Dear Readers,

Welcome to the new issue of the IEEE Biometrics Newsletter! We hope you enjoyed relaxing vacations and are ready for a fruitful new year!

The spotlight in this issue is devoted to celebrate a very important achievement of members of our community. Ishan Nigam, Rohit Keshari, Mayank Vatsa, Richa Singh and Kevin Bowyer published a paper on one of the most prestigious scientific journals in the world, namely Nature! The paper deals on how phacoemulsification cataract surgery affects the discriminative ability to recognize the iris pattern. This topic is of increasing importance due to the increasing use of iris as an authentication biometrics.

The after-summer interview is with Jean-Christophe Fondeur, presently the CTO for IDEMIA. The company merges the former Safran Morpho and Oberthur Technology. Jean-Christophe has been leading Morpho Biometric research activity for more than 15 years, and it will be interesting to get an expert viewpoint on how the biometrics field is changing.

The paper that is summarized in this issue is “Multi-modal Biometric-based Implicit Authentication of Wearable Device Users” by SudipVhaduri and Christian Poellabauer, published on IEEE Transactions on Information Forensics and Security. We have already had in the past sections devoted to the continuous increase of the use of mobile strategies and architectures also for biometric applications. This paper explores the novel possibilities offered by the Internet of Things (IoT) and the number of devices and sensors involved to multimodal biometrics.

The interview with a junior researcher is with Rajeev Ranjan. Notwithstanding his quite recent PhD degree, he already reached a number of important achievements: the Best Poster Award at IEEE BTAS 2015, the UMD Outstanding Invention of the Year Award two times in the area of Information Science, and the Jimmy Lin Award for Invention in 2016 and 2018. He is currently working as a research scientist at Amazon.

The new database presented in this issue is the Mobile touch DB. It contains over 64K online character samples by 217 users using 94 different smartphones, with more than 300 samples per user. Therefore it may represent a precious testbed for applications based on touch interaction.

The section available open source code proposes an open and free framework allowing also non-technical users to exploit DeepFake techniques (Generative Adversarial Networks – GANs) to create fake faces. Of course ethical issues should be taken into account, especially after some recent episodes: the clearly and overtly playful video of a fake Matteo Renzi in Italy hardly criticizing all his political competitors (https://www.striscialanotizia.mediaset.it/video/il-fuorionda-di-matteo-renzi_50895.shtml) to the definitely less playful video of a falsely drunk Nancy Pelosi in USA (https://www.youtube.com/watch?v=EFmEntxmcDj). Pay attention! Once upon a time we used to say: “I will believe when I see”. Is this still possible?

The section about commercial products is devoted to IrisGuard, used to grant services to refugees using non-Invasive iris recognition. You will agree that nowadays this is without any doubt a very relevant topic.

The section devoted to emerging biometric traits (or even to emerging techniques to deal with popular ones) presents a paper from EST 2019 (International Conference on Emerging Security Technologies) that investigates the possibility to use skin texture biometrics for mixed resolution images.

For this issue, we also provide a short report about the annual conference of EAB (European Association for Biometrics), namely BIOSIG 2019. In addition, you will find links to active calls to events related to biometric research. Enjoy!

-Maria De Marsico
EU LISA is launching Framework Contract for EES

The European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) has launched the Framework Contract for the implementation and maintenance of the Entry/Exit System (EES).

The EU LISA agency has launched a contract with the winning tender, a consortium led by IBM Belgium. This is the beginning of an implementation, which will impact EU border management and internal security.

Read more:

Camvi ranked #1 in NIST Face Recognition Test

In the FRVT report released by NIST on July 31, 2019, Camvi’s advanced face recognition algorithm was ranked #1 as the most accurate algorithm for Mugshot Photos among 139 algorithms submitted by 88 companies around the world.

The Mugshot Photos dataset used in the NIST FRVT comprises millions of live capture mugshots from millions of subjects in the United States. It is one of the largest datasets tested in the NIST FRVT, which involved face images of the same subjects, taken 14 years apart. Face recognition accuracy over time, specifically spanning 10 years or more, is one of the most challenging scenarios for face identification systems today.

Read more:
http://www.planetbiometrics.com/article-details/i/10388\desc\camvi-ranked-1-in-nist-face-recognition-test/

JRC Report on DNA Profiling Published

The EU Joint Research Centre (JRC) has published its study on Study on DNA Profiling Technology for its Implementation in the Central Schengen Information System (SIS).

In 2018, Regulation (EU) 2018/1862 added the possibility to introduce DNA profiles in alerts related to missing persons, in the Schengen Information System (SIS), in order to contribute to their identification. The present report describes the state-of-the-art for the generation and use of DNA profiles for individualisation purposes. The objective is to inform on the type of data that compose a DNA profile, and to propose ways to evaluate its quality.

Access the report at:
http://publications.jrc.ec.europa.eu/repository/handle/JRC116742</a></p>

JRC Report on Face Identification Published

The EU Joint Research Centre (JRC) has published its study on Face Identification Technology for its Implementation in the Schengen Information System (SIS).

The report assesses the readiness and availability of automatic face recognition technology for its integration in SIS. This functionality has been introduced in the latest SIS Regulation adopted on the 28th of November 2018. The legislation determines the use of this technology first in the context of regular border crossing, however it also foresees its possible use in the near future in the context of police and judicial cooperation.

Access the report at:

Researchers introduce AI face anonymization model

The EU's GDPR imposed strict regulations to protect individuals and their data, with companies otherwise facing hefty fines. However, if the data can not be associated with a person, consent is no longer required and companies are free to use it as they please.

A group of researchers from the University of Science and Technology in Norway has introduced a new AI-based method that allegedly anonymizes faces in images to protect users’ privacy. The DeepPrivacy model is a conditional generative adversarial network (GAN), through which the researchers want to erase privacy-sensitive information, while creating a new face to preserve data visual integrity.

Read more:
https://www.biometricupdate.com/201909/researchers-introduce-ai-face-anonymization-model-to-secure-privacy

CEN/TS on Robustness against Biometric Presentation Attacks published

A new Technical Specification (TS) has been published as CEN/TS 17262, which deals with personal identification and robustness of European Automated Border Control against Biometric Presentation Attacks.

While more and more border crossings in Europe are equipped with Automated Border Control (ABC) systems, the potential vulnerability of such systems against Presentation Attacks (a.k.a spoofing attacks) is a concern. For this reason, techniques for Presentation Attack Detection (PAD) mechanisms are essential. CEN/TS 17262:2019 focuses on them, providing recommendations for the implementation of PAD mechanisms in Europe.

Read more:
Cataract Surgery and the Discriminative Capacity of Iris Recognition

Cataract is the clouding of the eye's natural lens. It is the most common cause of vision loss in people over age 40 and is also the principal cause of blindness in the world. Besides advancing age, cataract risk factors include ultraviolet radiation, diabetes, hypertension, obesity, smoking, prolonged use of corticosteroid medications, statin medicines used to reduce cholesterol, previous eye injury or inflammation, significant alcohol consumption, and family history. The World Health Organization (WHO) Vision 2020 initiative and similar programs have led to an increase in surgical interventions performed to combat this epidemic of preventable blindness. The prevalence of cataract as a public health issue continues to grow along with the worldwide mean life expectancy [1,5].

Why are we interested in problems related to cataract? Researchers in the community who tackle the problems related to iris recognition obviously know that this is a condition that can affect recognition in many respects: the iris pattern becomes occluded at different extents, and also pre- and post-surgery images may be problematic to compare. Recently, iris recognition methods are being integrated into large-scale authentication systems such as India’s Aadhar program. Therefore, it became imperative to study the effect of cataract surgery on the performance of the iris recognition system. Existing studies have analyzed the effect of cataract surgery on the iris pattern. Roizenblatt et al. [2] first studied the effect of cataract surgery on patients in South America and reported that surgical intervention affects iris biometric recognition. Dhir et al. [3] performed a preliminary study in Europe, suggesting that cataract surgery does not necessarily affect iris biometric recognition. Seyeddain et al. [4] conducted a study which concluded that iris biometric recognition may be affected by cataract surgery under certain circumstances. These aforementioned studies collected data and performed analysis using single iris sensor and algorithm, respectively. Therefore, generalizability of results could be questionable. Moreover, the medical procedures and the outcome were not uniform due to varying geographical locations and associated socio-economic conditions.

More robust results are available now. A recent study published by Nigam et al. [5] has been published in Nature, one of the most prestigious and influential scientific journals in the world. The study analyzed the effect of cataract surgery by collecting iris pattern data from cataract patients before and after surgical intervention performed via the phacoemulsification method. The database was captured from 132 cataract patients using three commercial iris sensors. Experimental evaluations using three biometric recognition systems suggest the drop-in performance when matching pre-operative images to post-operative images as compared to matching pre-operative images to pre-operative images. Authentication performance improved if cataract affected subjects are re-enrolled in the system. These finding suggests the need of methods to mitigate the effect of differential performance of subjects undergoing cataract surgery on iris recognition system.

References

Q1. Morpho has been among the historical stakeholders in the development of biometric applications. Do you see any relevant changes in the way open problems are tackled today? What would you change in past R&D strategies related to the field of biometrics?

You are right, these evolutions are significant. And I am proud to belong to a global group that contributes to these changes. Over the last 30 years, IDEMIA (created in 2017 by bringing together two very complementary and unique firms: Morpho, security and identity solutions world leader and Oberthur Technologies, leader in digital security solutions) has been providing many biometric and security solutions all over the world in fields as diverse as citizen identity, public security, border protection and digital transactions.

The biggest technological change in biometrics is of course the raise of artificial intelligence and deep learning, which we embraced from the beginning. AI that has been our R&D’s core focus over the last 20 years, is today the natural way to tackle many open algorithmic problems.

Of course, it takes much more than good algorithms to design a biometric systems. For example, in data processing, we always say ‘garbage in garbage out’, so you need to have good image acquisition devices; biometric systems often manipulate or protect very sensitive data so you need security and privacy by design techniques to protect them; they need to be scalable so system architecture is key; and because they are used by an increasingly large number of people in their daily life, they need to be easy to use, so design and ergonomics is fundamental.

So to answer your question, we need more and more to combine those multiple disciplines to design our system, and think them as holistic systems and not only algorithms. This is what IDEMIA has been doing for years and is more than ever true today.

Q2. What is your opinion about the future of biometrics? What are the most critical challenges we must face in the next 5 years?

Biometric is the only way to truly connect the individual you are in the physical world with the identities you have in the digital world. So in an increasingly digital world where security is fundamental, biometric is naturally a key technology, and this is why it is increasingly used in our daily lives.

Everyone today is seeking greater security when traveling, paying and logging on... but not at the expense of convenience. This is why we need to be able to provide simultaneously security and privacy by design for end users coupled with convenience for our customers. This is really a critical need: bringing new experience enabling convenience and a frictionless experience whenever and wherever security matters.

At the same time, those technologies (biometrics, but AI in general) have become so efficient that they enable new applications, and those new usages raise new questions. We see for example today the debate on the use of facial recognition for surveillance. As a scientific community and as industry, we must contribute to this debate, bring some solutions such as security and privacy by design. IDEMIA’s solutions are designed from the outset to provide for user privacy.

Q3. Can you give insights into privacy protection in operational biometric systems? Do current border crossing systems take into account template protection mechanisms?

Together with biometrics, security is the second strong pillar of our company (IDEMIA pioneered the use of smart card and secure element in banking, telecom and identity documents), and many of our solutions combine biometrics and security, to ensure end-to-end protection.

We treat data privacy as a fundamental human right and a statutory security obligation. We use encryption techniques to protect data at rest and in transit in our systems, and we develop and use secure element to store the most sensitive information such as citizen identity.

More importantly, we embrace Privacy-by-design principles, such as minimizing personal data to the very minimum needed, or leaving the end user in control of how their data whenever it is possible.

We also design and use privacy-Enhancing techniques such as match on card, homomorphic encryption, secure distributed computing or verifiable computing techniques to allow usage where the user’s data never leaves their personal device, for example.

About the author:

Jean-Christophe is the CTO for IDEMIA since the creation of the company in summer 2017 as the merger of Safran Morpho and Oberthur Technology. He has been leading Morpho Biometric research activity for more than 15 years and has been involved in all of the company’s breakthroughs in biometrics of the past 20+ years, including the development of fingerprint algorithms, of multi-biometrics systems for border crossing or the design of scalable architecture for very large biometric systems such as the FBI or UID in India. He holds more than 12 patents in the field of biometrics and is a senior member of IEEE.
Our technologies are opportunities for people to truly take ownership of their own data: they can decide if they want to share data and how to do so. They own their own data and must approve access to it for the government, institutions and businesses.

Q4. How has your professional journey prepared you for your current position?

I have been working in the field of biometrics and secured identity for more than 25 years. Looking back to answer your questions, I’d like to emphasize four points:

The first one is learning- Like many of us, it starts with strong engineering studies. During that time, I discovered technology of course, but maybe more importantly, I learned logic and scientific rigor, as well as non technical topics such as strategy, marketing, finance, social science, ... Even today, I like to continue learning, and it is a necessity because technology is evolving very rapidly.

Then comes business proximity- Most of my research has been in strong interaction with our customers and end users. The field experience and kind of feedback you get from is really defining the way you think and solve problems.

International experience is very important too: IDEMIA has customers and teams all over the world. Working with such a diversity of people, environments, mindset, customs and languages is not easy every day, but it forces to encompass the big picture. As our world is more and more global and international, this has been very important for me.

And finally, all over my career, I’ve had the chance to work with several extraordinary colleagues and managers who trusted me and taught me a lot about strategic thinking, networking and team management.

Q5. How has your professional journey prepared you for your current position?

I have been working in the field of biometrics and secured identity for more than 25 years. Looking back to answer your questions, I'd like to emphasize four points:

The first one is learning- Like many of us, it starts with strong engineering studies. During that time, I discovered technology of course, but maybe more importantly, I learned logic and scientific rigor, as well as non technical topics such as strategy, marketing, finance, social science, ... Even today, I like to continue learning, and it is a necessity because technology is evolving very rapidly.

Then comes business proximity- Most of my research has been in strong interaction with our customers and end users. The field experience and kind of feedback you get from is really defining the way you think and solve problems.

International experience is very important too: IDEMIA has customers and teams all over the world. Working with such a diversity of people, environments, mindset, customs and languages is not easy every day, but it forces to encompass the big picture. As our world is more and more global and international, this has been very important for me.

And finally, all over my career, I've had the chance to work with several extraordinary colleagues and managers who trusted me and taught me a lot about strategic thinking, networking and team management.

Q6. In Uganda, a re-registration of refugees using biometric technology restored confidence against fake registrations. In Jordan, some Syrian refugees pay for groceries by scanning their irises at checkout. The use of biometric data in aid delivery is currently controversial, given several privacy concerns related to keeping the details of vulnerable people safe. Can you discuss your thoughts?

IDEMIA has committed to principles that guide our deployment of biometrics that is a vital technology in our customer engagements. It is a matter of trust, and we believe that it is through regulation and transparency that biometric recognition can be fully accepted and integrated into everyone's daily life. Facial recognition is for instance an important and necessary technology advancement that improves public safety, aids in criminal investigations and ensures our communities are secure. IDEMIA relies on its sales team and employees all over the world to locally contribute to the public debate.
Rajeev Ranjan received the Ph.D. degree from the University of Maryland at College Park in 2019. His research interests include face detection, face recognition, activity detection, and machine learning. He was a recipient of the Best Poster Award at IEEE BTAS 2015, the UMD Outstanding Invention of the Year Award two times in the area of Information Science, and the Jimmy Lin Award for Invention in 2016 and 2018. He is currently working as a research scientist at Amazon.

Q1. You had a very productive Ph.D. experience, publishing several papers per year in high-impact venues. How did you remain consistent in these efforts? Were there any specific strategies (e.g., time management) that you used?

Thank you. Ph.D. was a fun experience for me. It wasn't something that I had to do just to build my career profile, I actually loved doing research. My lab was my playroom, and computer vision concepts were the toys that I used to solve the research problems at hand. Coming up with a novel solution to a problem is challenging and most of the times the ideas that I tried did not provide successful results. Instead of getting demotivated, I learned from my failures and modified my ideas accordingly. The trick was to keep on experimenting and exploring new ideas and read a lot of papers. The more experiments you run, higher are the chances of success. Working in a stress-free environment and loving my work helped me publish impactful papers consistently.

Q2. Identifying open research gaps can sometimes be challenging for Ph.D. students, especially on mature research topics such as face recognition. As a recent graduate, what advice would you give to new students regarding recognizing open problems?

Identifying open research problems to work on plays a crucial role in shaping one's Ph.D. thesis. Finding research gaps in face recognition is challenging as most of the problems in this field are almost solved. For example, face verification algorithms for frontal unconstrained images have already surpassed human performance. However, there still exist multiple unsolved problems such as frontal-to-profile face verification, cross-age face verification, face recognition for small faces, etc. Some of these problems haven't been explored due to the lack of proper training and evaluation dataset. Facial attributes recognition problem got a boost with the release of CelebA dataset (http://mmlab.ie.cuhk.edu.hk/projects/CelebA.html).

Similarly, serious research in tiny face detection problem started after the release of WIDER Face dataset (http://shuoyang1213.me/WIDERFACE). I would advise new PhD students to read papers regularly to get an understanding of the unsolved problems, and become aware of new challenges and datasets. Just create a new dataset if you don't find one for your problem.

Q3. What is the most valuable expertise you gained during your Ph.D.? What would you change if you could return back?

Discipline and time management are the most valuable skills that I learned during my Ph.D. In addition to working on a research problem, a Ph.D. involves course work, assignments, writing papers/thesis, preparing talks and presentations, etc. To execute these diverse set of tasks effectively, focus and commitment are imperative. I learned to plan my work schedules in advance and manage my time to meet deadlines. These skills helped me in maintaining a smooth work/life balance. I find them useful even after my PhD.

Q4. You are currently a Research Scientist at Amazon. What was your motivation to move from academia to industry? Do you plan to continue publishing research papers?

I feel accomplished when I find my research contributions getting used in real world applications. Having a publication in academia surely advances the research field, but in industry the research ideas are shaped into product that directly helps the users. This was my prime motivation to switch to industry. As a Research Scientist at Amazon, I get to innovate as well as apply my ideas to improve the efficiency of the product that I work on. I plan to continue publishing research papers and share my findings with other researchers in the field.

Q5. Face detection has evolved significantly in the last twenty years, which are under your point of view the most important current challenges?

Face detection has come a long way in the last couple of decades from Viola Jones algorithm to deep learning-based approaches. Deep Convolutional Neural Networks (DCNNs) are able to accurately detect large, high resolution faces. However, detecting tiny faces with size l...
Q7. Are data sets with more images per subject always better than those with more subjects?

Typically, datasets with more subjects are better than those with more images per subject for training a face recognition system. Having more images per subject adds coarser variations to the dataset such as pose, and expression which increases the intra-class compactness of the learned features. Having more subjects in the dataset increases the finer variations in the discriminative structure of a face which improves the inter-class separability of the learned features. Since face recognition systems are trained as a fine-grained classification task, the model gains discriminative power by learning the finer variations in the dataset. However, one should maintain an adequate number of images per subject. As a rule of thumb, a face recognition dataset of N images should have 25 images per subject and N/25 different subjects. A detailed experimental analysis can be found in the following paper:


Face detection processing speed is another major concern that needs attention. Most of the deep learning-based approaches are slow and unable to detect faces in real-time. Moreover, they require high computational resources which limits them to be implemented on mobile devices. Improving the face detection speed while maintaining the needed accuracy is an ongoing research problem.

Q6. When considering face recognition systems trained on images, until which extent can we expect they work on videos?

Faces acquired from images are mostly frontal, and typically of higher quality compared to the faces acquired from videos. One can expect a lot more variations in pose, expression, and resolution in a face captured from videos. Most face recognition systems trained on images are unfamiliar to these variations which results in decreased accuracy on videos. We can expect them to work on videos where the face quality does not digress much compared to the quality of training images.

Face recognition in videos is not all bad, it has some advantages of its own. We can extract multiple feature embeddings of same identity from a video and exploit the ensemble learning technique. Even simple averaging of these features creates an embedding which is much more robust compared to the embedding of a single frame.

Q8. If you had extra time and funds, which biometric topic would be of your interest?

If I had extra time and funds, I would work on voice recognition technology alongside face recognition. Both these biometrics are contactless which makes them applicable for the tasks of monitoring and surveillance. Similar to faces, voice signals can capture the emotion and expression of a person. They can be used to automatically detect the pain level in patients. Voice recognition can help victims in human trafficking or hostage situation by monitoring the emotional state in their voice. Voice biometric can assist a face recognition system to make a confident judgement, thus improving the accuracy of the application.
I. INTRODUCTION

With the emergence of the Internet of Things (IoT), we now have access to a multitude of devices with advanced capabilities that allow us to remotely collect information or control physical objects. Examples of such systems include alarm systems, entertainment devices, vehicles, smart build-ings, to name a few. At the same time, smartphones and wearables have also advanced in their sensing and compu-tational capabilities, which enable many new applications and usage scenarios. While smartphones are already widely used, wearables are still growing in popularity with the arrival of new applications, including the ability to identify a user to third party services, store sensitive user information (i.e., passwords, credit card information), unlock vehicles, access phones and other paired devices, manage financial payments, monitor or track individuals (e.g., child monitoring or fall detection), and assess an individual’s health and fitness.

However, wearables also raise new challenges, specifically in terms of security. Unauthorized access of a wearable can enable access to other sensitive IoT objects, which poses a significant risk [1]. Unauthorized users could also access data on the wearables, e.g., many applications and services provided by a wearable depend on sensor and user data stored on the device. Another concern is the reliability (i.e., trustworthiness) of the physiological and activity data collected by wearables, e.g., many healthcare providers and researchers rely on wearables to monitor their patients or study participants remotely, where users may be tempted to give their own devices to others, e.g., to reach a prescribed amount of activity or to contribute the required amount of data to maintain compliance and receive financial incentives. Therefore, there is a need for robust and accurate authentication mechanisms specifically for wearable device users.

Existing wearable device authentication mechanisms are often knowledge-based regular PIN locks or pattern locks [2], which suffer from a scalability issue [3], i.e., with an increasing reliance on protected devices, a user is often flooded with passwords or PIN requests to obtain access to various data and services. Knowledge-based approaches also require users to interact with the display, which may either be inconvenient or even completely absent in many wearables [1, 3]. Many times, users opt to completely disable security mechanisms out of convenience. Furthermore, knowledge-based approaches suffer from observation attacks such as shoulder surfing [3].

Therefore, in recent years, biometric-based solutions have been proposed, since they provide opportunities for implicit authentication by removing direct user involvement or attention [1, 3]. A market intelligence firm has also predicted that annual biometric hardware and software revenue will grow at a compound annual growth rate (CAGR) of 22.9% from $2.4 billion in 2016 to $15.1 billion worldwide by 2025 [4], which further provides evidence that there is an opportunity to utilize biometric-based authentication.

The authors are with the Department of Computer and Information Science, Fordham University, NY, USA and Department of Computer Science and Engineering, University of Notre Dame, IN, USA.

E-mail: vhaduri@gmail.com, cpoellab@nd.edu

However, biometric-based authentication also has challenges and shortcomings, specifically in terms of accuracy and usability. For example, behavioral biometric-based approaches such as gait or gesture analysis often fail to authenticate a user during sedentary periods [1]. Due to the limited computational capabilities and energy resources, most traditional user authentication approaches, e.g., using fingerprints, voice, breathing patterns, keystroke dynamics, head or arm movements, gait, electroencephalography (EEG), and electrocardiograms (ECG) are often not suitable for wearable devices. Furthermore, low-cost sensors in wearables may be less accurate (leading to noisy data recordings) or collect recordings very infrequently (e.g., only once per minute). The limited display sizes of wearables add another constraint that limits the choices of authentication mechanisms.

The main contribution of this paper is an implicit wearable device user authentication approach using three different types of biometric data: behavioral biometrics (step counts), physiological biometrics (heart rate), and hybrid biometrics (calorie burn and metabolic equivalent of a task or MET), all of which are easily obtainable in many state-of-the-art wearables. Our approach is to authenticate a user based on coarse-grained (i.e., one sample per minute instead of multiple samples per second or millisecond) processed (i.e., not raw) biometric data. We train and test different authentication models with different feature sets using a Support Vector Machine (SVM) classifier, which was found to be the most accurate in our previous work [5]. Our analysis using data from over 400 Fitbit users shows that our multi-biometric-based implicit approach is able to authenticate subjects with an average accuracy of about .93 (sedentary) and .90 (non-sedentary). We also find that the hybrid biometrics (i.e., calorie burn and MET) perform the best, whereas the behavioral biometrics (i.e., step counts) do not have a significant impact on authentication even during non-sedentary periods. Using error analysis we demonstrate the trade-off between usability and security of our authentication approach.

II. APPROACH

NetHealth Study Dataset: The NetHealth mobile crowd sensing (MCS) study [5]–[18] began at the University of Notre Dame with over 400 freshmen (age 18 1 years) recruited from the 2015 class. Subjects were instructed to continuously wear a Fitbit Charge HR device, which provided minute-level heart rate, calorie burn, metabolic equivalent of task or MET, physical activity level/intensity (e.g., sedentary, light, fair, and high), step count, sleep status, and self-recorded activity labels. These collected data can be divided into three biometric groups: behavioral (e.g., step counts, activity level/intensity), physiological (e.g., heart rate) and hybrid (e.g., calorie burn, MET) biometrics.

Pre-Processing and Feature Computation: We first remove periods of activity minutes that do not match with periods of
heart rate measurements. A similar filtering approach is applied for calorie burn and MET. Next, we segment continuous biometrics into five-minute non-overlapping windows starting from a change of activity levels. Each window contains five consecutive samples recorded at the same activity level. Table I presents the candidate feature set. We compute 108 features for each window, when considering all four biometrics together. For non-sedentary periods, we also consider the activity level (i.e., light, fair, and high) as an additional feature. Each biometric is referred to by its initial: “C” (calorie burn), “S” (step counts), “M” (MET), and “H” (heart rate). Combinations of these letters are used to represent the corresponding combinations of the biometrics, e.g., “CH” represents a combination of calorie burn and heart rate.

**Feature Selection:** First, we apply the Kolmogorov-Smirnov (KS)-test to select significant features from the candidate feature sets consisting of 27 features from each of the four biometrics. Then, we apply two separate approaches to reduce the feature count – (1) remove redundant features using the Pearson Correlation (PC)-based approach and (2) reduce the feature count using Standard Deviation (SD)-based feature selection approach.

**Authentication Models:** We use: (1) the binary Quadratic Support Vector Machine (q-svm), i.e., SVM with a second order polynomial kernel function defined as K(xi, xj) = (1 + yXT xj) d and (2) the unary Gaussian Support Vector Machine (g-svm), i.e., SVM with the Gaussian or Radial Basis Function (RBF) defined as K(xi, xj) = exp(−yXT xj), where kernel scale parameter δ = 1, degree d = 2, and xi and xj are two feature vectors/windows.

**Train-Test Sets:** For each feature set with N subjects, we build N separate models, one for each subject. When using the binary q-svm classifier, we train a model with 75% data of one subject (positive class) and 75% data from the rest of the N-1 subjects (negative class). However, when using the unary (i.e., 1-class) g-svm classifier, we train a model using a subject’s own data with a certain percentage of data being considered as outliers. For both types of classifiers, we test a model on the 25% data both from positive and negative classes. In all cases, we use balanced datasets.

**Performance Measures:** In addition to standard Accuracy (ACC), False Positive Rate (FPR), and False Negative Rate (FNR), we also use the Equal Error Rate (EER), which is defined as the point when FNR and FPR are equal, i.e., a trade-off between the two error measures (i.e., FNR and FPR). Note that literature often also uses False Acceptance Rate (FAR) and False Rejection Rate (FRR), which are exactly the same as FPR and FNR, respectively.

### III. RESULTS

**A. Comparing Biometrics and Feature Selection Approaches**

Table II summarizes the findings when applying q-svm on the three feature selection approaches. In the table, for each feature selection approach, we present the best biometrics, i.e., biometric combinations that optimize feature count and classification accuracy. Also, n, N, and W stands for the number of features in a feature set, the number of subjects for training-testing, and set of random windows picked from a subject, respectively. In the table, we observe that the KS- and SD-based approaches achieve similar performance. In Table II we observe that in general hybrid biometrics (i.e., “C” and “M”) perform better than other behavioral (“S”) and physiological ("H") biometrics, which happens because hybrid biometrics are derived from both behavioral and physiological biometrics in addition to demographic data such as weight and age of a user.

### B. Binary versus Unary Classification

The unary classifiers in Table II are built without considering any outlier (i.e., 0% outlier). We observe that the unary models achieve performance close to binary classification models for the KS- and SD-based approaches during sedentary periods. However, for non-sedentary periods, the difference between the two classification models is relatively high compared to sedentary periods. This is probably due to the variations of window counts across the three non-sedentary activity levels of individuals. In Figure 1a we observe that FPR goes below 0.05 = 4.6 with 10% and 30% outliers during sedentary and non-sedentary period models, respectively. Therefore, these could be used as appropriate outlier thresholds while designing unary models.

![Fig. 1: (a) FPR and FNR variations with changing outlier thresholds. (b) FNR, FPR, and ACC variations with varying probability thresholds for 5 minute windows using the KS-approach with CM.](image-url)
C. Error Analysis

In this section, we take into account the confidence level of a prediction in terms of a posterior probability, which indicates the likelihood of the prediction coming from a particular class. In Figure 1b we observe that with the increase of the probability threshold, FPR starts dropping sharply, while FNR and ACC increase steadily. After .9 probability all three measures change sharply. At a probability threshold of .95, we obtain an EER of .05. When FPR drops to .02, FNR increases to .1. At that point ACC increases above .97. For sedentary periods we observe similar patterns. This way a trade-off can be made between FPR and FNR to balance security (in terms of FPR) and usability.

<table>
<thead>
<tr>
<th>Feature selection approach</th>
<th>Sedentary</th>
<th>Non-sedentary</th>
</tr>
</thead>
<tbody>
<tr>
<td>KS</td>
<td>PC</td>
<td>SD</td>
</tr>
<tr>
<td>Best biometrics</td>
<td>CM</td>
<td>CMH</td>
</tr>
<tr>
<td>n</td>
<td>49</td>
<td>53</td>
</tr>
<tr>
<td>N</td>
<td>412</td>
<td>411</td>
</tr>
<tr>
<td></td>
<td>544</td>
<td>637</td>
</tr>
</tbody>
</table>

**Binary Classification**

<table>
<thead>
<tr>
<th>µ(ACC)</th>
<th>σ(ACC)</th>
<th>µ(FNR)</th>
<th>σ(FNR)</th>
<th>µ(FPR)</th>
<th>σ(FPR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>.93</td>
<td>.86</td>
<td>.93</td>
<td>.90</td>
<td>.86</td>
<td>.88</td>
</tr>
<tr>
<td>.03</td>
<td>.04</td>
<td>.04</td>
<td>.04</td>
<td>.05</td>
<td>.05</td>
</tr>
<tr>
<td>.04</td>
<td>.15</td>
<td>.03</td>
<td>.06</td>
<td>.10</td>
<td>.09</td>
</tr>
<tr>
<td>.03</td>
<td>.05</td>
<td>.03</td>
<td>.04</td>
<td>.05</td>
<td>.04</td>
</tr>
<tr>
<td>.10</td>
<td>.14</td>
<td>.11</td>
<td>.14</td>
<td>.18</td>
<td>.15</td>
</tr>
<tr>
<td>.05</td>
<td>.05</td>
<td>.06</td>
<td>.05</td>
<td>.06</td>
<td>.07</td>
</tr>
</tbody>
</table>

**Unary Classification**

<table>
<thead>
<tr>
<th>µ(ACC)</th>
<th>σ(ACC)</th>
<th>µ(FNR)</th>
<th>σ(FNR)</th>
<th>µ(FPR)</th>
<th>σ(FPR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>.88</td>
<td>.76</td>
<td>.90</td>
<td>.74</td>
<td>.64</td>
<td>.68</td>
</tr>
<tr>
<td>.07</td>
<td>.06</td>
<td>.07</td>
<td>.06</td>
<td>.07</td>
<td>.07</td>
</tr>
<tr>
<td>.14</td>
<td>.27</td>
<td>.09</td>
<td>.16</td>
<td>.07</td>
<td>.07</td>
</tr>
<tr>
<td>.08</td>
<td>.11</td>
<td>.07</td>
<td>.07</td>
<td>.04</td>
<td>.03</td>
</tr>
<tr>
<td>.11</td>
<td>.21</td>
<td>.12</td>
<td>.36</td>
<td>.64</td>
<td>.56</td>
</tr>
<tr>
<td>.16</td>
<td>.16</td>
<td>.16</td>
<td>.13</td>
<td>.14</td>
<td>.14</td>
</tr>
</tbody>
</table>

**TABLE II: Authentication Summary**

(in terms of FPR) of an implicit authentication system for wearable device users depending on the application scenario and user preference.

IV. DISCUSSION

To our best knowledge, our work is the first to use three different types of less informative coarse-grained processed biometric data (i.e., behavioral, physiological, and hybrid) to accurately authenticate the wearable-users implicitly during both sedentary and non-sedentary periods. Our detailed analysis shows the effectiveness and importance of different biometrics and feature selection approaches.

Our activity-level-based models are applicable to any un-known activity type since all types of activities belong to one of the four major activity levels used in our modeling. Homogeneity of subjects and similarity of their biometrics might have negatively impacted our results. Degradation of performance during non-sedentary periods indicates the need for better modeling, e.g., separate models for different activity levels, which our current dataset does not support due to the lack of sufficient numbers of highly active samples.

REFERENCES

15. ——, “Design and implementation of a remotely configurable and manageable well-being study,” in Smart City 360, 2016.
DeepFake

The question about whether photography is truth or fiction, has been around since its early years. David Hockney states its ambiguity and duality [1]. However, even when photographs are both facts and fiction, humans trust them. Tom Gunning created the term truth claim to describe the human belief that photography, more specifically traditional photography, depicts what is real [2]. In fact, expressions such as seeing is believing or see something with my own eyes evidence the power of what we see. Fake or hoax images have a long tradition even before digital imaging appeared. Since the XIX century photography retouching has been used to manipulate photographs [3]. Certainly, the digital era, has radically changed the way images are created. We live in an image-saturated society where the access to devices and software tools has been democratized. Nowadays, no longer an image is strictly depicting reality, and we humans are easily fooled.

Even though humans may be conscious about the possibility of image manipulation, we keep the illusion and we are still trusting images, believing what they contain when the images do not clearly evidence that they have been altered. Such an illusion may affect humans’ decisions. In a society where fake news is playing a relevant role, the possibility of manipulating videos and speech in a way to show them as the truth [4], may certainly modify people memory and behaviour [5].

With the deep learning hype, the term DeepFake has been created, combining fake and the mentioned deep learning. Many readers have for sure watched recent DeepFake demos, mostly created for fun. A wide collection is available at Ctrl Shift Face youtube channel. Their quality is increasing continuously, shocking viewers. In addition, FaceSwap claims to be the leading free and Open Source multi-platform DeepFakes software providing tools to swap faces in pictures and videos, created with the aim at easing its use by anyone without the need to be an expert in the field. The site points out the ethical uses required with the following statement:

1. FaceSwap is not for creating inappropriate content.
2. FaceSwap is not for changing faces without consent or with the intent of hiding its use.
3. FaceSwap is not for any illicit, unethical, or questionable purposes.
4. FaceSwap exists to experiment and discover AI techniques, for social or political commentary, for movies, and for any number of ethical and reasonable uses.

Even though, the software is out there, and inappropriate uses may be possible. A recent reported fraud was apparently achieved using a fake AI voice to convince a CEO to transfer $243,000 [6]. Therefore, tools are needed to recognize DeepFakes, as the discipline is growing and getting better results continuously. To this aim Facebook, the Partnership on AI, Microsoft, and academics from Cornell Tech, MIT, University of Oxford, UC Berkeley, University of Maryland, College Park, and University at Albany-SUNY have joined efforts to create a dataset freely available with the aim at detecting DeepFakes, the Deepfake Detection Challenge (DFDC), in order to increase the community interest in manipulation detection. Looking forward to see it.

References

1. David Hockney. Secret Knowledge: Rediscovering the lost techniques of the Old Masters. Thames and Hudson Ltd, 2006
2. Tom Gunning. What’s the point of an index? or, Faking photographs. NORDICOM Review. 5 (1/2), 2004
4. Shruti Agarwal, Hany Farid,Yuming Gu, Mingming He, Koki Nagano, and Hao LProtecting World Leaders Against Deep Fakes. CVPR, 2019
6. Ravie Lakshmanan. Fraudsters deepfake CEO’s voice to trick manager into transferring $243,000. The next web, 2019

[1] https://www.youtube.com/channel/UCKpH0CKltc73e4wh0_pgL3g
[3] deepfakedetectionchallenge.ai
IrisGuard Provides Essential Aid to Refugees Using Non-Invasive Iris Recognition

Tempestt Neal

Iris has a long-term reputation as one of the most robust biometric modalities [1]. Commercial iris recognition systems and solutions have emerged targeting challenging problems from mobile device user authentication [2] to access to university services [3]. A recent commercial application of iris recognition has significant societal impact, enabling refugees to make financial transactions without fear of someone stealing passwords privately and accurately.

IrisGuard recently announced this technology in its deployment of the EyePay Cash mobile platform [4]. They reported a user base exceeding 2.5 million refugees as of early September 2019, wherein participants of the program have access to essential resources such as automated teller machines and food purchases without a need for bank cards or knowledge-based authenticators such as PIN numbers. IrisGuard also boasts that their service reduces fraud and bank fees and supports additional services such as pension fund distribution. According to a patent, the company utilizes the reflective properties of the eye to combat circumvention from a photographed eye [5], a significant merit for this particular application.

The EyePay Cash platform is integrated into Zain Cash, Zain Group’s mobile wallet, in partnership with the United Nations High Commissioner for Refugees (UNHCR) [6-7]. The UNHCR has been a positive force for refugees, providing invaluable resources from fully subsidized healthcare to identity cards. UNHCR’s reliance on its Biometric Identity Management System makes many of these efforts possible in a non-invasive and cost-effective manner, a critical component of their operation that not only protects refugees, but also ensures their rights [8-9].

You can read more about IrisGuard technologies for iris recognition research in the following referenced publications, among several others [10-12].

References

The acquisition process of the new MobileTouchDB database: the database contains more than 64K on-line character samples performed by 217 users, using 94 different smartphone models, with an average of 314 samples per user. In each acquisition session, users had to draw all numbers (from 0 to 9), upper and lower-case letters (54), different symbols (8), and passwords composed of 4 numbers (6). Regarding the acquisition protocol, MobileTouchDB comprises a maximum of 6 captured sessions per subject with a total time gap of at least 3 weeks. This database studies an unsupervised mobile scenario with no restrictions in terms of position, posture, and devices. Users downloaded and used the acquisition app on their own devices freely. MobileTouchDB is publicly available in GitHub.

The benchmark evaluation of biometric authentication on the novel MobileTouchDB database: an easily reproducible framework. Two different experiments have been carried out: i) one-character analysis in order to evaluate the discriminative power of each character, and ii) character combination analysis so as to measure the robustness of our proposed approach when increasing the length of the passwords from 1 to 9 characters. The proposed approach has been compared to the e-BioDigit public database, achieving a final 3.1% EER absolute improvement under more practical experimental conditions (unsupervised scenario with 94 different smartphone models), proving the higher discriminative power of characters and symbols for the task of user authentication.

Description of the design and number of available users of the new MobileTouchDB database.

Evolution of the system performance in terms of EER (%) when increasing the length of the password.

The MobileTouchDB database opens the doors to many different applications: i) analyse the discriminative power of novel human touch interaction dynamics, ii) enhance traditional password authentication systems through the incorporation of touch biometric information as a second level of user authentication, and iii) analyse the way we interact with mobile devices on a daily basis in order to enhance continuous authentication systems.
Usability of Skin Texture Biometrics for Mixed-Resolution Images

Many biometric traits, in particular those related to the physical characteristics of a subject, suffer the well-known PIE-O issues (Pose, Illumination, Expression and Occlusions), so negatively affect the detection phase and the following preprocessing steps. In occasion of the IEEE Conference 2019 Eighth International Conference on Emerging Security Technologies (EST) held at the end of July in Colchester, UK, an interesting and futuristic approach has been proposed which aim at exploring the skin texture as biometric marker for subject recognition. In particular, the work explores the possibility of using mixed resolution facial images as a source of biometric information. The process proposed consists of four key steps, as outlined in the figure below:

1. A preprocessing step, including the facial image acquisition, the facial landmarks’ detection and the ROI localization;
2. A step in which the skin purity is evaluated;
3. The feature extraction step;

Firstly, the image is acquired and the face is normalized so as to obtain the eye centers located on a horizontal line; hence, 59 face landmarks are detected (10 for the eyes and 49 for mouth, nose and eyebrows) by means of the Chehra Face Tracker [1]; these points are used for isolating the regions of interest which are used in the following. The ROI regard the right and left cheeks, the forehead and the chin.

In order to simulate the acquisition of faces at different distances, and the following different resolution of faces, all the faces of the XM2VTS dataset [2] have been rescaled by exploiting the bicubic interpolation technique [3] with 4-by-4 neighborhood.

Once the ROIs are extracted, the Skin Purity Assessment step takes place. The adopted approach has been originally presented in [4] and it takes into account a color-based model for evaluating the purity of the skin. Compared to texture and other features, color seems more suitable for measuring the purity of a skin region, since it results easier to detect potential artifacts within the face image. The method in [4] is used for measuring the purity level. Those regions whose purity metric is greater than a certain threshold are divided in N non-overlapping regions, concatenated and passed to the feature extraction step. Here the LBP code is extracted from the regions and used for recognition purposes.

The experiments have been conducted over 1.128 images of the XM2VTS dataset, comprising about 295 individuals. These images are augmented by rescaling for simulating the multi-resolution. The published results show how the recognition accuracy vary according to the radius of the LBP kernel.

Especially for those regarding the forehead, the results suggest that the skin pattern owns a discrete degree of stability across different subjects, even when different resolution images are used as probe and gallery images. In the image above, the reader can appreciate how, the accuracy for the forehead recognition (across different resolutions) is able to reach almost the 64%.
References

In the first research contribution a online survey with more than 700 participants was conducted in order to estimate the public perceptions and preferences towards ATMs with biometric authentication in Austria. The study did not reveal strong majority preferences. The usage of cards together with PINs is still preferred but could be augmented with biometrics.

Subsequently, a session on the topic of face morphing gave insights on the vulnerability of face recognition towards attacks based on morphed face. It was shown that a separate weighting of warping and blending factors can be used to optimize to success rate of an attacker. Further, it was demonstrated that deep neural style transfer can be applied for improving the quality of morphed faces.

The next session featured three research contributions related to eye-based biometric recognition. Firstly, a presentation attack detection method based on adversarial learning was presented. Particular emphasis was put on the generalization to unseen attacks. Secondly, a new deep-learning based iris segmentation scheme was introduced. Finally, it was shown that a strong correlation between left and right retinal images of single person exists. The results were based on image data acquired with a special device of the Brno university, which simultaneously captures the iris and retina of a data subject.

The last research session of the first day focused on fingerprint recognition. On the one hand, a new deep-learning-based approach for fingerprint pre-alignment using Siamese networks was presented. On the other hand a novel 2400 dpi finger acquisition device was introduced which can be used to capture neonate fingerprints. Results from a field study in Kenia were shown.

Then, further conference contributions were presented in the poster session. The topics of the 9 posters ranged from homomorphic encryption for face identification to gender recognition in visual surveillance environments. The poster session got great reception from the attendees who afterwards joined the traditional barbeque leading to a lot of opportunities for networking and technical discussions.

The last day started with a keynote talk by Takashi Shinzaki from the Fujitsu research laboratory in Japan. He provided interesting details about the Fujitsu palm vein technology and discussed many relevant aspects including efficient one-to-many comparison and template protection.

Following the keynote speech, a research work on finger vein recognition was presented tackling the problem of longitudinal finger rotation during finger vein acquisition. Afterwards a multi-spectral presentation attack detection approach was presented which makes use of laser speckle contrast imaging on fingerprints with a multi-algorithm feature extraction.

In a final research session works on the application of deep-learning for biophysical biometrics (keystrokes and gait recognition) as well as clothes recognition in urban environment have been presented.

Eventually, Walter Scheirer from the University of Notre Dame discussed the limits and potentials of deep learning for facial analysis in his well-attended keynote talk. He showed experiments on the effects of different image processing, such as blur, contrast and rotation, on the recognition accuracy of different deep face recognition. Obtained results were compared with human recognition capabilities. It was demonstrated that visual psychophysics is a viable methodology for making face recognition algorithms more explainable. In the second part of his talk, the potential of deep-learning for describable visual facial attribute modelling was explored.

Attendees of the conference voted for the best paper and best poster presented during the conference which was honored with a prize and a certificate. Participants decided for the work of Yoshinori Koda (NEC Corporation) "Development of 2,400ppi Fingerprint Sensor for Capturing Neonate Fingerprint within 24 Hours after Birth". The winning poster was presented by Pawel Drozdowski with the topic “On the Application of Homomorphic Encryption to Face Identification”.

The BIOSIG conference was preceded by several events: the meeting of the TeleTrusT Biometric Working Group, the EAB Research Project Conference, the EAB Biometrics Research and Industry Award and the general assembly of the European Association of Biometrics. The 2019 BIOSIG conference was jointly organized by the Competence Center for Applied Security Technology (CAST) and the special interest group BIOSIG of the Gesellschaft für Informatik V. (GI).

The conference was technically co-sponsored by IEEE Biometric Council and the papers will be added to IEEE Xplore. Next year the BIOSIG conference will take place between September 16 to 18, 2020 in Darmstadt, Germany. See: www.biosig.org
Conferences

**IJCB 2020**

The 2020 International Joint Conference on Biometrics (IJCB 2020) combines two major biometrics research conferences, the Biometrics Theory, Applications and Systems (BTAS) conference and the International Conference on Biometrics (ICB). The blending of these two conferences in 2020 is through a special agreement between the IEEE Biometrics Council and the IAPR TC-4, and should present an exciting event for the entire worldwide biometrics research community.

First round paper submission deadlines:
- Paper submission: December 9, 2019
- Decision to authors: February 11, 2020
- Camera ready: March 9, 2020

Second round paper submission deadlines:
- Paper submission: April 6, 2020
- Decision to authors: June 9, 2020
- Camera ready: July 6, 2020

More at: https://iee-ieee-biometrics.org/ijcb2020/

**CVPR 2020**

CVPR is the premier annual computer vision event comprising the main conference and several co-located workshops and short courses. With its high quality and low cost, it provides an exceptional value for students, academics and industry researchers.

CVPR 2020 will take place at The Washington State Convention Center in Seattle, WA, from June 16 to June 20, 2020.

Paper submission deadline: November 15, 2019


Special Issue

**Novel Insights on Ocular Biometrics In Image and Vision Computing**

Notwithstanding the enormous potential of the traits in the ocular region for biometric applications, this line of research still raises several open issues, which justifies the ongoing research efforts. For instance, the relatively recent emergence of the periocular and sclera traits makes it worth recording the progress of this area. Also, all the traits underlying ocular biometrics and their possible combination still need to be more thoroughly investigated, not only to improve recognition robustness, but also to perceive the potential of this kind of traits to play a significant role in solving emerging problems in the biometrics domain. This special issue aims at providing a platform to publish and record the recent research on ocular biometrics in order to push the border of the state-of-the-art.

Tentative important dates:
1. Paper submission deadline: 31st December 2019
2. The first round of reviews completed: 31st January 2020
3. The second round of reviews completed: 20th March 2020
4. Final paper submission for publication: 31st March 2020

Read more at: https://www.journals.elsevier.com/image-and-vision-computing/call-for-papers/special-issue-on-novel-insight
Executive Committee

- President: Sudeep Sarkar, University of South Florida, USA
- Past-President: Mark S. Nixon, University at Southampton, UK
- VP Conferences: Vishal Patel, Johns Hopkins University, USA
- VP Education: Karthik Nandakumar, IBM Singapore Lab, Singapore
- VP Finances: Damon Woodard, University of Florida, USA
- VP Publications: Richa Singh, IIIT Delhi, India
- VP Technical Activities: Pong-Chi Yuen, Hong Kong Baptist University, Hong Kong

Society Representatives (in alphabetical order by society)

- Ljiljana Trajkovic (Canada), IEEE Circuits and Systems Society
- Joel J Rodrigues (Brazil), IEEE Communications Society
- Mihail Popescu (USA), IEEE Computational Intelligence Society
- Saurabh Bagchi (USA), IEEE Computer Society
- Peter M Corcoran (Ireland), IEEE Consumer Electronics Society
- Voicu Z Groza (Canada), IEEE Instrumentation and Measurement Society
- Bruce Hecht (USA), IEEE Solid-State Circuits Society
- Yong Xu (China), IEEE Systems, Man and Cybernetics Society

Newsletter Editorial Board

Editor-in-Chief: Maria De Marsico, Sapienza Università di Roma, Italy

Associate Editors:

- Barra, Silvio University of Cagliari, Italy
- Dhamecha, Tejas I. IBM IRL, India
- Alonso-Fernandez, Fernando Halmstad University, Sweden
- Marasco, Emanuela George Mason University, USA
- Nagpal, Shruti IIIT-Delhi, India
- Neal, Tempestt University of South Florida, USA
- Rathgeb, Christian Salzburg University, Austria
- Rattani, Ajita Univ. of Missouri, Kansas City, USA
- Castrillón-Santana, Modestoón Universidad de Las Palmas de Gran Canaria, Spain
- Tolosana, Ruben Universidad Autonoma de Madrid, Spain