our technology, both in terms of technology and approach. The challenges for our council include a need for increasing engagement by recruiting new and innovative members into our community. We continue with the proposal for an IEEE Transactions associated with the Biometrics Council, provisionally entitled the IEEE Transactions on Biometrics and Identity Science, and we hope to communicate positive news in the future.

I look forward to working with all of you as we address these issues and I shall intend that in my presidency that we shall create new success stories and a wider remit in our service for the biometrics community.
Aadhaar program surpasses one billion people registered

The Unique Identification Authority of India (UIDAI) generated the Aadhaar number to over one billion people, touching the landmark in a span of five-and-a-half years since the first Aadhaar was issued in 2010. This comes just a few days after a historic legislation Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act 2016 has been notified by the Government. Aadhaar coverage now is at 93 percent among people above the age of 18 (as per projected population figures of 2015).

Read more: http://tinyurl.com/zstooqz

Distance Learning Program in Biometrics

The Swiss Distance Learning University in cooperation with the IDIAP Research Center is launching an online distance learning program on Biometrics and Privacy. The program will deliver a Certificate of Advanced Studies (12 ECTS) covering 6 main topics:

- Biometric technologies
- Security and Privacy-Preserving Biometrics
- Biometrics Standards
- Legal Aspects
- Ethics, Culture and Society
- Forensic Science

Read more: http://distanceuniversity.ch/casbiometrics/

IBM Turns Cognitive Behavioural Solutions on Cyberfraudsters

Multinational tech firm IBM has announced new behavioural biometric analysis capabilities in its digital banking fraud prevention technology, IBM Security Trusteer Pinpoint Detect.

IBM said that the solution uses patented analytics and machine learning for real-time cognitive fraud detection. The new behavioural biometric capabilities incorporate the use of machine learning to help understand how users interact with banking websites, creating gesture models based on patterns of mouse movements that become increasingly more accurate over time.

Read more: http://tinyurl.com/h24q4b7

Biometrics Use a Driving Trend in Australian Mobile Consumer Retail Behaviour

Deloitte’s Mobile Consumer Survey 2016 report finds that biometrics use is a driving trend in Australian mobile consumer retail behaviour, with one in three smartphones having a fingerprint scanner, and of these almost 70% of owners use this function regularly, according to a report in Image and Data Manager.
"Australians make an estimated 100 million imprints a day using smartphone fingerprint scanners, showing that we are becoming more comfortable with our fingerprint being used for authentication," according to Stuart Johnston, Partner and the leader of Deloitte’s Technology, Media and Telecommunications (TMT) group.

“By 2020, Deloitte forecasts that users may have as many as 200 online accounts, each requiring secure controls over access. Biometrics and our smartphone can provide a simple, convenient and quick single tap solution to this challenge.” Johnston added that with the increasing acceptance of biometrics, the range of applications in which fingerprint readers are used is expected to grow. “Initially we have seen fingerprints being used as a faster alternative to a numeric password to unlock phones, but this has now extended to unlock applications, and authorize payments for online content from an app store.”

Read more: http://tinyurl.com/zmwldch

Study Disproves Child Fingerprint Aging Concerns

Biometric researchers at Michigan State University prove in a new study that the digital fingerprints of a six-month old can be used for authentication one year later. The findings refute a prevailing theory that the fingerprints of infants grew too fast to make them reliable identifiers.

“Despite efforts of international health organizations and NGOs, children are still dying because it’s been believed that it wasn’t possible to use body traits such as fingerprints to identify children. We’ve just proven it is possible,” said Jain, a University Distinguished Professor of Computer Science and Engineering at Michigan State University.

Read more: http://tinyurl.com/hmax4sm

The European Association for Biometrics (EAB) awarded young researchers for their outstanding works in the area of biometrics. An international jury chose 3 candidates out of a broad range of submitted high quality papers to present their significant contribution in front of the jury, the EAB members and the public audience.

The European Biometrics Research Award 2016 has been given to Mateusz Trokielewicz from Biometrics Laboratory, Research and Academic Computer Network (NASK), Warsaw University of Technology, Poland for his thesis titled Iris Recognition Reliability in the Context of Template Aging, Ocular Disorders, and Death.

This year European Biometrics Industry Award goes to Chiara Galdi from EURECOM, France for the thesis titled Combining Iris and Sensor Recognition on Mobile Phones.

Special honours were given by the jury to finalist Javier Franco-Pedroso from Universidad Autónoma de Madrid, Spain for his contribution titled Feature-Based Likelihood Ratios for Speaker Recognition from Linguistically-Constrained Formant-Based i-Vectors.

The European Biometrics Research and Industry Award is 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. The intention of the award is to stimulate innovation in academic research as well as in industry.

The call for submissions for the EAB Research and Industry Award 2017 is now available.

Read more: http://eab.org/award
**BIOMETRICS INTERVIEW**

CHRISTOPHER BOEHNEN

**Question:** As stated on its web page, IARPA takes “real risks, solve hard problems and invest in high-risk/high-payoff research” that has the potential to provide US with an overwhelming intelligence advantage. In your opinion, what are the most evident hard problems in biometrics?

**Chris:** I think the most pressing need for the biometrics community is improved presentation attack (spoofing) detection. Biometrics has matured to the point that we have high performing systems able to recognize people to the level of one in a million or better depending upon the specifics. However, depending on the use case, the average deployed biometric system can be defeated by a high school student with access to YouTube, using over the counter supplies as simple as silly putty/wood glue or a printer. In many governmental use cases, we mitigate this risk with the use of a human security presence to ensure the integrity of the process. While a human security presence can be effective, we need to increase the security of the technology itself, as is the goal of the IARPA Odin program.

**Question:** The balance between privacy and security in modern societies is a sensitive point, and motivates dramatically different perspectives. In your view, considering the increasing security trends (due to terrorist attacks such as Boston 2013 or Paris 2015), is “Big Brother’s” automata unavoidable in the future of our societies? If yes what impact do you think it will have on the society?

**Chris:** Finding the right balance between privacy and security is a complex societal question, and there is no single correct answer. Worldwide, this balance will always be different depending upon societal norms and threats faced. Even within the US, the right answer for San Francisco has been very different from Chicago with respect to CCTV cameras. When it comes to biometrics, people commonly jump straight to a discussion of governmental based concerns. However, the vast majority of biometric systems today are for commercial applications and this trend is likely to continue. More biometric fingerprint systems have been deployed on mobile devices in the last five years than have ever been deployed in the history of biometrics. I am personally much more concerned with the private sectors use of my data than I am the governments’ use of data. As biometrics is predominately a means of identifying fully cooperative individuals, I find it unlikely to play a role in any potential ‘big brother’ like security environment (if one were to occur at all). As an example, mobile phones provide much greater data with respect to temporal/geo location than biometrics ever will.
**Question:** When it comes to securing biometric systems spoofing against attacks, is academic research able to successfully propose solutions for the difficult spoofing cases envisioned by the IARPA? If that is not the case, can you tell us where academic research is lagging, and can you tell us about the strategies to encourage researchers to sync up – test beds, operational data, etc.?

**Chris:** IARPA’s goal with the Odin program is to develop systems to perform PAD (Presentation Attack Detection) on known and unknown PAs (spoofs). This program is open both to academic and private institutions. As there is no standard test bed or data set, there is no standard by which to answer your question. Odin is developing both a test bed and data set that we hope will be a better representation of possible presentation attacks. All of our performers will be tested against this same standard.

**Question:** The goal of the Odin program you are overseeing is to develop various biometric presentation attack detection technologies. Many challenges have been organized recently, aiming at measuring the ability of either commercial or academic biometric systems to detect spoofing. Do you think that the benchmarks used for these challenges can be considered, in general, as reliable samples of real-world conditions for this kind of issues? Do you see some specific problem that is not sufficiently addressed yet by the scientific community?

**Chris:** The small scale academic benchmarks that have been previously attempted are a good start, but they are not representative of real world conditions from several perspectives. Previous benchmarks typically provided foreknowledge of the attacks and did not assess the ability for the same PAD system to detect multiple types of unknown attacks simultaneously. Additionally, the sample sizes were too low to determine false alarm rates in a real world environment/population.

**False Alarm / False Detect** rates are critical to many real world deployments of PAD technologies. Even a rate as ‘low’ as 1% is too high for many use cases. Further, understanding how a real world population with different factors such as skin tone, makeup usage, and medications affects alarms has largely not been studied at all.

**Question:** The wide deployment of biometric recognition systems in the last two decades has raised privacy concerns regarding the storage of biometric data. The use of homomorphic encryption to permanently protect biometric records has long been labeled unpractical due to its high computational requirements. Do you think that with the increased computational power available today homomorphic encryption is now becoming more relevant? And, do you believe that the use of homomorphic encryption could improve public confidence and acceptance of biometrics?

**Chris:** Homomorphic encryption and biometric fuzzy hashing has the potential to be an all-around win for security and privacy. While it is too early to assess technical viability, I think it has the potential to improve public confidence, privacy, and security. Current state of the art generic homomorphic encryption is still far too computationally expensive for almost all biometric scenarios, although it is worth noting that it has been decreasing in overhead costs faster than Moore’s law. Depending upon how long that trend continues, and how much faster hardware gets, it could become viable in the next 5-10 years for biometric applications.

Beyond generic homomorphic encryption, which could be utilized for any computing environment, biometrics has the potential to produce much more customized variants capable of producing similar positive effects for privacy and security. These customized variants are commonly referred to as ‘fuzzy hash’ approaches. They enable biometric matching without the raw/original sample. They are likely computationally viable (with an overhead cost of under an order of magnitude) currently. The challenge is that these approaches are still in the proof of concept phase and are not ready to be utilized operationally.

Christopher Boehnen is Senior Program Manager at Intelligence Advanced Research Projects Activity (IARPA), Office of the Director of National Intelligence. He leads Janus unconstrained face recognition program, the Odin biometric presentation attack detection program, and the Nail to Nail (N2N) fingerprint prize challenge in addition to numerous seedlings. Additionally, he has a joint faculty appointment in the University of Tennessee’s Anthropology department where he works primarily with the Anthropological Research Facility commonly referred to as the body farm. Finally, he is on ‘loan’ to IARPA from Oak Ridge National Laboratory via an intergovernmental personal act assignment (IPA).
This spotlight is devoted to iris (again), since news about the growing interest of research as well as of security managers all around the world testify the relevant role played by this trait.

Theory – Notwithstanding the patents registered and the increasing accuracy achieved by iris matching, it still quite mysterious why two irises match each other. Available methods work by transforms and coding processes that return a result which is not interpretable by humans in terms of concretely observable features. This makes unfeasible a human recognition process comparable to that applied e.g., for face and most of all for fingerprints. In the latter case, the presence of special kinds of minutiae and patterns like circles can be easily detected even by non-expert users, and possibly be the object of comparison among expert opinions. This is not possible at present for iris. The aim of the research carried out by a group of researchers at University of Notre Dame, including Patrick Flynn, the present editor in Chief of IEEE Biometrics Compendium, was to investigate new recognition methods to close this gap, that hinders a wide use of iris trait in forensics. Notre Dame’s Office of Technology Transfer publicly released the software in October, and made it freely available to any potential collaborators. Jianxu Chen, one of the researchers involved in the project, explained the decision to make the software open source. It is obviously motivated by the desire to improve the accuracy of the achieved results, that are still below state-of-the-art. However, the merit of the method, that exploits features that are visualizable and interpretable by humans, is to allow experts to judge the correctness of the results.

The software code, available at http://tinyurl.com/hl7fpkt, exploits iris features (i.e., crypts) that are extracted and presented to the user for positive matching in a way similar to fingerprint analysis. The matching scheme is claimed to be robust even when topological changes occur to the detection of the same crypts across multiple acquisitions. The interested reader can refer to the paper:

Practice – One more country will use iris recognition for border control. In the context of their new entry-exit system based on biometric traits, including the worth mentioning the BIKES (Biometric Identification of Motorbikers) System, Singapore’s parliament has passed an amendment to its National Registration Act that prescribe the introduction of iris checks at borders before 2018. The Immigration and Checkpoints Authority (ICA) already exploits biometric checks based on face images and fingerprints, but from next year it will start collecting iris images from Singaporeans and Permanent Residents. This will be done during ICA interactions during the IC registration and re-registration process, as well as during passport applications and collection. Iris, which is contactless and quite easy to capture, should also help solving the problem often reported for automated clearance gates. Here, travelers often find difficulties caused by a poor fingerprint acquisition, possibly due to poor fingerprint quality. However, just because iris scans are contactless, issues related to covert scanning arise, as opposed to fingerprint scans that assure subject awareness, and this is still object of debate.

ADVERSARIAL BIOMETRICS RECOGNITION: A REVIEW ON BIOMETRICS SYSTEM SECURITY FROM THE ADVERSARIAL MACHINE LEARNING PERSPECTIVE

Battista Biggio, Giorgio Fumera, Paolo Russu, Luca Didaci, and Fabio Roli
(battista.biggio, fumera, paolo.russu, luca.didaci, roli)@diee.unica.it
University of Cagliari, Italy

Pattern-recognition and machine-learning techniques are used in many security-related applications, including biometric identity recognition, in which intelligent and adaptive adversaries are interested in subverting system operation. As these techniques have not been originally designed to operate in adversarial settings, they are in principle vulnerable to well-targeted attacks [1,2,3]. Existing research efforts in the field of biometric systems have provided a detailed view of their “attack surface”, addressing different vulnerabilities and specific attacks that can exploit them, and proposing countermeasures and approaches for security evaluation [4,5]; however, specific vulnerabilities introduced by pattern-recognition algorithms have not been investigated thoroughly so far. We argue that looking at biometric system security from the novel perspective given by adversarial machine learning provides an original categorization of existing attacks, and allows us to envision novel threats and attacks that can target vulnerabilities of learning algorithms and to exploit countermeasures proposed in the field of adversarial learning. We then discuss two examples of non-trivial attacks suggested by our original categorization [1].

Adversarial biometric recognition. Fig. 1 shows the architecture of a biometric system, and eight potentially vulnerable adversarial attack points (attack surface) identified so far (red circles 1–11), categorized according to the targeted component: 1: attacks to the sensor (spoofing attacks); 2, 4, 7: attacks to interfaces and channels connecting different modules (replay attacks, and - only 2 and 4 - hill-climbing attacks 3, 5, 8–11: attacks to processing modules and algorithms (e.g., buffer overflow); 6: template theft, substitution, and deletion attacks to the template database.

We analyze biometric system security in terms of an attacker model that we developed as part of a more general framework for adversarial machine learning, aimed at analyzing vulnerabilities of learning algorithms, devising specific attacks that can target them, and developing the corresponding countermeasures, through a proactive approach. Our model generalizes existing ones, makes explicit assumptions about the attacker’s goal, knowledge of the targeted system, and capabilities of manipulating the input data or the system’s components [3]. For biometric applications the following assumptions can be made. The adversary’s goal can be to impersonate a genuine user (integrity violation), to compromise their template galleries to deny them access to the system (availability violation), or to violate their privacy, e.g., by inferring their templates through a hill-climbing attack (privacy violation). The knowledge (typically limited) of the system’s components (see Fig. 1) is related to: the kind of sensor (point 1), the interfaces/channels that implement connections (2, 4, 7), how the modules/ algorithms work and whether they are vulnerable (3, 5, 8–11), and some of the stored templates (6). The capability is defined in terms of: (i) manipulating the input data, and how they are used to update the system; (ii) the location at which the attack is staged, i.e., the sensor (1), interfaces/channels (2, 4, 7), the internals or even the output of modules and algorithms (3, 5, 8–11), or the template database (6). An optimal attack strategy can be defined accordingly to implement the attack.

![Figure 1. The architecture of a biometric verification system and its attack surface [1,4,5].](image-url)
Our model allows us to identify three main attack scenarios (Fig. 2) that re-categorize known attacks and countermeasures, and include novel potential attacks [1]:

(1) **Evasion attacks** aim at impersonating a client, usually by submitting a fake trait (spoof) to the sensor, or by replaying the acquired image into the system; this requires some knowledge of the client’s biometric trait through, e.g., template stealing (perfect knowledge) or a latent fingerprint (limited knowledge), and the capability of manipulating data during verification.

(2) **Poisoning attacks** modify the template gallery of a user, either by introducing an attacker’s template, which allows the adversary to impersonate the victim using her own biometric trait, or by compromising the victim’s templates, causing a denial of service. This is achieved by submitting fake traits that are erroneously used to update the template gallery of a given client, potentially compromising also the victim’s templates.

(3) **Privacy attacks** aim at retrieving one or more templates, typically as a preliminary step before performing another kind of attack. This can be performed by sending query images through a remote channel and observing the available system’s feedback, e.g., the outcome of the verification decision or the score value (as in hill-climbing attacks).

Our model can be exploited in biometric systems to provide a different categorization of known defense mechanisms, and to identify novel countermeasures among those proposed in the literature of adversarial learning. This contributes to extend to biometric systems the paradigm of security by design [3]. In the paper we discuss some possible novel countermeasures in the attack scenarios above: secure learning against evasion and poisoning; data sanitization against poisoning; randomization and disinformation techniques, following the paradigm of security by obscurity, against privacy attacks [1].

**Application examples.** To show how our framework allows one to envision novel attacks to biometric systems, and to adapt countermeasures from the field of adversarial learning, in the paper we give two application examples related to sophisticated spoofing and poisoning attacks against face verification systems [1]. We show that a face verification system can be spoofed with higher probability by combining multiple face images of the targeted victim to construct a fake face image, while exploiting knowledge of the internals of the verification algorithm. We then consider a template update mechanism during operation, and show that it allows to easily poison the gallery by a carefully-crafted sequence of fake face images. We then propose a countermeasure based on sanitizing the update procedure, by modeling normal updates against anomalous (poisoning) ones.

**References**


![Figure 2](image-url). A conceptual representation of the adversary model and of the corresponding attack scenarios [1].
BIOMETRICS INDUSTRY: A BROAD TECHNICAL PERSPECTIVE

Over past few years, some observable changes are taking place within the biometrics industry. There is likely a shift in the nature of the employed algorithms, the challenges addressed, as well as the overall operating scenario. As IT industry, in general, adopts cloud technology, application softwares are refactored into services. This has also affected the way biometrics solutions are used. Further, the trend of open source technology also seems to be getting adopted.

Traditionally, there have been companies that provide **End-to-End biometric solutions**. This includes companies such as CogentTM, NECTM, Neurotechnology, CognitecTM, Veridium (formerly Hoyos labs), and Ayonix. CognitecTM and Ayonix are majorly focused on face recognition technology, while CogentTM, NECTM, and Veridium provide solutions involving multiple biometric modalities. Apart from biometric solutions, Neurotechnology offers vision based solutions too. Widely, the products are targeted for enterprise and government organizations. Systems are either deployed for processing on site or in the cloud.

Companies such as GoogleTM, FacebookTM, and Apple® have **Integrated Functionalities** of biometric authentication in their products. For example, iPhone® 5s (and later) have fingerprint recognition functionally as a security feature. In WWDC 2016, Apple announced use of face recognition in Photos application. PicasaTM (now discontinued) could organize and tag similar photos. Google PhotosTM has capability to search photos based on textual query. These functionalities range from biometrics to computer vision, in general. In a similar utilization of face detection and recognition, Facebook detects and suggests tags to peoples’ faces in the uploaded photos.

Face.com (acquired by Facebook), AlchemyAPITM (acquired by IBMTM), and Face++ started with offerings of **Software-as-a-service APIs** for recognition. Of three major modalities of face, fingerprint, and iris, face seems to have been most compatible for this mode of products. The fact that specialized hardware is not required to capture face images, may have been a driving factor for this compatibility. Giants such as IBM, Google, and Microsoft have also entered in the space with their own products. This includes, IBM’s Visual Recognition API, Microsoft’s Face and Emotion APIs, and Google’s Cloud Vision API. These SaaS APIs use REST protocol to send an image to cloud (where it is processed) and to transmit the attributes/face detections/search results/affects back. As opposed to the traditional deployed systems, these systems follow per-transaction pricing model, typically.

There is a push in the industry to **Open Source** their recognition engines. Google has open sourced their machine learning library TensorFlow, which includes visual recognition functionalities. Similarly, three months ago, Facebook has open sourced their visual understanding and face recognition libraries, namely DeepMask, SharpMask, MultiPathNet, and DeepFace. The monetization model, if any, of these open source technologies are somewhat unclear. However, they surely stand as very important resources to advance research.

---

**Annotated Web Ears Toolbox and Dataset**

Researchers from the University of Ljubljana are introducing the Annotated Web Ears (AWE) datasets for research in unconstrained ear recognition. AWE is a dataset of ear images gathered from the web and in the current form contains 1000 ear images of 100 distinct subjects. All images in the dataset were labeled according to yaw, roll and pitch angles, ear occlusion, presence of accessories, ethnicity, gender and identity. The dataset comes with a Matlab toolbox dedicated to research in ear recognition that implements several state-of-the-art ear recognition techniques and allows for rapid experimentation with the AWE dataset as well as other biometrics datasets.

The dataset and toolbox are made publicly available to the research community and can be downloaded from: [http://awe.fri.uni-lj.si/](http://awe.fri.uni-lj.si/)
In 2016, BTAS completed 10 years and for the first time it was held outside the DC area, at Niagara Falls, Buffalo, New York. Along with the opening talk by General Chairs, Prof. Bowyer, the General Chair of the first BTAS (in 2007) reflected on the journey on BTAS in the last 10 years. The conference was full of engaging activities starting with tutorials, keynote presentations, oral and poster presentation sessions, and special sessions.

BTAS 2016 received 133 paper submissions. With the help of 105 Reviewers and 21 Area Chairs, 56 papers were selected for the conference program (24 oral presentations and 32 poster presentations) with an overall acceptance rate of 42%. These papers were organized in seven oral sessions and three poster sessions. Among the seven oral sessions, there were three special sessions dedicated to emerging hot topics in the field of biometrics including Biometrics on Mobile Devices, Face Representation Learning, and Biometrics in Forensics. The papers showed an increasing focus on use of deep learning algorithms and recognition in unconstrained and challenging scenarios.

The conference had four distinguished keynote speakers. Prof. Mark Frank from SUNY, University at Buffalo discussed his research in the area of deception detection. Deep learning techniques have taken biometrics to newer levels. Prof. Lior Wolf from Tel Aviv University, Israel discussed his research in transfer learning for face recognition using deep learning methods. Mr. Chris Miles from Department of Homeland Security shared the progress and accomplishments made in the RapidDNA technology. DNA based identification has been a key technology in the area of family relationship establishment. Prof. Kalanit Grill-Spector from Stanford University shared her research experiences in the fMRI based studies of human brain on face recognition and shed light on how a human brain can recognize faces with such ease. The conference was generously supported by nVIDIA, Safran Identity and Security, Cognitec, IBM Research, and Progeny Systems Corporation.

The conference had four tutorials offered by renowned experts in biometrics, computer vision and machine learning: Prof. Kevin Bowyer from University of Notre Dame gave a tutorial on Iris Recognition: Fundamentals to Future Topics, Dr. Yunbin Deng from BAE Systems presented about Advances in Mobile and Remote Biometrics, Prof. Arun Ross from Michigan State University and Prof. Mark Nixon from University of Southampton gave a tutorial on Soft Biometrics: Algorithms and Applications, and Dr. Mayank Vatsa from IIIT Delhi and Dr. Vishal Patel from Rutgers University on Deep Learning for Biometrics.

The conference also featured a panel discussion on Future Directions of Biometrics with the panelists being Prof. Lior Wolf from Tel Aviv University, Prof. Kalanit Grill-Spector from Stanford University, Michael King from University of Florida and Yunbin Deng from BAE Systems. The conference also had an industry session where Peter Ilo from Safran Morpho, John Schenider from Qualcomm, and Bob Keating from nVIDIA shared their experiences. They shared their visions for furthering the research in biometrics in the direction of understanding human cognition, quality, and real world applications.
BTAS 2016 also marked the commencement of the Senior Leadership Award by the IEEE Biometrics Council. The first award was presented to Prof. Rama Chellappa from University of Maryland, College Park. Several awards related to conference program were presented during the banquet. The Best Paper Award was presented to the paper titled 'Environmental Effects on Biometrics during Natural Human Decomposition'. nVIDIA Best Paper Award was given to Triplet Probabilistic Embedding for Face Verification and Clustering, Best Paper Award – Runner Up was awarded to 'Estimation of Visible Spectrum Faces from Polarimetric Thermal Faces', and Best Student Paper Award went to the paper titled 'Fastfood Dictionary Learning for Periocular-Based Full Face Hallucination'. Continuing the BTAS tradition of Best Poster Awards, Best Poster Awards were presented to the papers titled 'RGB-D Face Recognition via Learning based Representation' (for Day 1), 'Active User Authentication for Smartphones: A Challenge Data Set and Benchmark Results' (for Day 2), 'Biometric Authentication Using Photoplethysmography Signals' (for Day 3), and 'Adaptive Techniques for Intra-User Variability in Keystroke Dynamics' (for Day 3). The conference also featured six competitions related to different biometrics including video face recognition, mobile iris, cross-spectral periocular, sclera segmentation, keystroke, and speaker anti-spoofing.
CALL OF AWARDS, PAPERS, AND PARTICIPATION

IEEE Biometrics Council Meritorious Service Award

Nominations are invited for the inaugural “IEEE Biometrics Council Meritorious Service Award” to honor outstanding service in the field of biometrics. The award is administered by the IEEE Biometrics Council Awards Committee, which is responsible for reviewing and recommending candidates to the IEEE Biometrics Council Executive Committee. This award will be presented at the ISBA-2017 conference in New Delhi, India.

Eligibility: Any current IEEE member of the member societies of the Biometrics Council who has been active in the fields of interest of the IEEE Biometrics Council for more than 15 years at the time of nomination. Current officers of the Society’s Executive Committee are ineligible. Please provide: i) Nominee’s name, contact address, ii) nominator contact details, iii) URL of nominee’s website with bio and CV, iv) URL of google scholar citations, v) statement (500 words max), vi) names of three references willing to write supporting letters.

Prize Items: Plaque and $1,000 honorarium. Only one recipient and the award cannot be split.

Deadline: January 15, 2017

Send the nominations to: ikakadia@central.uh.edu

IEEE International Conference on Identity, Security, and Behavior Analysis 2017 (ISBA)

ISBA2017 will have two keynote speakers: Prof. Nasir Memon (NYU) and Dr. Gang Hua (Microsoft). Details of ISBA2017 are available at: http://ieee-biometrics.org/isba2017

Registration details are available at: http://ieee-biometrics.org/isba2017/registration.html

2017 IEEE/IAPR International Joint Conference on Biometrics (IJCB 17)

The International Joint Conference on Biometrics (IJCB 2017) combines two major biometrics research annual conferences, the Biometrics Theory, Applications and Systems (BTAS) conference and the International Conference on Biometrics (ICB). IJCB 17 will be held from October 1 till October 4, 2017 in Denver, CO. IJCB 2017 solicits submissions related to biometrics. Call of papers is available at: http://www.ijcb2017.org/

Paper submission deadline is April 15, 2017.

IEEE Winter School on MLIB-2017

Speakers of MLIB include Prof. Rama Chellappa, Prof. Venu Govindaraju, Prof. Narendra Ahuja, Dr. Nalini Ratha, Dr. Ajay Kumar, and Dr. Vishal Patel.

Registration Details of MLIB are available at: http://iab-rubric.org/mlib2017/