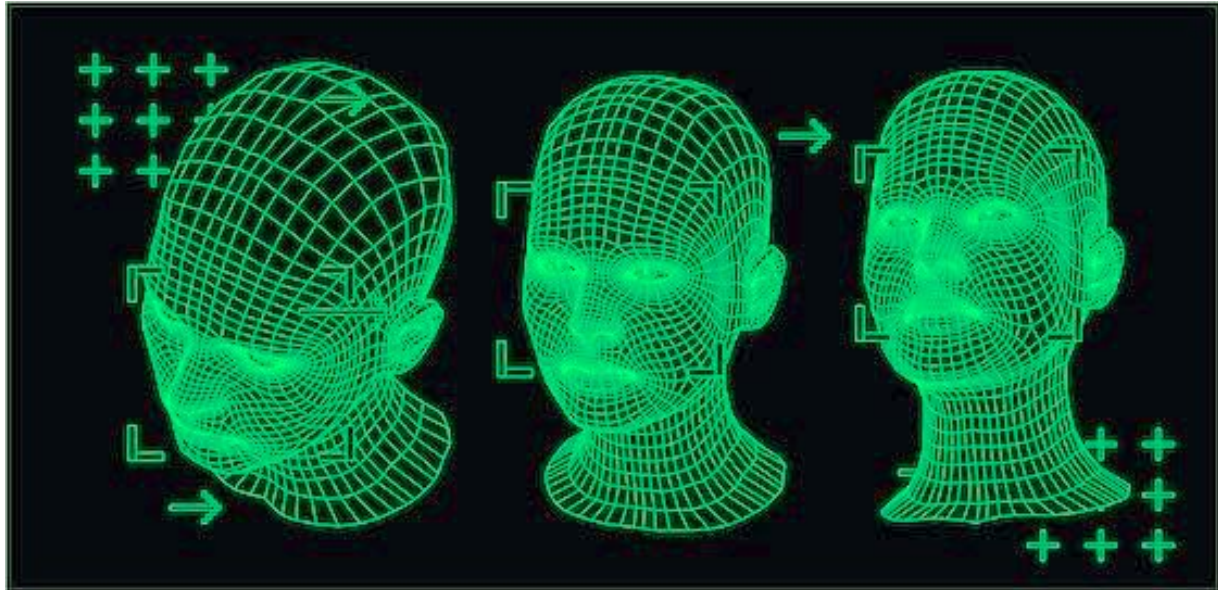


IEEE BIOMETRICS COUNCIL NEWSLETTER



Volume 48, December 2023

IN THIS ISSUE

PG. 5

Call for 2024 Council awards

PG. 8

Summary of results from the 2023 Fingerprint Liveness Detection Competition

PG. 21

Profile of Adam Philpott, new President and CEO at Fingerprint Cards AB

Cracking the password barrier

In this issue, we turn the spotlight on one of the many EU sponsored research projects we routinely list in this newsletter. The TReSPAss project is training a new generation of cyber professionals capable of shifting security from traditional techniques like passwords and tokens to new biometric strategies. Read more about the project starting on page 15. You can also learn more about the type of issues TReSPAss addresses in the profile of Ph.D. student Hatef Ostroshi on pages 25-27.

FIRST YEAR REFLECTIONS FROM THE VP, PUBLICATIONS

By Patrizio Campisi, Professor, Università degli Studi "Roma TRE," Rome, Italy and Vice President for Publications, IBC



“It is my pleasure to write to you one year after starting my endeavor as Vice President for Publications for the IEEE Biometrics Council. In the recently concluded year, we dedicated our efforts to undertaking numerous initiatives to further enhance the visibility of the Biometrics Council.”

Through a series of strategic activities and proactive measures, we sought to elevate the Council's profile and increase its recognition within relevant spheres. Our endeavors encompassed a diverse range of undertakings and were geared towards not only expanding the reach and influence of the Council, but also to fostering a deeper understanding of its mission and contributions within the broader community.

One noteworthy achievement among our endeavors is the establishment of a new website (<https://ieee-biometrics.org/>). The website serves as a comprehensive hub, meticulously designed to provide a user-friendly experience while effectively showcasing the myriad opportunities and resources we offer. Through this digital gateway, members can seamlessly access a wealth of information, including a comprehensive list of opportunities, valuable resources, and pertinent updates. The website serves as a centralized repository, ensuring that members can easily stay informed about the latest developments, opportunities, and initiatives within the Biometrics Council. As we look to the future, this digital presence will play a pivotal role in further elevating the visibility of the Council, amplifying our collective voice, and reinforcing our position as a leading authority in the realm of biometrics technology.

Furthermore, as part of our commitment to ensuring that our members stay consistently informed and abreast of the latest developments, we have successfully revived a dedicated news blog. This revitalized platform serves as a dynamic and real-time source of information, delivering updates on a wide spectrum of initiatives within the Biometrics Council. The news

blog covers a range of topics, providing timely insights into key events such as the Summer and Winter Biometrics Schools, our flagship conferences, IJCB and FG, as well as updates on our publications, *IEEE Transactions on Biometrics, Behavior, and Identity Science*, *IEEE T-BIOM*, and this newsletter. It also serves as a go-to resource for the latest information on our diverse technical activities, the renowned Distinguished Lecture series, and upcoming webinars. By consolidating all these updates in a central location, the news blog aims to offer a comprehensive and easily accessible overview of the vibrant activities and advancements within the Biometrics Council.

This revitalized news blog not only strengthens communication channels but also fosters a sense of community and collaboration among our members, ensuring that they are well-equipped with the knowledge needed to actively engage in, and contribute to, the thriving landscape of biometrics technology.

The Biometrics Council is also pleased to announce the inclusion of new Associate Editors who will enrich the expertise and perspectives on the Editorial Board of our esteemed Newsletter. Their contributions promise to enhance the quality and breadth of content, ensuring that our members receive timely and insightful updates on the latest trends and breakthroughs in the field. Further bolstering our editorial leadership, we are excited to introduce our new Editor in Chief, Andrew Ben Jin Teoh, hailing from Yonsei University in Korea. Dr. Teoh brings a wealth of experience and a fresh perspective to guide the editorial direction of the Newsletter, reinforcing its position as a premier source of information within the biometrics community.

Lastly, recognizing the importance of social media as a powerful tool for communication and engagement, the Biometrics Council has intensified its presence on platforms such as LinkedIn and Facebook. By leveraging these channels, we aim to broaden our outreach, connect with a wider audience, and facilitate meaningful discussions on the latest developments in biometrics technology. Through these efforts, we aspire to make our presence felt not only within our immediate community but also across the broader landscape of professionals, researchers, and enthusiasts interested in the evolving field of biometrics.

As we embark on this journey of knowledge dissemination and collaboration, we extend our warmest wishes to all our members and readers. Your engagement with our publications is pivotal in shaping the discourse and progress within the Biometrics Council. Your insights and perspectives are invaluable to us. We invite you to share your thoughts, suggestions, and ideas to help us continually enhance and tailor our services to better meet your needs. Your feedback serves as a guiding force, ensuring that our initiatives align with the expectations and aspirations of our vibrant community.

Thank you for being an integral part of the Biometrics Council. Your active participation and support contribute significantly to the advancement of biometrics technology, and we look forward to fostering a collaborative and enriching journey together. Happy reading, and please don't hesitate to reach out with your thoughts and suggestions. Your input is instrumental in shaping the future of the Biometrics Council.

GREETINGS FROM THE EIC

Dear Readers,



I hope this new issue finds you safe and in good health, and that you feel rejuvenated following a restful break!

The News and Council's Activities section features calls for nominations for the **IEEE Biometric Council** and **T-BIOM Best Papers Awards**, both with a submission deadline of March 1, 2024. Another noteworthy highlight in this edition is a profile of **TReSPAsS-ETN**, an EU-funded initiative to train a new cohort of researchers specializing in secure and privacy-preserving biometrics. These researchers have developed and honed presentation attack detection methods, explored

privacy-enhancing techniques, and equipped early-stage researchers with the skills to build next-generation biometric systems to safeguard security and individual privacy. The article summarizes the program's final workshop at EURECOM in Sophia Antipolis, France, which was held on September 13-14, 2023. Showcasing the culmination of the TReSPAsS-ETN project, the two-day program highlighted the advancements and insights gained in pursuing secure and privacy-preserving biometric technologies.

This issue also includes a comprehensive report on Fingerprint Presentation Attack Detection (FPAD) from the **International Fingerprint Liveness Detection Competition**, and an insightful interview with **Adam Philpott**, President and CEO of Fingerprint Cards. Mr. Philpott articulates the company's vision and mission, emphasizing its commitment to delivering a secure and seamless user authentication experience across diverse digital interactions.

Our **Researcher on the Rise** column features an interview with **Hatef Otroshi**, who has already been acclaimed for his exceptional contributions across prestigious venues like ICCV, NeurIPS, IEEE TPAMI, TIFS, and TBIOM. Mr. Otroshi's noteworthy efforts have earned him recognition through the 2023 European Association for Biometrics (EAB) Research Award and a prestigious H2020 Marie Skłodowska-Curie Fellowship (TReSPAsS-ETN) for his advancements in biometric security.

Additionally, this issue presents in our **Lecture Notes** the first part of a tutorial that delves into **European Union regulations** about the processing of biometric data. The tutorial aims to give readers a deeper understanding of the regulatory landscape surrounding biometric data processing. It particularly focuses on data protection and future artificial intelligence (AI) systems, and underscores the importance of distinguishing between legislative frameworks.

The article also comprehensively presents the definition, principles, and notable criticisms of the General Data Protection Regulation. This tutorial aims to give readers a deeper understanding of the regulatory landscape surrounding biometric data processing.

The featured paper in this edition is "MD-Pose: Human Pose Estimation for Single-Channel UWB Radar," which was recently published in *IEEE Transactions on Biometrics, Behavior, and Identity Science*. **Database Digest** introduces the Multi-Movement Finger-Video (MMFV) Database for Contactless Fingerprint Recognition, from the IIID group in Delhi. In the **Source Code** section, we highlight a PyTorch library called Malafide, generously made available by Chiara Galdi and Michele Panariello. Additionally, the **COTS** section showcases Qualisys' Gait Analysis module, which presents a streamlined workflow for efficient gait analysis.

Your participation in this exciting journey is greatly appreciated. I anticipate your continued support, as together we aim to solidify the IEEE Biometrics Council Newsletter as an indispensable resource within the biometrics community

Warm regards,

Andrew Teoh



COUNCIL NEWS

CALL FOR AWARDS NOMINATIONS

The IEEE Biometrics Council is seeking nominations for a number of annual awards. The awards are supervised by the IEEE Biometrics Council Award Committee, which is responsible for reviewing and recommending candidates to the IEEE Biometrics Council Executive Committee. The awards will be presented at IJCB 2024. Questions about any of the awards should be directed to the Awards Committee Chair, Dr. P. Jonathon Phillips at biometrics.council.awards@gmail.com or VP Technical Activities, Professor Vitomir Štruc at vitomir.struc@fe.uni-lj.si

For a list of eligible member societies, see the Society Representatives section here at <https://ieee-biometrics.org/index.php/homepage/committees>. **Nomination forms for all awards and templates for all recommendation letters are available in both PDF and Word formats at <https://ieee-biometrics.org/2024-award-nominations-open/>.**

IEEE Biometrics Council Meritorious Service Award

Deadline: March 1, 2024

	<p>2023 Meritorious Service Award winner Mayank Vatsa</p> <ul style="list-style-type: none">- Professor, IIT Jodhpur- Swarna Jayanti Fellow- Fellow, IEEE, IAPR, AIAA
---	--

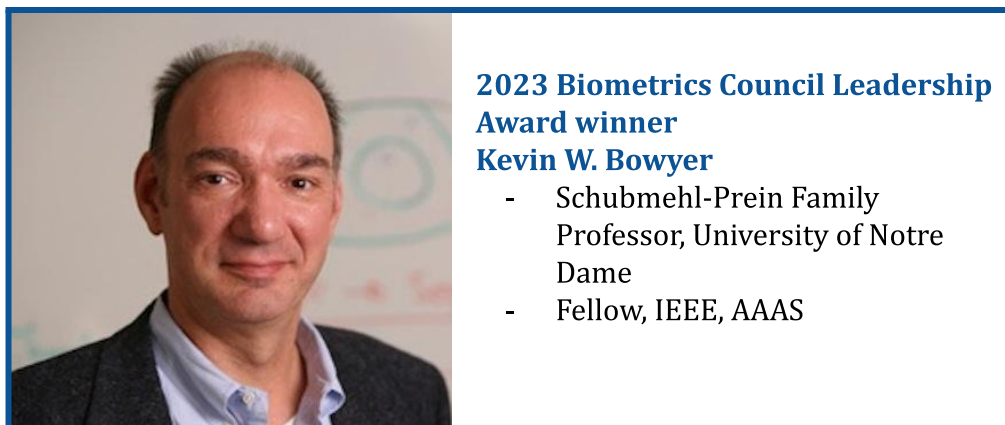
The **IEEE Biometrics Council Meritorious Service Award** honors outstanding service in the field of biometrics. Any current IEEE member of the member societies of the Biometrics Council who has been active in the fields of interest of the IEEE Biometrics Council for more than fifteen years is eligible. The awardee will receive a plaque and \$1,000 honorarium. Current officers of the Biometric Council’s Executive Committee are ineligible, and self-nominations are not permitted. A qualified nominator should be at least a senior member of the IEEE and the Biometric Council.

A nomination should include the following information:

- Nominee's name, address and contact details
- Nominator name, address, and contact details
- URL of nominee's website with bio and CV
- URL of nominee's Google Scholar citations
- Two-page statement summarizing the nominee's service activities
- Names of three references willing to write supporting letters. The supporting letters should be sent by the endorsers directly to the Awards Committee Chair in accordance with the instructions in the Meritorious Service Reference Letter template found at https://iee-biometrics.org/wp-content/uploads/Meritorious-Service-Reference-Form_VB.pdf.

IEEE Biometrics Council Leadership Award

Deadline: March 1, 2024



The IEEE Biometrics Council Leadership Award recognizes outstanding leadership in the field of biometrics. 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 fifteen years is eligible. Current officers of the Biometric Council's Executive Committee are ineligible. A qualified nominator should be at least a senior member of the IEEE and the Biometrics Council. Self-nominations are not permitted.

A nomination should include the following information:

- Nominee's name, address and contact details
- Nominator name and contact details
- URL of nominee's website with bio and detailed CV
- URL of nominee's Google scholar citations
- A two-page statement summarizing the nominee's leadership activities

- Names of three references willing to write supporting letters. The supporting letters should be sent by the endorsers directly to the Awards Committee Chair in accordance with the instructions in the Leadership Reference Letter template https://iee-biometrics.org/wp-content/uploads/Leadership-Reference-Form_VB.pdf.

The awardee will receive a plaque and \$2,000 honorarium.

IEEE Biometrics Council Best Doctoral Dissertation Award

Deadline: March 1, 2024

To express recognition of, and to promote outstanding effort and contributions within, doctoral dissertations in fields of interest to the IEEE Biometrics Council, the IEEE Biometrics Council Best Doctoral Dissertation Award was established in 2019. Any current member of IEEE is eligible to be nominated for this award. The nomination should originate from the nominee's dissertation advisor. An advisor can nominate only one dissertation per year. Self nominations are not permitted.

The nomination should be within one year after the successful defense date. The dissertation can be written in any language. However, to be eligible for nomination, an English language version must be provided. The award includes a \$1,000 USD honorarium and a commemorative plaque.

The nominator is required to submit the following materials:

- A nomination letter from the advisor of the student that includes the following information
 - Nominee information, including name, affiliation, and email address
 - The date and outcome of the thesis defense
 - The technical contributions of the thesis and a summary of how the field of biometrics has been advanced by the thesis work
 - The broader societal and economic impact of the thesis work
 - The quality of writing and organization of the material in the thesis
 - Any additional justification about why the nominee deserves this award.
 - A statement that the nominee is a current member of the IEEE
- A letter from the University/Institution showing the successful defense date.
- The nominated dissertation in English and in its original language, if that language is other than English
- Other information that will be useful for the evaluation of the dissertation, if any.

T-BIOM Best Paper Award Nominations

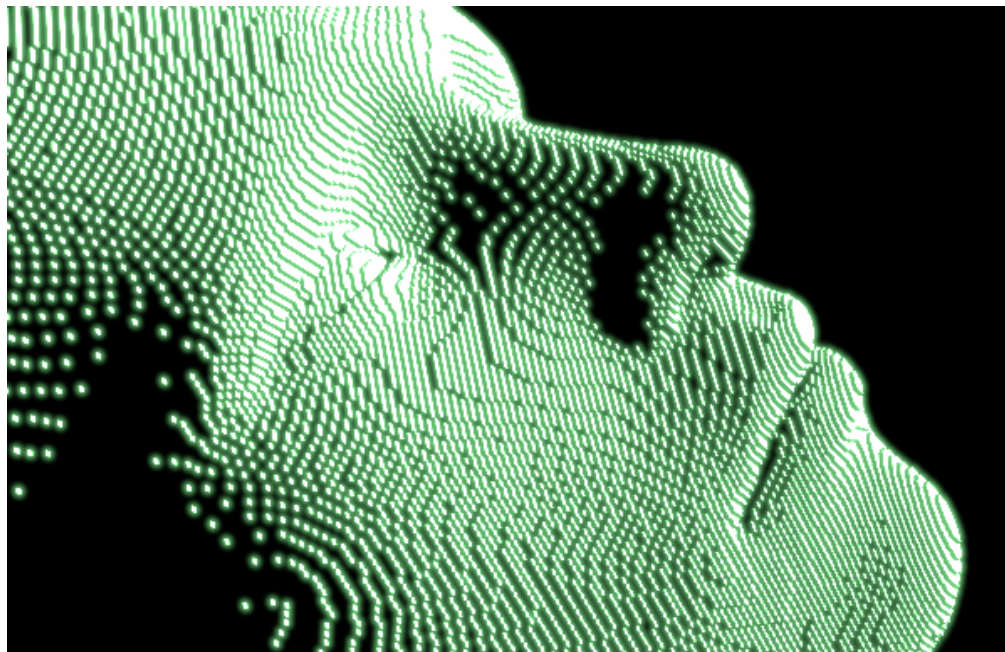
Deadline: March 1, 2024

This annual award recognizes a highly influential and impacting article published in *IEEE Transactions on Biometrics Behavior and Identity Science (TBIOM)* in the preceding two calendar years. Any paper published in the 2022 or 2023 issues of T-BIOM is eligible for nominations. Nominations are solicited through Editorial Board members of T-BIOM. For more details on the eligibility, nomination process, and basis for judging, go to <https://ieeebiometrics.org/awards/transactions-on-biometrics-behavior-identity-science-best-paper-award/>. Nominations are accepted till March 1, 2024.

T-BIOM Best Student Paper Award Nominations

Deadline: March 1, 2024

This annual award recognizes a highly influential and impacting article published in *IEEE Transactions on Biometrics Behavior and Identity Science (TBIOM)* in the preceding two calendar years. Any paper published in the 2022 or 2023 issues of T-BIOM is eligible for nominations. Nominations are solicited through Editorial Board members of T-BIOM. Please see more details on the eligibility, nomination process, and basis for judging at <https://ieeebiometrics.org/awards/ieee-biometrics-council-transactions-on-biometrics-behavior-identity-science-best-student-paper-award/>. Nominations are accepted till March 1, 2024.



REPORT ON THE 2023 FINGERPRINT LIVENESS DETECTION COMPETITION

By Gian Luca Marcialis, Associate Professor, Università Degli Studi di Cagliari, Cagliari, Italy



Every two years, business and academic participants are invited to demonstrate their progress in Fingerprint Presentation Attack Detection (FPAD) at the International Fingerprint Liveness Detection Competition (LivDet). The two tasks in LivDet2023—Liveness Detection in Action and Fingerprint Representation—were designed to assess the usefulness and compactness of feature sets, as well as the effectiveness of the PAD method incorporated in verification systems. By adding two subsets to the training set with unknown sensor information present, the competition incorporates a third, "hidden" challenge that assesses the participants' capacity to generalize their models. Participants were only given authentic fingerprint samples, and competitors evaluated and reported on how well their algorithms performed as a result of this data availability constraint.

Challenges, Dataset, and Competitors

Like the previous edition, the LivDet2023 contest was divided into two main challenges:

Challenge 1, *Liveness Detection in Action*: Participants were required to submit an algorithm that could generate an "integrated score" combining the previous score with the likelihood of

being the claimed user, as well as the “score,” which is the probability of the fingerprints being a bona fide sample. It is up to the challenge participants to decide whether to use the proper "user-specific" information.

Challenge 2, *Fingerprint Representation*: To guarantee excellent performance in terms of accuracy and speed, feature vectors in modern authentication systems must be compact and discriminable. We asked competitors to submit PADs that return the feature embeddings for the input image in order to fulfill the requirements previously mentioned.

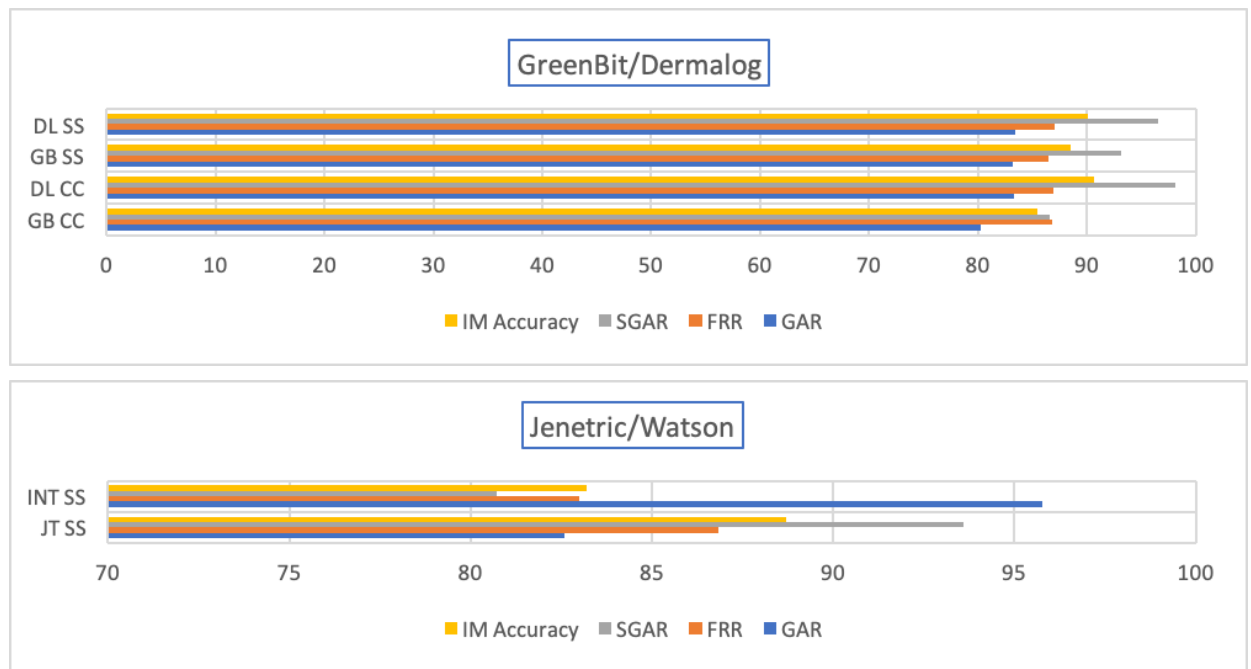


Figure 1. Results of Challenge 1 show an average performance of all 17 algorithms for known and unknown sensors

The training set and test set contained fingerprint images acquired by GreenBit DactyScan 84C, Dermalog LF10, Jenetric LiveTouch Quattro, and Integrated Biometrics Watson Mini scanners. The names, brands, and technical specifications of the first two scanners are well-known to competitors. A total of 2,750 samples to the training set were contributed by 25 users and then split into 1,250 bona fide and 1,500 PAs obtained via the traditional consensual method. Conversely, Jenetric and Integrated Biometrics were unidentified scanners, as we withheld any information about them from competitors. Of the five teams that competed, São Paulo State University (UNESP) presented the only two hand-crafted-based algorithms, while the other 15 algorithms submitted by Peking University (China), Hanbat National University (South Korea), Federico II University (Italy) and the Chinese company JIIOV Technology, were all deep

learning-based. Only five of the algorithms were trained using data from a single scanner, while the remaining were trained using all data from all scanners.

Results and Conclusions

The eighth edition of the Fingerprint Liveness Detection Competition allowed for the assessment of existing PAD interoperability, as well as the effect of integrating a PAD system

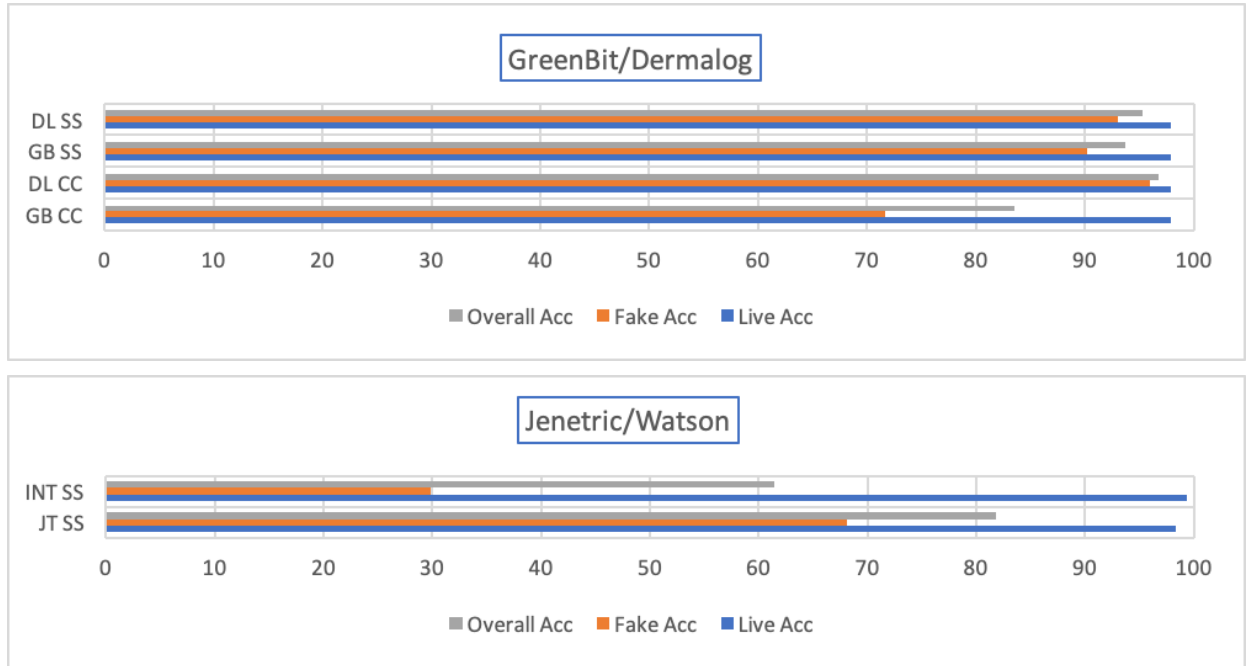


Figure 2. Results of Challenge 2 show average performance of all 6 algorithms for known and unknown sensors

with an automated fingerprint identification system, and evaluating the corresponding levels of compactness, speed, and representativeness. The proposed algorithms reported a good degree of compactness, with feature vectors ranging between 32 and 800 elements, while maintaining performances comparable with the algorithms of previous editions.

The competitors approached the hidden challenge in a variety of ways. Some trained using only the data from the other sensors to perform a sort of transfer domain; others used data from multiple sensors to increase the PAD's ability to generalize. Still others used information from the training data to generate unknown PAs synthetically.

Sam Altman’s bizarre eyeball-scanning crypto project Worldcoin makes global debut, *New York Post* (July 24, 2023)

<https://nypost.com/2023/07/24/sam-altmans-eyeball-scanning-worldcoin-makes-global-debut/>

Sam Altman, the co-founder of OpenAI, recently introduced WorldCoin, a cryptocurrency coin that could guarantee the development of a “privacy-preserving” global financial system. The system requires customers to scan their eyes using a device called an “Orb” that performs iris recognition and outputs a so-called “World ID” unique to each user. The potential and controversies of this system still remain to be fully evaluated.

Home Office secretly backs facial recognition technology to curb shoplifting, *The Guardian* (July 29, 2023)

<https://www.theguardian.com/technology/2023/jul/29/home-office-secretly-backs-facial-recognition-technology-to-curb-shoplifting>

The article discusses the possibility that covert UK government strategies could support the use of electronic surveillance in shops. Such a decision would raise several issues and contrast sharply with the EU ban on the use of AI in public spaces.

Amazon’s Instant ID Points Toward Instant Payments, *Forbes* (July 31, 2023)

<https://www.forbes.com/sites/davidbirch/2023/07/31/amazons-instant-id-points-toward-instant-payments/>

Amazon One, a recently introduced product from Amazon, relies on palm-based biometric authentication to offer a number of services at more than 500 Whole Foods and Amazon Fresh locations across America. Services could include payment, identification, loyalty, and entry.

Beyond Just Ethics: The Implications of Biometrics and Data Privacy, *Forbes* (August 2, 2023)

<https://www.forbes.com/sites/forbestechcouncil/2023/08/02/beyond-just-ethics-the-implications-of-biometrics-and-data-privacy/>

Data privacy is considered one of the most sensitive issues associated with the use of biometric recognition systems. This article discusses how the methods used to collect, employ, and store data may raise significant concerns about the acceptability of biometric solutions in many areas. It also mentions some guidelines organizations should consider to preserve data privacy and protect consumer data.

China set to limit facial recognition technology after backlash, *The Times (UK)* (August 8, 2023)

<https://www.thetimes.co.uk/article/china-seeks-to-restrict-facial-recognition-technology-after-backlash-0pc2m2jss>

The article discusses rising concerns in China against the massive use of facial recognition technology, which is currently employed even in such intrusive areas as public lavatories. The

Cyberspace Administration of China (CAC) suggests that image-capturing and scanning devices should be used only for specific purposes and with individuals' consent, and therefore avoided in places such as hotel rooms, gyms, and changing rooms. An exception would be devices installed in public spaces in the interests of national security, provided warning signs were posted.

TechScope: "Are you kidding, carjacking?" – The problem with facial recognition in policing, *The Guardian* (August 15, 2023)

<https://www.theguardian.com/newsletters/2023/aug/15/techscope-facial-recognition-software-detroit-porcha-woodruff-black-people-ai>

The article reviews the case of a falsely arrested woman and how it points to bias in facial recognition for forensics applications.

X, formerly Twitter, to collect biometric and employment data, *BBC* (September 1, 2023)

<https://www.bbc.com/news/technology-66679922>

In an update to its privacy policy, X, formerly known as Twitter, will collect certain biometric data on its users, such as a photograph of their face. Its rationale was to be able to offer a more targeted and individual experience for users, and advance the ambition to turn X into an "everything app."

Facial recognition could transform policing in the same way as DNA, says Met chief, *The Guardian* (September 11, 2023)

<https://www.theguardian.com/uk-news/2023/sep/11/facial-recognition-could-transform-policing-in-way-dna-testing-did-says-met-chief>

The article shares the opinions of Britain's most senior police officer who believes facial recognition technology will transform criminal investigations as significantly as DNA testing once did.

India points the way to digital access across Africa, *The Financial Times* (September 18, 2023)

<https://www.ft.com/content/3c1504ef-96f7-4656-a5cf-d474123dc31e>

The article discusses the so-called India Stack, i.e., the public digital infrastructure that enables payments and biometric identification for millions of individuals in India. Given the success of the Indian experience in squeezing corruption, increasing tax efficiency, and empowering citizens previously excluded from formal health, education, or banking systems, this model is currently being considered by several other countries seeking to boost economic growth and meet sustainable development goals. Supporters suggest the wide scale adoption of this model could have a similar effect on countries in Africa as well.

One of the world's busiest airports will reduce the need to present your passport, *USA Today* (September 20, 2023)

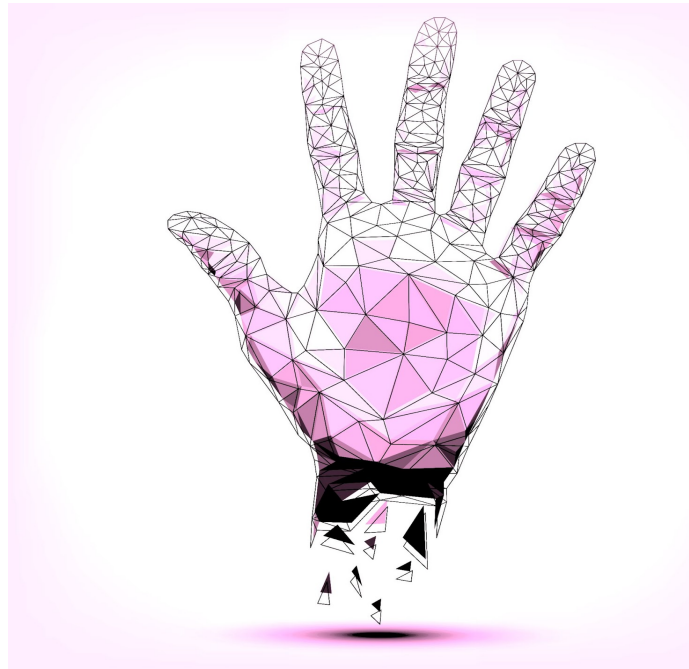
<https://eu.usatoday.com/story/travel/news/2023/09/20/singapore-changi-airport-passport-travel/70914756007/>

Singapore has recently passed a new law to allow passport-free travel as soon as the first half of 2024. The article outlines how Singapore Changi Airport will use biometric sensors targeting the faces of passengers departing the island nation in place of passports. It also mentions that some U.S. airports and airlines, such as Delta Air Lines' terminals in Atlanta, are also using biometric technology, and that Dubai Airports is also introducing passport-free travel, to be implemented with Emirates Airlines.

Deepfakes make banks keep it real, *Financial Times* (September 21, 2023)

<https://www.ft.com/content/6ca90b12-3ee6-409c-968d-1cffe29ee973>

The article discusses how AI-generated deepfakes can be used to bypass biometric security systems, such as facial recognition, in order to create counterfeit ID documents. The authors propose using behavioural biometrics to assess and learn how a user handles a device, such as a smartphone, or behaves when using a computer, in order to combat this type of ID theft.



SPECIAL FEATURE: SPOTLIGHT ON EU PROGRAMS

TReSPAsS-ETN: TRaining in Secure and PrivAcy-preserving biometricS - Early Training Networks

By Massimiliano Todisco, Associate Professor and Chiara Galdi, Assistant Professor, EURECOM, Biot, France



Logo for the TReSPAsS-ETN project

The TReSPAsS-ETN project (1) a landmark initiative in biometric recognition technology, is steering Europe towards significant advancements in this domain. By transcending the traditional reliance on passwords or tokens, which are often susceptible to loss or theft, the project embraces biometric technology that utilises unique biological and behavioural traits for identity verification. This shift from traditional security techniques is

increasingly important in an era dominated by cloud applications, which demand robust security measures for distributed personal authentication. Concurrently, the project is in alignment with the strict privacy regulations of the European General Data Protection Regulation (GDPR).

Europe is fostering a new wave of researchers skilled in biometrics whose

focus is on innovating technologies that uphold both security and privacy. The TReSPAsS-ETN Marie Skłodowska-Curie Early Training Network project is at the forefront of this endeavor. Aimed at improving security through advanced presentation attack detection (PAD), and bolstering privacy through efficient encryption methods, these cutting-edge technologies are being integrated into commercial systems. By doing so, users can ensure compliance with GDPR and reinforce European research leadership, while supporting the growing biometric market.

The project's training programme is comprehensive, merging specific technical skills with broader competencies like entrepreneurship and innovation. This approach equips 14 Early Stage Researchers (ESRs) with the necessary skills to lead the next generation of secure, privacy-conscious biometric technologies.

The TReSPAsS-ETN consortium is a collaborative network of seven universities and eight industrial entities from across Europe, including France, Germany, the Netherlands, Switzerland, Spain, Sweden, and Belgium. The multidisciplinary instruction combines expertise in biometrics, security, law, and ethics to foster innovative, secure, and privacy-preserving biometric technologies. Members of the consortium include EURECOM in France; Hochschule Darmstadt, Fraunhofer Institute for Computer Graphics Research IGD, the Humboldt Institute for Internet and

Society, and Deaudat GmbH in Germany; the European Association for Biometrics (EAB) and the University of Groningen in the Netherlands; IDIAP Research Institute, St. Gallen University, and OneVisage in Switzerland; Universidad Autónoma de Madrid, and Biometric Vox in Spain; and Katholieke Universiteit Leuven in Belgium.

The training programme includes a blend of existing and newly developed courses, covering both the technical and ethical aspects of biometrics. It is organized around three general themes:

- **Next Generation Privacy Preservation:** Focusing on safeguarding biometric systems against risks like identity theft and unauthorised cross-matching.
- **Next Generation Security Protection:** Concentrating on the security of biometric systems, particularly against attacks in deep neural network-based systems.
- **Ethical, Legal, and Societal Acceptance Dimensions:** Bridging the gap between technical expertise and ethical, legal, and societal considerations, this theme advocates a holistic understanding of biometrics within these broader frameworks.

Collectively, these themes represent a holistic approach to training and research in biometrics, blending technical proficiency with an understanding of the

broader ethical, legal, and societal implications.

The programme culminates in industry networking and a final workshop, delivered by a combination of academic and industrial partners, and supplemented with dedicated network-wide training events. These events include existing internal courses which will be offered to all TReSPAsS-ETN ESRs. Others are newly created training courses that complement existing courses, and represent the added value of the TReSPAsS-ETN training programme.

The final workshop of the project was entitled “Workshop on Frontiers in Privacy and Security for Biometrics in Europe: Outcomes from PriMa & TReSPAsS-ETN EU Projects.” This event served as a concluding chapter, bringing together the progress and insights gained from these important EU projects. As a collaboration between the consortia of the PriMa [1] & TReSPAsS-ETN [2] EU Projects, it marked a significant and somewhat rare event in European Union research initiatives. This partnership showcased a proactive and integrated approach towards addressing complex challenges, particularly in the fields of privacy and security for biometrics.

The joint workshop was held at EURECOM in Sophia Antipolis, France, on September 13-14, 2023. Aiming to drive adoption and societal acceptance of biometrics, it featured sessions on technical advancements, threat management, usability, impact assessments, and legalities. Researchers across disciplines

shared solutions and insights to improve security, address privacy concerns, and ensure legal compliance.



Raymond Veldhuis (I) and Massimiliano Todisco, coordinators for PriMa and TReSPAsS-ETN, respectively, at the final joint workshop held at EURECOM on September 13-14, 2023.

In the following, we present a concise summary of the key points and insights shared by the invited speakers during their talks.

Tom Bäckström, D.Sc. (tech.), Associate Professor at Aalto University, Finland
“[Conceptual Framework for Privacy in Voice Technology](#)”

Bäckström unveiled his comprehensive framework designed to enhance privacy in voice and speech technology. This framework, developed over several years, aims to catalyse discussions, dissemination, and performance evaluation of complete systems in this

rapidly evolving field. Bäckström’s framework is characterised by its dual



focus on objective protections and user interface design. Objective protections pertain to securing private messages and their related side-information against unauthorised access. At the same time, the framework addresses the design of user interfaces. Bäckström advocates for interfaces that clearly represent the level of privacy protection a system actually offers. Such transparency is essential to user trust and awareness, allowing individuals to make informed decisions about their data. Bäckström also identifies several challenges and future directions in his framework. In research, the focus areas include subjective privacy, which deals with individual perceptions of privacy, development of theoretical metrics for privacy evaluation, addressing computational complexity, and exploring methods for disentanglement in data processing. Equally important is the challenge of dissemination, particularly in

communicating the uncertainties inherent in results. This involves ensuring that end-users and stakeholders understand the limitations and reliability of privacy protections in voice and speech technology systems.

Arun Ross, Professor in the Department of Computer Science and Engineering at Michigan State University, USA



“Deepening Trust: Biometrics in a Deep Learning World”

This comprehensive speech delved into the progress made in the field of biometrics over the past decade, highlighting the integration of deep learning, and addressing key challenges. Ross began by outlining the diverse applications of biometrics, ranging from border security to smartphones. He noted the significant impact of deep learning and deep neural networks in enhancing the capabilities of biometric systems. This evolution has led to more efficient, accurate, and robust biometric recognition techniques. A key focus of the speech was the innovative

work Ross conducted in his laboratory, including the development of techniques for presentation attack detection. Furthermore, he discussed their efforts in privacy-enhancing technologies and the creation of synthetic biometrics, demonstrating a proactive approach to addressing privacy concerns and data security. Despite these advancements, Ross underscored several challenges that biometrics still faces. These include ensuring data integrity, combating presentation attacks, and protecting personal privacy. Addressing these challenges is crucial for deepening societal trust in biometric technology. Ross emphasised the need for ongoing research and collaboration across disciplines to overcome these hurdles. He advocated for a balanced approach that advances biometric technology while upholding ethical standards and privacy considerations.

Franck Dumortier, Researcher in the Cyber & Data Security Lab at the Vrije Universiteit Brussel, Ixelles, Belgium.

[“The Processing of Facial Images & the Law”](#)

Dumortier's talk offered a critical examination of the legal landscape surrounding face recognition systems and synthetic image data under the GDPR, the Police & Justice Directive, and the draft AI Act. In an era where all biometric technologies, and particularly face recognition systems, are increasingly prevalent, understanding the legal implications of their use is crucial.

Dumortier pointed out that, under current legal frameworks, face recognition systems are deemed "sensitive" when used for



authenticating or identifying individuals. He detailed how the GDPR and the Police & Justice Directive navigate these technologies, especially considering their potential for privacy intrusion and ethical concerns. The speech delved into the provisions of the current draft AI Act, which introduces safeguards for processing operations involving face recognition. A notable aspect is the explicit prohibition of using real-time remote biometric identification systems in publicly accessible spaces. A significant part of Dumortier's discussion revolved around the legal ambiguities concerning databases containing images of natural persons not intended for unique identification or authentication. He raised important questions about the legal regime applicable to such data repositories. Furthermore, Dumortier explored the legal dimensions of synthetic image data generated by AI models. He examined how current laws apply to this kind of data and

pondered the legal implications should it be used for scientific biometric research.

Nikolaos Ioannidis, Doctoral researcher at the interdisciplinary Research Group on Law, Science, Technology & Society of Vrije Universiteit Brussel, Ixelles, Belgium
“Impact assessment for artificial intelligence under a fundamental rights lens”



Ioannidis' presentation critically examined the rising reliance on algorithms for decision-making, and the impact of this reliance on human agency and rights. He began by noting the widespread adoption of algorithms in decision-making processes, which has been facilitated by data processing, profiling, and inference drawing. While acknowledging the efficiency brought by these complex algorithms, he highlighted some inherent challenges, such as the risk of perpetuating stereotypes and societal biases. Ioannidis

pointed out that these can infringe upon the rights and freedoms of natural persons, transforming data subjects into mere data objects. A key focus of the speech was on data protection law as an essential framework for safeguarding biometrics and personal data in the era of AI. He emphasised the importance of these laws in providing a foundational basis for protecting fundamental rights against the potential harms of algorithmic decision-making. The speech also delved into artificial intelligence law. Ioannidis explored how the process of Data Protection Impact Assessment (DPIA) could serve as an effective means to protect fundamental rights in AI contexts. He argued for the necessity of thorough impact assessments to evaluate and mitigate the risks associated with AI technologies.

NOTES:

1. PriMa has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 860315
2. TReSPAsS-ETN has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 860813

EXPERT PERSPECTIVES: *Adam Philpott*

Interview conducted by Dr. João Neves, Assistant Professor of Computer Science at the University of Beira Interior, Covilhã, Portugal



Adam Philpott assumed the post of President and Chief Executive Officer at Fingerprint Cards AB in September 2023, after serving on its Board of Directors for three months. Previously, he held the position of Chief Revenue Officer (CRO) at Trellix, a cybersecurity company formed in October 2021 from the merger of McAfee Enterprise and FireEye. Philpott is a strong business leader with an extensive track record in leading significant change while driving high-performing teams. Prior to joining Trellix in 2022, he worked for McAfee for more than four years, first as leader of the company's EMEA business and later as CRO. Philpott's earlier experience included more than 15 years in a variety of leadership positions across Australia, Japan, and the Asia-Pacific region at Cisco, finally leading the company's EMEA Security Sales business.

NEVES: You have recently been appointed as the CEO of Fingerprint Cards after building a proven track record in the management of cybersecurity companies. What advantage do you think this background will bring to your new role?

Philpott: Throughout my career, there are three core pillars that have evolved for me and apply to my role at Fingerprints:

1. **Customer centricity** – I've spent a significant portion of my career working directly with customers. As a result, customer centricity has been deeply ingrained into my leadership style. Business is a value exchange, underpinned by empathy towards the challenges our customers face. We must be

relentless in tracing all our objectives and strategy to the wants and needs of our customers and potential customers.

2. **Leadership** – Of course, my role will focus on creating a clear vision for the short- and long-term future of Fingerprints. I also want to share my skills and experience internally, to empower our workforce to become leaders in their own right. Only by doing this will we be fully equipped to fulfill our customers' needs at every level, across business units.
3. **Identity** – Security was historically underpinned by the 'trust but verify' model. In today's digital

world, this has changed to one of 'zero trust.' Identity has been thrust into the heart of the cybersecurity spotlight. I want to use my own and Fingerprints' wealth of identity experience to address today's number one cybersecurity vulnerability: passwords.

NEVES: Even though you have only been CEO for a couple of months, you have previously been on the Board of the company. So, considering that fingerprinting is one of the most mature biometric recognition modalities, can you tell us the main challenges and innovations that Fingerprint Cards have focused on in the last years?

Philpott: I joined the Board in May 2023 because I was fascinated by what Fingerprints has already done in the market. But what interests me even more is where the company is going.

In the face of rapid and all-encompassing digitization, legacy identity security, authentication and access methods have become hopelessly outdated. There are countless ways in which we interface with both the physical and digital worlds, and passwords and PINs are a significant part of this. Yet, passwords and PINs are simply no longer able to meet today's digital security challenges. According to a recent survey of the causes of data breaches, 80% of computer hacks and cyber-crimes can be traced back to compromised passwords (see

<https://www.verizon.com/business/resources/reports/dbir/>).

Our mission has been, and will continue to be, to create a secure and frictionless user authentication experience for the myriad of different ways in which we engage with the digital world. Due to continued digitization, the opportunities to apply this are endless. The mobile, PC, access control, and payment industries are already wise to

“Our mission has been, and will continue to be, to create a secure and frictionless user authentication experience for the myriad of different ways in which we engage with the digital world.”

the value of biometrics. Over the coming years, we expect to leverage existing and new modalities to consolidate these markets. This could include expansion into new and exciting ecosystems across physical and logical access in our homes and buildings, and even across the internet worlds of mixed, augmented and virtual reality.

NEVES: Apart from fingerprint recognition, the company has also developed products

based on other biometric modalities, such as iris images. Based on the different solutions advertised in the website (e.g., access control in buildings, PC and mobile-device authentication), it seems that the company has been primarily focused on constrained and cooperative scenarios. Has the company ever tried to develop biometric recognition products capable of operating in unconstrained scenarios in which the user does not explicitly cooperate with the acquisition system?

Philpott: We place the customer at the center of product strategy. Within the current market, user appetite for constrained, cooperative solutions remains high. Over years of familiarization, consumers are now comfortable with, and value, this kind of biometric solution, such as fingerprint or IRIS recognition in our phones. This is not to say that our focus will not expand beyond constrained and cooperative solutions.

As a company that prides itself on its roots in R&D, we're constantly looking at how we can thoughtfully expand our offerings to include new and innovative solutions. Our new biometric platform strategy will aim to incorporate a variety of constrained/unconstrained and cooperative/uncooperative solutions for a range of existing and new use-cases.

NEVES: Staying on the topic of innovation, we would like to know if your research team is a big part of the company, and how important the latest advances in the field of biometrics are to the company. Also,

what is the company's relationship with the academic community working on the topic?

Philpott: Since our foundation in 1997, research has been essential to the growth of the company. I'd argue Fingerprints invented modern and scalable capacitive fingerprint sensing, and this has required extensive R&D investment. This focus on research will not change now. Current market conditions and the economic climate have placed constraints on capital, and by proxy, R&D investment. Yet we know that innovation and research requires risk.

We've therefore updated our governance model to be more efficient and agile. This enables us to focus on priority innovation areas, but still allows for risk in pursuit of new solutions as market and consumer needs continue to evolve. Over recent years we've also created new, and nurtured existing, relationships with strategic and academic partners, as well as industry talent. Last year we joined the World Economic Forum's "New Champions Community" as its first biometrics company member (see press release at <https://ml-eu.globenewswire.com/Resource/Download/b1cd3ca1-5e6d-4380-9e3e-49a3c141623a>). We've also announced a new functional organization model in which we're recruiting the best industry talent. As the economy recovers, we're keen to prioritize this area of the business again.

NEVES: In a recent interview, you mentioned that a large majority of security

breaches are related to passwords, and therefore these identifiers should be

“... it amazes me that passwords and PINs still form the basis of most personal and organizational security.”

replaced by biometric ID to enhance security and user experience. When do you expect that passwords will be replaced completely by biometric authentication systems?

Philpott: I’ve been working in cybersecurity for more than 20 years and it amazes me that passwords and PINs still form the basis of most personal and organizational security. While passwords are deeply embedded in our security processes, and not to mention they are a cheap strategy, they are unsecure and inconvenient, especially in the context of today’s connected world. Ten years ago we may have had to deal with myths and misconceptions, today countless industries are already wise to the value offered by biometrics. As a result, biometrics is becoming the preferred authentication method for consumers. One recent survey found that 52% of those who use biometrics prefer it over any other authentication method (see <https://www.insiderintelligence.com/content/consumers-feel-smartphones-safe-but-prefer-biometric-methods>).

We are also seeing some standardization in security as the industry moves away from passwords towards passkeys and multi-factor authentication. As biometrics becomes increasingly incorporated within these authentication methods, this will accelerate the shift to the end-user becoming the key. My guess is that within a decade the industry will be rid of passwords. My hope is that this day comes sooner. As we move towards biometrics though, it’s important to remember that this alone will not eradicate risk. Users will still need to be cautious with attacks like social engineering, but we can certainly bring the risk level down significantly.

NEVES: In one of the latest press releases from the company you mentioned the need to diversify its revenue streams to avoid dependence on mobile-based authentication sensors. Based on this comment, we are curious to know which biometric recognition products you foresee in the future?

Philpott: Our biometrics platform strategy will seek to incorporate a variety of innovative modalities across use cases that meet the challenges of the digital world today and tomorrow. The platform itself is broken down into four layers:

- *How we capture* – Not only will this include our proven fingerprint and IRIS modalities, but we also want to expand into the latest biometric modalities as well. This could

include facial, behavioral, voice and movement biometrics.

- *How we process* – Determining the processes to extract key indicators from software modalities, such as fingerprints, iris, face or gait.
- *How we expand analytics* – This refers to the software analytics engines, such as algorithms that match the signal to a given outcome such as identity or behavior. AI and machine learning offer significant opportunities here.
- *How we make the match* – Specifying the software data layer where the information is managed and securely stored. The distributed data model stored and encrypted on the device is perfect for many use cases, but there are opportunities and business models for using more virtualized mechanisms, such as cloud and blockchain, further down the line.


Overall, our goal is to continue creating a user authentication experience that makes engaging with the digital world easy and secure. There are a multitude of development and expansion opportunities. We are exploring new software modalities, such as face and health; analytics engine expansion for outcomes beyond identity with AI; new verticals, including retail and government; and new use cases including FIDO (Fast Identity Online) and KYC (Know Your Customer).

To sum up, Fingerprints continues to be a leader in premium biometrics solutions. By evolving to a new dynamic organization, we're well positioned to drive future innovation and deploy our expertise and technology in new, impactful ways.



RESEARCHER ON THE RISE: *Hatef Otroshi*

Interview conducted by Dr. Ruben Tolosana, Assistant Professor of Biometrics and Data Pattern Analytics - BiDA Lab at the Universidad Autonoma de Madrid, Spain.



Hatef Otroshi received his B.Sc. degree (Hons.) in electrical engineering from the University of Kashan in 2016, and his M.Sc. degree in electrical engineering two years later from the Sharif University of Technology. He is currently pursuing a Ph.D. in Switzerland at the École Polytechnique Fédérale de Lausanne, and serving as a research assistant with the Biometrics Security and Privacy Group at the Idiap Research Institute. Through the latter group, Otroshi received the H2020 Marie Skłodowska-Curie Fellowship (TReSPAsS-ETN), and spent six months as a Visiting Scholar with the Biometrics and Internet Security Research Group at Hochschule Darmstadt in Germany. His honors include the 2023 European Association for Biometrics (EAB) Research Award.

TOLOSANA: Despite being a very young researcher, you have already published several papers in the main track of top conferences, such as ICCV, NeurIPS, ICIP, and top journals such as *IEEE TPAMI*, *TIFS*, and *TBIOM*. What are the strategies and key factors that have encouraged this level of productivity?

Otroshi: I always try to find interesting research questions and approach them with new solutions. Understanding the limitations of previous works in the literature and being familiar with state-of-the-art techniques in different domains helps me develop new ideas for new solutions. In addition, I often try to divide my working hours and work on different problems in parallel. This allows me to proceed with multiple works and explore

new problems in-between. When one work is finished, I am already in the middle of another work and have developed this second work to some state. Thus, I do not need to spend time finding a new problem and exploring potential solutions. In addition to my independent research, I also collaborate with different researchers, and I am always open to new collaborations.

TOLOSANA: You did both your B.Sc. and M.Sc. degrees in Iran and now you are pursuing your Ph.D. in Switzerland. What was your motivation to move from one place to another? Was it difficult for you? What can you suggest to young aspirant researchers about relocation?

Otroshi: I received my B.Sc. as a first-rank student from University of Kashan, and

then, for my M.Sc., I attended Sharif University of Technology, which is the best engineering university in Iran. Moving to a different country for my Ph.D. had some challenges, such as cultural differences and being far from family and friends. However, it brought me some great opportunities. EPFL is one of the best universities (top 20) in the world, and working on my Ph.D. thesis as a research assistant at the Biometrics Security and Privacy group of Idiap Research Institute means being part of one of the pioneer research groups in the field of biometrics. I also received the H2020 Marie Skłodowska-Curie fellowship, which allowed me to extend my network with peers in the field across different universities and research institutes. In fact, moving to a new country can be challenging, but it can also provide new opportunities in your work and enlarge your network. In addition, you will gain more experience in your life, such as learning a new language and experiencing a different culture.

TOLOSANA: As you mentioned, you have received a H2020 Marie Skłodowska-Curie Fellowship (TReSPAsS-ETN) for your current doctoral program. Could you share your experience and the significance of this fellowship in your research journey?

Otroshi: I received the fellowship through the TReSPAsS-ETN project as an Early Stage Researcher (ESR). This project provided a unique opportunity to collaborate with researchers in a consortium of seven universities/research institutes, supported by seven industrial entities, located in

“Moving to a new country can be challenging, but it can also provide new opportunities in your work and enlarge your network.”

France, Germany, Netherlands, Switzerland, Spain, and Belgium. We had several training events, as well as project meetings, that facilitated collaboration and the exchange of ideas with other ESRs and peers in the field of biometrics. In addition, each ESR could experience research internships in other universities and industrial partners.

TOLOSANA: You also have recently conducted a six-month research internship with the Biometrics and Internet Security Research Group at Hochschule Darmstadt in Germany. How important do you rate internships and collaborations with other institutions for a Ph.D. student? What is the major impact this experience has had on your way of conducting research?

Otroshi: An internship offers a good opportunity to collaborate with experts in another place and extend your network. In addition, it allows learning from the expertise of the host team, as well as experiencing a different research approach. During my internship at Hochschule Darmstadt (HDA), I was able to work on homomorphic encryption, as an approach to protect biometric templates. I learned many things from the team in

HDA, and I am happy that our collaboration led to several publications. In addition, during my internship at HDA we initiated a joint collaboration with Universidad Autónoma de Madrid (UAM) that also resulted in several joint publications.

TOLOSANA: In your Ph.D. you are working extensively in the topic of biometric template protection. What challenges has your Ph.D. addressed and what are, in your opinion, the ones yet to be solved?

Otroshi: Biometric template protection (BTP) is an emerging research topic that is more recognized in the light of data protection regulations that consider biometric data as sensitive information. One important part of my PhD has been focused on reconstructing face images from face templates under different threat models. My research shows that there are several practical situations where an adversary can generate a rough estimate of the underlying face image if given a leaked facial template. Such a scenario threatens both the security and privacy of face recognition systems. This is why we need to protect biometric templates, and I have proposed several different protection schemes. However, even after we apply such protection, the question remains how can we measure the leakage of information in protected biometric systems? I tried to use information theoretic measures to evaluate this leakage, but there are still many open questions. For example, one of the important requirements of BTP methods is that the protected templates should be irreversible. Therefore, an open question is how can we have a general

method to quantify the irreversibility of different protected templates.

TOLOSANA: In addition to research publications, you also have received some US patents. Could you please provide more information about the motivation for this and the origin of this collaboration with the other inventors? Also, could you please highlight the significance of these patents for the topic of quality assessment?

Otroshi: In my M.Sc. I contributed to several works that led to US patents, including three patents that were directly logged from my thesis and based on new methods with potential industrial applications. While previous works on quality assessment of digital media (image, video, or voice) were based on estimating the mean opinion score (MOS), our new methods could predict the distribution of opinion scores, which provides more information than a single average value. Patents are, in fact, an important type of intellectual property that can be useful for both academic and industrial communities. In particular, when researchers find innovative methods that can have broad industrial applications, they should publish their methods as patents. In this way, inventors can share new ideas with others, but if some companies wish to use this new method in their products, they need to request permission or a license from the owners. Patenting helps you protect your innovations while still sharing them with society.

TOLOSANA: If you had extra time and funds, which topic would you be interested in pursuing?

Otroshi: During my Ph.D., I tried to explore different areas, including minimising privacy-sensitive information in biometric templates, template protection mechanisms, and measuring the leakage of information in biometric systems; the security aspect of face recognition systems,

such as template inversion and presentation attacks; and generative models for reconstructing face images from facial templates and also generating synthetic face images for training face recognition. In each of these topics, there are still several open questions that I am interested in and can be further explored in the future.



LECTURE NOTES

EU BIOMETRIC DATA REGULATION: PAST, PRESENT, AND A LOOK INTO THE FUTURE (Part 1)

By Els J. Kindt, Associate Professor and Researcher at eLaw - Center for Law and Digital Technologies, Leiden University, Leiden, The Netherlands

Els J. Kindt is an associate professor and affiliated senior researcher with eLaw, the Center for Law and Digital Technologies of Universiteit Leiden, (<https://www.universiteitleiden.nl/en/law/institute-for-the-interdisciplinary-study-of-the-law/elaw>), The Netherlands, as well as the Centre for IT and IP Law (CITIP) of KU Leuven, Belgium (<https://www.law.kuleuven.be/citip/en/>). She also has her own research and advice company, RADL. Kindt has been working for more than 20 years in law and biometric-related projects, resulting in many publications, teaching posts, and conference presentations. In 2020, she set up the Biometric Law Lab (BLL) for exchanging legal knowledge in this domain.

Abstract: The collection and use of biometric data has become an eager goal for many stakeholders. The reason is the very nature of the data itself. Biometric data are uniquely linked to individuals and therefore a good identifier across domains. At the same time, the same properties also lead to serious risks when biometric data are tied to the rights and freedoms of citizens, and for society, when it comes to such risks as tracking and surveillance. Legislation has attempted to regulate the use of these technologies. This tutorial provides a succinct discussion and some insights into EU regulation applicable to biometric data processing, especially in the domain of data protection and for future AI systems. Part I found below explains the need to distinguish between the applicable legislative frameworks, and provides a rationale for their implementation. We zoom into the definition and main principles of the General Data Protection Regulation with regard to biometric data, including its application to research activities. At the same time, we also discuss some criticism and unveil the imperfections. In Part II, which will follow later this year, we discuss the regulation of biometric data use in the upcoming Artificial Intelligence Act.

Biometric data: Distinct legislative frameworks for a myriad of uses

Biometric information, such as fingerprint and facial images, has long been used to

search for, and to identify suspects and criminals when no other information (such as a name) is available. The use of automation, such as the Automated

Fingerprint Identification System ('AFIS') deployed by police worldwide, and the collection, database storage, and exchange of biometric information for crime investigation over the years has led to specific provisions in national criminal (procedure) law and the legal frameworks of international cross-border police cooperation. ⁽¹⁾

Besides criminal investigation, biometric data has also proven useful for migration and identity control at borders. After the 9/11 terrorist attacks in the U.S. in 2001, border control in many countries became much stricter, and procedures and systems were instituted, such as the US -VISIT program of the U.S. Department of Homeland Security, for the collection and use of biometric information. As a result, biometric information became mandatory in travel documents for EU citizens and EU Member States began collecting biometric information from citizens who apply for an ePassport. ⁽²⁾ The EU large scale IT systems assuring the Union's integrated border management also gradually increased the use of biometric data for the Schengen border checks, which each time was subject to detailed specific regulations. ⁽³⁾

In the slipstream of the aforementioned rapid spread of the automated use of biometric information by law enforcement and border control authorities, the use of this data became more 'accepted' and increasingly 'mainstream.' Many public entities, such as cities, use or experiment with biometric data collection (e.g., facial

images) to ensure public security and safety. But, an increasing number of private players are also interested in using biometric information for security and/or convenience. For example, financial institutions use biometric information in multi-factor authentication strategies for securing customers' access to their bank accounts. And, social media are entertaining their audiences by pushing users to upload their facial images and to experiment with augmented reality filters and spoken commands. The increasing uses of biometric data in these wider public and private domains have led to regulatory bodies tackling the processing of biometric data in general data protection legislation, particularly in the General Data Protection Regulation ('GDPR') that took effect as of May 2018. ⁽⁴⁾

Some researchers also depend on biometric data for their activities worldwide. Although researchers usually have no intention to use such data in direct combination and application to the individuals from whom data are collected, the GDPR nevertheless still applies. In combination with national legislation, this imposes strict rules on how such information may be employed.

For all these applications, first and above all, fundamental rights and freedoms must at all times be kept in mind. This is important insofar as these rights play a key role in democratic societies, and the use of biometric information does pose a risk.

First and above all: any biometric data use shall respect the fundamental rights and freedoms

Fundamental rights ('FR') are established in national constitutions and in binding supranational conventions, such as the European Convention on Human Rights ⁽⁵⁾ and the EU Charter of Fundamental Rights. ⁽⁶⁾ These rights and freedoms will also always apply to any use of biometric data. These fundamental rights are the "ground truth" for biometric applications in case of risks, even if such applications would comply 100% with the requirements of data protection. ⁽⁷⁾ Any use (e.g. the collection and storage of fingerprints) will be unlawful if interferences with fundamental rights (e.g., a large collection of biometric data stored in a central database) do not meet the requirements of (i) a law for any such interference ⁽⁸⁾ e.g., for using facial images in public places for public security, (ii) a legitimate aim mentioned in the FR (e.g., a general interest recognized by the Union) ⁽⁹⁾ and (iii) the necessity and proportionality test for such interferences. Users but also (inter)national courts perform this test. ⁽¹⁰⁾

Why is a Fundamental Rights Impact Assessment ('FRIA') test needed ?

As mentioned, biometric data is special because it uniquely identifies people and makes this possible, even without additional information, such as a name. ⁽¹¹⁾ Biometric data relies upon, and is based on, unique human features that are part of one's body. These features cannot (easily) be changed. Moreover, a person cannot

control and will not notice if biometric information is collected, such as fingerprints, or a face collected in a private or a public place by CCTV cameras. Any infrastructure for collecting biometric data hence poses serious risks, such as unknown tracking, surveillance, and discrimination, just to name a few. In principle these are contrary to fundamental rights. The risks of tracking and monitoring are even more eminent with the advent of internet-connected health and lifestyle wearables. Therefore, fundamental risks always need to be assessed first before designing and rolling out any application. In brief, while limitations and technical and organizational safeguards are needed for each biometric application that poses a risk, the result shall be assessed and (re)-evaluated each time through a fundamental rights impact assessment ('FRIA') to see if the interference could be sufficiently mitigated when justified and lawful.

The need to understand the rationale of distinct regulatory frameworks

While in the past there were many gaps in protecting how biometric information was regulated, the law is now gradually filling up these gaps. Distinct regulatory frameworks governing biometric information, each having specific legal objectives, have emerged for the various uses of biometric information. It is important to understand the aims and intentions of the legislators when enacting each of these laws.

The “rule of law:”

Detailed specific provisions for biometric information used for criminal investigation and conviction, in travel documents, and for large scale EU systems regulations

National criminal (procedure) law and international police cooperation frameworks aim to provide a legal basis, legal certainty and compliance with the rule of law⁽¹²⁾ for the use of biometric information in crime investigation. To avoid arbitrary prosecution and punishment in a democratic society, such regulations need to contain specific provisions referring to the use of biometric information. The same rationale applies for the detailed regulations adopted over the years for EU large-scale IT systems, including biometric information and its use at the Schengen borders.

Where biometric information and data are unique tools for identity control, such as where false names are used, and for the investigation of crime, clear laws are needed and must be adopted. The regulations for these IT systems therefore include detailed provisions on how biometric information shall be collected, stored, used and exchanged. Another example is the imminent adoption and use of Digital Travel Credentials (DTC), which allows identity information from an ePassport, including biometric information, to be stored in digital carriers like a smartphone. This use will require not only standardization, but also detailed legislation covering such use.

But the legislative process and the adoption of law at large is slow. As a result, practices sometimes emerge, such as police use of Clearview AI images, without a specific law or where the general framework remains unambiguous. Regulatory bodies⁽¹³⁾ try to fill up these gaps by issuing guidelines and opinions and mandating fines. Their work hence adds to the legislative framework and is often an indispensable complement in understanding the law.

As a general regulation was needed in view of the risks to fundamental rights when using biometric information, such use is now also governed by explicit provisions in the General Data Protection Regulation (‘GDPR’), which was adopted in 2016 and in effect since 2018.

The General Data Protection Regulation (EU) 2016/679 (GDPR)

The GDPR is a general legislation framework (‘lex generalis’) aimed at providing sound rules for the use of biometric data in the public and private domain, no matter what the application and purpose.⁽¹⁴⁾ For this purpose, the GDPR offers, for the first time, a general definition of biometric data. The GDPR further adopted a restrictive approach to using biometric data, in line with Convention 108+ of the Council of Europe, an organization larger than the European Union. More precisely, the GDPR states that the processing of biometric data “for uniquely identifying ‘a person’ is in principle prohibited,” because biometric

data “is considered to pose serious risks for the fundamental rights and freedoms of persons, similar to other specific categories of personal data (“sensitive data”), such as data concerning health (Art. 9.1 GDPR). There are however exceptions to this general GDPR prohibition.

The GDPR provisions, however, remain general, and do not focus on any specific biometric application. This sometimes leads to interpretation difficulties.

The exceptions (Art. 9.2 GDPR) include the explicit (freely given, specific, informed and unambiguous by statement or clear affirmative action) consent. Financial institutions may rely upon this exception and basis to collect biometric information from customers to secure digital access. A substantial public interest is another possibly relevant exception for biometric data processing (Art. 9.2 (g) GDPR)⁽¹⁵⁾. For example, the fight against terrorism or serious crime (as defined) could be such ‘substantial public interest.’

Besides these specific provisions for biometric data, all other GDPR obligations and rights for the persons concerned will apply. As with any other processing, this holds true whether the system is for security or for convenience. This includes the information and transparency obligation. We do not discuss these general GDPR provisions here however.

How GDPR applies to research

The use of biometric data for research purposes also falls under the GDPR, because biometric data is, in principle, personal data, and thus cannot be anonymized. The rationale of the GDPR is that any potential impact on individuals shall be minimized when their personal data is used for research.

For the first time, the GDPR provides for research⁽¹⁶⁾ an explicit legal exception to the overall prohibition to the processing of ‘sensitive’ data (see Art. 9.2 (j) GDPR), provided that minimization is applied and technical and organizational safeguards are taken (Art. 89 GDPR). However, the GDPR exception by itself is not sufficient. One also needs and shall follow national legislation addressing personal data use for research.⁽¹⁷⁾

Reducing the impact when conducting research is obtained by following technical and organizational safeguards—which are sometimes also clarified by national data protection authorities—and hence protecting any personal data that cannot be or is not anonymised if used for research (see Art. 89.1 GDPR). This could imply, for example, that biometric data shall be encrypted, access to the data be limited and logged, transfers limited, and any additional identifying details – if needed - shall be kept and stored in separate places.⁽¹⁸⁾

Research with biometric data, hence, requires checking national legislation to ascertain the measures it imposes to minimize the impact and thus safeguard the rights of the individuals involved.

Member states may impose further conditions for biometric data

For biometric data processing, one shall always also check national law, as the GDPR allows that further conditions and restrictions can be imposed (Art. 9.4 GDPR). The EU Commission keeps a list of such national adopted laws containing conditions for “sensitive” data.

Legal bases for Art. 6 GDPR

A legal basis is needed for any personal data processing, The GDPR mentions six legal bases for lawful processing, including consent, the performance of a contract or compliance with a legal obligation, performance of a task in the public interest or for exercising official authority, or, if necessary for a legitimate interest (Art. 6.1 GDPR). Any one of these legal bases could be sufficient if the processing does not fall under the prohibition of Art. 9 GDPR.

One could argue that when biometric data is used in research, such data is not used to uniquely identify the person from whom the data were collected. This would imply that the prohibition of Art. 9 GDPR, as such, is not applicable. All that is needed is to provide a legal basis of art.

A closer look at some GDPR provisions: Some ambiguities

First general definition of biometric data

Because of the increasing use of biometric data and the risks for individuals and society associated with it, the GDPR – following the work for Council of Europe’s Convention 108+ - has come up with the first general regulation of biometric data. This general definition refers to data based upon human characteristics that contain a certain (alleged) uniqueness. Biometric data is defined as “personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of the natural person, such as facial images or dactyloscopic data”(Art. 4(14) GDPR).

While many uncertainties remain...

As mentioned above, the processing of biometric data is prohibited if processed for “unique identification” safe exceptions (Art. 9(1) GDPR). The legislation, however, did not explain what “unique identification” means and whether, for example, both the use of biometric data for identification purposes (1:n) and for verification purposes (1:1) are forbidden, save for exceptions. Some argue that both are, in principle, forbidden, while others argue that the prohibition only pertains to its use for identification.

Secondly, the legislation also added, upon request of the Council of Member States in the last drafts of the GDPR text, that

biometric data refers to only data “resulting from specific technical processing,” without further explanation. This also leads to uncertainty. Most understand this overall as requiring a biometric comparison technical process for the prohibition to apply.

But what happens if only images with biometric information, such as facial images and fingerprints, are collected and stored? Facial images are explicitly mentioned in the definition of biometric data, but if they are, as such not (yet) the result of a specific biometric comparison, would they fall under the general prohibition of Art. 9(1) GDPR? The legislation seemingly wanted to be more nuanced, for example, facial images as such. Recitals 51 GDPR states that “the processing of photographs” should not systematically be considered as processing of special categories of data because it lacks processing through a specific technical means. Hence, it should not be considered biometric data. This has been criticized because the mere collecting and storing of facial images or fingerprints allow for (unique) identification and also constitute a (serious) risk.⁽¹⁹⁾ The ClearView AI facial images collection, scraped from the internet, and used by police worldwide in combination with other identifying information when comparing faces of people in public streets to identify “wanted persons,” illustrates this risk very well.⁽²⁰⁾

A third point of criticism and of confusion instigated by the legislation is that the

GDPR definition deviates from the concept of biometric data in other specific legislation, such as that for biometric large IT systems⁽²¹⁾, or a general understanding in the technical biometric community. Even the definition in the ISO/IEC 2382-37:2022 Harmonized Biometric Vocabulary from JTC SC37 is different.⁽²²⁾

Another point of criticism is that protection is limited in scope. What about sensitive information, such as that relating to health that can be found in a voice sample, facial or iris images? Does this not always render biometric information as “sensitive,” as mentioned in Art. 9.1 GDPR? Furthermore, the prohibition only applies when biometric data are processed for “unique identifying.” Some argue that this prohibition is not taking into account more recent, and potentially harmful uses of biometric information, such as when it is used for extracting and recognizing emotions or categorization. The GDPR definition may therefore already be outdated, especially in view of regulating AI applications.⁽²³⁾ The AI Act, which we will discuss in Part II of this article, may be able to fill this gap.

Conclusion

One could conclude that the GDPR, while attempting to provide a general regulation of the risks of biometric information, has too limited a scope of protection, raises too many questions, and could lead to controversy in the legal community. Therefore, a revision and update of the

current definition of biometric data and of the prohibitions is needed.

The upcoming Artificial Intelligence Act builds on the definition of biometric data in the GDPR. It further regulates biometric prohibited practices and biometric high-risk systems. This will be discussed in Part II of our contribution in an upcoming issue.

Footnotes

1. The Prüm Treaty, signed in 2005 by seven EU Member States, was later opened up to all member States by EU Council Decision 2008/615/JHA of 2008, and is now being expanded into Prüm II. See also C. Jasserand, "Reprocessing of Biometric Data for Law Enforcement Purposes: Individuals' Safeguards Caught at the Interface between the GDPR and the 'Police' Directive?" 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4298545
2. See *Council Regulation (EC) No. 2252/2004*. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32004R2252>
3. For example, see the *SIS Regulation 1987/2006*, the *VIS Regulation 767/2008*, the *Entry/Exit System (EES) Regulation 2017/2226* and the *Interoperability Regulations 2019/817* and *2019/818*, which all register or use biometric data from third country nationals.
4. *Regulation (EU) 2016/679 of 27 April 2016*. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>
5. Council of Europe, European Convention on Human Rights, 4/11/1950. <https://www.echr.coe.int/european-convention-on-human-rights>
6. Charter of Fundamental Rights of the European Union, 2012/C326/02. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>.
7. See also E.J. Kindt, *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*, Dordrecht, Springer, 2013, p. 228 et seq. <https://link.springer.com/book/10.1007/978-94-007-7522-0>.
8. This is to avoid 'at choice' or arbitrary interferences.
9. See Article 52-Scope and Interpretation of the *EU Charter of Fundamental Rights*. <https://fra.europa.eu/en/eu-charter/article/52-scope-and-interpretation-rights-and-principles#charter>. Such general interest could be the fight against terrorism.
10. For example, see the European Court of Justice affirming the legitimate aim and the necessity and proportionality of the use of biometric data in the ePassport chip, as noted in *Schwarz vs Bochum* in 2013 (<https://curia.europa.eu/juris/document/document.jsf?text=&docid=143189&pageIndex=0&doclang=en&>

- [mode=lst&dir=&occ=first&part=1&cid=142520](#)).
11. Such identification also happens by “singling out” an individual from a group. To assess identifiability, one shall take into account all the means reasonably likely to be used, either by the controller or any third person, to identify directly or indirectly. Because of the widespread monitoring and collection of images, including in databases, one can only in a very exceptional case argue that such identification would not be possible. One such case might be a single image of an individual living in a secluded place in the Amazon rainforest with no internet use, for whom biometric data had not previously been collected or stored.
 12. The rule of law refers to a main principle in democratic countries. It implies the existence of legislative provisions as a distinct set of rules voted and adopted by democratic bodies which executive bodies, such as government entities, but also including law enforcement entities, shall respect. An example might be allowing access to a national territory, or when investigating and prosecuting a crime. Sufficiently precise and accessible legal provisions are needed to avoid the use of discretionary powers, including arbitrary prosecution, and any application shall be supervised by an independent judiciary.
 13. For the European Union, these regulatory data protection bodies include, besides the national data protection authorities, the European Data Protection Board (EDPB) (https://edpb.europa.eu/edpb_en) and the European Data Protection Supervisor (EDPS) (<https://edps.europa.eu/en>).
 14. Biometric data will, in principle, be personal data, that is information relating to an identified or identifiable person. This would also remain in the case of protecting the biometric information, such as upon the use of “protected templates.”
 15. The EU or national legislation, however, will have to justify and confirm that the use of the biometric information is necessary and proportional for meeting the named substantial public interest, while imposing specific safeguards, such as limited access or publication..
 16. Such scientific research is understood as including both non-commercial (academic) as well as commercial research.
 17. The GDPR further specifies that such national law shall be “proportionate,” and “respect the essence of the right to data protection,” and provide measures to safeguard the fundamental rights

(see Art. 9.2 (j) GDPR). A quick review though shows that few national laws address such needed safeguards for research.

18. The Court of Justice stated that the controller bears the burden to prove the appropriateness of such measures, which must be assessed by a national court without necessary recourse to expert evidence: ECJ, NAP case C-340/21, 14.12.2023.

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=280623&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1087509>.

19. E.J. Kindt, "Having Yes, Using No? About the new legal regime for biometric data," *Computer Law and Security Report*. 2018, 523-538.

<https://www.sciencedirect.com/science/article/abs/pii/S0267364917303667?via%3Dihub>.

The images as such should be considered as having the potential for biometric comparisons (identification or verification). This can happen beyond the knowledge of the individual and should therefore fall in the category of "biometric data" as well. It is also the first time that general data protection defines the special

category of personal data from the processing point of view (use-based approach) rather than from the view of the type and nature of the data (objective approach).

20. Several European data protection authorities have, therefore, also clearly prohibited these practices and imposed serious fines.
21. A face or fingerprint image is therein mentioned as biometric data as of the collection, regardless of any further "specific processing." See for example Regulation EU) 2019/817, Art. 4 (9) - (11).
22. For these terms, see also Christoph Busch, "Harmonized Biometric Vocabulary." <https://www.christoph-busch.de/standards.html>
23. See also E. J. Kindt, "A First Attempt at Regulating Biometric Data in the Union," *Regulating Biometrics. Global Approaches and Urgent Questions*, A. Kak (ed.) AINow Institute, New York University, New York, September 1, 2020, pp. 62-69. <https://ainowinstitute.org/wp-content/uploads/2023/09/regulatingbiometrics-kindt.pdf>.

NOTED IN THE LITERATURE

MD-Pose: Human Pose Estimation for Single-Channel UWB Radar

A summary of an article in the October 2023 issue of IEEE Transactions on Biometrics, Behavior, and Identity Science, prepared by its authors X. Zhou, T. Jin, Y. Dai, Y. Song and Z. Qiu

Introduction

Human pose estimation based on optical sensors is difficult to resolve under harsh environments and shielding. In this paper, we propose MD-Pose, a Micro-Doppler (MD)-based human pose estimation method for single-channel ultra-wideband (UWB) radar. The MD characteristic reflects human kinematics and provides a unique identification method that reveals a more comprehensive perception of human posture. We explore the relationship between the human skeleton and the MD signature, which reveals the fundamental origins of these previously unexplained phenomena. Though single-channel ultra wide band (UWB) radar is widely used because of its small size, low cost, and portability, its resolution is lower than that of the multiple-input/multiple-output (MIMO) UWB radar. Therefore, this paper reveals how to implement fine-grained human posture estimates based on the MD signature while using fewer channels. The MD spectrogram of the human target is obtained by the short-time Fourier transform (STFT), which is the input data of the proposed MD-Pose. A quasi-symmetric U-Net neural network is trained with the UWB radar MD spectrogram, which can estimate the human keypoints. The experiments show quantitative results comparable to state-of-the-art human pose estimation methods and provide the underlying insights needed to guide the design of radar-based human pose estimation.

Proposed Method

Based on the development of MD spectrum and deep learning technology, our team designed a framework for human pose estimation that utilizes an MD signature through UWB radar. Figure 1 shows the overall flowchart of our proposed HPE framework. The MD-Pose framework contains two stages. The first is the MD signature dataset collection stage, also known as the dataset production stage. The second is the network architecture, or the deep learning network structure used by the HPE to learn the information in the MD signature map. The structure of the radar MD signature-based human pose estimation network framework proposed in this paper is described in detail.

The network architecture is a quasi-symmetric U-Net neural network, as shown in Figure 3. It is an end-to-end encoder-decoder network, where the backbone network is designed based on Resnet, and the head network is composed of multiple deconvolution modules. The framework takes as input data the MD signature of UWB radar, which contains the time-varying motion of the human torso, arms, legs, hands, and feet. This results in a unique MD signature, which is first extracted from the human target by a convolution module as the input radar data and then aggregated by a max-pooling operation. Four Resnet blocks process the output to extract the deep features. Then, after five deconvolution operations, the user obtains the location confidence probability maps of the human pose. Each location map represents the possible location for every pixel where the confidence probability of the joint location is higher than other pixels. Finally, the confidence probability maps are converted into 2D pose coordinates of human targets through the soft-argmax operation.

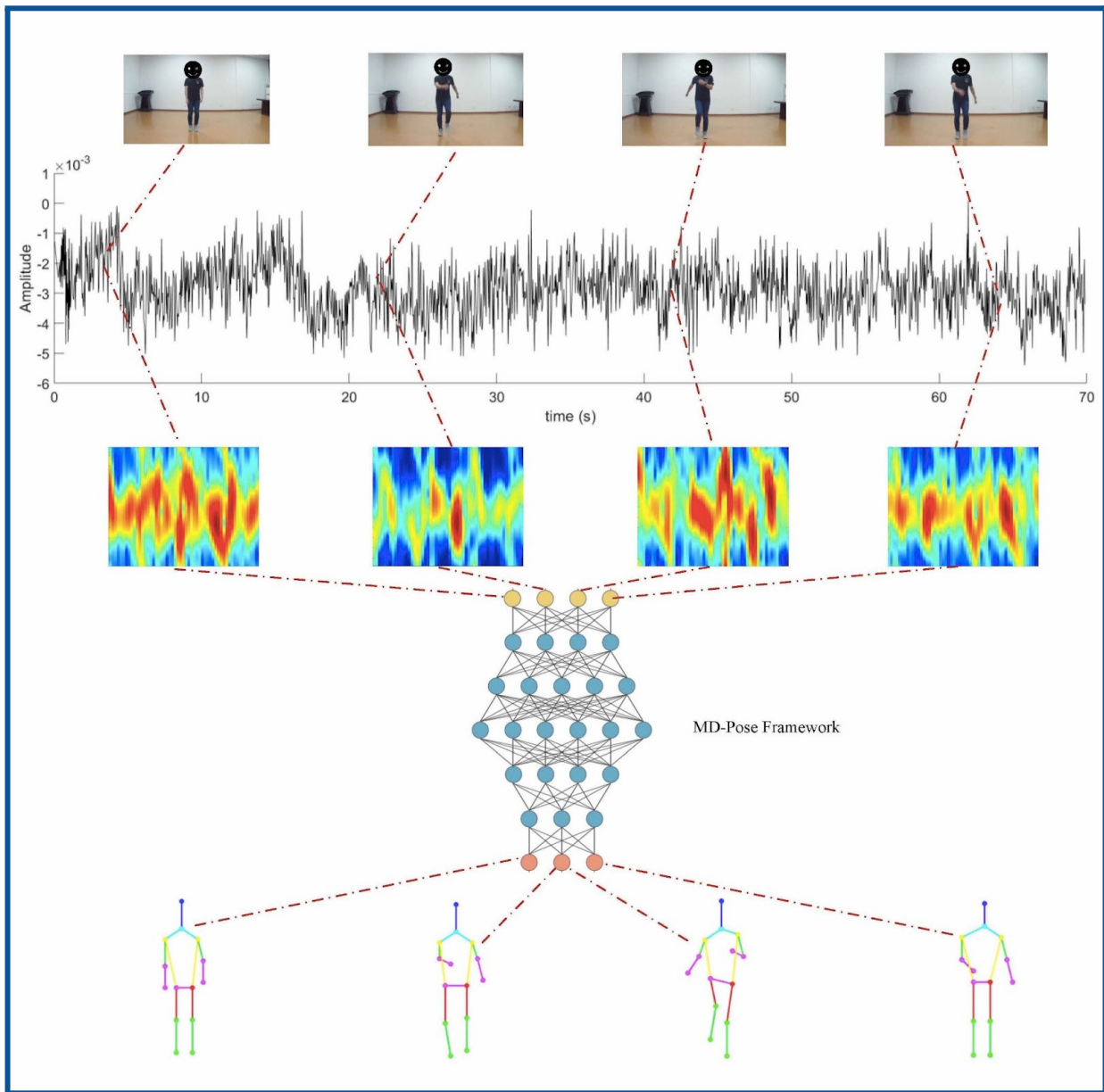
Results

The original radar echo signals of human targets are quite different. The human torso echo signal is firm, which means that the multiple harmonics of other body parts, such as the head, hands, feet, et al., are mixed. It is impossible to estimate information from these components directly from the original echo signal. When the STFT method was used to obtain the Micro-Doppler spectrum of the human target under a specific posture, some information about the human target keypoint could be seen. However, it is still unable to directly present information on skeleton keypoints. The MD-Pose framework for single-channel UWB radar used in our paper gathers information on 14 joint keypoints, namely the head, spine, shoulder (left and right), elbow (left and right), wrist (left and right), hip (left and right), knee (left and right) and foot (left and right) to estimate human pose.

If the ground truth label and the pixels of the estimation pose the value of the 14 human skeleton keypoints, we find that the estimated keypoints are consistent with the ground truth labels. Also, we calculated the pixel errors between the ground truth labels and the estimated values, as shown in column 4 of Table 1. To better evaluate the MD-Pose framework ability to estimate human pose, we used a straightforward method to convert the pixel error between ground truth labels and estimation value into physical space error. The results are reflected in column 5 of Table 1.

We report the results of all test samples and select a set of data in the test dataset. The pixel of the ground truth label and the pixels of the estimation pose value of the 14 human skeleton keypoints. As shown in Table II, we find that the estimated keypoints are consistent with the

Figure 1: Overview of the MD-Pose single-channel ultra-wideband (UWB) radar system.



We report the results of all test samples and select a set of data in the test dataset. The pixel of the ground truth label and the pixels of the estimation pose value of the 14 human skeleton

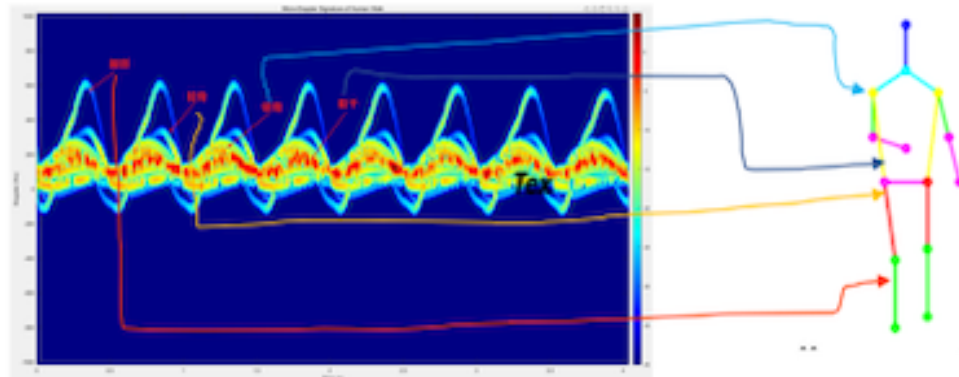


Figure 2. The relationship between MD spectrum and human skeleton. The image on the left is the human micro-doppler spectrum, while the image on the right is the human pose estimation.

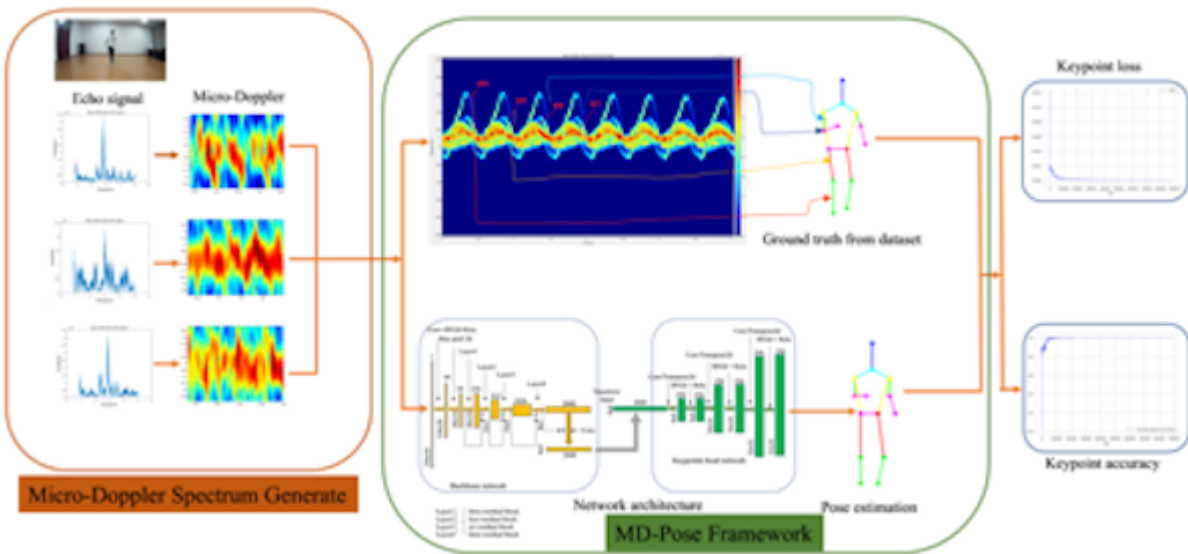


Figure 3: The MD-Pose 2.0 framework

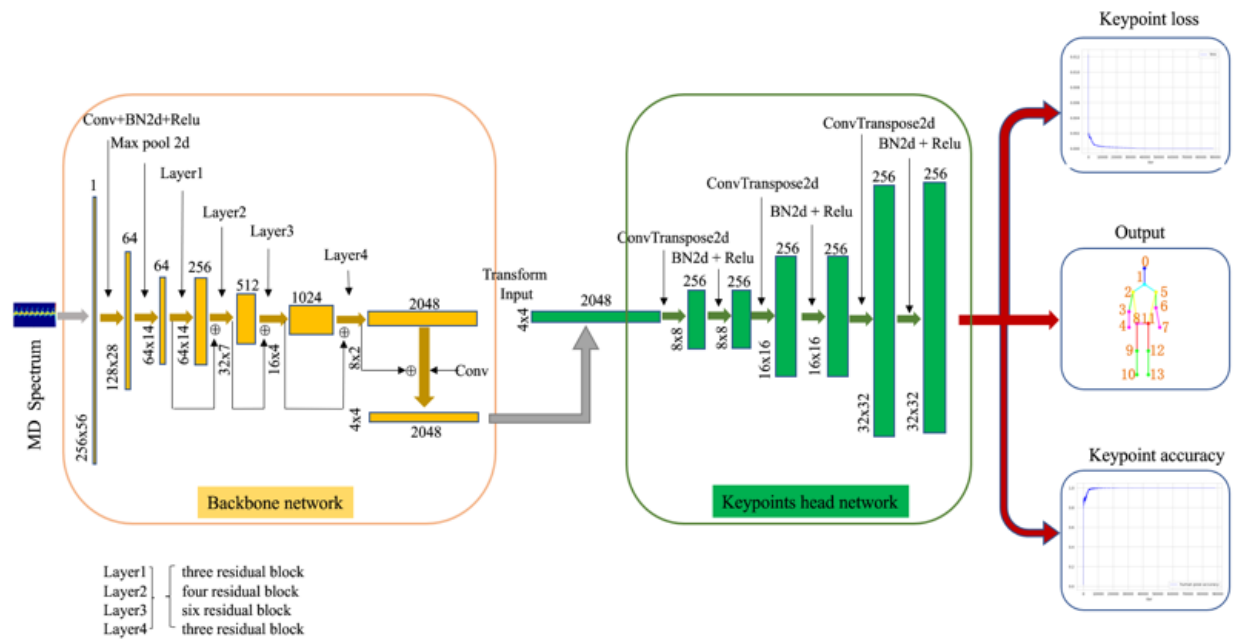


Figure 4. The quasi-symmetric U-Net neural network architecture

Skeleton Point	The Pixel of True Label	The Pixel of Predicted	The Pixel error of Label and Predicted	The Physical space error (mm)
1	(143, 227)	(135, 225)	(8, 2)	19.00
2	(209, 227)	(202, 225)	(7, 2)	16.66
3	(222, 188)	(225, 195)	(3, 7)	10.17
4	(287, 174)	(270, 180)	(17, 6)	40.62
5	(339, 174)	(337.5, 180)	(1.5, 6)	7.18
6	(222, 266)	(225, 270)	(3, 4)	8.22
7	(274, 266)	(270, 270)	(4, 4)	10.32
8	(326, 266)	(315, 285)	(9, 19)	29.04
9	(339, 201)	(315, 195)	(24, 6)	57.01
10	(417, 201)	(427, 195)	(10, 6)	24.42
11	(496, 201)	(495, 195)	(1, 6)	6.68
12	(326, 240)	(315, 225)	(9, 15)	26.37
13	(417, 240)	(427, 240)	(10, 0)	23.61
14	(496, 240)	(517, 240)	(22, 0)	51.94

Table 1. The human pose estimation in a set of test datasets

Keypoints are shown in Table I, we find that the estimated keypoints are consistent with the ground truth labels. Also, we calculated the pixel errors between the ground truth labels and the estimated values, as shown in column 4 of Table 1. To better evaluate the MD-Pose

framework ability to estimate human pose, we used a straightforward method to convert the pixel error between ground truth labels and estimation value into physical space. The results are reflected in column 5 of Table 1.

Conclusion

This paper presents a novel human pose estimation framework called MD-Pose, which is based on the MD signature through single-channel UWB radar. It contains a quasi-symmetric U-Net neural network that can extract velocity information of various human body parts from the MD signature for up to 14 skeletal keypoints and reconstruct fine-grained human pose with subject-independence and environment-independence. The MD signature of human activity based on the radar is consistent with the information contained in the pose estimation task. Therefore, we explore the inherent relationship between the human skeleton and the MD signature, which reveals the mechanism of mapping various parts of the human body to the keypoints of the human skeleton.

Experimental results show that the test dataset's MPJPE value of human pose estimation is between 4.32mm and 39.38mm, demonstrating that the MD-Pose framework is effective and generalizable for human pose estimation task using single-channel UWB radar. This work opens exciting research opportunities for radar-based human pose estimation methods that use the MD signature as they are less susceptible to environmental influences than imaging-based methods.

References

- 1) Zhao, M., Li, T., Abu Alsheikh, M., Tian, Y., Zhao, H., Torralba, A. and Katabi, D., 2018. "Through-wall Human Pose Estimation using Radio Signals." In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (pp. 7356-7365).
- 2) Zhao, M., Tian, Y., Zhao, H., Alsheikh, M.A., Li, T., Hristov, R., Kabelac, Z., Katabi, D. and Torralba, A., 2018, August. "RF-based 3D Skeletons." In *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication* (pp. 267-281).
- 3) Zheng, Z., Pan, J., Ni, Z., Shi, C., Ye, S. and Fang, G., 2021. "Human Posture Reconstruction for Through-the-Wall Radar Imaging Using Convolutional Neural Networks." *IEEE Geoscience and Remote Sensing Letters*, 19, pp.1-5.
- 4) Sengupta, A. and Cao, S., 2022. "mmPose-NLP: A Natural Language Processing Approach to Precise Skeletal Pose Estimation Using mmWave Radars." *IEEE Transactions on Neural Networks and Learning Systems*.

X. Zhou, T. Jin, Y. Dai, Y. Song and Z. Qiu, "MD-Pose: Human Pose Estimation for Single-Channel UWB Radar," in *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 5, no. 4, pp. 449-463, Oct. 2023, doi: 10.1109/TBIOM.2023.3265206.

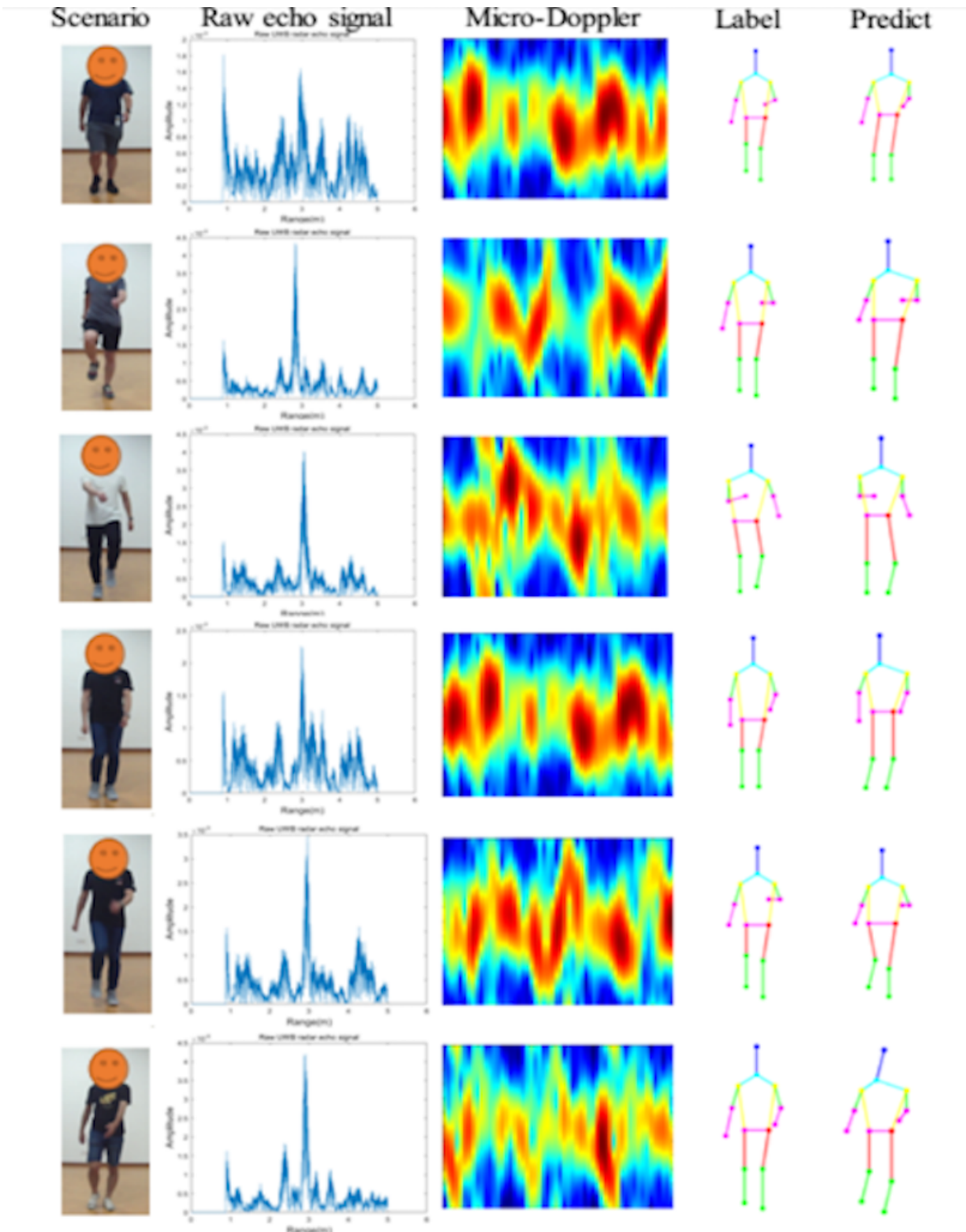


Figure 5. Visual results of the 2D human pose estimation task based on MD-Pose framework

DATABASE DIGEST

Multi-Movement Finger-Video (MMFV): Database for Contactless Fingerprint Recognition

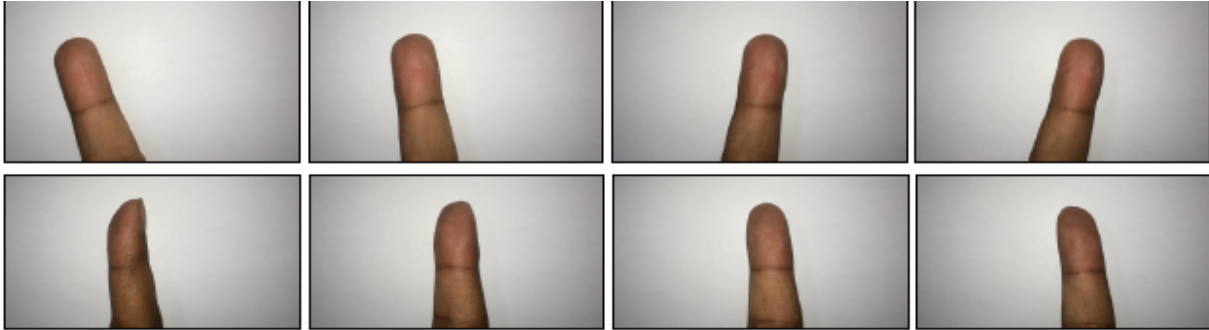
By Emanuela Marasco, Assistant Professor, Information Sciences and Technology (IST) Department and Center for Secure Information Systems, George Mason University, Fairfax, VA, USA

MMFV has been introduced by the IIID group in Delhi to support research on contactless fingerprint recognition. MMFV contains more than 3,700 videos from 336 classes, recorded over two sessions and covering three varieties of movement. For each video, 200 frames have been sampled. This database is designed to facilitate the development of video-based contactless fingerprint recognition approaches for unlocking smartphones, identification, frame selection tasks, and applications related to motion/pose.

The MMFV database consists of 3,792 videos of 336 movement classes with three movement types for each finger: pitch, yaw, and roll. The total frame count is 750,391, or about 200 or so per single video. The videos were taken with an 8MP Apple iPhone 5 camera using Flash LED and auto-focus, thus preserving the high standard of image quality necessary for precise analysis. The initial distance from the finger to the camera was only 9 cm, but this varied slightly according to motions between fingers, more so, especially with yaw movements. This extensive dataset is vital in investigating numerous aspects of finger photo recognition because it precisely captures hand movements and offers high-quality imaging.

The baseline experimental results include the fine-tuning of a Siamese network base for contactless fingerprint verification, which achieved an EER of 2.70% for various movements, and six other deep learning algorithms inspired by researchers like Chopra et al., Lin and Kumar, and Malhotra et al. Each method varied in recognition performance, with the Siamese network notably effective in handling diverse finger movements.

MMFV can be used for liveness detection, continuous authentication, and frame selection, addressing challenges such as motion blur and geometric variations due to different finger movements.



Top Figure: Movement 1-Pitch; **Bottom Figure:** Movement 2- Roll

Agreement: https://iab-rubric.org/images/pdf/LICENSE_AGREEMENT_MMFV_Database.pdf

Download: [MMFV Database License Agreement](#)

SOURCE MATERIAL: A.Malhotra, M. Vatsa, and R. Singh. "MMFV: A Multi-Movement Finger-Video Database for Contactless Fingerprint Recognition." *IEEE International Workshop on Biometrics and Forensics (IWBF) 2023*.

SOURCE CODE

Malafide: A Novel Adversarial Convolutional Noise Attack Against Deepfake and Spoofing Detection Systems

By Chiara Galdi, Assistant Professor, and Michele Panariello, Ph.D. candidate, EURECOM, Biot, France

Voice biometrics is increasingly being used as a means of authentication. While this technology has many benefits, it also raises the concern of *voice spoofing* (or *presentation attacks*). In this attack, a voice cloning algorithm is maliciously used to impersonate an individual in a biometric system and is thus able to falsely authenticate as that person. This threat has led to the development of *spoofing countermeasures* [1], or speech systems that can detect spoofed speech.

The development of spoofing countermeasures are partly made possible by studying their vulnerabilities. That is, knowing how an attacker can evade a countermeasure enables the design of more robust defensive mechanisms.

One such technique is Malafide [2], which is designed to evade speech spoofing countermeasures that rely on certain acoustic artefacts [3] for the detection of

artificially-generated speech. It consists of a linear time-invariant (LTI) filter that is optimised to conceal such artefacts, and therefore bypass the spoofing countermeasure.

Malafide, which is based on the principle of adversarial attacks against neural architectures, differs from other works that have experimented with conducting adversarial attacks to spoofing countermeasures. Most of these other systems operate on single utterances [4] or specific speakers [5]. Instead, Malafide aims to conceal the artefacts within any utterance produced by a chosen speech synthesis system, regardless of either the spoken content and/or the speaker.

The weights of the Malafide LTI filter are optimised using spoofed speech data. Before being fed into the countermeasure system, the spoofed waveform is convolved in the time domain with the filter. A loss function over the prediction of the countermeasure system is computed, and its gradients are propagated back to the filter. The weights of the filter are adjusted with gradient descent to maximise the loss of the spoofing countermeasure. In doing so, it attempts to cause a misclassification of the fake utterance as an authentic one. This process is iterated for a large number of spoofed utterances, until a “universal filter” that can mask the acoustic artefacts is produced by the malicious speech synthesis algorithm. At inference time, the optimised Malafide LTI filter can be used on new utterances generated by that algorithm.

Michele Panariello and Wanying Ge, both PhD students in EURECOM’s Audio, Security and Privacy group [6], have made the Malafide source code available on GitHub. While the provided implementation is based on PyTorch, the attack is conceptually straightforward and can be easily ported to other deep learning frameworks.

REFERENCES

1. Liu, X., et al. “Asvspoof 2021: Towards Spoofed and Deepfake Speech Detection in the Wild.” *ACM Transactions on Audio, Speech, and Language Processing*. (2023).
2. Panariello, Michele, et al. "Malafide: A Novel Adversarial Convolutional Noise Attack Against Deepfake and Spoofing Detection Systems." *24th Conference of the International Speech Communication Association (INTERSPEECH 2023)*. https://www.isca-speech.org/archive/pdfs/interspeech_2023/panariello23b_interspeech.pdf (2023).
3. Ge, Wanying, et al. "Explaining Deep Learning Models for Spoofing and Deepfake Detection with SHapley Additive exPlanations." *2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (2022).
4. Kassis, Andre, and Urs Hengartner. "Practical Attacks on Voice Spoofing Countermeasures." arXiv preprint:2107 <https://arxiv.org/pdf/2107.14642.pdf> (2021).

5. Zhang, Xingyu, et al. "Waveform Level Adversarial Example Generation for Joint Attacks Against Both Automatic Speaker Verification and Spoofing Countermeasures." *Engineering Applications of Artificial Intelligence* 116 (2022): 105469.
6. Open source code: <https://github.com/eurecom-asp/malafide>.

COMMERCIAL OFF-THE-SHELF SYSTEMS

Streamlined Gait Analysis Workflow with the Qualisys Gait Analysis Module

By Chiara Galdi, Assistant Professor, EURECOM, Biot, France

Behavioural biometrics is emerging as a powerful alternative to traditional biometric systems. Unlike traditional methods that require specific actions from users, like scanning a fingerprint or iris, behavioural biometrics offers a seamless experience that does not require high levels of cooperation or conscious effort from the user. By analysing patterns, such as typing rhythm, mouse movements, or even walking patterns, behavioural biometrics provides a non-intrusive yet secure way of verifying identity. As such, it is increasingly popular in applications where user convenience and continuous authentication are crucial.

In this issue we explore Qualisys' Gait Analysis module, which represents a significant advancement in motion capture technology, with broad applications in both research and practical settings. This module is part of their advanced motion capture system, which provides a streamlined workflow for gait analysis. The Qualisys Clinical System, a subset of this technology, has been approved for medical use, meeting regulatory requirements for patient diagnosis, treatment assessment, and monitoring.

The technical specifications of the Qualisys Gait Analysis module emphasizes its high precision and flexibility. The module is designed for both full-body and lower-body analysis, supports various marker sets and event modes, and is compatible with a range of hardware devices. The system also integrates seamlessly with additional technologies, such as force plates, EMG, and eye-trackers, which can enable comprehensive data capture. This versatility makes it suitable for diverse research and clinical applications. Its adaptability to different protocols enhances its utility in detailed motion analysis, particularly in understanding gait dynamics in various contexts.

Qualisys, a Swedish company, has established itself as a leading provider of precision motion capture and 3D positioning tracking systems. With more than 30 years of experience, the company has supplied diverse industries with high-quality camera systems and expert knowledge. Their operations span various environments, including indoor, outdoor, ground-to-air, and underwater settings. Their commitment to quality and customer service is evident in their ISO 9001:2015 certification and compliance with the Medical Device Directive 93/42/EEC.

For more detailed information on the module, please visit their website at <https://www.qualisys.com/>.

EU PROJECT UPDATES

REVIEWING ONGOING EU-FUNDED BIOMETRIC RECOGNITION PROJECTS

By Emanuele Maiorana, Assistant Professor - BioMedia4n6 Lab, Roma Tre University, Rome, Italy

The European Commission is currently financing several projects associated with biometric recognition. The goals of these projects range from developing novel devices and IoT infrastructures, to guaranteeing greater security in critical scenarios like border control, to preventing potential threats to the privacy of citizens. Please note that this is a potentially non-exhaustive list of these projects.

Convenient, Advanced, Secure and Touchless fingerprint scanning for identification purposes (CAST)

HORIZON.3.1 – GA 190188065

1 March, 2023 - 28 February, 2025

Overall budget € 5 717 750,00

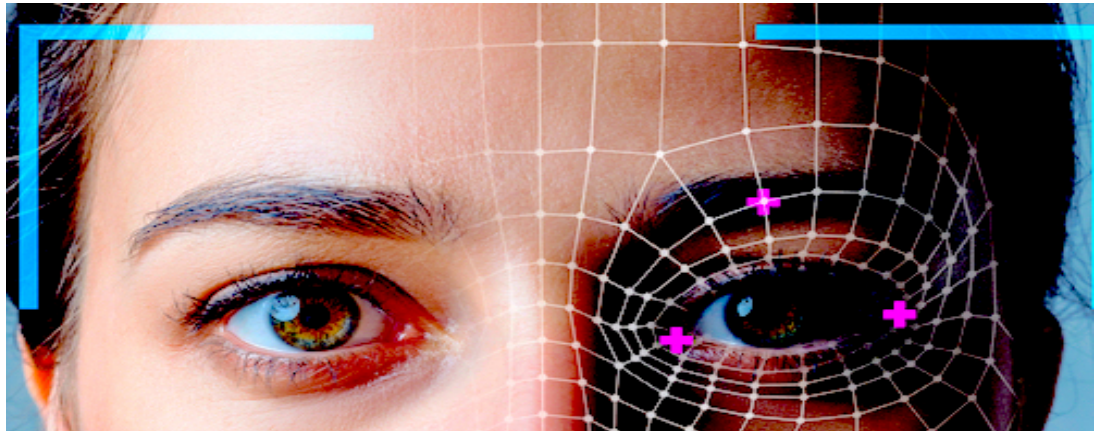
1 Partner

<https://cordis.europa.eu/project/id/190188065>

The solution sought in this project is the first contactless multi-fingerprint scanner for identification purposes which can scan the ridge and valley structure of the human finger in full 3D. This enables the differentiation between the fingerprint's ridges and valleys and ensures the interoperability with contact-based scanners, where only the ridges are

scanned in 2D. This interoperability enables access to the governmental biometrics market where compatibility with existing databases is a must have.

Furthermore, the 3D Scanner is hard to fake as the 3D structure of a finger with its fine details is really difficult to reproduce. This gives a huge security boost to the system compared to contact-based systems, where you leave your fingerprints on the device as latent imprints. The AI-supported data evaluation and the specialized design lead to a unmatched user experience in terms of convenience and security.



Flexible and Improved Border-Crossing Experience for Passengers and Authorities (FLEXI-cross)

HORIZON.2.3 – GA 101073879

1 September, 2022 - 31 August, 2025

Overall budget € 5 019 000,00

12 Partners

<https://cordis.europa.eu/project/id/101073879>

The EU has made significant efforts to improve the management of borders, and enhance the security and reliability of border checks for people and goods. In this context, the EU-funded FLEXI-cross project will develop and deploy innovative solutions in real-life environments covering road, rail and port borders. Specifically, it will develop a toolkit offering new capabilities, such as flexible and cost-effective deployment of border checkpoints, secure biometric checks, real-time person verification, secure and private data exchange, and improved safety and experience for border personnel. The project brings together key European border authorities, end users, leading software developers, research organisations and innovative SMEs to codesign the requirements and validate the

outcomes. Furthermore, it will organise three border-checking real-life trial facilities to enable trials in diverse operational environments, namely vehicle-based road border crossings, rail-based border-crossings, and port embarkation/disembarkation.

Algorithmic Societies: Ethical Life in the Machine Learning Age (ALGOSOC)

ERC-2019-ADG – GA 883107

1 October, 2020 - 30 September, 2025

Overall budget € 2 150 686,00

1 Participant

<https://cordis.europa.eu/project/id/883107>

Rapid advancements in machine learning technologies are transforming social and political life in ways that uniquely challenge how we live in relation to others. The life chances of a person are now intimately connected to the attributes that an algorithm has learned from the data patterns of unknown others. The EU-funded ALGOSOC project is developing a new approach to understanding and responding to the consequences of machine learning algorithms for contemporary societies. The project will examine how 21st century machine learning algorithms learn to recognise, attribute and infer the characteristics of people, groups and objects. In order to do this, the project will conduct a series of path-defining studies of societal domains of machine learning, including behavioural biometrics and biomedical object recognition; consumer recommendation and criminal justice scoring; oncology treatment pathways and anomaly detection for security. Though these domains share algorithms in common, they have not previously been researched in combination.

reliable biomeTric tEchNologies to asSist Police authorities in cOmbating terrorism and oRganized crime (TENSOR)

HORIZON-CL3-2021-FCT-01 – GA 101073920

1 January, 2023 - 31 December, 2025

Overall budget € 5 739 725,00

19 Partners

<https://cordis.europa.eu/project/id/101073920>

Fingerprint identification is one of the oldest and most well-known forms of biometrics used by the police. But, other forms of biometrics, including face, voice, gait and behaviour-based recognition, are also being applied. The EU-funded TENSOR project will provide police authorities and forensic institutes a platform to make it easier to extract, share and store biometric evidence in cross-border environments. To assist in the faster adoption of modern biometric solutions, the project will design the first European Biometric Data Space that provides a common ground among police authorities, forensic

institutes, and security researchers. Novel tools will be developed to perform all of the above processes in a secure, automated and scalable manner that also ensures privacy.

Secure and Frictionless Identity for EU and Third Country National Citizens (SafeTravellers)

HORIZON.2.3 – GA 101121269

1 January, 2024 - 31 December, 2026

Overall budget € 7 477 390,02

23 Partners

<https://cordis.europa.eu/project/id/101121269>

Identity theft is rapidly expanding, causing substantial financial loss to millions of people around the world. This invisible crime is also widespread across EU countries, where a growing number of citizens are targeted by sophisticated online and offline fraudulent attacks each year. SafeTravellers value proposition aims to: a) strengthen security at the borders, and b) improve the productivity of the Border Authorities and LEAs by providing them with the appropriate tools to combat identity fraud at the hardware, identity and travel document, and biometrics level, while c) offering a frictionless border crossing experience for EU/TCN citizens by eliminating stop at border checkpoints. SafeTravellers is both proposing a new method of citizen identification based on multiple biometrics instead of problematic identity documents, and enhancing the current ways of identity verification at the borders. The latter is done through a set of tools that will detect attacks on biometric hardware, and identity and travel document fraud, as well as attempts to falsify biometrics.

Interoperable applications suite to enhance European identity and document Security and fraud detection (EINSTEIN)

HORIZON.2.3 – GA 101121280

1 January, 2024 - 31 December, 2026

Overall budget € 6 297 950,00

19 Partners

<https://cordis.europa.eu/project/id/101121280>

Combating fraud on identity and travel documents is a key mission of law enforcement agencies and border guards, and industries have been working on new means to address these issues. Public authorities are using numerous technologies to accomplish their mission, but permanent innovation is required to fight highly skilled defrauders. The objective of EINSTEIN is to significantly enhance existing public authorities' means through innovation, building on technologies proven in the labs, but not yet sufficiently mature for

operational usage. EINSTEIN will deliver six applications essential to fight identity frauds: 1) online ID issuance using a secure cloud-based server for real-time biometric quality checks and fraud detection, 2) mobile document and identity checks using commercially-available smartphones, 3) a document authentication module to detect fraudulent documents, 4) pre-registration for land-border crossings including biometrics and DTC, 5) an EES kiosk with advanced fraud detection using video surveillance, and 6) fast track processing for enrolled travelers using on-the-move face and iris. To ensure TRL7 at a minimum, practitioners will run six different pilot use cases in their own environment.

Doing Digital Identities (DigID)

ERC-2021-STG – GA 101039758

1 February, 2023 - 31 January, 2028

Overall budget € 1 495 050,00

1 Participant

<https://cordis.europa.eu/project/id/101039758>

Digital ID devices, such as electronic ID cards, provide access to government services via PINs, biometric databases, and blockchain-secured digital identity wallets. Public debate around these devices often centres on the ramifications of their criminal misuse, instead of their intended use by the majority of citizens. The European Research Council DigID project aims to evaluate how technologies and infrastructure used for citizenship purposes are being transformed in the digital age. It will explore how citizen and government relations are being reshaped through digital ID devices with respect to birth registration, citizen-government transactions, and border controls.

The project investigates transformations of citizen-state relations through digital ID devices at three sites: birth registration, citizen-government transactions, and border controls. Theoretically, the project draws on science and technology and data studies to propose a conception of material citizenship as performative and sociotechnical, and to advance a research agenda that focuses on the practical, epistemic, political, and ethical implications of digital identification. Methodologically, the project combines multi-sited ethnographies, textual analysis, and mapping to study the design, implementation, and use of digital ID devices in one international and four national case studies. In this way, DigID sheds light on the much-neglected material dimension of citizenship and shows how digital ID devices reshape the lived experience of citizenship as a legal status, a form of membership in a political community, and a set of bottom-up practices enacting the “right to have rights.”

BIOMETRIC COMPENDIUM ALERT

January 2024

By Dr. Carmen Bisogni, Research Fellow, Biometric and Image Processing Laboratory, University of Salerno, Salerno, Italy, and David Freire-Obregón, Associate Professor, University of Las Palmas de Gran Canaria, Gran Canaria Island, Spain

Below is a list of the latest papers that have been accepted (via early access) or published in various IEEE Journals that address topics within biometrics.

BIOMETRICS ENCRYPTION AND TEMPLATE SECURITY

1. L. Zhang, A. Li, S. Chen, W. Ren and K-K. R. Choo, "A Secure, Flexible, and PPG-Based Biometric Scheme for Healthy IoT Using Homomorphic Random Forest," in *IEEE Internet of Things Journal*, vol. 11, no. 1, pp. 612-622, 1 Jan.1, 2024. DOI: [10.1109/JIOT.2023.3285796](https://doi.org/10.1109/JIOT.2023.3285796)

FACE RECOGNITION

1. A. George, C. Ecabert, H.O. Shahreza, K. Kotwal and S. Marcel, "EdgeFace: Efficient Face Recognition Model for Edge Devices," in *IEEE Transactions on Biometrics, Behavior, and Identity Science*. DOI: [10.1109/TBIOM.2024.3352164](https://doi.org/10.1109/TBIOM.2024.3352164)
2. Z. Li et al., "Identity-Aware Variational Autoencoder for Face Swapping," in *IEEE Transactions on Circuits and Systems for Video Technology*. DOI: [10.1109/TCSVT.2024.3349909](https://doi.org/10.1109/TCSVT.2024.3349909)
3. Z. Blasingame and C. Liu, "Leveraging Diffusion For Strong and High Quality Face Morphing Attacks," in *IEEE Transactions on Biometrics, Behavior, and Identity Science*. DOI: [10.1109/TBIOM.2024.3349857](https://doi.org/10.1109/TBIOM.2024.3349857)
4. Y. Pang, J. Mao, L. He, H. Lin and Z. Qiang, "An Improved Face Image Restoration Method Based on Denoising Diffusion Probabilistic Models," in *IEEE Access*, vol. 12, pp. 3581-3596, 2024. DOI: [10.1109/ACCESS.2024.3349423](https://doi.org/10.1109/ACCESS.2024.3349423)
5. N.A. Talemi, H. Kashiani and N.M. Nasrabadi, "CATFace: Cross-Attribute-Guided Transformer with Self-Attention Distillation for Low-Quality Face Recognition," in *IEEE Transactions on Biometrics, Behavior, and Identity Science*. DOI: [10.1109/TBIOM.2023.3349218](https://doi.org/10.1109/TBIOM.2023.3349218)
6. Y. Yang, W. Hu and H. Hu, "Unsupervised NIR-VIS Face Recognition via Homogeneous-to-Heterogeneous Learning and Residual-Invariant Enhancement," in

-
- IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 2112-2126, 2024. DOI: [10.1109/TIFS.2023.3346176](https://doi.org/10.1109/TIFS.2023.3346176)
7. M. Zhang, R. Liu, D. Deguchi and H. Murase, "Texture-Guided Transfer Learning for Low-Quality Face Recognition," in *IEEE Transactions on Image Processing*, vol. 33, pp. 95-107, 2024. DOI: [10.1109/TIP.2023.3335830](https://doi.org/10.1109/TIP.2023.3335830)
 8. H. Fang et al., "Surveillance Face Anti-Spoofing," in *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 1535-1546, 2024. DOI: [10.1109/TIFS.2023.3337970](https://doi.org/10.1109/TIFS.2023.3337970)
 9. J. Xin, Z. Wei, N. Wang, J. Li and X. Gao, "Large Pose Face Recognition via Facial Representation Learning," in *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 934-946, 2024. DOI: [10.1109/TIFS.2023.3329686](https://doi.org/10.1109/TIFS.2023.3329686)
 10. D. Liu, X. Gao, C. Peng, N. Wang and J. Li, "Universal Heterogeneous Face Analysis via Multi-Domain Feature Disentanglement," in *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 735-747, 2024. DOI: [10.1109/TIFS.2023.3327666](https://doi.org/10.1109/TIFS.2023.3327666)
 11. X. Long, J. Zhang, S. Wu, X. Jin and S. Shan, "Dual Sampling Based Causal Intervention for Face Anti-Spoofing With Identity Debiasing," in *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 851-862, 2024. DOI: [10.1109/TIFS.2023.3326370](https://doi.org/10.1109/TIFS.2023.3326370)
 12. W. Zhao, X. Zhu, K. Guo, H. Shi, X-Y. Zhang and Z. Lei, "Masked Face Transformer," in *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 265-279, 2024. DOI: [10.1109/TIFS.2023.3322600](https://doi.org/10.1109/TIFS.2023.3322600)
 13. H. Zhou et al., "Crafting Transferable Adversarial Examples Against Face Recognition via Gradient Eroding," in *IEEE Transactions on Artificial Intelligence*, vol. 5, no. 1, pp. 412-419, Jan. 2024. DOI: [10.1109/TAI.2023.3253083](https://doi.org/10.1109/TAI.2023.3253083)
 14. R. Shao, P. Perera, P.C. Yuen and V.M. Patel, "Federated Generalized Face Presentation Attack Detection," in *IEEE Transactions on Neural Networks and Learning Systems*, vol. 35, no. 1, pp. 103-116, Jan. 2024. DOI: [10.1109/TNNLS.2022.3172316](https://doi.org/10.1109/TNNLS.2022.3172316)
 15. T-H. Shahreza, S-H. Choi and Y-H. Choi, "Instance-Agnostic and Practical Clean Label Backdoor Attack Method for Deep Learning Based Face Recognition Models," in *IEEE Access*, vol. 11, pp. 144040-144050, 2023. DOI: [10.1109/ACCESS.2023.3342922](https://doi.org/10.1109/ACCESS.2023.3342922)
 16. C. Oinar, B.M. Le and S.S. Woo, "KappaFace: Adaptive Additive Angular Margin Loss for Deep Face Recognition," in *IEEE Access*, vol. 11, pp. 137138-137150, 2023. DOI: [10.1109/ACCESS.2023.3338648](https://doi.org/10.1109/ACCESS.2023.3338648)
 17. H. Gu, J. Chen, F. Xiao, Y-J. Zhang and Z-M. Lu, "Self-Attention and MLP Auxiliary Convolution for Face Anti-Spoofing," in *IEEE Access*, vol. 11, pp. 131152-131167, 2023. DOI: [10.1109/ACCESS.2023.3335040](https://doi.org/10.1109/ACCESS.2023.3335040)

18. Y. Zhou, Y. Liang and P. Tan, "Design of an Intelligent Laboratory Facial Recognition System Based on Expression Keypoint Extraction," in *IEEE Access*, vol. 11, pp. 129805129817, 2023. DOI: [10.1109/ACCESS.2023.3329575](https://doi.org/10.1109/ACCESS.2023.3329575)
19. D. Wang and R. Li, "Enhancing Accuracy of Face Recognition in Occluded Scenarios With Occlusion-Aware Module-Based Network," in *IEEE Access*, vol. 11, pp. 117297-117307, 2023. DOI: [10.1109/ACCESS.2023.3326235](https://doi.org/10.1109/ACCESS.2023.3326235)
20. S. Shahed, Y. Lin, J. Hong, J. Zhou and F. Gao, "Explicitly Semantic Guidance for Face Sketch Attribute Recognition With Imbalanced Data," in *IEEE Signal Processing Letters*, vol. 30, pp. 1502-1506, 2023. DOI: [10.1109/LSP.2023.3324579](https://doi.org/10.1109/LSP.2023.3324579)
21. X. Luan, Z. Ding, L. Liu, W. Li and X. Gao, "A Symmetrical Siamese Network Framework With Contrastive Learning for Pose-Robust Face Recognition," in *IEEE Transactions on Image Processing*, vol. 32, pp. 5652-5663, 2023. DOI: [10.1109/TIP.2023.3322593](https://doi.org/10.1109/TIP.2023.3322593)
22. Y. Zhu, X. Shen and P. Du, "Denoising-Based Decoupling-Contrastive Learning for Ubiquitous Synthetic Face Images," in *IEEE Access*, vol. 11, pp. 104946-104954, 2023. DOI: [10.1109/ACCESS.2023.3318595](https://doi.org/10.1109/ACCESS.2023.3318595)
23. O. Agbolade, A. Nazri, R. Yaakob and Y. K. Cheah, "Homologous Anatomical-Based Facial-Metrics Application to Down Syndrome Face Recognition," in *IEEE Access*, vol. 11, pp. 104879-104889, 2023. DOI: [10.1109/ACCESS.2023.3317889](https://doi.org/10.1109/ACCESS.2023.3317889)
24. Z. Wang, J. Zhang, T. Chen, W. Wang and P. Luo, "RestoreFormer++: Towards RealWorld Blind Face Restoration From Undegraded Key-Value Pairs," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 45, no. 12, pp. 15462-15476, Dec. 2023. DOI: [10.1109/TPAMI.2023.3315753](https://doi.org/10.1109/TPAMI.2023.3315753)
25. H.O. Shahreza, A. Veuthey and S. Marcel, "Toward High-Resolution Face Image Generation From Coded Aperture Camera," in *IEEE Sensors Letters*, vol. 7, no. 11, pp. 1-4, Nov. 2023, Art no. 7006004. DOI: [10.1109/LSSENS.2023.3315248](https://doi.org/10.1109/LSSENS.2023.3315248)

FINGER KNUCKLE BIOMETRICS

1. S. Li, B. Zhang, L. Wu, R. Ma and X. Ning, "Robust and Sparse Least Square Regression for Finger Vein and Finger Knuckle Print Recognition," in *IEEE Transactions on Information Forensics and Security*. DOI: [10.1109/TIFS.2024.3352389](https://doi.org/10.1109/TIFS.2024.3352389)
2. Z. Zhou and A. Kumar, "Finger-Knuckle Assisted Slap Fingerprint Identification System for Higher Security and Convenience," in *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 441-454, 2024. DOI: [10.1109/TIFS.2023.3318938](https://doi.org/10.1109/TIFS.2023.3318938)

IRIS AND PERIOULAR RECOGNITION

1. D.P. Benalcazar, J.E. Tapia, M. Vasquez, L. Causa, E.L. Droguett and C. Busch, "Toward an Efficient Iris Recognition System on Embedded Devices," in *IEEE Access*, vol. 11, pp. 133577-133590, 2023. DOI: [10.1109/ACCESS.2023.3337033](https://doi.org/10.1109/ACCESS.2023.3337033)

SOFT BIOMETRICS

1. J.N. Chaudhari, H. Galiyawala, M. Kuribayashi, P. Sharma and M.S. Raval, "Designing Practical End-to-End System for Soft Biometric-Based Person Retrieval from Surveillance Videos," in *IEEE Access*, vol. 11. DOI: [10.1109/ACCESS.2023.3337108](https://doi.org/10.1109/ACCESS.2023.3337108)
2. P. Rot, K. Grm, P. Peer and V. Štruc, "PrivacyProber: Assessment and Detection of Soft-Biometric Privacy-Enhancing Techniques," in *IEEE Transactions on Dependable and Secure Computing*. DOI: [10.1109/TDSC.2023.3319500](https://doi.org/10.1109/TDSC.2023.3319500)
3. L. Cascone, V. Loia, M. Nappi and F. Narducci, "Soft Biometrics for Cybersecurity: Ongoing Revolution for Industry 4.0," in *Computer*, vol. 57, no. 1, pp. 40-50, Jan. 2024. DOI: [10.1109/MC.2023.3292715](https://doi.org/10.1109/MC.2023.3292715)

SIGNATURE/WRITER RECOGNITION

1. Z. Wang, M. Muhammad, N. Yadikar, A. Aysa and K. Ubul, "Advances in Offline Handwritten Signature Recognition Research: A Review," in *IEEE Access*, vol. 11. DOI: [10.1109/ACCESS.2023.3326471](https://doi.org/10.1109/ACCESS.2023.3326471)

SPEECH/SPEAKER IDENTIFICATION

1. F.A. Dal Rí, F.C. Ciardi and N. Conci, "Speech Emotion Recognition and Deep Learning: An Extensive Validation Using Convolutional Neural Networks," in *IEEE Access*, vol. 11. DOI: [10.1109/ACCESS.2023.3326071](https://doi.org/10.1109/ACCESS.2023.3326071)
2. F. Dong, Y. Qian, T. Wang, P. Liu and J. Cao, "A Transformer-Based End-to-End Automatic Speech Recognition Algorithm," in *IEEE Signal Processing Letters*, vol. 30. DOI: [10.1109/LSP.2023.3328238](https://doi.org/10.1109/LSP.2023.3328238)
3. Q. Zhang and K. Tong, "Vocal Cord Vibration Signal Recognition Model Based on Feature Engineering Preprocessing," in *IEEE Sensors Journal*, vol. 23, no. 24. DOI: [10.1109/JSEN.2023.3321987](https://doi.org/10.1109/JSEN.2023.3321987)
4. Y. Cao et al., "Live Speech Recognition via Earphone Motion Sensors," in *IEEE Transactions on Mobile Computing*. DOI: [10.1109/TMC.2023.3333214](https://doi.org/10.1109/TMC.2023.3333214)
5. N. Wankhede and S. Wagh, "Enhancing Biometric Speaker Recognition Through MFCC Feature Extraction and Polar Codes for Remote Application," in *IEEE Access*, vol. 11. DOI: [10.1109/ACCESS.2023.3333039](https://doi.org/10.1109/ACCESS.2023.3333039)
6. T. Kang, S. Lee, S. Song, M.R. Haghghat and M.P. Flynn, "A Multimode 157 μ W 4-Channel 80 dBA-SNDR Speech Recognition Frontend With Direction-of-Arrival Correction Adaptive Beamformer," in *IEEE Journal of Solid-State Circuits*. DOI: [10.1109/JSSC.2023.3327967](https://doi.org/10.1109/JSSC.2023.3327967)

PALMPRINT BIOMETRICS

1. D. Fan, X. Liang, C. Zhang, W. Jia and D. Zhang, "AMGNet: Aligned Multilevel Gabor Convolution Network for Palmprint Recognition," in *IEEE Transactions on Circuits and Systems for Video Technology*. DOI: [10.1109/TCSVT.2023.3327012](https://doi.org/10.1109/TCSVT.2023.3327012)

DATASETS AND OVERVIEW SURVEY

1. B. Fu and N. Damer, "Biometric Recognition in 3D Medical Images: A Survey," in *IEEE Access*, vol. 11. DOI: [10.1109/ACCESS.2023.3331118](https://doi.org/10.1109/ACCESS.2023.3331118)
2. Z. Wang, M. Muhammad, N. Yadikar, A. Aysa and K. Ubul, "Advances in Offline Handwritten Signature Recognition Research: A Review," in *IEEE Access*, vol. 11. DOI: [10.1109/ACCESS.2023.3326471](https://doi.org/10.1109/ACCESS.2023.3326471)

VASCULAR BIOMETRICS

1. T. Eglitis, E. Maiorana and P. Campisi, "Open-Source Finger Vein Acquisition Device for Biometric Applications," in *IEEE Transactions on Instrumentation and Measurement*, vol. 72. DOI: [10.1109/TIM.2023.3324681](https://doi.org/10.1109/TIM.2023.3324681)
2. T.V. Nguyen, S.J. Horng, D.T. Vu, H. Chen and T. Li, "LAWNet: A Lightweight Attention-Based Deep Learning Model for Wrist Vein Verification in Smartphones Using RGB Images," in *IEEE Transactions on Instrumentation and Measurement*, vol. 72. DOI: [10.1109/TIM.2023.3328702](https://doi.org/10.1109/TIM.2023.3328702)
3. M. Zhang, J. Li, Y. Wang and G. Xu, "CECNet: Coordinate Encoding Competitive Neural Network For Palm Vein Recognition by Soft Large Margin Centralized Cosine Loss," in *IEEE Access*, vol. 11. DOI: [10.1109/ACCESS.2023.3341229](https://doi.org/10.1109/ACCESS.2023.3341229)
4. Z. Huang and C. Guo, "Towards Cross-Dataset Finger Vein Recognition with SingleSource Data," in *IEEE Transactions on Instrumentation and Measurement*. DOI: [10.1109/TIM.2023.3348905](https://doi.org/10.1109/TIM.2023.3348905)





IEEE International Joint Conference on Biometrics



CALL FOR PAPERS

15-18 September 2024

Buffalo/Niagara Falls, New York, USA

<https://fg2024.ieee-biometrics.org/>

About IJCB 2024

The IEEE International Joint Conference on Biometrics (IJCB) is the premier international forum for research in biometrics and related technologies. It combines two major biometrics conferences, the IEEE Biometrics Theory, Applications, and Systems (BTAS) conference and the International Conference on Biometrics (ICB), and is made possible through a special agreement between the IEEE Biometrics Council and the IAPR TC-4. IJCB 2024 is the 8th iteration of this major joint event and will be held in Buffalo/Niagara Falls, New York, United States, between September 15-18, 2024 as an in-person conference.

Call for Contributions

IJCB 2024 is intended to have a broad scope and invites papers that advance biometric technologies, sensor design, feature extraction and comparison algorithms, security and privacy, and social impact of biometrics technology. Topics of interest include, but are not limited to:

- Face, Iris, Fingerprint, Palmprint
- Periocular, Ear, Vein, Speech
- Behavioral and Gait Recognition
- Human Action Recognition
- Multi-modal and Multi-Spectral Biometrics
- Mobile-based Biometrics
- Biometrics at Altitude and Range
- Attribute Prediction via Biometric Modalities
- Template Protection and Cryptosystems
- Privacy, Demographic Bias, Fairness
- Biometrics Explainability and Interpretability
- Template Design, Selection and Update
- Datasets, Evaluation, Benchmarking
- Performance Modeling and Prediction
- Large Scale ID Management
- Presentation Attack Detection (e.g. Anti-spoofing), Morphing Attack Detection
- Biometric DeepFakes, Digital Data Forensics
- Biometric-related Law Enforcement and Forensics
- Biometrics in Healthcare, Banking, IoT
- Synthetic Data & Realities for Biometrics
- Ethical, Social and Legal Issues
- Biometrics for Social Good

Paper Submission

Submitted papers may not be accepted or under review elsewhere. Submissions may be up to eight pages, plus additional references, in IEEE conference format. Please visit the submission page for additional details on paper formatting. Accepted papers will be submitted for inclusion into IEEE Xplore Xplore's scope and quality requirements. Submission is through CMT - <https://cmt3.research.microsoft.com/IJCB2024/>.

Awards and TBIOM Special Issue

Several awards will be given out to the best papers from IJCB 2024, including (1) Best Paper award, (2) the Best Student Paper award, (3) Daily Best Poster awards.

The awards will consist of a commemorative plaque as well as award money. Additionally, the authors of the best-reviewed papers will be invited to submit an extended version of their paper to a special issue of the *IEEE Transactions on Biometrics, Behavior, and Identity Science* (IEEE-TBIOM).

Timeline

Tutorial proposal deadline: **February 20, 2024**

Paper submission deadline: **March 15, 2024**

Supplementary material: **March 22, 2024**

Special session proposal deadline: **April 24, 2024**

Review comments to authors: **April 30, 2024**

Rebuttal deadline: **May 7, 2024**

Decisions to authors: **May 17, 2024**

Camera-ready papers due: **June 30, 2024**

More details can be found at <https://ijcb2024.ieee-biometrics.org/>.

CALL FOR CONTRIBUTIONS AND PARTICIPATION

18th IEEE International Conference on Automatic Face and Gesture Recognition

27-31 May 2024, Istanbul, Türkiye

<https://fg2024.ieee-biometrics.org/>



The 18th IEEE International Conference on Automatic Face and Gesture Recognition, organized between 27-31 May 2024 in Istanbul, received 300 submissions for the main conference. The program includes keynotes by Mohamed Daoudi, Beatrice de Gelder, and Shiguang Shan, as well as an “Ask me Anything” session with Takeo Kanade. The call for papers is still out for the seven workshops organized at FG’24. These will be held on either

May 27 or May 31, 2024, in the same venue as the FG 2024 main conference (the exact program will be announced closer to the conference). Workshop papers will be published with the main conference proceedings.

IEEE BC will make **Diversity, Equity and Inclusion Grants** available to support the participation of researchers who self-identify as marginalised and/or underrepresented in the community (e.g., scholars who come from non-WEIRD – Western, Educated, Industrialized, Rich, Developed – societies, scholars from LGBTQ+ and underrepresented ethnic backgrounds) and who lack other funding opportunities to support their participation. Further information is available on the [FG DEI website](#).

The FG'24 conference features three competitions:

1. The **Synthetic Data for Face Recognition Competition** invites teams to propose clever ways to use synthetic face recognition datasets (either existing or new datasets) to train face recognition models. The competition is split into two tasks, where the first task involves a predefined face recognition backbone and limits the dataset size to focus on the quality of synthesized face datasets, while the second task provides almost complete freedom on the model backbone, the dataset and the training. Website: <https://www.idiap.ch/challenge/sdfr/>
2. **REACT 2024 - The Second REACT Challenge** focuses on developing generative models that can automatically output multiple appropriate, diverse, realistic and synchronised facial reactions under both online and offline settings. The challenge encourages the participants to generate realistic images and video clips as results of their submission. Website: <https://sites.google.com/cam.ac.uk/react2024/home>
3. The **Brain Responses to Emotional Avatars Challenge** shares a special database collected from 40 subjects with an EEG device. The subjects are asked to show emotions they see on an avatar's face on the screen. The objective of this challenge is to conduct an analysis of EEG signals in order to accurately identify and classify different emotional states. Website: <https://voxellab.pl/EmoNeuroDB/>

The FG 2024 is also hosting a series of workshops on recent and new topics in face and gesture recognition, biometrics, applications and related emerging topics. Please refer to the workshop links below for the exact submission deadlines in March.

1. Fourth Workshop on Applied Multimodal Affect Recognition - <https://cse.usf.edu/~tjneal/AMAR2024/>

-
2. SkatingVerse: Segmentation and Assessment of Continuous Video in Figure Skating Competition and the 1st SkatingVerse Workshop & Challenge –
<https://skatingverse.github.io/>
 3. Second Workshop on Learning with Few or without Annotated Face, Body and Gesture Data –
<https://sites.google.com/view/lfa-fg2024/home>
 4. Advancements in Facial Expression Analysis and Synthesis: Past, Present, and Future -
<https://sites.google.com/view/afeas-24/home>
 5. Second Workshop on Privacy-aware and Acceptable Video-based Assistive Technologies -
<https://goodbrother.eu/conferences/privaal2024/>
 6. Synthetic Data for Face and Gesture Analysis -
<https://sites.google.com/view/sd-fga2024/>
 7. First International Workshop on Responsible Face Image Processing -
<https://responsiblefaceimageprocessing.github.io/fg2024/>

UPCOMING CONFERENCES IN 2025

IJCB 2025 is planned for 8-11 September 2025 (tentative dates), in Osaka, Japan. The general chairs are Yasushi Yagi (Osaka University), Mark Nixon (University of Southampton), Hitoshi Imaoka (NEC), and Md Atiqur Rahman Ahad (University of East London). Program chairs are Vitomir Struc (University of Ljubljana), Karthik Nandakumar (Mohamed Bin Zayed University of Artificial Intelligence), Xiangyu Zhu (Chinese Academy of Sciences), and Lale Akarun (Bogazici University).

FG 2025 will be held between 12-15 May 2025 (tentative dates), in Tampa/Clearwater, USA. The general chairs are Shaun Canavan (University of South Florida), Lijun Yin (Binghamton University), Mohamed Daoudi (IMT Nord Europe), and the program chairs are Tempestt Neal (University of South Florida), Jeffrey Girard (University of Kansas), Shiguang Shan (Chinese Academy of Sciences), and Zakia Hammal (Carnegie Mellon University).

IBCN EDITORIAL REVIEW BOARD

Editor in Chief

ANDREW TEOH BENG JIN

Yonsei University, Korea

Associate Editors

FERNANDO ALONSO-FERNANDEZ

Halmstad University, Sweden

SILVIO BARRA

University of Naples Federico II, Italy

APARNA BHARATI

Lehigh University, USA

CARMEN BISOGNI

University of Salerno, Italy

DAVID FREIRE-OBREGON

Universidad de Las Palmas de Gran
Canaria, Spain

EMANUELE MAIORANA

Roma Tre University, Rome, Italy

EMANUELA MARASCO

George Mason University, USA

SHRUTI NAGPAL

IIIT-Delhi, India

JOÃO NEVES

University of Beira Interior, Portugal

CHIARA GALDI

EURECOM, France

CHRISTIAN RATHGEB

Hochschule Darmstadt, Germany

THOMAS SWEARINGEN

Michigan State University, USA

RUBEN TOLOSANA

Universidad Autonoma de Madrid, Spain

Publications Committee

PATRIZIO CAMPISI (Chair) Roma Tre University, Rome, Italy

CLINTON FOOKES Queensland University of Technology, Australia

JOSEF KITTLER University of Surrey, UK

RICHA SINGH IIT Jodhpur, India

Nalini Ratha, SUNY, University at Buffalo, USA

Many thanks to those who contributed articles to this issue:

Dr. Fernando Alonso-Fernandez, who curated the article selected for this issue's *Noted in the Literature* section.

Dr. Carmen Bisogni, and **David Freire-Obregón**, who compiled the *Biometric Alerts* column.

Dr. Chiara Galdi, who selected and prepared both the *Source Code* (with Michele Panariello, Ph.D. candidate, EURECOM, Biot, France) and *Commercial Off-the-Shelf* biometric products columns, and co-wrote the *Special Feature* on the TRSPAS-ETN with Massimiliano Todisco, also an Assistant Professors, Eurecom, Biot, France.

Dr. Els J. Kindt, Associate Professor and Researcher at eLaw - Center for Law and Digital Technologies, Leiden University, Leiden, The Netherlands, who wrote about EU Biometric Data Regulation in the first of a two-part series in our *Lecture Notes* column.

Dr. Emanuele Maiorana, who selected and compiled the items for our *In the News* section, as well as the list of *EU Project Updates*.

Dr. Emanuela Marasco, who summarized a presentation by Malhotra et al. for our *Database Digest* section.

Dr. Gian Luca Marcialis, Associate Professor, Università Degli Studi di Cagliari, Cagliari, Italy, who wrote the report on the 2023 Fingerprint Liveness Detection Competition.

Dr. João Neves, who interviewed Adam Philpott for our *Expert Perspectives* column.

Dr. Ruben Tolosana, who interviewed Ph.D. student Hatef Otroshi for the *Researcher on the Rise* section.