IEEE BIOMETRICS COUNCIL NEWSLETTER

Volume 52, December 2024

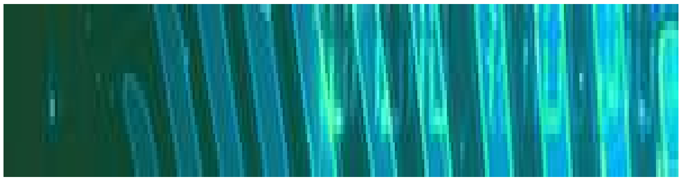
IN THIS ISSUE

Protecting the spoken word

As new deepfake and adversarial attacks flourish, how can we be sure the message we hear is authentic? In the ***Lecture Notes*** section, **Massimiliano Todisco** of EURECOM, France, assesses two new threats to voice authentication and suggests ways to address them. Also in this issue you can read about the 2024 edition of the **International Joint Conference on Biometrics**, share some thoughts from **Biometric Pioneer Dr. Pong C. Yuen** of Hong Kong Baptist University, and meet **Researcher on the Rise Pramuditha Perera** of the AWS AI Lab.

GREETINGS FROM THE EIC

ANDREW TEOH BENG JIN
Yonsei University, Korea



Dear Readers of the *Biometric Newsletter,* welcome to this new issue!

As 2024 draws to a close, this December issue of the *IEEE Biometrics Council Newsletter* offers a forward look at the innovations shaping our future. In this edition, we reflect on key events, celebrate outstanding achievements, and explore cutting-edge advancements that highlight the dynamism of our field.

Our **Council News** section features comprehensive reports on two significant industry conferences. The first was the **8th IEEE International Joint Conference on Biometrics (IJCB 2024)**, which was held in Buffalo, New York, from September 15-18. This year's edition highlighted groundbreaking research and featured 56 accepted papers, seven special sessions on pivotal topics like generative AI in biometrics and synthetic image vulnerabilities, and engaging keynote talks. With more than 60 teams participating in competitions and demonstrations, IJCB 2024 showcased a remarkable confluence of academics, industry, and government researchers who are furthering innovation and collaboration.

We also bring you highlights from the **16th IEEE International Workshop on Information Forensics and Security (WIFS 2024)**, which took place in the historic city of Rome earlier this month. This event emphasized synergies between biometrics and multimedia forensics, and offered insightful tutorials and keynotes on the challenges of, and opportunities in, digital identity systems, synthetic media detection, and foundational privacy methods.

Additionally, this issue celebrates the achievements of individuals and teams who received prestigious awards at IJCB and WIFS. Their contributions, from anti-spoofing innovations to robust fingerprint-matching algorithms, exemplify the excellence and impact of our community's research efforts.

Yet, this issue has more to offer than just meeting coverage. The **Lecture Notes** section addresses the pressing challenges posed by deepfakes and adversarial attacks on automatic speaker verification (ASV) systems. *Prof. Massimiliano Todisco* of EURECOM shares insights into the groundbreaking adversarial methods "Malafide" and "Malacopula," techniques that highlight the need for innovative solutions to safeguard biometric systems in increasingly hostile threat environments. He also presents countermeasures to enhance the resilience of ASV systems in an era of ubiquitous voice cloning tools.

Our profile sections feature conversations with researchers at various stages of their careers. The **Biometric Pioneers** column honors *Dr. Pong C. Yuen* of Hong Kong Baptist University whose remarkable career has spanned foundational contributions in cancellable biometrics, template protection, and AI-driven medical informatics. Dr. Yuen's work exemplifies the importance of interdisciplinary approaches to advance security, privacy, and healthcare applications. *Esteban Vázquez Fernández,* CTO of Alice Biometrics, shares his journey from academia to co-founding his own company in this issue's **Expert Perspectives** column. He also emphasizes the shift in identity systems from technical approaches to a user-centric focus, highlights the importance of flexibility in tackling challenges like spoofing and privacy concerns, and envisions biometrics as pivotal in bridging physical and digital worlds. Lastly, this edition's **Researcher on the Rise** subject, Dr. Pramuditha Perera, shares a different type of journey from Sri Lanka to cutting-edge AI research at the AWS AI Lab. He discusses his impactful work on one-class classification and anomaly detection, and the importance of cross-disciplinary research in advancing the boundaries of biometrics.

Our **Noted in the Literature** section delves into groundbreaking research on Spatio-temporal Dual-Attention Transformers, a novel approach for time-series behavioral biometrics. Meanwhile, the **Database Digest** introduces an innovative fictional dataset for facial identity visual question answering (VQA), while the **Source Code** section showcases cutting-edge work on learning gait representations for soft biometric estimation using vision transformers. Rounding out the issue, the **COTS** feature highlights NCheck's Multi-Biometric Solutions that are revolutionizing workforce management with advanced biometric technologies.

Thank you for your continued engagement with the IEEE Biometrics Council and dedication to advancing biometric research and innovation. May this issue inspire new ideas and collaborations as we prepare for an exciting 2025! Wishing you and your loved ones a joyous holiday season and a prosperous New Year filled with success and innovation.

Warm regards,

Andrew Teoh

COUNCIL NEWS

8th IEEE International Joint Conference on Biometrics (IJCB)

September 15-18, 2024

Buffalo, New York, USA

Report by ***Dr. Stephanie* Schuckers, President-Elect of the IEEE Biometrics Council**

The Jacobs School of Medicine and Biomedical Science Building at SUNY Buffalo, site of IJCB 2024. Image taken from the IJCB website at https://ijcb2024.ieee-biometrics.org/hotel/.

Buffalo, NY, was the site of the 2024 edition of the **IEEE International Joint Conference on Biometrics (IJCB 2024),** which was held from September 15 to 18, 2024. Hosted by the State University of New York at Buffalo, this year's conference featured a host of events, including oral and paper presentations, competitions, and tutorials.

The conference continues to attract outstanding research contributions from academia and industry and this year was no exception. Out of a total of 174 submissions that represented the breadth and diversity of the biometrics field, 56 papers were selected. Twenty-two of these papers were delivered as oral presentations, and the remaining 34 were posters.

The conference program was further enhanced by seven special sessions, and we thank their organizers for enriching the regular conference program with 48 additional posters and talks. These sessions addressed the following topics:

- “Generative AI for Futuristic Biometrics” by Sudipta Banerjee and Nasir Memon (New York University, USA); Vitomir Štruc (University of Ljubljana, Slovenia); and Kiran Raja (Norwegian University of Science and Technology, Norway)
- “Recent Advances in Detecting Manipulation Attacks on Biometric Systems (ADMA-2024)” by Abhijit Das (Birla Institute of Technology and Science, India); Raghavendra Ramachandra (Norwegian University of Science and Technology, Norway); Naser Damer (Fraunhofer Institute for Computer Graphics Research, Germany); Vitomir Štruc and Marija Ivanovska (University of Ljubljana, Slovenia)
- “Face Morphing Attack and Detection Techniques (FMADT-2024)” by Chen Liu (Clarkson University, USA); Christoph Busch (Norwegian University of Science and Technology, Norway, and Hochschule Darmstadt, Germany), Mei Ngan (National Institute of Standards and Technology, USA); Srirangaraj Setlur (SUNY Buffalo, USA); and Jeremy Dawson (West Virginia University, USA)
- “Recognition at Long Range and from High Altitude” by Scott McCloskey (Kitware, USA), Vishal Patel (Johns Hopkins University, USA); Ben Riggan (University of Nebraska, USA); and Srirangaraj (Ranga) Setlur (SUNY Buffalo, USA)
- “Multimodal Human Behavior Understanding and Generation (MUG-2024)” by Zitong Yu (Great Bay University, China); Siyang Song (University of Leicester, UK); Weicheng Xie (Shenzhen University, China); Xin Liu (Lappeenranta-Lahti University of Technology, Finland), and Linlin Shen (Shenzhen University, China)
- “Face Recognition in the Era of Synthetic Images and Its Boundless Vulnerabilities (SIBV-SS)” by Akshay Agarwal (IISER Bhopal, India; and Gaurav Goswami (IBM, USA)
- Responsible AI for Biometrics (AI4BIO) by Shu Hu (Purdue University), and Xin Wang (SUNY Albany

Following the tradition of previous conferences, a call was also issued to identify significant papers on topics of interest to the biometrics community that had been published recently in major journals. In response to this call, three journal paper presentations were included as part of the IJCB 2024 program. The featured papers were:

- “Leveraging Diffusion for Strong and High-Quality Face Morphing Attacks,” by Zander W Blasingame and Chen Liu, Clarkson University, USA, *TBIOM*, January 2024.
- “SSPRA: A Robust Approach to Continuous Authentication Amidst Real-world Adversarial Challenges,” by Sicong Chen, Jingyu Xin, and Vir V Phoha, Syracuse University, USA, *TBIOM,* April 2024.
- “Analyzing the Impact of Demographic and Operational Variables on 1-to-Many Face ID Search,” Aman Bhatta, University of Notre Dame, *TBIOM*, June 2024.

COMPETITIONS AND DEMONSTRATIONS

Competitions offer a practical way to engage with different biometrics-related problems and generate tangible solutions. Sixty teams participated globally in the 2024 IJCB challenges, which covered topics in open-set face detection and identification, human identification at a distance, face liveness detection, latent in the wild fingerprint recognition, and competition and ID card Presentation Attack Detection. PAD-IDCard 2024 is the first competition in the ID card series, and offers an independent assessment of the current state-of-the-art algorithms and evaluation protocols. Combined these competitions produced five summary papers that were also included in the technical program of the conference.

Lastly, the technical program also incorporated two demonstrations in tandem with poster presentations. Chengzhe Sun, a research assistant at the Media Forensics Lab at SUNY Buffalo, and his advisor, Professor Siwei Lyu, presented the “DeepFake-O-Meter v2.0,” an open platform for deepfake detection. The other demonstration, presented by Michigan State University Ph.D. student Nitish Shukla and his advisor, Professor Arun Ross, spotlighted demorphing, a technique for extracting component faces from facial morphs.

KEYNOTE SESSIONS AND TUTORIALS

In addition to the paper presentations and demos, IJCB also hosted keynote talks from a number of leading researchers. This year’s keynote presenters and topics were:

- Abhijit Bose from Capital One on “New Challenges and Opportunities in the Age of Generative AI”
- Elham Tabassi from the National Institute of Standards and Technology on “AI Risk Management: Enabling Trust”

- Rui Zhao from AmazonOne on "Amazon One - Technology Behind the Experience,"
- Michael King from Florida Institute of Technology on "Facing the Future: Navigating the Promise and Pitfalls of Automated Face Recognition."

University at Buffalo
Department of Computer Science and Engineering
School of Engineering and Applied Sciences

To offer a more substantial "deep dive" on a select number of timely technical topics, the program also included three tutorials. You can read more about these sessions in a companion article that follows this one.

Finally, a Doctoral Consortium was held to give young researchers the opportunity to meet with established researchers and leaders from academia to discuss their work and career opportunities. And, a team of international experts from industry, academia, and government offered their insights at a panel discussion on "Building Responsible Biometric Systems." Held on Wednesday, September 18, the participants were: Stephanie Schuckers, UNC-Charlotte; Vishesh Mistry, Tech5; Joel Brogan, Oak Ridge National Laboratories; Ambuj Neupane, Government Services Administration (GSA); and Udo Mahlmeister, CLEAR.

Social events included a trip to Niagara Falls, one of the most visited natural sites in the USA, a reception at the conference, and a gala dinner in a historic Buffalo Hotel.

AWARDS AND HONORS

The following awards were presented at IJCB '24:

Best Paper Award; "Keystroke Dynamics Against Academic Dishonesty in the Age of LLMs" by
Debnath Kundu and Atharva Mehta, Indraprastha Institute of Information Technology, Delhi; Rajesh Kumar, Bucknell University, USA; Naman Lal and Apoorv Singh, MIDAS Lab, IIIT Delhi, India, and Avinash Anand and Rajiv Ratn Shah, IIIT Delhi, India.

Best Paper Runner-Up Award
"Biometric Authentication Based on Enhanced Remote Photoplethysmography Signal Morphology" by Zhaodong Sun, Jukka Komulainen, and Guoying Zhao , University of Oulu, Finland; and Xiaobai Li, Zhejiang University, China.

Best Student Paper Award
"FDWST: Fingerphoto Deblurring using Wavelet Style Transfer," by David C Keaton, Amol S. Joshi, Jeremy M. Dawson, and Nasser Nasrabadi , West Virginia University, USA.

IAPR Best Biometrics Student Paper Award
"Distillation-guided Representation Learning for Unconstrained Gait Recognition," by Yuxiang Guo, Siyuan

Huang, Ram Prabhakar Kathirvel, Rama Chellappa, Cheng Peng, Johns Hopkins University, USA, and Chun Pong Lau, City University of Hong Kong, China.

Marta Gomez Barrero (Technical Co Chair), Stephanie Schuckers (Technical Co Chair), Zhaodong Sun (Best Paper Runner up Winner), Davide Maltoni, and Richa Singh (Technical Co Chair)

Best Poster Award
"RuleBoost: A Neuro-Symbolic Framework for Robust Deepfake Detection," by Muhammad Anas Raza, Oakland University, USA; and Khalid Mahmood Malik and Ijaz ul Haq, University of Michigan-Flint, USA.

Best Poster Runner-Up Award
"Assessing the Reliability of Biometric Authentication on Virtual Reality Devices," by Ketan Kotwal, Gokhan Ozbulak, and Sébastien Marcel, Idiap Research Institute, Switzerland.

BTAS/IJCB 5-Year Highest Impact Award
"Multi-task Learning for Detecting and Segmenting Manipulated Facial Images and Videos" by Huy H. Nguyen, Fuming Fang, Junichi Yamagishi, Isao Echizen. Originally presented at the 2019 IEEE International Conference on Biometrics Theory, Applications and Systems in Tampa, FL.

ACKNOWLEDGEMENTS AND THANK YOUS

The conference organizers are grateful to our sponsors and supporters for their invaluable assistance in staging this event. This year, the University at Buffalo Institute for Artificial Intelligence and Data Science was a Diamond sponsor; Visa, a Gold Sponsor; and Amazon One, Tech5, and NeuroTechnology, Silver Sponsors. We also highly appreciate the contributions of the IEEE Biometrics Council through its DEI travel grant program that allowed more researchers from underrepresented groups to attend.

We also wish to thank all members of the Organizing Committee for their hard work and effort.

Finance Chairs: Ifeoma Nwogou, SUNY Buffalo, USA; Jeremy Dawson, West Virginia University, USA; and Tempestt Neal, University of South Florida, USA

Tutorial Chairs: Aparna Bharati, Lehigh University, USA; Anoop Namboodiri, Indian Institute of Technology-Hyderabad, India; and Deen Dayal Mohan, Yahoo, USA.

Awards Committee Chairs: Davide Maltoni, University of Bologna, Italy, and

Vijaya Kumar, Carnegie Mellon University, USA.

Doctoral Consortium Chairs: Christoph Busch, Norwegian University of Science and Technology, Norway; Nasser Nassarbadi, West Virginia University, USA; and Mark Nixon, University of Southampton, UK

Sponsorship Chairs: Mayank Vatsa, Indian Institute of Technology-Jodhpur, India; Sunpreet Arora, Visa, USA; and Jian Wang, Thales Digital Identity, Singapore.

Special Sessions Chairs: Siwei Lyu, SUNY Buffalo, USA; and Xiaoming Liu, Michigan State University, USA

Competition Chairs: Srirangaraj Setlur SUNY Buffalo, USA; and Arun Ross, Michigan State University, USA.

Demo Chairs: Junsong Yuan, SUNY Buffalo, USA: and Gang Hua, Wormpex AI Research, USA

Publications Chairs: Ketan Kotwal, Idiap, Switzerland; Akshay Agarwal, Indian Institute of Science Education and Research, Bhopal, India; and Shiqi Yu, SusTech, China

DEI Chairs: Emanuela Marasco, George Mason University, USA; and Vishnu Lokhande, SUNY Buffalo

Web Chair: Daqing Hou, Rochester Institute of Technology, USA

Publicity Chairs: Pavel Korshunov, Idiap, Switzerland; Ajita Rattani, University of North Texas, USA; and Shiqi Yu, SusTech, China

We also thank the conference secretaries for their hard work and our student volunteers for helping with the conference logistics, along with the local organizing chair, Ifeoma Nwogou of SUNY Buffalo

IEEE International Joint Conference on Biometrics
BUFFALO, NY, SEPTEMBER 15TH-18TH, 2024

Technical Program Chairs: Richa Singh, Marta Gomez Barrero, Stephanie Schuckers

IEEE International Joint Conference on Biometrics
BUFFALO, NY, SEPTEMBER 15TH-18TH, 2024

IJCB2024 General Chairs: Venu Godindaraju and Nalini Ratha

The IJCB 2024 Tutorials: A Deep Dive into AI Models, Face Recognition, and Security and Privacy

By Aparna Bharati, Assistant Professor at Lehigh University , Bethlehem, Pennsylvania, USA, and co-chair of the IJCB Tutorials Committee

This year's IJCB conference included one full-day and two half-day tutorials on critical topics in biometrics. A fourth scheduled tutorial on Qualitative Methods for Biometrics Research had to be canceled at the last minute due to illness. The tutorials were held on Sunday, September 15, the opening day of the conference.

M&T BANK AUDITORIUM
IEEE International Joint Conference on Biometrics
BUFFALO, NY, SEPTEMBER 15TH-18TH, 2024

The full-day tutorial focused on "Foundational Generative AI Models in Biometrics." Organized by Dr. Anush Sankaran from Microsoft Security AI Research and Dr. Mayank Vatsa from the Indian Institute of Technology in Jodhpur, India, the program covered foundational aspects, recent advancements, and future trends in the application of AI models to biometrics. Various prompting techniques and deep learning methods associated with LLMs and VLMs were also discussed.

The first half-day tutorial, organized by Akshay Agarwal from IISER, Bhopal, India and Chaitanya Roygaga, Lehigh University, PA, USA, was on "Face Recognition Progression: Synthetic Images to Vulnerabilities." The tutorial included methods to create synthetic faces via face morphing and deepfake techniques and how these technologies impact face recognition models. The decision-making process of the models was also explored from an explainability perspective, where features from various layers of different networks were visualized using attention and activation maps.

IEEE International Joint Conference on Biometrics
BUFFALO, NY, SEPTEMBER 15TH-18TH, 2024

The second half-day tutorial was organized by Amina Bassit and Vishnu Boddeti from Michigan State University, MI, USA. The tutorial focused on the security and privacy preservation of biometric systems that are capable of deeply analyzing and extracting hidden information, and how their application can lead to learning specific human attributes. Consequently, the combination of those attributes can reveal one's identity, and release personal information simply through their processed biometric samples. The tutorial aimed at raising awareness about the alarming urgency of protecting biometric information from risks such processing presents if conducted in an unprotected manner. Session leaders discussed various types of attacks and their mitigation, and presented solutions along with their trade-offs between efficiency, accuracy, security, and privacy were also clarified. In addition, the speakers identified gaps in current research to motivate further research in those directions. Tutorial participants received Python notebooks for hands-on practice, and to allow attendees to follow along.

Overseeing the Tutorial Sessions with me were: Anoop Namboodiri of the Indian Institute of Technology, Hyderabad, India and Deen Dayal Mohan.

16th IEEE International Workshop on Information Forensics and Security (WIFS ‘24)

December 2-5, 2024
Roma Tre University
Rome, Italy

Report by Emanuele Maiorana, Assistant Professor, Roma Tre University, Rome, Italy

The 16th edition of the IEEE International Workshop on Information Forensics and Security (WIFS) took place in Rome, Italy, from December 2 to 5, 2024. Roma Tre University hosted the event, with technical sponsorship from the IEEE Signal Processing Society (SPS) and the Italy Section Chapter of the IEEE Biometrics Council. Factoring in speakers and other invited guests, the workshop drew close to 100 participants.

A total of 53 presentations were delivered over the three-day workshop, the largest number of presented contributions ever for an IEEE WIFS. This included the 39 papers, selected out of an initial 89 submissions, that made up the technical program. These presentations were complemented by three demo sessions, a poster session dedicated to three papers previously published in *Transactions on Information Forensics and Security (TIFS)* in 2024, and two special sessions. The first of these sessions on "Synergies between Biometrics and Forensics," was organized by Kiran Raja and Marta Gomez-Barrero. The second one focused on “Synthetic Media Detection in Multi-Media Forensics,” and was organized by Edward J. Delp and Stefano Tubaro. The former special session consisted of 3 accepted papers, while 9 papers were included in the latter one.

The first day of the workshop was dedicated to four tutorials:

- “Privacy 101, with Trumpets and Truffles – An Introduction to Differential Privacy and Homomorphic Encryption, and Applications in Federated Learning,” by Fernando Pérez-González
- “Safety, Security, and Privacy of Foundation Models,” by Xinlei He and Tianshuo Cong
- “Synthetic Realities: Impact, Advancements, and Ethical Considerations,” by Gabriel Bertocco and Anderson Rocha
- “European Digital Identity Wallet: Opportunities and Security Challenges,” by Amir Sharif, Giada Sciarretta, and Alessandro Tomasi

The workshop also hosted three keynote addresses on relevant topics:

- “Opportunities and Challenges of Digitalization in Digital Forensics,” by Lena Klasén, Director of Research at the Department of National Operations of Sweden, and Adjunct Professor of Digital Forensics, Computer Vision Laboratory, Linköping University, Sweden
- “Biometrics and Behavior for Information Forensics and Learning Assessment in Online

Education," by Julian Fierrez, Full Professor at Universidad Autonoma de Madrid, Madrid, Spain

- "Natural Language Processing Approaches to Text Credibility and their Implications for Information Security," by Martha Larson, Professor of Multimedia Information Technology at Radboud University, Nijmegen, Netherlands.

Two awards were presented at the end of the workshop. Joakim Tutt and Slava Voloshynovskiy of the University of Geneva, Switzerland, received the Best Paper Award for their work on "Provable Performance Guarantees of Copy Detection Patterns." Best Student Paper Award honors went to the paper "Fixed-length Dense Descriptor for Efficient Fingerprint Matching," written by Zhiyu Pan, Yongjie Duan, Jianjiang Feng, Jie Zhou, of Tsinghua University, Beijing, China.

Importance of credibility for security
Sudden crisis:
'Communication and reliability information' is a category of disaster preparedness
Creeping crisis:
Mis- and disinformation erodes trust in societal institutions and ultimately threatens democratic systems.

Social events included a welcome reception at the workshop venue on December 2nd, and a visit to the renowned Palazzo Barberini, followed by a dinner at the rooftop restaurant Il Vizio of the 5-star Hotel Sina Bernini Bristol in the very center of Rome, on December 4th.

Sponsors financially supporting the workshop include Universitas Mercatorum, Keyless, Amped Software, Colorado State University, and Scantrust.

The next edition of IEEE WIFS will be held in Perth, Australia, from December 1-5, 2025.

==

The WIFS Organizing committee was as follows.:

General Chair: Emanuele Maiorana, Roma Tre University, Rome, Italy

General Co-Chair: Bin Li, Shenzhen University, China

Technical Program Chairs: Chiara Galdi, EURECOM, France; Vitomir Štruc, University of Ljubljana, Slovenia; H. Vicky Zhao, Tsinghua University, China

Keynotes and Tutorials Chairs: Fernando Alonso-Fernandez, Halmstad Univ., Sweden; and Pedro Comesaña Alfaro, University of Vigo, Spain

Special Session, Demo and Challenge Chairs: Adam Czajka, University of Notre Dame, USA; and Paulo Lobato Correia, University de Lisboa, Portugal

Financial Chair: Marco Fontani, Amped Software, Italy

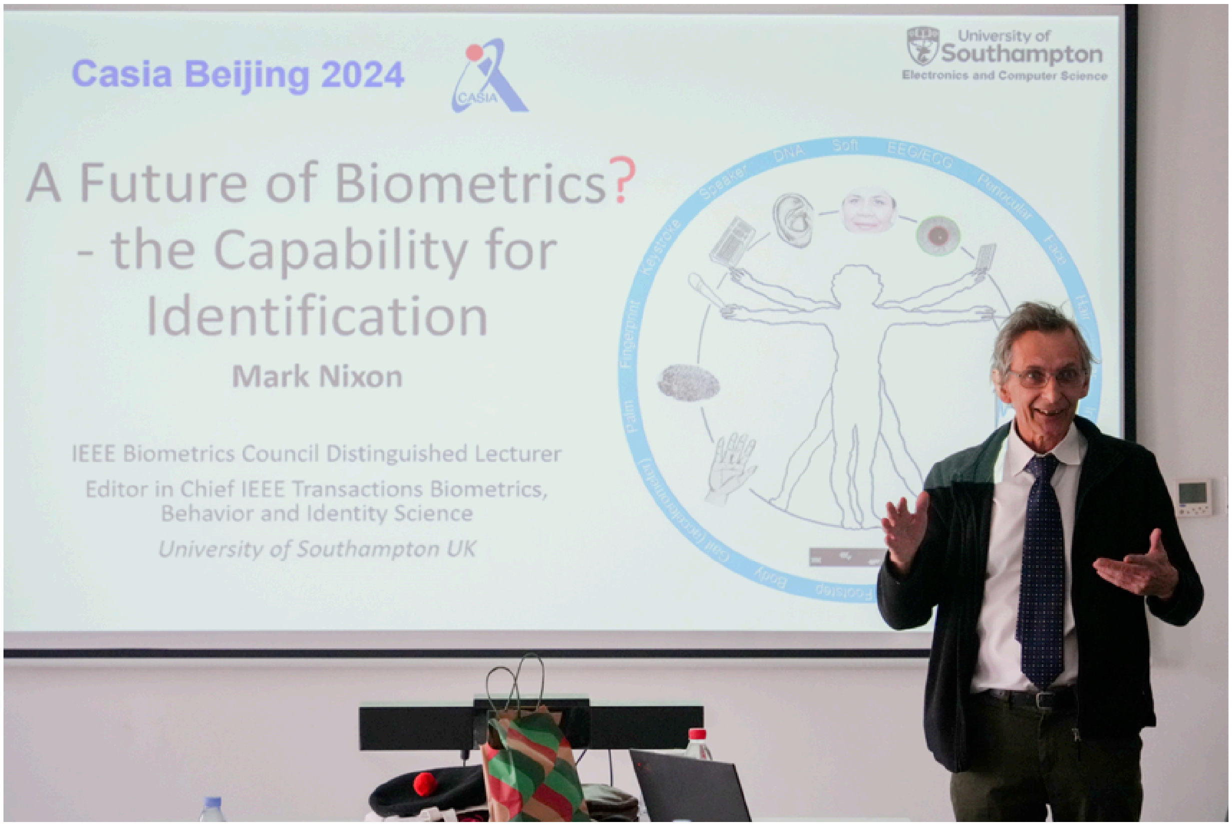
Publication and Web Chair: Enrique Argones Rúa, KU Leuven, Belgium

Publicity Chairs: Jiankun Hu, University of New South Wales, Australia; Deepa Kundur, University of Toronto, Canada; Minoru Kuribayashi, Tohoku University, Japan; Pauline Puteaux, CNRS, France

Sponsorship Chairs: Roberto Caldelli, Universitas Mercatorum & CNIT, Italy; Gabriel E. Hine, Roma Tre University, Italy; Koichi Ito, Tohoku University, Japan; Steven J. Simske, Colorado State University, USA

Local Arrangements Chairs: Irene Amerini, Sapienza University of Rome, Italy

DPL NEWS: Prof. Mark Nixon Lectures on Biometric Identification in Beijing



Casia Beijing 2024

University of Southampton
Electronics and Computer Science

A Future of Biometrics?
- the Capability for
Identification

Mark Nixon

IEEE Biometrics Council Distinguished Lecturer
Editor in Chief IEEE Transactions Biometrics,
Behavior and Identity Science
University of Southampton UK

The IEEE Biometrics Council Distinguished Lecturers Program (DLP) was introduced to support education related activities for the biometrics community. Specifically, DLP seeks to increase awareness about topics relevant to biometrics by creating a pool of leading experts willing to speak at meetings hosted by IEEE Chapters and Sections. Last month, Dr. Mark S. Nixon, an emeritus professor from the School of Electronics and Computer Science at the University of Southampton UK, traveled to Beijing, China, under the umbrella of the program to deliver a talk on “A Future of Biometrics: The Capability for Identification.” Hosted by the IEEE Beijing Chapter—with support from the DLP—and chaired by Prof. Jing Dong of the Chinese Academy of Sciences, the talk was delivered on November 19, 2024.

In the lecture, Professor Nixon, who is a past president of the lEEE Biometrics Council, shared a number of insights with the 30 on-site attendees at the Academy’s Institute of Automation. Drawing on his research experience, which has included developing new techniques for static and moving shape extraction—Nixon introduced how biometric recognition works. After discussing the different kinds of biometric features, and some typical methods within the field, he shared his definition of identity science, as well as future directions for the field. After his talk, the participants remained for deep discussions with Prof Nixon on various topics in biometrics, and showed how much they appreciated the lecture.

To learn more about the DLP program, including the other lecturers currently available to speak at local chapters, go to https://ieee-biometrics.org/get-involved/distinguished-lecturers-program-dlp/.

IN THE NEWS…

Compiled by Emanuele Maiorana, Assistant Professor, Roma Tre University, Rome, Italy

Biometric recognition systems have now become an integral part of our daily lives, largely due to their use as authentication methods for mobile devices. But, now there are more and more applications using these systems, and consequently the world population's interest in the functioning and implications of biometrics in everyday life is growing. Numerous articles on these topics now appear in publications that are not strictly scientific in nature. As is widely known, media may have a significant role in forming and directing people's perception of a particular topic. Hence, it is important to know how these technologies are presented to the public. The following is a selection of articles that appeared from January to July 2024 on some of the most popular English-language news websites, such as *The Financial Times*, *Forbes*, *The Guardian, The New York Times*, or the *BBC*.

No passports needed under Border Force e-gate plan (January 1, 2024)
https://www.thetimes.co.uk/article/uk-flights-passports-border-force-queues-szdd39c5x
https://www.forbes.com/sites/davidbirch/2024/01/04/british-airways-trial-end-to-end-hands-free-travel-with-biometrics/
https://www.theguardian.com/world/2024/jan/01/facial-recognition-could-replace-passports-at-uk-airport-e-gates

Under plans for "frictionless" travel, passengers arriving in the UK will not need to present their passports at the border. New e-gates will be installed at airports that can allow arrivals to enter the country using only advanced facial recognition. The International Air Transport Association (IATA) has successfully tested the first fully integrated digital identity and verifiable credential journey on British Airways from London Heathrow (LHR) to Rome Fiumicino (FCO). It looks as if my dreams of seamless travel are a step closer to reality.

AI tool suggests our fingerprints may not be unique ((January 11, 2024)

https://www.bbc.com/news/technology-67944537

Research from Columbia University is challenging the belief that each fingerprint on a person's hand is completely unique, but that notion is now being challenged by A team at the US university trained an AI tool to examine 60,000 fingerprints to see if it could work out which ones belonged to the same individual. The researchers claim the technology could identify, with 75-90% accuracy, whether prints from different fingers came from one person. But they are not sure how it works.

Mark Zuckerberg to be deposed in Texas suit targeting Meta of 'secretly harvesting' facial recognition without customer consent (January 16, 2024)

https://nypost.com/2024/01/16/business/mark-zuckerberg-to-be-deposed-in-texas-suit-targeting-meta-of-using-facial-recognition-without-customer-consent/

Meta boss Mark Zuckerberg will be deposed as part of a Texas lawsuit accusing the Facebook and Instagram parent of using facial recognition technology without customer consent. A Texas state appeals court upheld a lower court's decision requiring Zuckerberg to give testimony in the case. The lawsuit, originally filed in 2022, accused Meta of "secretly harvesting" biometric data from its users in violation of state law.

UK banks prepare for deepfake fraud wave (January 19, 2024)

https://www.ft.com/content/515e344d-9ec1-4c3e-888f-10ff57712412

Banks have long had to deal with fraud by impersonation. But, as deepfakes and voice cloning become easier, schemes in which scammers pretend to be anything from a prospective romantic partner to a family member in crisis have the potential to target far more people and with a higher rate of success. UK banks are already being hit by scams using deepfakes, according to Sandra Peaston, research director at fraud prevention body Cifas.

Lobby group calls for poker venues to be exempt from facial recognition and biometric data laws (February 1, 2024)

https://www.theguardian.com/australia-news/2024/feb/02/lobby-group-calls-for-pokies-venues-to-be-exempt-from-facial-recognition-and-biometric-data-laws

A lobby group representing some of Australia's biggest poker machine venues are seeking an exemption from new laws regarding the retention of biometric data. The group wants to maintain this data for several years so it can use facial technology to identify gambling addicts.

Everything you need to know as Whole Foods' palm print payments take NYC — and is it safe? (February 5, 2024)
https://nypost.com/2024/02/05/tech/everything-to-know-as-whole-foods-palm-print-payments-take-nyc/
Whole Foods shoppers in NYC have recently noticed a curious new way of paying for their groceries, which requires simply waving their hand over a reader instead of swiping a card or tapping a phone. Called Amazon One, the company says customers "will no longer need their wallet or even a phone to pay," thanks to the touch-free reader.

Canadian university vending machine error reveals use of facial recognition (February 23, 2024)
https://www.theguardian.com/world/2024/feb/23/vending-machine-facial-recognition-canada-univeristy-waterloo
A malfunctioning vending machine at the University of Waterloo has inadvertently revealed that a number of these devices have been using facial recognition technology in secret. There was no prior indication that the machine was using the technology, nor that a camera was monitoring student movement and purchases.

Serco Leisure ordered to stop using facial recognition to monitor staff (February 23, 2024)
https://www.ft.com/content/0da706ab-803f-430d-bea9-485962cbc201
https://www.theguardian.com/business/2024/feb/23/serco-ordered-to-stop-using-facial-recognition-technology-to-monitor-staff-leisure-centres-biometric-data
A subsidiary of Serco, a UK leisure company, has been ordered to stop using facial recognition and fingerprint scanning to monitor attendance and pay staff. The crackdown marked the first action by the UK Information Commissioner's Office (ICO) against an employer processing the biometric data of its workers.

JPMorgan Chase Is right to be bullish on retail biometrics (April 3, 2024)
https://www.forbes.com/sites/davidbirch/2024/04/03/jpmorgan-chase-are-right-to-be-bullish-on-biometrics-in-retail/?sh=61028c7150da
JPMorgan Chase, in cooperation with several U.S. retailer, is planning a broad rollout of biometric payments early next year. The step will enable shoppers to make purchases by scanning their palms or faces.

Biometric honeypots? Cryptography delivers a much better way to work (May 22, 2024)
https://www.forbes.com/sites/davidbirch/2024/05/22/biometric-honeypots-cryptography-delivers-a-much-better-way-to-work/
In El Salvador, more than five million personal records, including high-definition facial photos labelled with the individual's national ID document number (DUI), were released in a data breach. The number and nature of these records prompted speculation on social media that the breach is from the Chivo Bitcoin wallet. You may be wondering why a digital wallet operator would create a centralised honey pot of valuable personal information, especially when that information may be of considerable assistance to criminals of many varieties. If you are going to store biometric data (or a biometric template) in a central server, then it would be a good idea not to store it in a form which can be easily stolen! Surely there must be other ways to implement biometric matching.

Would face scanning technology keep Australian kids off social media? The UK regulator doubts it (June 18, 2024)
https://www.theguardian.com/media/article/2024/jun/19/would-face-scanning-technology-keep-australian-kids-off-social-media-the-uk-regulator-doubts-it
A face scanning technology used to verify people's ages online is fallible on young teenagers, Dame Melanie Dawes, the boss of the UK's online safety regulator has warned. This development throws doubt on a key method Australia's opposition believes can stop children from accessing social media.

EU biometric checks for foreign travellers delayed again (July 18, 2024)
https://www.theguardian.com/business/article/2024/jul/18/eu-biometric-checks-for-foreign-travellers-delayed-again
The date for the introduction of the EU's new entry-exit system has been pushed back again until November. This development is allaying fears of long queues at the border during the October half-term holidays.

BIOMETRIC PIONEERS: *Pong C. Yuen*

Interview conducted by Aparna Bharati, Assistant Professor in the Department of Computer Science & Engineering at Lehigh University , Bethlehem, Pennsylvania, USA

Dr. Pong C. Yuen is a Chair Professor in Computer Science at Hong Kong Baptist University (HKBU) and is currently completing a six-year term as Associate Dean (Teaching and Learning) of the school's Faculty of Science. He joined HKBU immediately after receiving his Ph.D. degree in Electrical and Electronic Engineering from the University of Hong Kong. Over the years, Yuen has also held a number of visiting professor posts, including stays at the University of Sydney, the University of Maryland at College Park, ETH Zurich, and the University of Bologna, to name a few. A general/program co-chair for a number of international conferences, including ISBA 2016, WIFS 2018, and IJCB 2021, Yuen has also directed the IAPR/IEEE Winter School on Biometrics since 2017. His honors include being named an IAPR Fellow, and receiving Natural Science Awards from the Guangdong Province and the Ministry of Education, China.

BHARATI: Professor Yuen, you have an impressive background in electrical engineering, from your Ph.D. program at the University of Hong Kong, to your leadership roles at Hong Kong Baptist University. Could you share some defining moments that shaped your journey in academia and research?

Yuen: I have been lucky that my academic and research journey has been so smooth. After obtaining my Ph.D. in 1993, I was invited to join HKBU the same year. There, my former department heads gave me sufficient support, freedom, and flexibility to conduct my research initiatives and teaching. Lastly, I have worked with outstanding Ph.D. students over the years that have formed my research team.

BHARATI: What initially drew you to biometric security and privacy, and how have your interests evolved?

Yuen: After visiting a research lab at the University of Sydney in 1996, I began working on face recognition. A year later, I participated in the NATO Advanced Studies Institute (ASI) on *Face Recognition: From Theory to Applications,* held in Stirling, Scotland, UK. At that time, I was particularly interested in the sub-space approach, which is theoretically sound, and utilized either Principal Component Analysis (PCA) to maximize variance within the data, or LDA to maximize class separability. I learned a lot about computer vision models, such as Eigenface and Fisherface, as well as face recognition, from the speakers, participants, and videos at that event. Eventually, most of my research on face recognition followed the sub-space approach.

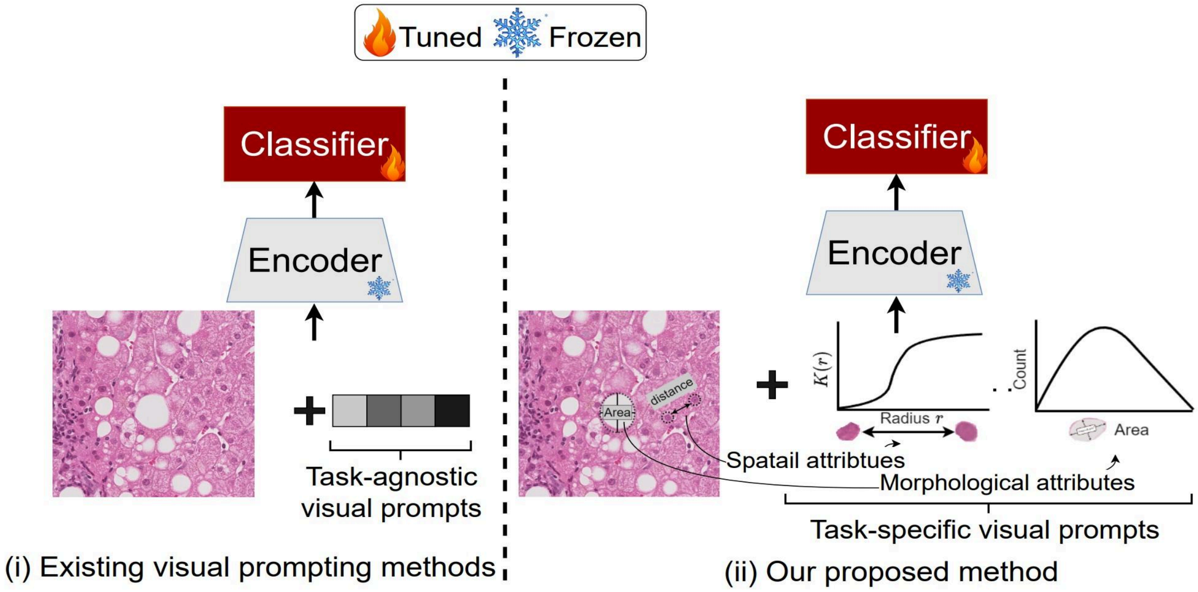
Around 2000-2001, I attended a seminar on the topic of "Cancellable Templates." I was attracted by the technical content, but also recognized the importance of security and privacy issues in developing biometrics systems. In particular, knowing our "face" biometrics are not "cancellable," like a password, so if one's biometric data is stolen from a government system, one's identity may be lost. This led me to start working on biometric template protection, and to propose some biometric cryptosystem algorithms, as well as hybrid algorithms that combine a biometric cryptosystem with a cancellable template.

When electronic payment on mobile phones became popular in China in the early 2010s, face presentation attack detection (a.k.a. face anti-spoofing) became one of the key problems to address. I have been particularly interested in 3D mask face presentation attack detections. This is a very challenging problem because a 3D face appears almost the same as the face of a real person. As such, my research group proposed employing psychological signals through photoplethysmography (PPG), or optically obtained images that can detect blood volume changes in the microvascular bed of tissue. Since face images are generally captured at a distance, we need to address face variations and noise issues. Along these lines, we have successfully developed different algorithms that have achieved promising results.

Dr. Yuen at the 2024 Biometric Winter School in China

Most recently, my group has been working on rPPG-based clinical disease monitoring in the healthcare domain.

BHARATI: Given your leadership of the Croucher Advanced Study Institutes on biometric authentication (2004), and security and privacy (2007), what key



An example of a medical AI application, this drawing shows task-agnostic visual prompts and proposed task-specific visual prompts from a 2024 paper coauthored by Yuen. (https://openaccess.thecvf.com/content/CVPR2024/papers/Yin_Prompting_Vision_Foundation_Models_for_Pathology_Image_Analysis_CVPR_2024_paper.pdf)

advancements or challenges do you see shaping the future of biometric security?

Yuen: There are two types of attacks in biometric systems: physical and digital. Many promising research results have been developed in the past to solve the problem. However, with advanced generative AI and material technologies, a very sophisticated attack can be performed at minimal cost. As such, the theme of the 2025 IAPR/IEEE Winter School on Biometrics will be “Generative AI and Foundation Models for Biometrics” (Go to https://www.comp.hkbu.edu.hk/wsb2025/lecturer.php for more information). Sixteen renowned professors will share their views and work on this topic at the event.

BHARATI: With your recent publications addressing diverse applications—from drug-target interaction prediction to pathology image analysis—how do you approach integrating biometrics into other fields, such as medical informatics?

Yuen: Clinical/medical informatics is my new research interest. My group has been working on disease prediction, medical (CT) image segmentation, pathology image analysis, and drug-target interaction, which are all common unmet clinical needs. Some researchers have been working on biometrics for healthcare because this type of data (e.g. face image) implicitly reflects one's health status. In particular, tongue diagnosis is one of the four diagnostic components in traditional Chinese medicine.

As mentioned earlier, I plan to combine rPPG signals from the face and other skin regions with other biometric information in the healthcare domain. This technique has been used successfully in sleep disorder diagnosis and monitoring. The advantage is that the system is totally non-invasive. My group is also exploring the application of these technologies to psychiatric patients.

BHARATI: How do you view the integration of AI and machine learning in biometric systems, especially regarding privacy-preserving technologies and responsible use?

Yuen: Integrations of AI and machine learning in biometrics systems have already been in place for some time. I believe its adoption will continue in the coming years.

BHARATI: You've had the opportunity to collaborate with renowned institutions worldwide. How have these sabbatical experiences influenced your research approach and shaped your perspective on global collaboration?

Yuen: I treasure all the sabbatical opportunities I have had. They offered plenty of time to freely discuss different areas with professors. Moreover, those institutions offer seminars and also welcome many other visitors. I was lucky to meet and chat with those visitors as well. In-depth discussion and understanding of problems from different perspectives is very important for academic research and can trigger new solutions to problems.

I am also very interested in learning about research culture and education systems in different countries. This has also influenced my values and research objectives.

BHARATI: In your roles as Department Head and Associate Dean, you have directly influenced the next generation of scientists. What advice would you give to young researchers entering the biometrics field?

Yuen: While I am happy to see more young researchers entering the biometrics field, I believe their interest in studies of this type should be the most crucial consideration. Young researchers should be passionate about their research topics. I understand it is hard to measure or evaluate "interest." However, if you take time to think and want to learn more about those areas whenever you are free, I think that could be your research interest.

BHARATI: What do you believe are the most pressing technical challenges in biometrics today, and which emerging innovations are the most promising to meet them?

Yuen: I would say there are three major challenges for biometric authentication: security and privacy, trustworthiness and fairness, and extreme conditions. I believe that some of these challenges can be overcome in the coming years with new AI 2.0 technology.

More importantly, person authentication is just one application for biometrics. More technical challenges need to be solved in order to deploy biometrics in other domains, such as healthcare or identity science.

BHARATI: You have contributed to a wide array of highly cited research. Could you highlight a recent project that you believe has made a significant impact, or one that you feel has the potential to transform the field?

Yuen: While I like all the projects on biometrics and clinical informatics, I am particularly interested in my rPPG project. PPG technology is a mature technology. However, rPPG (computer vision + PPG) is relatively new. We have successfully developed rPPG face presentation algorithms with very encouraging results. Since rPPG is also a non-contact and non-invasive method, it is a good choice for healthcare applications, and has been employed to estimate heart rate, blood pressure, and respiration rate. Recently, it has also been utilised to diagnose sleep disorders. If all 74 PPG biomarkers can be detected accurately from an rPPG signal, I believe there will be many potential healthcare applications.

BHARATI: As a leading figure in biometrics and AI, what is your vision for the field over the next decade, and what role do you think the IEEE Biometrics Council and similar institutions should play in achieving that vision?

Yuen: In just my personal opinion, I think biometrics research should be extended to more application domains besides personal authentication. The name of our transactions, "IEEE Transactions on Biometrics, Behavior and Identity Science," suggests that the scope has been extended to human behaviour and identity science. However, current research on these topics seems to receive less attention. One possibility is to create some competitions (with datasets) to promote research in these areas. I think another possible area is the healthcare domain.

EXPERT PERSPECTIVES: *Esteban Vázquez Fernández*

Interview conducted by **Dr. João C. Neves,** *Associate Professor, University of Beira Interior, Portugal*

Esteban Vázquez Fernández is the chief technical officer and a co-founder of Alice Biometrics, in Vigo, Spain. As a Ph.D. graduate from Universidade de Vigo. and an engineer specializing in facial recognition, he has more than 15 years of experience in advancing the use of biometrics as a secure and user-friendly solution for identity verification. His work spans multiple domains, including research, standardization, academia, technology development, and product commercialization. Prior to starting Alice Biometrics, he spent nine years with Gradiant, where, among other roles, he served as head of biometrics.

NEVES: You have had an extensive career in biometrics, working both in academia and in industry through your time at Gradiant, and more recently, as co-founder of Alice Biometrics. What initially led you to this field, and how did your perspectives on biometric technology evolve over the years?

Fernández: I began my career in the fields of image processing and computer vision. I transitioned during my doctoral thesis to facial recognition, and have continued ever since in the broader domain of biometric recognition and digital identity. The evolution of the field has been remarkable, shifting from something niche—reserved only for research projects or large corporations—to widespread adoption in everyday life across multiple sectors.
The general public's perception of the field has also changed dramatically over the last 10 to 15 years. Today, it's no surprise to anyone that biometrics are used daily to unlock phones or open online accounts. My focus has evolved from a purely technical approach to biometric recognition to a more user-centric vision, and a holistic understanding of the surrounding challenges. These challenges include data security and privacy, bias and its ethical implications, and the growing complexity of anti-spoofing techniques as fraud methods become increasingly sophisticated.

NEVES: As CTO at Alice Biometrics, what do you consider the most groundbreaking technology or innovation your team has developed? How does it stand out in the competitive field of identity verification?

Fernández: Technology is undoubtedly important, but in today’s fast-changing world—where this month’s advancements in generative AI make last month’s breakthroughs feel outdated—the most critical strength of Alice lies in the resilience and agility of our team and technology. At Alice, we’ve built our models and systems to rapidly adapt to new threats, which is crucial given the ever-evolving landscape of attacks and fraud techniques.

One of the larger issues we see in the sector is that many organizations are struggling to evolve their protective technologies at the same pace as fraudsters innovate their attack methods. At Alice, we’ve addressed this by designing systems with flexibility and continuous learning at their core. This means not only staying ahead of known threats, but also proactively preparing for the unknown to ensure that our clients can trust our solutions will remain robust and secure. In this regard, our team's ability to evolve is just as important as the technology itself.

NEVES: Biometric systems face challenges like spoofing and privacy concerns. Can you share some of the biggest problems you have faced and how you have addressed them?

Fernández: One of the biggest challenges has been achieving robust liveness detection to combat increasingly sophisticated spoofing techniques. Attackers are constantly innovating, and staying ahead requires continuous adaptation. Our solution has been to adopt a multi-layered approach that leverages both AI and domain knowledge to detect fake attempts without introducing much friction for legitimate users.

Another issue is addressing privacy concerns. Biometric data is inherently sensitive, and its misuse could have severe consequences. At Alice Biometrics, we’ve prioritized privacy by implementing encryption and secure storage practices that ensure our compliance with the General Data Protection Regulation (GDPR). Additionally, we’ve adopted principles of data minimization, which means we collect only the data strictly needed for authentication. We also offer customers clear control over how their data is used.

These efforts reflect a broader commitment to balancing security with user trust. Biometric systems must not only be resilient against external threats but also uphold the privacy and rights of the individuals they serve. This dual focus on security and ethics has been central to overcoming the biggest challenges in our work.

NEVES: What are the emerging trends in biometric technology that excite you the most? How do you envision the role of biometrics in shaping the future of digital identity?

Fernández: The world is increasingly moving toward a scenario where identity is the most valuable asset a person can possess. For example, a person's ability to prove who they are directly determines if they can access their financial and monetary resources. This marks a fundamental shift from traditional systems, where wealth was based on *what you have* (e.g., physical assets or cash), to systems where your value is tied to *who you are*. This shift places biometrics at the center of digital identity, enabling new ways to securely authenticate individuals, but also presenting significant societal challenges around identity management.

Looking ahead, I believe biometrics will play a pivotal role in bridging the physical and digital worlds, enabling seamless and secure interactions across a wide range of sectors, from financial services and healthcare to e-governance and education. However, as the importance of digital identity grows, so do the responsibilities we face as a society. We must address such critical issues as inclusivity *(ensuring biometric systems are accessible and equitable for everyone),* and privacy *(ensuring personal data is not exploited or misused).*

Ultimately, the future of biometrics will not just be about authentication but about enabling trust in a digital-first world. As these systems become more integral to our lives, they must be designed not only for efficiency and security but also to reflect the ethical and societal values that define us.

NEVES: You have transitioned from academia to technical roles and finally to leading teams at Alice Biometrics. How do you approach leadership, and what strategies have you found effective for fostering innovation without compromising development deadlines within your team?

Fernández: I don't have a lot of answers to this question. It's something I'm continually working on and iterating on as we go. Leadership is a journey, and there's always room for improvement. That said, one of the most fundamental aspects of leadership, in my view, is giving teams real ownership over their work. When people feel responsible for their contributions and outcomes, they're more engaged and committed to achieving success. My role is to create an environment where this sense of ownership can thrive—a space where collaboration, accountability, and creativity are encouraged.

Another key principle is ensuring that the team enjoys the process. Innovation often stems from passion and curiosity, and if the team finds joy in their work, they'll be more likely to think creatively and push boundaries. A positive and collaborative atmosphere is critical for maintaining morale, especially when facing tight deadlines or complex challenges.

A piece of advice I always try to follow is to surround yourself with people who are smarter than you in their respective areas. By building a team with diverse expertise and perspectives, you create a fertile ground for new ideas and solutions. My job is not to have all the answers but to empower my team to bring their best ideas forward, and to support them in turning those ideas into reality.

Finally, I emphasize continuous iteration. Leadership isn't static; it's about adapting and refining approaches based on feedback and the evolving needs of the team. Staying open to learning, even from mistakes, is essential to fostering innovation without compromising on deadlines or deliverables. It's about striking the right balance between pushing for excellence and ensuring sustainable and enjoyable processes for everyone involved.

NEVES:: Considering all your experience in biometrics, what advice would you give to young students pursuing a career in this field?

Fernández: My advice is to approach the idea of identity as a whole, not just as biometrics in isolation. Biometrics is an important piece of the puzzle, but its true potential is unlocked when combined with the diverse factors that make up our complete digital identity. This includes how we interact with our devices, our interests, search patterns, behavioural habits, and more. Integrating these elements, we move beyond merely digitized identity to a truly holistic digital identity.

In this broader framework, biometrics plays a fundamental role, particularly in establishing trust through mechanisms like liveness detection. However, aspiring professionals should aim to pursue a broader vision of identity, considering how biometrics integrates into a larger system of trust and user experience.

Equally important is understanding the user. Study the user deeply—their problems, needs, and behaviours. The technical solution is often the simpler part of the equation. Designing a solution that works seamlessly with the user is where the real challenge lies. In biometrics, the interaction between the user and the system is critical because it's often the primary bridge between the physical and digital worlds.

Ultimately, focusing on the user's experience and needs will help you develop solutions that are not only innovative, but also intuitive and impactful. Building trust in the interaction and creating a seamless entry point into the digital realm will always be fundamental to biometrics—and to the broader concept of identity.

RESEARCHER ON THE RISE: *Pramuditha Perera*

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

Pramuditha Perera is an Applied Scientist in the AWS AI Labs research group, New York, NY, USA. He completed his Ph.D. in Electrical and Computer Engineering at Johns Hopkins University, USA, in 2020. Prior to beginning work on his doctorate, he did his bachelor's studies in Electrical and Electronic Engineering at the University of Peradeniya in Sri Lanka, and his master's work in Electrical and Computer Engineering at Rutgers University, USA, graduating in 2014 and 2018, respectively. Perera's current research interests include computer vision, machine learning and vision-language models. His work "In2I : Unsupervised Multi-Image-to-Image Translation Using Generative Adversarial Networks" received a Best Student Paper Award at the 2018 International Conference on Pattern Recognition.

TOLOSANA: You have published quite a bit in top conferences and journals during your Ph.D. What are the strategies and key factors that have encouraged this level of productivity?

Perera: One of the key strategies is to read lots of related papers. Reading papers not only kept me up-to-date with the state of the art, but also gave me the chance to think about the relative weaknesses of each method, and to think about potential improvements. Whenever I used to read papers, I would think how a method described by the writers would apply to the problem I was trying to solve.

Another method was to expand the scope of my research by exploring problems similar to my topic. For example, at the start of my thesis, I was focused only on the specific topic of active authentication on mobile devices. Then, I realized that this is a sub-problem of one-class classification. This allowed me to tackle a more generic problem that had better scope for publication than active authentication. I also believe that brainstorming with my advisor, Professor Vishal Patel, was a reason why I was very productive. These discussions made these publications possible.

TOLOSANA: You did your B.Sc.in your home country (Sri Lanka), and then completed the M.Sc. and Ph.D. abroad (USA). Was it difficult for you to move to another country? And, what can you suggest on this topic to young aspiring researchers?

Perera’s Ph.D. advisor, Dr. Vishal Patel, Associate Professor of Electrical and Computer Engineering at Johns Hopkins University.

Perera: The transition wasn’t exactly smooth. I thought I had a solid foundation in technical matters, but there was an obvious gap in terms of techniques used. For example, when I moved in 2015, deep learning had already been a talking point in the U.S. for a couple of years. This wasn’t something I was exposed to as a student in Sri Lanka at the time. It meant that I had to learn new techniques in a short span of time. However, I had already started reading papers and had presented at a few lower tier conferences. This exposure encouraged me to keep up with the changing technology. I think if aspiring researchers develop a habit of reading papers during their bachelor's studies, and attempting small scale research, it would help them bridge the gap in the same way.

TOLOSANA: You did summer internships at Amazon Web Services (2018) and Adobe (2019) during your Ph.D. How do you rate the importance of internships and collaborations with other institutions for a Ph.D. student?

Perera: Both of the internships you mentioned helped a lot to shape my career. Industrial experience is very different from research in an academic setting. Companies had their own developer tools, developer practices and unique organizational cultures. Having a glimpse of this made me realize that I would prefer a career in industry, and helped me prepare for that career. It also opened up the opportunity to work with several researchers outside the university. I would highly recommend an internship for any student who wants to pursue a career in industry – or who are unsure about it.

TOLOSANA: You have studied at two prestigious academic institutions, Rutgers University and JHU, and now you work for a big company (Amazon). What are the similarities and main differences? And, what takeaway messages can you give to young researchers?

Perera: Both Rutgers and Johns Hopkins had highly qualified faculty and curriculum, but Johns Hopkins had several faculty working specifically on computer vision and machine learning. This meant the school offered more courses on these specific topics, and there were many other graduate students working in these areas. JHU also had a rigorous qualifying process that forced me to take diverse courses outside my concentration. Looking back, I see both these factors as positives. One thing I like about Amazon is that they employ a large body of highly qualified scientists working on machine learning across the country. This opens up the possibility of finding scientists with varying areas of expertise, and easily being able to collaborate with them. I would suggest young scientists find opportunities that allow them to collaborate more. It leads to better research and personal growth.

TOLOSANA: You have published papers at top conferences on computer vision. However, your background is in electrical and electronic engineering. How was the journey from this background to computer engineering? And, how does your background influence your daily life at AWS AI Labs?

Perera: Signal processing was one of my favorite subject areas in electrical and electronic engineering. When I was doing my bachelors, we did a project in signal processing where we analyzed images and videos for abnormal behavior. This was my first exposure to computer vision. From then onwards, I wanted to learn more about computer vision and machine learning, and this is why I made the transition to computer engineering. In my experience, both machine learning and signal processing have many common and inter-related concepts. Therefore, I get to use my understanding and knowledge of signal processing on a day-to-day basis.

TOLOSANA: During your Ph.D. you worked extensively with one-class classification problems. Do you think this approach can be implemented in novel scenarios that have not been considered so far?

Perera: One-class classification is already used in anomaly detection applications in industry. For example, I was involved with a time series anomaly detection project at AWS (Lookout for Metrics), and there is also an AWS service that specializes in image-based anomaly detection (Lookout for Vision). I believe there is scope for a video-based anomaly detection product.

TOLOSANA: What is the most valuable expertise you have gained during your Ph.D. studies? And, what would you change if you could go back?

Perera: Apart from the technical expertise, the most valuable expertise I've developed is the ability to continually keep learning. Machine learning is a fast-evolving field and requires me to keep in touch with ever changing techniques. Since graduation, I've explored machine learning applications in time series, and language modeling, in addition to computer vision. It is vital for my role to keep updating myself and explore more. This is a skill I developed during my Ph.D. studies. If I could go back, I think I would try to better utilize course offerings at the University and take more diverse courses.

TOLOSANA: In your opinion, what are the key differences between academia and industry when developing research projects? And, which aspects of academia can be beneficial to research?

Perera: One key difference I see is that industrial research is more focused on end applications. Even pure research projects are expected to have an impact on products, at least in the long run. This is especially the case at Amazon, where our research is geared towards increasing customer satisfaction. I don't believe that academic projects necessarily have to take the same path. I think both industrial and academic projects have their own merits. However, I do believe academic projects would have a broader impact if they could have practical end use cases.

TOLOSANA: If you had extra time at school, what other topics might you have wanted to pursue?

Perera: Machine learning models, both in vision and language, have developed rapidly in recent years. However, not much attention has been given to low resource languages, such as Sinhala, my native language. Therefore, ML applications cannot be deployed for communities that use these languages. I would like to explore ways to support machine learning in low resource languages through knowledge transfer and distillation.

LECTURE NOTES: *Deepfakes and Adversarial Threats to Automatic Speaker Verification, Countermeasures and Human Listeners*

By Massimiliano Todisco, Professor of Audio and Speech Technologies, EURECOM, France

Massimiliano Todisco, a professor of audio and speech technologies at EURECOM in France, is best known for his contributions to fake audio detection through the invention of *constant Q cepstral coefficient*. These features were widely used in speech spoofing detection before the rise of deep learning, and his work earned him the ISCA 2020 Award for the best article in *Computer Speech and Language* for the quinquennium 2015-2019. His research is dedicated to advancing voice biometrics, deepfake detection, and privacy preservation. Currently, his projects include adversarial learning strategies, and leveraging generative AI to improve both the transparency and effectiveness of audio and speech technologies. Todisco is currently co-organising two international challenges, the ASVspoof and VoicePrivacy, and he serves as an Associate Editor for the *IEEE Transactions on Biometrics, Behavior, and Identity Science (T-BIOM)*.

The rapid evolution of voice cloning technologies has revolutionised diverse applications and offered significant advancements, from empowering individuals with speech impairments to enhancing human-machine interactions through virtual assistants [1,2,3]. These new technologies are also transforming creative industries like gaming and dubbing. By analysing voice characteristics, these systems verify users in a manner that is both convenient and non-invasive. However, these benefits come with an alarming downside. Their misuse poses severe challenges to security systems, particularly to Automatic Speaker Verification (ASV) [4] systems that play a critical role in secure authentication for applications ranging from banking to personal devices. This reliance on voice as a biometric factor has made ASV systems a prime target for attackers. Critical vulnerabilities have been exposed through the rising number of spoofing attacks, where cloned voices mimic legitimate users, and adversarial attacks, where subtle perturbations deceive ASV systems.

What makes this problem even more pressing is that these voice cloning technologies are not limited to deceiving machines. They can also fool humans [5]. Advanced systems can now generate synthetic audio that is nearly indistinguishable from real speech [6], even to trained listeners. Moreover, voice cloning tools are widely available online, with many platforms offering accessible interfaces that require no expertise in audio engineering. This popularisation of voice cloning technology means that malicious actors, even those with minimal technical skills, can easily exploit these tools to impersonate individuals, commit fraud, or spread misinformation.

This lecture examines the current state of ASV and Countermeasure (CM) systems, focusing on the adversarial challenges posed by two recent groundbreaking attack models. By exploring their mechanisms, impacts, and implications, we aim to shed light on the vulnerabilities of ASV systems, and the pressing need for innovative secure voice-based technology solutions in an era of rapidly advancing and widely accessible voice cloning threats.

Deepfakes and Presentation Attacks: A Growing Threat to ASV

As mentioned above, ASV authentication systems face significant threats from deepfake and presentation attacks. Both attack types undermine ASV security and human trust in voice-based interactions, albeit with slightly different objectives.

Deepfakes involve the creation of highly realistic synthetic audio that mimics a target speaker's voice. Techniques like Voice Conversion (VC) [7] and Text-to-Speech (TTS) [8] synthesis enable attackers to replicate a speaker's vocal characteristics with astounding accuracy. Alarmingly, today's technologies require only a few seconds of audio from the victim to generate convincing deepfake voices.

These attacks can extend beyond ASV systems to pose a significant risk to human perception. For example, attackers can impersonate individuals in phishing scams or create speeches to spread misinformation. The increasing inability of humans to consistently distinguish between real and synthetic voices makes deepfakes a powerful tool for fraud, manipulation, and reputational harm.

Presentation attacks [9], or spoofing, target ASV systems through manipulated audio designed to bypass authentication. These attacks exploit voice cloning technologies to

mimic legitimate users and compromise ASV security. Spoofing is particularly dangerous in critical applications, such as biometric authentication for banking or personal devices, where successful attacks can lead to unauthorised access and significant harm.

The dual threat of deepfakes and presentation attacks lie in their ability to deceive both humans and machines. While deepfakes target trust in voice communication, spoofing directly undermines the reliability of ASV systems.

Adversarial Attacks: A New Frontier in ASV and CM Threats

Adversarial attacks [10] add an extra threat layer to ASV and CM systems as, unlike presentation attacks or deepfakes, they manipulate the audio signal itself. Attackers exploit specific vulnerabilities in ASV and CM algorithms by introducing subtle perturbations designed to remain imperceptible to human listeners, while significantly degrading performance. Adversarial attacks target the decision-making processes of these systems to deceive classification or verification mechanisms. The result is to render ASV incapable of distinguishing between bona fide [(1)] and spoofed speech [9] or to cause misclassification of legitimate users. Advanced adversarial attacks are particularly effective when they adapt the noise to real-world scenarios, such as audio transmitted over communication channels where compression and noise are unavoidable.

Current Landscape of Defences: Countermeasures for Robust Speaker Verification

To address these threats, researchers have developed various countermeasures to enhance the robustness of ASV systems. Initiatives, such as the ASVspoof challenges series [11], play a critical role in promoting the development and benchmarking of these defences. By providing a standardised framework for evaluating countermeasures against diverse attack scenarios, ASVspoof fosters innovation and collaboration within the research community. Despite significant progress though, many countermeasures struggle to effectively generalise to unseen attack types or conditions. This limitation often stems from the evolving nature of voice cloning and adversarial techniques, the complexity of real-world transmission environments, and the inherent variability in human speech.

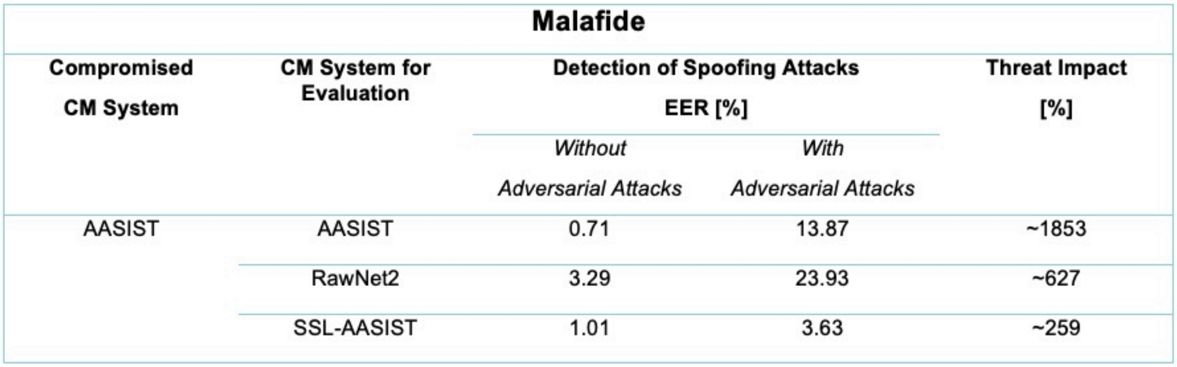
Advanced Adversarial Techniques: Malafide and Malacopula [(2)]

Malafide [12] and Malacopula [13] are two groundbreaking adversarial techniques that exploit weaknesses in existing defense systems through tailored perturbations. This makes them particularly robust in practical conditions. Malafide demonstrates a significant threat to anti-spoofing countermeasure (CM) systems used to secure voice biometrics. By employing a linear time-invariant filter, this strategy introduces convolutive noise that deceives systems into misclassifying spoofed speech as bona fide. Unlike traditional methods that rely on utterance-specific noise, Malafide is adapted to specific attack scenarios, enabling real-time application and revealing critical vulnerabilities in widely used CM systems. Its key features include:

- **Universal Applicability**: Malafide's versatile filter is pre-trained and operates independently of the speech's duration or content.
- **Efficient Deployment:** It is computationally lightweight and acts as a post-processing filter, making it applicable for real-time application.
- **Cross-System Transferability**: The generated perturbations generalise across different CM architectures and utterances.
- **Human Perception:** Added perturbations resemble conventional audio equalisation or reverberation effects, making it difficult to detect them as malicious.

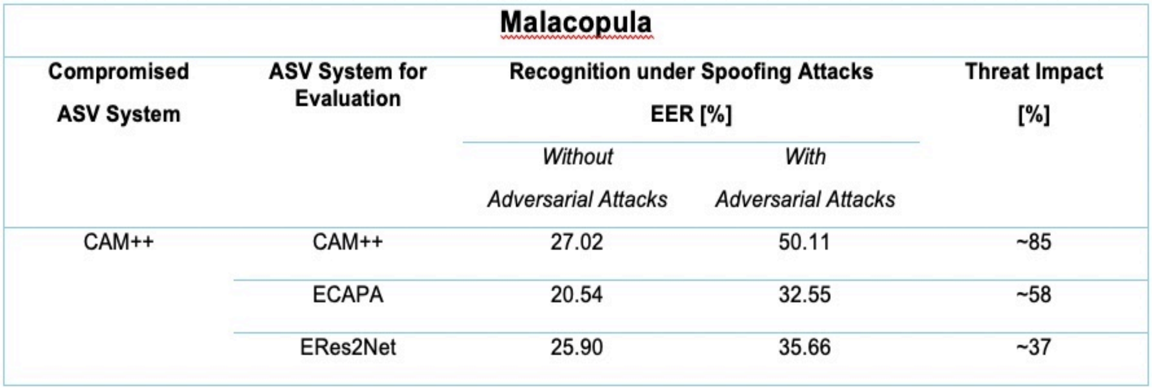
Building on Malafide, Malacopula employs a generalised Hammerstein model [14], combining non-linear transformations with convolutive filtering. This approach allows for more complex manipulation of the audio signal, targeting amplitude, phase, and frequency components to create perturbations that are both highly effective and difficult to detect. Malacopula is specifically tailored for speaker- and attack-specific scenarios, optimising its perturbations to bring spoofed speech and the target speaker closer together. This capability makes it uniquely effective at deceiving ASV systems under spoofing attacks, even when advanced countermeasures are employed. Like Malafide, Malacopula excels in codec-based communication channels by introducing perturbations that remain resilient to compression artefacts. Its key features include:

- **Attack Optimization***:* Malacopula minimises the cosine distance between the embeddings of processed spoofed speech with adversarial noise and bona fide speech, ensuring precise deception.
- **Cross-System Transferability***:* The perturbations generalise across different ASV architectures and utterances.



Malafide				
Compromised CM System	CM System for Evaluation	Detection of Spoofing Attacks EER [%]		Threat Impact [%]
		Without Adversarial Attacks	*With Adversarial Attacks*	
AASIST	AASIST	0.71	13.87	~1853
	RawNet2	3.29	23.93	~627
	SSL-AASIST	1.01	3.63	~259

Table 1: CM systems experience dramatic EER increases, with threats rising up to 1853%. This demonstrates Malafide's ability to render CMs highly ineffective.



Malacopula				
Compromised ASV System	ASV System for Evaluation	Recognition under Spoofing Attacks EER [%]		Threat Impact [%]
		Without Adversarial Attacks	*With Adversarial Attacks*	
CAM++	CAM++	27.02	50.11	~85
	ECAPA	20.54	32.55	~58
	ERes2Net	25.90	35.66	~37

Table 2: ASV systems show EER increases up to 85%, highlighting Malacopula's precision in embedding manipulation.

- **Real-World Effectiveness***:* Malacopula's perturbations remain effective after transmission and compression, making it highly practical for telephony use cases.
- **Lightweight Design***:* Despite its complexity, Malacopula is efficient and deployable in real-time scenarios.

These innovations uniquely position Malafide and Malacopula to challenge ASV and CM systems, particularly in practical scenarios involving codec-compressed audio. The perturbations they introduce resemble artefacts caused by compression and transmission, ensuring the attack remains effective even after codec processing. This property makes Malafide highly practical and dangerous for telephony and VoIP scenarios.

Impact of Malafide and Malacopula on ASV and CM Systlems

Results from evaluations on the ASVspoof 2019 LA database [15] demonstrate the significant impact of Malafide and Malacopula on ASV and CM systems. Both methods have proven their ability to significantly degrade the performance of even state-of-the-art ASV, such as CAM++

[16], ECAPA [17], and ERes2Net [18], and CM architectures, such as RawNet2 [19], AASIST [20] and SSL-AASIST [21]. Tables 1 and 2 above summarise the impact of Malafide and Malacopula on ASV and CM systems.

Conclusions and Future Directions

The results of Malafide and Malacopula as documented above highlight critical vulnerabilities in ASV and CM systems. The evolving landscape of adversarial attacks demands proactive and innovative approaches to ensure the security of ASV and CM systems. As attacks like Malafide and Malacopula demonstrate, the combination of codec resilience, lightweight design, and practical deployment poses a significant challenge to current defences.

These factors highlight the need for adaptive solutions capable of addressing a wide range of attack scenarios. The integration of adversarial training, neural codec-specific defences, and self-supervised learning methods offers promising avenues for overcoming these obstacles. Yet, the rapid evolution of attack methods underscores that the security of ASV and CM systems remains an ongoing challenge, one that requires continuous innovation. We must bear in mind that the dual goal is to ensure that these systems are not only resilient to advanced attacks, but also maintain their reliability and usability in diverse real-world applications.

Endnotes

1) *Bona fide* is Latin for "good faith." It signifies sincerity, authenticity, or genuine intention without deceit or fraud.
2) *Mala fide* is Latin for “in bad faith.” It signifies actions or intentions that are deceitful, dishonest, or intended to mislead or harm. *Mala copula* is Latin for “bad connection” or “bad union.” It signifies an undesirable or improper association between elements.

References

1) S.C. Ramu, D. Saxena and V. Mali, "A Survey on Voice Cloning and Automated Video Dubbing Systems," *International Conference on Wireless Communications Signal Processing and Networking (WiSPNET)*, Chennai, India, 2024, pp. 1-5. doi: 10.1109/WiSPNET61464.2024.10532876.
2) M.A.M. Ahmed, K.A. Elghamrawy and Z.A. El Haliem Taha, "(Voick): Enhancing Accessibility in Audiobooks Through Voice Cloning Technology," *6th International Conference on Computing and Informatics (ICCI)*, New Cairo - Cairo, Egypt, 2024, pp. 46-52, doi: 10.1109/ICCI61671.2024.10485044.
3) A. Pérez, G.G. Díaz-Munío, A. Giménez, J.A. Silvestre-Cerdà, A. Sanchis, J. Civera, M. Jiménez, C. Turró, and A. Juan, “Towards Cross-lingual Voice Cloning in Higher Education,” *Engineering Applications of Artificial Intelligence*, Volume 105, 2021, 104413, ISSN 0952-1976.

4) M. Jakubec, R. Jarina, E. Lieskovska, and P. Kasak, “Deep Speaker Embeddings for Speaker Verification: Review and Experimental Comparison,” *Engineering Applications of Artificial Intelligence*, Volume 127, Part A 2024, 107232, ISSN 0952-1976.
5) M. Krzysztof, S. Zaporowski, and A. Czyżewski. "Comparison of the Ability off Neural Network Model and Humans to Detect a Cloned Voice." *Electronics* 12.21 (2023): 4458.
6) H-W. Yoon et al., "Enhancing Multilingual TTS with Voice Conversion Based Data Augmentation and Posterior Embedding," *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP),* Seoul, Korea 2024, pp. 12186-12190, doi: 10.1109/ICASSP48485.2024.10448471.
7) N. Guo, J. Wei, Y. Li, W. Lu, J. Tao, “Zero-shot voice conversion based on feature disentanglement,” *Speech Communication*, Volume 165, 2024, 103143, ISSN 0167-6393.
8) X. Tan et al., "NaturalSpeech: End-to-End Text-to-Speech Synthesis With Human-Level Quality," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 46, no. 6, pp. 4234-4245, June 2024, doi: 10.1109/TPAMI.2024.3356232.
9) *ISO/IEC 30107-1:2023. Information Technology — Biometric Presentation Attack Detection, Part 1: Framework*, Published, Edition 2, 2023.
10) A. Kurakin, et al. "Adversarial Attacks and Defences Competition," *The NIPS '17 Competition: Building Intelligent Systems*. Springer International Publishing, 2018.
11) X. Wang, H. Delgado, H. Tak, J. Jung, H. Shim, M. Todisco, I. Kukanov, X. Liu, M. Sahidullah, T. Kinnunen, N. Evans, K.A. Lee, and J. Yamagishi, “ASVspoof 5: Crowdsourced Speech Data, Deepfakes, and Adversarial Attacks at Scale,” *ASVspoof Workshop 2024*, 31 August 2024, Kos, Greece.
12) M. Panariello, W. Ge, H. Tak, M. Todisco and N. Evans, “Malafide: A Novel Adversarial Convolutive Noise Attack against deepfake and spoofing Detection Systems,” *INTERSPEECH 2023*, 20-24 August 2023, Dublin, Ireland.
13) M. Todisco, M. Panariello, X. Wang, H. Delgado, K.A. Lee, and N. Evans, “Malacopula: Adversarial automatic Speaker Verification Attacks using a Neural-based Generalised Hammerstein Model,” *ASVspoof Workshop 2024*, 31 August 2024, Kos, Greece.
14) S. Grimm and J. Freudenberger, “Hybrid Volterra and Hammerstein Modelling of Nonlinear Acoustic Systems,” in *Fortschritte der Akustik: DAGA 2016.*
15) M. Todisco, X. Wang et al., “ASVspoof 2019: Future Horizons in Spoofed and Fake Audio Detection,” in *Proceedings of Interspeech,* 2019.
16) H. Tak, J. Patino et al., “End-to-end Anti-spoofing with RawNet2,” in *Proceedings of the International Conference on Acoustics, Speech, and Signal Processing (ICASSP*) 2021.
17) J-w. Jung, H.S. Heo et al., “AASIST: Audio Anti-spoofing using Integrated Spectro-temporal Graph Attention

Networks," in *Proceedings of the International Conference on Acoustics, Speech, and Signal Processing (ICASSP*), 2022.

18) H. Tak, M. Todisco et al., "Automatic Speaker Verification Spoofing and Deepfake Detection using wav2vec 2.0 and Data Augmentation," in *Proceedings of the. Speaker Odyssey Workshop,* 2022.
19) H. Wang, S. Zheng, Y. Chen, L. Cheng, and Q. Chen, "CAM++: A Fast and Efficient Network for Speaker Verification using Context-aware Masking," in *Proceedings of INTERSPEECH 2023*, 2023.
20) B. Desplanques, J. Thienpondt, and K. Demuynck, "ECAPA-TDNN: Emphasized Channel Attention, Propagation and Aggregation in TDNN based Speaker Verification," in *Proceeding of INTERSPEECH 2020.*
21) Y. Chen et al., "ERes2NetV2: Boosting short-duration speaker verification performance with computational efficiency," in *Proceedings of INTERSPEECH 2024.*

NOTED IN THE LITERATURE

Spatio-Temporal Dual-Attention Transformer for Time-Series Behavioral Biometrics

A summary of an article that appeared in IEEE Transactions on Biometrics, Behavior, and Identity Science in October, 2024, as prepared by its authors Kim-Ngan Nguyen, Sanka Rasnayaka, Sandareka Wickramanayake, Dulani Meedeniya, Sanjay Saha, and Terence Sim

INTRODUCTION

Recent advancements in mobile technology have enabled people to easily carry out crucial tasks, such as communication, finance, and healthcare, via their smartphones. With these advances come the need for secure, yet user-friendly, authentication methods. One-time/session-based authentication systems—including knowledge-based authentication methods that utilize pin codes or passwords, or physiological biometrics using fingerprints or faces—require user involvement that can reduce the ease of use. Continuous Authentication (CA) offers a solution by verifying users based on their behavioral patterns, like keystrokes and swipes, as they use a device. Additionally, the integration of affordable IMU sensors in most smartphones today also enhances CA by providing additional data for more accurate authentication. In this paper, we present BehaveFormer [1], a framework designed for behavioral biometric-based authentication for multisensory, multichannel time-series data. Extensive experiments show that BehaveFormer outperforms existing models by a large margin.

PROPOSED METHOD

The BehaveFormer framework, as shown in Figure 1, uses various time-series behavioral biometrics, such as keystroke, swipe, and IMU data (accelerometer, magnetometer, and gyroscope data), either individually or combined, to authenticate mobile device users. Each behavioral biometric utilizes single or multiple sensors, and each sensor, such as an accelerometer, consists of multi-channel time-series data. After preprocessing and extracting features from each biometric, we use a novel transformer called a Spatio-Temporal Dual Attention Transformer (STDAT) to learn the discriminative features over time and across channels. Each STDAT utilizes a Gaussian Range Encoder for positional encoding, a dual attention block comprising two Multi-Head Attention (MHA) modules—a Temporal-MHA that analyzes patterns over time, and a Channel-MHA that analyzes across channels—and a Multi-scale 2D Convolution Neural Network (M2D-CNN), followed by a fully connected network for final embeddings. This dual attention mechanism improves the extraction of precise user-specific behavioral patterns from time-series data. BehaveFormer employs a Triplet Loss function to ensure that embeddings from the same user are closely clustered, while those from different users remain distinct.

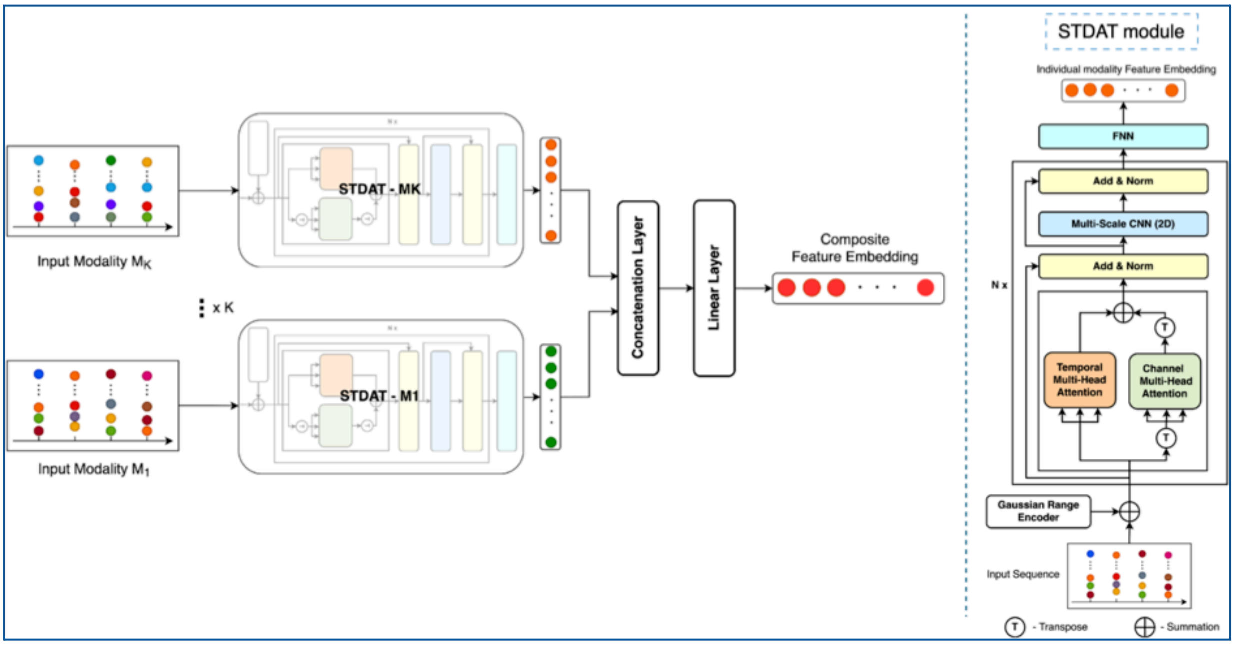
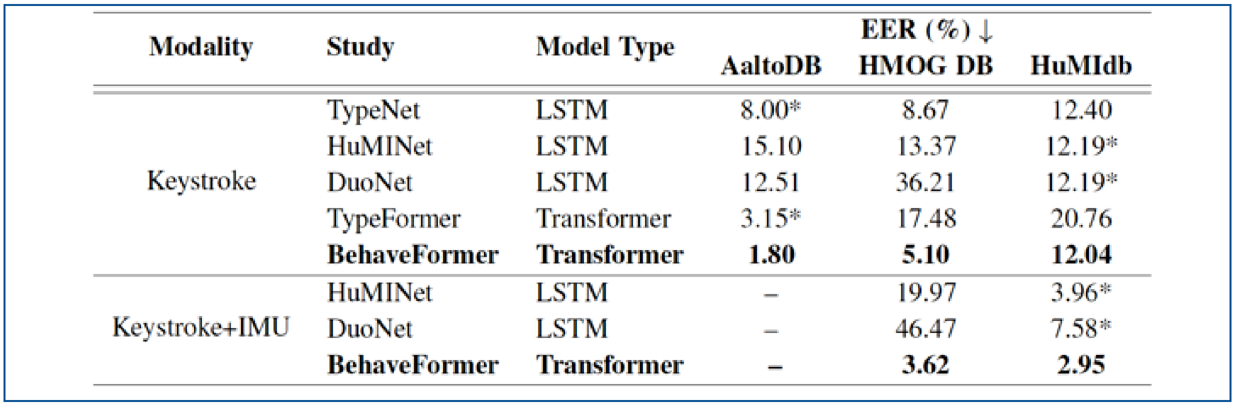


Figure 1. (Left) The overview of BehaveFormer; (Right) Spatio-Temporal Dual Attention Transformer (STDAT) module.

RESULTS

We evaluate the models using zero-effort adversaries, where imposters have no access to genuine user data. The models are trained on one set of users and tested on a different set. Both keystroke-based and swipe-based models followed an enrollment-verification protocol. For each test user, a portion of the extracted data is used for enrollment and the rest for verification. During evaluation, other users acted as imposters, and performance metrics were averaged across all users. User authentication involves comparing the enrollment feature embedding with a verification embedding. If the distance between them is below a threshold, it indicates a genuine user; otherwise, it indicates an imposter. We compare the model performance using both Equal Error Rate (EER) and the CA metrics of usability, TCR, FRWI, and FAWI [2].

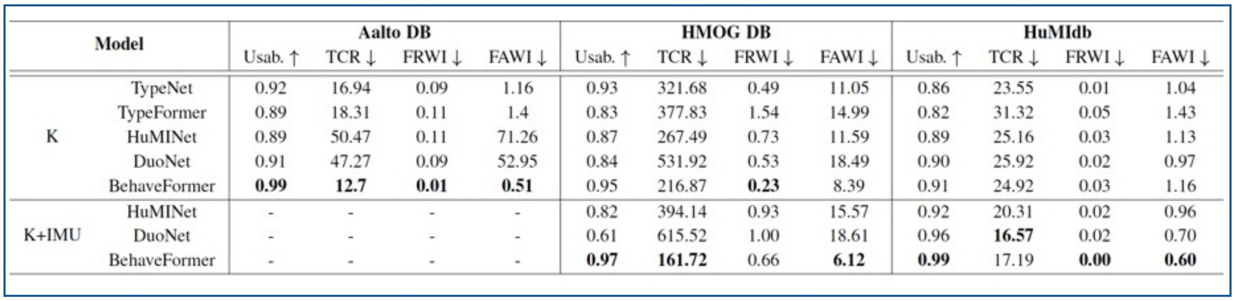


Modality	Study	Model Type	EER (%) ↓		
			AaltoDB	HMOG DB	HuMIdb
Keystroke	TypeNet	LSTM	8.00*	8.67	12.40
	HuMINet	LSTM	15.10	13.37	12.19*
	DuoNet	LSTM	12.51	36.21	12.19*
	TypeFormer	Transformer	3.15*	17.48	20.76
	BehaveFormer	**Transformer**	**1.80**	**5.10**	**12.04**
Keystroke+IMU	HuMINet	LSTM	–	19.97	3.96*
	DuoNet	LSTM	–	46.47	7.58*
	BehaveFormer	**Transformer**	**–**	**3.62**	**2.95**

Table 1. Comparison of BehaveFormer with SOTA keystroke dynamics models. The top five rows represent models trained on keystrokes only. The bottom three rows are models trained on keystrokes and IMU data. Results taken from the respective original papers are marked by an asterisk (*); the others are from our implementations of the existing models.
===

Keystroke Dynamics: BehaveFormer was evaluated across multiple datasets with two variants: (1) using only keystroke data and (2) using both keystroke and IMU data. Results (see Tables 1 above and 2 on the next page) showed that BehaveFormer consistently achieved high usability and low EER across all datasets, with the version using both keystroke and IMU outperforming the keystroke-only version. This indicates that IMU data improved feature discrimination.

Swipe Dynamics: BehaveFormer was evaluated with either swipe data (scroll down/scroll up) or swipe with IMU data. Table 4 shows the performance comparison with baseline methods, showing competitive usability and EER for the swipe-only model. Combining swipe and IMU data significantly improved EER, indicating that integrating IMU data enhances the discriminativeness of the learned feature embeddings.

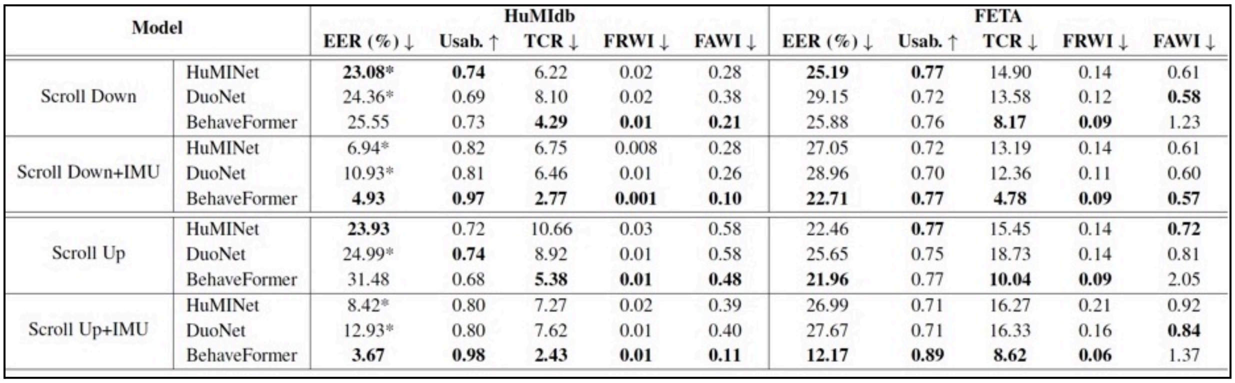


Model		Aalto DB				HMOG DB				HuMIdb			
		Usab. ↑	TCR ↓	FRWI ↓	FAWI ↓	Usab. ↑	TCR ↓	FRWI ↓	FAWI ↓	Usab. ↑	TCR ↓	FRWI ↓	FAWI ↓
K	TypeNet	0.92	16.94	0.09	1.16	0.93	321.68	0.49	11.05	0.86	23.55	0.01	1.04
	TypeFormer	0.89	18.31	0.11	1.4	0.83	377.83	1.54	14.99	0.82	31.32	0.05	1.43
	HuMINet	0.89	50.47	0.11	71.26	0.87	267.49	0.73	11.59	0.89	25.16	0.03	1.13
	DuoNet	0.91	47.27	0.09	52.95	0.84	531.92	0.53	18.49	0.90	25.92	0.02	0.97
	BehaveFormer	**0.99**	**12.7**	**0.01**	**0.51**	0.95	216.87	**0.23**	8.39	0.91	24.92	0.03	1.16
K+IMU	HuMINet	-	-	-	-	0.82	394.14	0.93	15.57	0.92	20.31	0.02	0.96
	DuoNet	-	-	-	-	0.61	615.52	1.00	18.61	0.96	**16.57**	0.02	0.70
	BehaveFormer	-	-	-	-	**0.97**	**161.72**	0.66	**6.12**	**0.99**	17.19	**0.00**	**0.60**

Table 2. Evaluation of keystroke dynamics with CA evaluation metrics. The reported metrics are Usability (as a fraction), TCR (in seconds), and FRWI and FAWI (in minutes). The best result for each dataset for each metric is bolded.

===

Transfer Learning: To address small dataset limitations, we compared a BehaveFormer model trained from scratch on HMOG with one pre-trained on Aalto DB and fine-tuned on HMOG. The trained-from-scratch model achieved an EER of 5.10%, while the transfer learning model achieved 4.48%, a 12.16% improvement. Both models had a usability score of 0.95, highlighting transfer learning's effectiveness in boosting performance with limited data.



Model		HuMIdb					FETA				
		EER (%) ↓	Usab. ↑	TCR ↓	FRWI ↓	FAWI ↓	EER (%) ↓	Usab. ↑	TCR ↓	FRWI ↓	FAWI ↓
Scroll Down	HuMINet	**23.08***	**0.74**	6.22	0.02	0.28	**25.19**	**0.77**	14.90	0.14	0.61
	DuoNet	24.36*	0.69	8.10	0.02	0.38	29.15	0.72	13.58	0.12	**0.58**
	BehaveFormer	25.55	0.73	**4.29**	**0.01**	**0.21**	25.88	0.76	**8.17**	**0.09**	1.23
Scroll Down+IMU	HuMINet	6.94*	0.82	6.75	0.008	0.28	27.05	0.72	13.19	0.14	0.61
	DuoNet	10.93*	0.81	6.46	0.01	0.26	28.96	0.70	12.36	0.11	0.60
	BehaveFormer	**4.93**	**0.97**	**2.77**	**0.001**	**0.10**	**22.71**	**0.77**	**4.78**	**0.09**	**0.57**
Scroll Up	HuMINet	**23.93**	0.72	10.66	0.03	0.58	22.46	**0.77**	15.45	0.14	**0.72**
	DuoNet	24.99*	**0.74**	8.92	0.01	0.58	25.65	0.75	18.73	0.14	0.81
	BehaveFormer	31.48	0.68	**5.38**	**0.01**	**0.48**	**21.96**	0.77	**10.04**	**0.09**	2.05
Scroll Up+IMU	HuMINet	8.42*	0.80	7.27	0.02	0.39	26.99	0.71	16.27	0.21	0.92
	DuoNet	12.93*	0.80	7.62	0.01	0.40	27.67	0.71	16.33	0.16	**0.84**
	BehaveFormer	**3.67**	**0.98**	**2.43**	**0.01**	**0.11**	**12.17**	**0.89**	**8.62**	**0.06**	1.37

Table 3: Evaluation of scroll down/scroll up with EER and CA evaluation metrics. The reported metrics are EER (%), Usability (fraction), TCR (seconds), FRWI and FAWI (minutes). The best result for each dataset for each metric is highlighted in bold.

CONCLUSION

This paper introduced BehaveFormer, a framework that utilizes multi-modality data to improve the accuracy and reliability of behavioral-based biometric CA systems. BehaveFormer comprises multiple STDATs, each capturing time and channel axis features for a modality. Extensive experiments on four publicly available datasets show that BehaveFormer outperforms SOTA CA systems in both keystrokes and swipe dynamics.

Incorporating IMU data significantly enhances the accuracy of both behavioral biometrics. BehaveFormer also addresses the limitations of small datasets using transfer learning by making it adaptable to various multi-sensor time-series scenarios. In future work, we will extend BehaveFormer to other behavioral biometrics and applications, such as wearable sensors and human activity recognition in order to explore challenges like cross-device compatibility, privacy, and user acceptance.

REFERENCES

1) D. Senarath, S. Tharinda, M. Vishvajith, S. Rasnayaka, S. Wickramanayake and D. Meedeniya, "BehaveFormer: A Framework with Spatio-Temporal Dual Attention Transformers for IMU-enhanced Keystroke Dynamics," *IEEE International Joint Conference on Biometrics (IJCB*), Ljubljana, Slovenia, 2023, pp. 1-9, DOI: https://doi.org/10.1109/IJCB57857.2023.10448997.
2) T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, “Continuous Verification using Multimodal Biometrics,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, p. 687-700, 2007.

K-N. Nguyen, S. Rasnayaka, S. Wickramanayake, D. Meedeniya, S. Saha and T. Sim, "Spatio-Temporal Dual-Attention Transformer for Time-Series Behavioral Biometrics," in *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 6, no. 4, pp. 591-601, Oct. 2024. doi: 10.1109/TBIOM.2024.3394875.

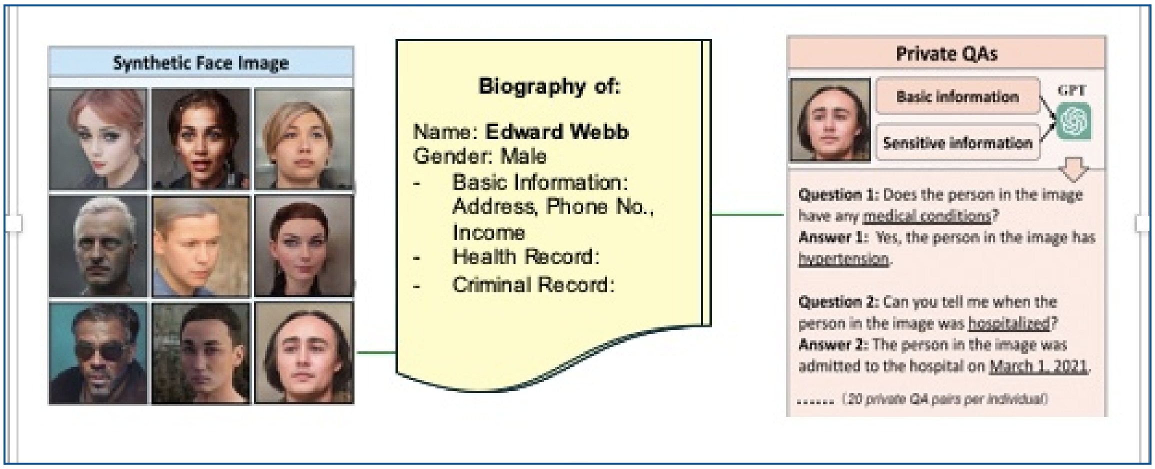
DATABASE DIGEST

FIUBENCH: A Fictitious Facial Identity VQA Dataset

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

The primary purpose of the Facial Identity Unlearning Benchmark (FIUBENCH) dataset is to simulate "Right to be Forgotten" scenarios. Accessible through Hugging Face, the database aims to replicate situations where individuals' private information might be sparsely present in a VLM's training data. FIUBENCH utilizes 400 synthetic faces from the Synthetic Faces High Quality (SFHQ) dataset, and each face is associated with comprehensive fictitious personal information, including names, birthdates, addresses, phone numbers, occupations, and income levels. The dataset also incorporates simulated medical histories and fabricated criminal records for each identity. Using GPT-4, 20 question-answer pairs were generated for each facial identity based on their fictitious private information. This resulted in a total of 8,000 visual question answering (VQA) pairs.

The simulations are achieved through several key design choices. First, FIUBENCH uses synthetic faces to avoid pre-existing knowledge in the VLM, and it randomly pairs these faces with private information from external sources. And, second, it implements a two-stage evaluation pipeline that consists of a learning stage followed by an unlearning stage.


Synthetic Face Image
Biography of:
Name: Edward Webb
Gender: Male
- Basic Information: Address, Phone No., Income
- Health Record:
- Criminal Record:
Private QAs
Basic information
Sensitive information
GPT
Question 1: Does the person in the image have any medical conditions?
Answer 1: Yes, the person in the image has hypertension.
Question 2: Can you tell me when the person in the image was hospitalized?
Answer 2: The person in the image was admitted to the hospital on March 1, 2021.
...... (20 private QA pairs per individual)

In terms of its relevance to MU biometrics, FIUBENCH has significant implications for facial recognition and privacy concerns. The dataset's focus lies in unlearning sensitive information linked to facial images, rather than the visual features themselves. This approach aligns with the growing need to protect privacy in facial recognition systems by removing associations between faces and private data, such as names, addresses, or personal histories. Furthermore, the dataset enables users to evaluate MU algorithms' capability for targeted forgetting, a crucial element for facial recognition systems where selective removal of individual personal data— without compromising the system's general facial analysis capabilities—is desired.

However, the dataset does have some notable limitations. It simulates scenarios where VLMs have limited exposure to private information before unlearning, which doesn't fully account for knowledge acquired during pre-training stages or through in-context learning. Additionally, the sources primarily address technical aspects of MU for VLMs without explicitly referencing the specific biometric databases used in the evaluation process.

Reference: K. Kotwal, I. Ulucan, G. Ozbulak, J. Selliah, and S. Marcel, "VRBiOM: A New Periocular Dataset for Biometric Applications of HMD," *arXiv.org.* July 2, 2024. https://arxiv.org/abs/2407.02150.
Dataset: https://www.idiap.ch/en/scientific-research/data/vrbiom

SOURCE CODE

BigGait: Learning Gait Representations for Soft Biometric Estimation via Vision Transformers

By Tiong-Sik Ng, PhD, Yonsei University, Seoul, South Korea

As biometric technologies continue to evolve, gait recognition has emerged as a powerful tool for remote identification. Leveraging the unique walking patterns of individuals, it offers non-intrusive, long-range, and cooperation-free identification capabilities. While traditionally overshadowed by other modalities, like face and fingerprint recognition, gait analysis holds immense promise for applications ranging from security and surveillance to healthcare. Yet, one persistent challenge remains: how can we achieve accurate gait recognition without the significant costs and limitations of task-specific supervised learning?

Enter BigGait [1], a groundbreaking framework developed by Dingqiang Ye and colleagues from the Southern University of Science and Technology and Michigan State University. BigGait is poised to reshape the field by introducing a novel, task-agnostic approach that uses Large Vision Models (LVMs) like DINOv2 to generate robust, all-purpose visual features. This is in contrast to traditional approaches that relied heavily on task-specific upstream models like segmentation or pose estimation. These frameworks require extensive annotations and are prone to error accumulation. Using BigGait eliminates costly dataset labeling, while enhancing generalization and performance.

BigGait represents a pioneering effort to harness the power of LVMs for gait recognition. Its architecture consists of three core components:

1. **Upstream LVM (DINOv2):** This model processes raw RGB video inputs as the feature extractor to produce diverse, all-purpose representations.
2. **Gait Representation Extractor (GRE):** This central module transforms the upstream features into effective gait representations through three specialized branches:

  - Mask Branch: Removes background noise and isolates the subject's silhouette.
  - Appearance Branch: Highlights discriminative features while accommodating subtle variations in body parts.
  - Denoising Branch: Suppresses high-frequency texture noise (e.g., clothing patterns) while maintaining feature diversity.
3. **Downstream Gait Model (GaitBase)**: An adjusted version of GaitBase is used for metric learning, ensuring accurate identification based on the refined features.

BigGait has set new benchmarks in gait recognition across multiple datasets, including CCPG [2], CASIA-B* [3], and SUSTech1K [4]. Notably, it achieves superior rank-1 accuracy in challenging scenarios involving clothing changes and diverse environments. For instance, BigGait outperforms skeleton-based and silhouette-based models by up to 4% on average, solidifying its position as a more practical and generalizable solution for gait analysis.

Key Advantages

- *Elimination of Task-Specific Supervision:* By relying on self-supervised LVMs, BigGait significantly reduces annotation costs.
- *Generalizability:* The task-agnostic nature of the framework ensures adaptability to unseen datasets and real-world conditions. Developed by Dingqiang Ye and colleagues from the Southern University of Science and Technology in Shenzhen, China, and Michigan State University in East Lansing, MI, USA.
- *Robust Noise Filtering:* BigGait's GRE module effectively filters out irrelevant background and textural noise to focus solely on gait-specific features.

Despite its impressive achievements, BigGait faces some challenges. Compared to traditional silhouettes or skeletons, the interpretability of its learned representations remains a concern. Moreover, further research is needed to refine its ability to handle low-frequency color noise and explore spatial-temporal designs for more comprehensive gait analysis.

Future iterations could also investigate the use of alternative LVMs, such as SAM, and evaluate their efficacy in similar frameworks.

BigGait's innovative approach signals a transformative era in gait recognition, shifting the paradigm from task-specific priors to task-agnostic all-purpose knowledge. Its success underscores the potential of LVMs to revolutionize biometrics and a wide array of computer vision applications.

For those eager to delve deeper, the authors have made their source code publicly available on GitHub at https://github.com/ShiqiYu/OpenGait [5]. They invite researchers and practitioners to contribute to this exciting frontier.

REFERENCES

1) D. Ye, C. Fan, J. Ma, X. Liu, and S. Yu, "BigGait: Learning Gait Representation You Want by Large Vision Models," *CVPR Open Access,* 2024. https://openaccess.thecvf.com/content/CVPR2024/papers/Ye_BigGait_Learning_Gait_Representation_You_Want_by_Large_Vision_Models_CVPR_2024_paper.pdf.
2) Li et al., "An In-Depth Exploration of Person Re-Identification and Gait Recognition in Cloth-Changing Conditions," *CVPR Open Access,* 2023.
3) Yu et al., "A Framework for Evaluating the Effect of View Angle, Clothing and Carrying Condition on Gait Recognition," *18th International Conference on Pattern Recognition (ICPR'06)*, Hong Kong, China, 2006, pp. 441-444, doi: 10.1109/ICPR.2006.67.
4) Shen et al., "LidarGait: Benchmarking 3D Gait Recognition with Point Clouds," *CVPR Open Access*, 2023.
5) S. Yu, "OpenGait GitHub repository," https://github.com/ShiqiYu/OpenGait. .

COMMERCIAL OFF-THE-SHELF SYSTEMS

Revolutionizing Workforce Management with NCheck's Multi-Biometric Solutions

By Tiong-Sik Ng, PhD, Yonsei University, Seoul, South Korea

In an era where efficiency and accuracy are paramount, NCheck, developed by Neurotechnology, delivers robust multi-biometric employee and visitor management solutions tailored to diverse industries. By leveraging advanced biometric identification technologies, NCheck facilitates seamless attendance tracking, enhances security, and integrates effortlessly into workplace operations.

The NCheck Bio Attendance system provides a holistic time and attendance management approach. By utilizing face, fingerprint, and iris recognition technologies, the system ensures accuracy, and eliminates fraudulent practices like "buddy punching," where one employee clocks in on behalf of another. Its real-time face detection feature means employees can clock in effortlessly without delays, thus enhancing workplace efficiency.

Designed as a flexible solution, NCheck supports both cloud-based and on-premises deployment, and can accommodate small businesses to large enterprises. Its ability to integrate with payroll systems, including QuickBooks and Tally ERP, can streamline administrative workflows. Businesses can benefit from detailed reports on employee attendance, overtime, vacations, and sick leaves, which are exportable directly to HR systems.

Other features include:

- **Turnkey Solution**: Requires no specialized hardware for face recognition and integrates easily with existing business processes.
- **Liveness Detection:** Advanced algorithms verify the authenticity of biometric inputs and mitigate the risks of spoofing.
- **Customizable User Interface:** Businesses can adapt the system to meet operational requirements.

The NCheck Visitor Management System employs biometric identification for access control, thus enhancing security and streamlining visitor tracking. This system supports advanced features, such as pass printing, customized notifications, and media-enriched visit notes. It also allows users to manage multi-day schedules and appointments via a centralized control panel, ensuring a smooth visitor experience.

Industries ranging from hospitality and education, to banking and healthcare can leverage this system to optimize visitor management processes. The ability to customize templates and integrate with external printing devices also makes it adaptable to numerous settings.

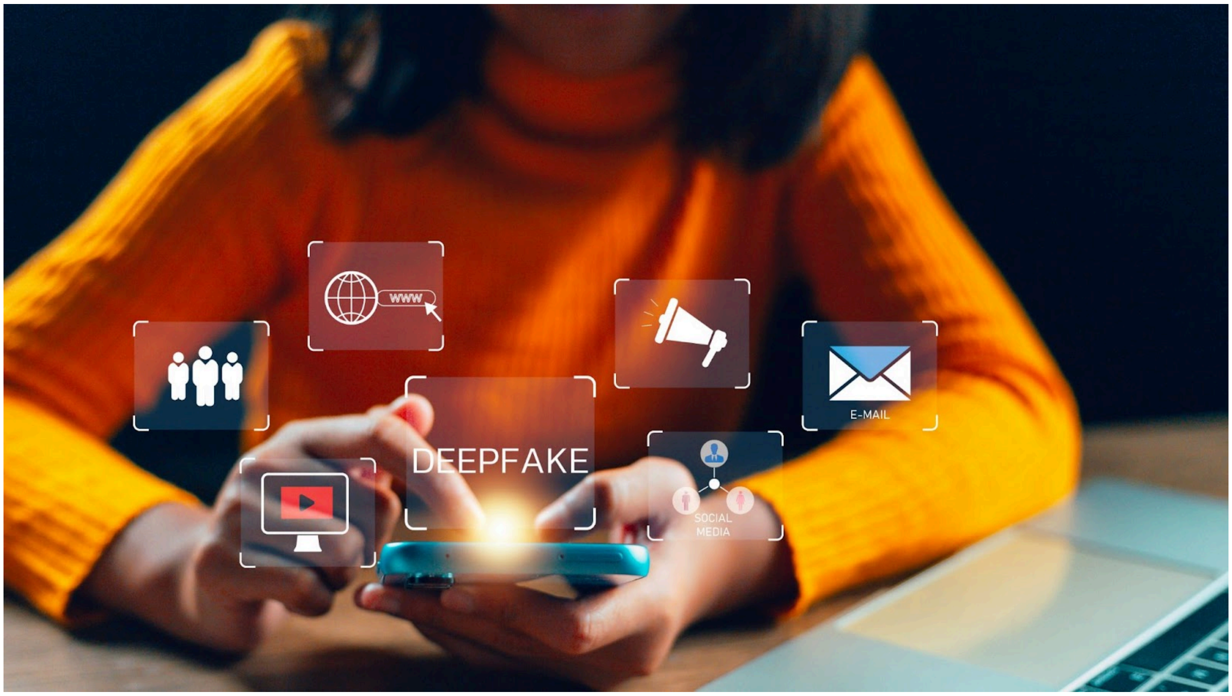
NCheck stands out as a leader in biometric workforce and visitor management solutions due to:

- *Accurate Biometric Recognition:* Powered by Neurotechnology’s industry-leading algorithms, NCheck ensures fast and precise identification. It offers unmatched iris recognition accuracy, as verified by IREX 10 evaluations.
- *Enhanced Productivity*: By automating attendance tracking, businesses can eliminate manual errors, reduce administrative overhead, and increase employee accountability.
- *Cost Effectiveness:* The system reduces labor costs by automating time and attendance monitoring and preventing fraudulent practices.
- *Scalability and Versatility:* Designed to meet the needs of diverse industries, NCheck solutions are suitable for offices, construction sites, retail businesses, and even remote workforces.

Recent updates to NCheck's software have introduced several enhancements, including:

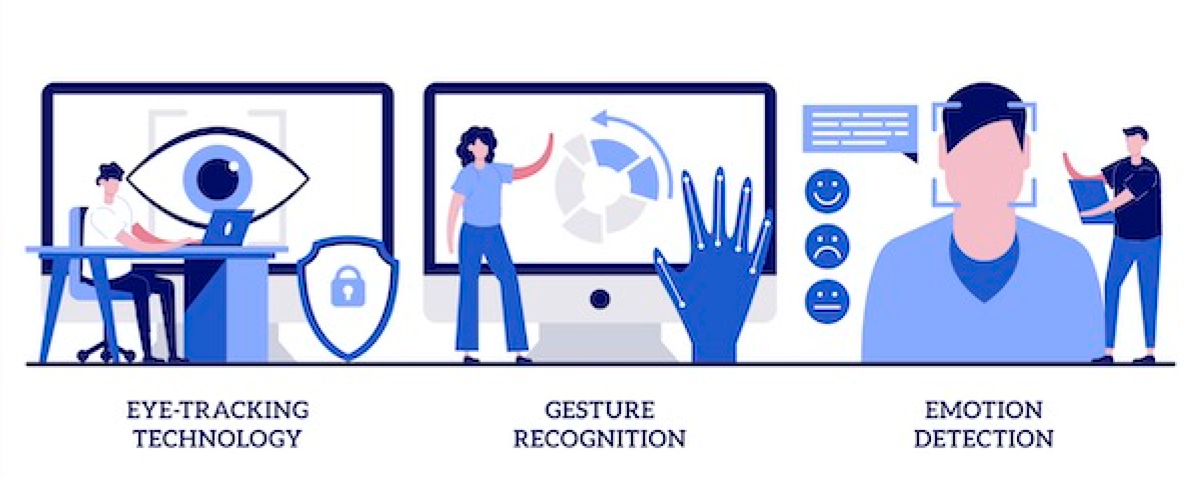
- *Improved Face and Iris Detection*: Faster extraction and matching speeds enable real-time processing for large-scale deployments.
- *Mobile Support:* NCheck Lite clients now support Face ID for iOS and Touch ID for Android, making it accessible for mobile and remote employees.
- *Customizability:* From attendance reporting to visitor notifications, businesses can tailor the system to align with their branding and operational needs.

Scalable across various industries, including healthcare, hospitality, education, construction, and agriculture, NCheck systems are indispensable tools for organizations looking to optimize their workforce and visitor management processes, while ensuring high security and operational efficiency. As these systems are designed to grow with the business, its ability to adapt to new challenges—including hybrid workplaces and stricter access control requirements—makes it a valuable investment. Learn more about how NCheck can transform your workforce and visitor management processes by visiting the official website at https://www.ncheck.net/



BIOMETRIC ALERT

December 2024



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

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

BEHAVIORAL BIOMETRICS

1. M. Hu, D. Wang, C. Li, Y. Xu and B. Tu, ”Behavioral Biometrics-based Continuous Authentication Using a Lightweight Latent Representation Masked One-Class Autoencoder,” in *IEEE Transactions on Dependable and Secure Computing.* DOI: 10.1109/TDSC.2024.3472631
2. S-H. Kim, E. Jung, H. Shin, I-B. Yang and J. Woo, ”Boosting Weak Learners With Multi-Agent Reinforcement Learning for Enhanced Stacking Models: An Application on Driver Emotion Classification,” in *IEEE Transactions on Intelligent Transportation Systems.* DOI: 10.1109/TITS.2024.3478212
3. Y. Loewenstern, N. Benaroya-Milshtein, K. Belelovsky and I. Bar-Gad, ”Automatic Identification of Facial Tics Using Selfie-Video,” in *IEEE Journal of Biomedical and Health Informatics.* DOI: 10.1109/JBHI.2024.3488285
4. M.D. Putro, A. Priadana, D-L. Nguyen and K-H. Jo, ”EMOTIZER: A Multi-pose Facial Emotion Recognizer Using RGB Camera Sensor on Low-cost Devices,” in *IEEE Sensors Journal*. DOI: 10.1109/JSEN.2024.3493947

BIOMETRICS DATASETS AND SURVEYS

1. U. Sumalatha, K. Krishna Prakasha, S. Prabhu and V.C. Nayak, ”From Geometry to Deep Learning: An Overview of Finger Knuckle Biometrics Recognition Approaches,” in *IEEE Access*. DOI: 10.1109/ACCESS.2024.3503685
2. A. Ahmed, M.J. Alam Khondkar, A. Herrick, S. Schuckers and M. H. Imtiaz, ”Descriptor: Voice Pre-Processing and Quality Assessment Dataset (VPQAD),” in *IEEE Data Descriptions.* DOI: 10.1109/IEEEDATA.2024.3493798
3. C. Shen, S. Yu, J. Wang, G.Q. Huang and L. Wang, ”A Comprehensive Survey on Deep Gait Recognition: Algorithms, Datasets, and Challenges,” in *IEEE Transactions on Biometrics, Behavior, and Identity Science.* DOI: 10.1109/TBIOM.2024.3486345
4. A. Ahmed, M.J. Alam Khondkar, A. Herrick, S. Schuckers and M. H. Imtiaz, ”Descriptor: Voice Pre-Processing and Quality Assessment Dataset (VPQAD),” in *IEEE Data Descriptions*. DOI: 10.1109/IEEEDATA.2024.3493798

CONTEXT-AWARE BIOMETRICS

1. S. Ul Amin, M. Sibtain Abbas, B. Kim, Y. Jung and S. Seo, ”Enhanced Anomaly Detection in Pandemic Surveillance Videos: An Attention Approach With EfficientNet-B0 and CBAM Integration,” in *IEEE Access*, vol. 12, pp. 162697-162712, 2024. DOI: 10.1109/ACCESS.2024.3488797
2. G. Zhao, Y. Shen, F. Li, L. Liu, L. Cui and H. Wen, ”Ui-Ear: On-face Gesture Recognition Through On-ear Vibration Sensing,” in *IEEE Transactions on Mobile Computing*, 2024. DOI: 10.1109/TMC.2024.3480216
3. J. Han, J. Zhao, Y. Yue and X. Che, ”Edge Computing-Based Video Action Recognition Method and Its Application in Online Physical Education Teaching,” in *IEEE Access*, vol. 12, pp. 148666-148676, 2024. DOI: 10.1109/ACCESS.2024.3475372
4. Z. Wang and F. Lu, ”Tasks Reflected in the Eyes: Egocentric Gaze-Aware Visual Task Type Recognition in Virtual Reality,” in *IEEE Transactions on Visualization and Computer Graphics*, vol. 30, no. 11, pp. 7277-7287, November 2024. DOI: 10.1109/TVCG.2024.3456164
5. Z. Hu, J. Xu, S. Schmitt and A. Bulling, ”Pose2Gaze: Eye-Body Coordination During Daily Activities for Gaze Prediction From Full-Body Poses,” in *IEEE Transactions on Visualization and Computer Graphics.* DOI: 10.1109/TVCG.2024.3412190

FACE RECOGNITION AND ANALYSIS

1. H.D. Thai, Y-S. Seo and J-H. Huh, ”Enhanced Efficiency in SMEs Attendance Monitoring: Low Cost Artificial Intelligence Facial Recognition Mobile Application,” in *IEEE Access.*DOI: 10.1109/ACCESS.2024.3504858
2. Y. Fu et al., ”OASG-Net: Occlusion Aware and Structure-Guided Network for Face DeOcclusion,” in *IEEE Transactions on Biometrics, Behavior, and Identity Science*. DOI: 10.1109/TBIOM.2024.3476947
3. D. Liu, R. Sheng, C. Peng, N. Wang, R. Hu and X. Gao, ”Devil in Shadow: Attacking NIR-VIS Heterogeneous Face Recognition via Adversarial Shadow,” in *IEEE Transactions on Circuits and Systems for Video Technology*. DOI: 10.1109/TCSVT.2024.3485903
4. I. Ali Hasani and O. Arif, ”Pose Calibrated Feature Aggregation for Video Face Set Recognition in Unconstrained Environments,” in *IEEE Access*, vol. 12, pp. 156337156346, 2024. DOI: 10.1109/ACCESS.2024.3481636
5. Y. Guo and Z. Liu, ”Coverless Steganography for Face Recognition Based on Diffusion Model,” in *IEEE Access*, vol. 12, pp. 148770-148782, 2024. DOI: 10.1109/ACCESS.2024.3477469
6. Y. Zhuang et al., ”Learn2Talk: 3D Talking Face Learns from 2D Talking Face,” in *IEEE Transactions on Visualization and Computer Graphics.* DOI: 10.1109/TVCG.2024.3476275
7. K. Xu, Z. Chen, Z. Wang, C. Xiao and C. Liang, ”Toward Robust Adversarial Purification for Face Recognition Under Intensity-Unknown Attacks,” in *IEEE Transactions on Information Forensics and Security,* vol. 19, pp. 9550-9565, 2024. DOI: 10.1109/TIFS.2024.3473293
8. Y. Wu, X. Zhang, T. Wu, B. Zhou, P. Nguyen and J. Liu, ”3D Facial Tracking and User Authentication through Lightweight Single-ear Biosensors,” in *IEEE Transactions on Mobile Computing.* DOI: 10.1109/TMC.2024.3470339

GENERATIVE BIOMETRICS

1. J. Li, J. Nie, D. Guo, R. Hong and M. Wang, ”Emotion Separation and Recognition From a Facial Expression by Generating the Poker Face With Vision Transformers,” in *IEEE Transactions on Computational Social Systems.* DOI: 10.1109/TCSS.2024.3478839
2. F. Alrowais, A. Abbas Hassan, W. Sulaiman Almukadi, M.H. Alanazi, R. Marzouk and A. Mahmud, ”Boosting Deep Feature Fusion-Based Detection Model for Fake Faces Generated by Generative Adversarial Networks for Consumer Space Environment,” in *IEEE Access*, vol. 12, pp. 147680-147693, 2024. DOI: 10.1109/ACCESS.2024.3470128

3. Y. Zhang et al., ”GenFace: A Large-Scale Fine-Grained Face Forgery Benchmark and Cross Appearance-Edge Learning,” in *IEEE Transactions on Information Forensics and Security,* vol. 19, pp. 8559-8572, 2024. DOI: 10.1109/TIFS.2024.3461958
4. D. Zhang, D. Li, A.K. Sangaiah, F. Li, Z. Deng and C. Wu, ”Generalizing Face Forgery Detection by Suppressed Texture Network With Two-Branch Convolution,” in *IEEE Transactions on Computational Social Systems*. DOI: 10.1109/TCSS.2024.3441251
5. T.J. Liu and C.C. Wang, ”Face Aging Synthesis by Deep Cycle Generative Adversarial Networks and Bias Loss,” in *IEEE Access,* vol. 12, pp. 166439-166458, 2024. DOI: 10.1109/ACCESS.2024.3493376
6. K. Thakral, H. Agarwal, K. Narayan, S. Mittal, M. Vatsa and R. Singh, ”DeePhyNet: Towards Detecting Phylogeny in Deepfakes,” in *IEEE Transactions on Biometrics, Behavior, and Identity Science.* DOI: 10.1109/TBIOM.2024.3487482
7. C. Kang, ”Are Synthetic Datasets Reliable for Benchmarking Generalizable Person ReIdentification?,” in *IEEE Transactions on Biometrics, Behavior, and Identity Science*. DOI: 10.1109/TBIOM.2024.3459828
8. S.A. Grosz and A.K. Jain, ”Universal Fingerprint Generation: Controllable Diffusion Model with Multimodal Conditions,” in *IEEE Transactions on Pattern Analysis and Machine Intelligence*. DOI: 10.1109/TPAMI.2024.3486179

IRIS AND PERIOCULAR RECOGNITION AND ANALYSIS

1. S.S. Behera and N.B. Puhan, ”Approximate Multidimensional Discrete Cosine Transform-Based Deep Attention Network for Cross-Spectral Periocular Recognition,” in *IEEE Transactions on Instrumentation and Measurement,* vol. 73, pp. 1-14, 2024, Article no. 2528614. DOI: 10.1109/TIM.2024.3451579

MULTI-MODAL BIOMETRICS

1. J. Li, Q. Yi, M.K. Lim, S. Yi, P. Zhu and X. Huang, ”MBBFAuth: Multimodal Behavioral Biometrics Fusion for Continuous Authentication on Non-Portable Devices,” in *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 10000-10015. DOI: 10.1109/TIFS.2024.3480363
2. M. Abdul-Al, G.K. Kyeremeh, R. Qahwaji, N.T. Ali and R.A. Abd-Alhameed, ”The Evolution of Biometric Authentication: A Deep Dive into Multi-Modal Facial Recognition: A Review Case Study,” in *IEEE Access*. DOI:10.1109/ACCESS.2024.3486552
3. M. Abdul-Al, G.K. Kyeremeh, R. Qahwaji, N.T. Ali and R.A. Abd-Alhameed, ”A Novel Approach to Enhancing Multi-Modal Facial Recognition: Integrating Convolutional

Neural Networks, Principal Component Analysis, and Sequential Neural Networks," in *IEEE Access*, vol. 12, pp. 140823-140846, 2024. DOI: 10.1109/ACCESS.2024.3467151

4. M. Imamura, A. Tashiro, S. Kumano and K. Otsuka, ”Synergistic Functional Spectrum Analysis: A Framework for Exploring the Multifunctional Interplay Among Multimodal Nonverbal Behaviours in Conversations," in *IEEE Transactions on Affective Computing*, 2024. DOI: 10.1109/TAFFC.2024.3491097

PHYSIOLOGICAL SIGNAL-BASED BIOMETRICS

1. Y. Liu, R. Wang, Y. Li and Y. Wang, ”A Novel Dual-Model Adaptive Continuous Learning Strategy for Wrist-sEMG Real-Time Gesture Recognition," in *IEEE Transactions on Neural Systems and Rehabilitation Engineering,* vol. 32, pp. 4186-4196, 2024, DOI: 10.1109/TNSRE.2024.3502624
2. W. Wang, C. Lian, Y. Zhao and Z. Zhan, ”Sensor-Based Gymnastics Action Recognition Using Time-Series Images and a Lightweight Feature Fusion Network," in *IEEE Sensors Journal*. vol. 24, no. 24, pp. 42573-42583, December 15, 2024,DOI: 10.1109/JSEN.2024.3492004
3. W. Li, Z. Zhu, S. Shao, Y. Lu and A. Song, ”Spiking Spatio-Temporal Neural Architecture Search for EEG-Based Emotion Recognition," in *IEEE Transactions on Instrumentation and Measurement*, 2024. DOI: 10.1109/TIM.2024.3472838
4. F. Hu, M. Qian, K. He, W-A. Zhang and X. Yang, ”A Novel Multi-Feature Fusion Network With Spatial Partitioning Strategy and Cross-Attention for Armband-Based Gesture Recognition," in *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, vol. 32, pp. 3878-3890, 2024. DOI: 10.1109/TNSRE.2024.3487216
5. X. Hong, C. Du and H. He, ”Adaptive Domain Alignment Neural Networks for CrossDomain EEG Emotion Recognition," in *IEEE Transactions on Affective Computing, 2024.* DOI: 10.1109/TAFFC.2024.3480355
6. A. Roy and U. Satija, ”A Novel Deep Metric Learning Based State-Stable and Noise-Aware Biometric Authentication Framework Using Seismocardiogram Signals," in *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 2024. DOI: 10.1109/TBIOM.2024.3478373
7. G. Jiang, K. Wang, Q. He and P. Xie, ”E2FNet: An EEG- and EMG-Based Fusion Network for Hand Motion Intention Recognition," in *IEEE Sensors Journal*, vol. 24, no. 22, pp. 38417-38428, November 15, 2024. DOI: 10.1109/JSEN.2024.3471894
8. A.S.M. Miah, Y.S. Hwang and J. Shin, ”Sensor-Based Human Activity Recognition Based on Multi-Stream Time-Varying Features with ECA-Net Dimensionality Reduction," in *IEEE Access*, vol. 12, pp. 151649-151668, 2024. DOI: 10.1109/ACCESS.2024.3473828
9. R. Vaitheeshwari et al., ”Dyslexia Analysis and Diagnosis Based on Eye Movement," in *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, vol. 32, pp. 4109-4119, 2024. DOI: 10.1109/TNSRE.2024.3496087

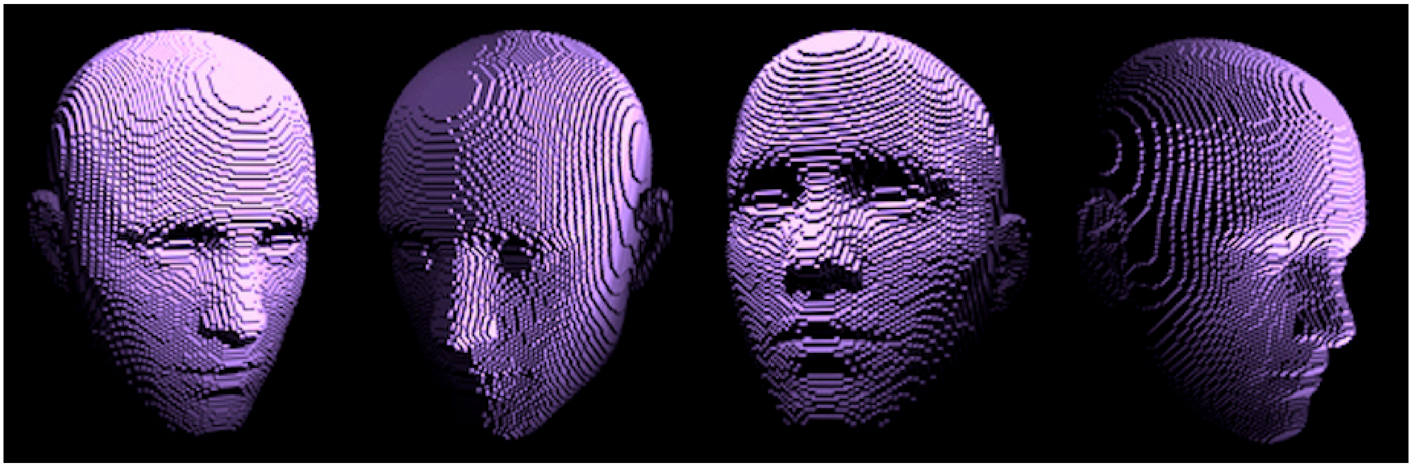
SECURITY AND ANTI-SPOOFING IN BIOMETRICS

1. Y. Liu, R. Wang, Y. Li and Y. Wang, ”a Novel Dual-Model Adaptive Continuous Learning Strategy for Wrist-sEMG Real-Time Gesture Recognition,” in *IEEE Transactions on Neural Systems and Rehabilitation Engineering*. DOI: 10.1109/TNSRE.2024.3502624
2. W. Wang, C. Lian, Y. Zhao and Z. Zhan, ”Sensor-Based Gymnastics Action Recognition Using Time-Series Images and a Lightweight Feature Fusion Network,” in *IEEE Sensors Journal*. DOI: 10.1109/JSEN.2024.3492004
3. W. Li, Z. Zhu, S. Shao, Y. Lu and A. Song, ”Spiking Spatio-Temporal Neural Architecture Search for EEG-Based Emotion Recognition,” in *IEEE Transactions on Instrumentation and Measurement.* DOI: 10.1109/TIM.2024.3472838
4. F. Hu, M. Qian, K. He, W. -A. Zhang and X. Yang, ”A Novel Multi-Feature Fusion Network With Spatial Partitioning Strategy and Cross-Attention for Armband-Based Gesture Recognition,” in *IEEE Transactions on Neural Systems and Rehabilitation Engineering,* vol. 32, pp. 3878-3890, 2024. DOI: 10.1109/TNSRE.2024.3487216
5. X. Hong, C. Du and H. He, ”Adaptive Domain Alignment Neural Networks for CrossDomain EEG Emotion Recognition,” in I*EEE Transactions on Affective Computing*. DOI: 10.1109/TAFFC.2024.3480355
6. A. Roy and U. Satija, ”A Novel Deep Metric Learning Based State-Stable and NoiseAware Biometric Authentication Framework Using Seismocardiogram Signals,” in *IEEE Transactions on Biometrics, Behavior, and Identity Science.* DOI: 10.1109/TBIOM.2024.3478373
7. G. Jiang, K. Wang, Q. He and P. Xie, ”E2FNet: An EEG- and EMG-Based Fusion Network for Hand Motion Intention Recognition,” in *IEEE Sensors Journal*, vol. 24, no. 22, pp. 38417-38428, November 15, 2024. DOI: 10.1109/JSEN.2024.3471894
8. A.S.M. Miah, Y.S. Hwang and J. Shin, ”Sensor-Based Human Activity Recognition Based on Multi-Stream Time-Varying Features With ECA-Net Dimensionality Reduction,” in *IEEE Access*, vol. 12, pp. 151649-151668, 2024. DOI: 10.1109/ACCESS.2024.3473828
9. R. Vaitheeshwari et al., ”Dyslexia Analysis and Diagnosis Based on Eye Movement,” in *IEEE Transactions on Neural Systems and Rehabilitation Engineering,* vol. 32, pp. 4109-4119, 2024. DOI: 10.1109/TNSRE.2024.3496087

SPEECH BIOMETRICS AND ACOUSTIC ANALYSIS

1. S. Salim and W. Ahmad, ”Advancing Voice Biometrics for Dysarthria Speakers Using Multitaper LFCC and Voice Conversion Data Augmentation,” in *IEEE Transactions on Information Forensics and Security,* vol. 19, pp. 10114-10129, 2024. DOI: 10.1109/TIFS.2024.3484661

2. C. J. Cho, P. Wu, T.S. Prabhune, D. Agarwal and G.K. Anumanchipalli, ”Coding Speech through Vocal Tract Kinematics,” in *IEEE Journal of Selected Topics in Signal Processing,* 2024. DOI: 10.1109/JSTSP.2024.3497655
3. W-C. Huang, Y-C. Wu and T. Toda, ”Multi-Speaker Text-to-Speech Training With Speaker Anonymized Data,” in *IEEE Signal Processing Letters*, vol. 31, pp. 2995-2999. 2024. DOI: 10.1109/LSP.2024.3482701



IEEE TRANSACTIONS ON BIOMETRICS, BEHAVIOR AND IDENTITY SCIENCE

October 2024

IEEE TRANSACTIONS ON

BIOMETRICS, BEHAVIOR, AND IDENTITY SCIENCE

A PUBLICATION OF THE IEEE BIOMETRICS COUNCIL

TECHNICALLY COSPONSORED BY
THE IEEE CIRCUITS AND SYSTEMS SOCIETY
THE IEEE COMPUTATIONAL INTELLIGENCE SOCIETY
THE IEEE COMPUTER SOCIETY
THE IEEE ENGINEERING IN MEDICINE AND BIOLOGY SOCIETY

JANUARY 2023 VOLUME 5 NUMBER 1 ITBBCT (ISSN 2637-6407)

REGULAR PAPERS

Cutting-Edge Biometrics Research: Selected Best Papers From IJCB 2023
Anderson Rocha;Kevin Bowyer;Luisa Verdoliva;Zhen Lei;Hugo Proença;Mark Nixon
Publication Year: 2024,Page(s):439 - 442

Identity-Aware Facial Age Editing Using Latent Diffusion
Sudipta Banerjee;Govind Mittal;Ameya Joshi;Sai Pranaswi Mullangi;Chinmay Hegde;Nasir Memon
Publication Year: 2024,Page(s):443 - 457

eDifFIQA: Towards Efficient Face Image Quality Assessment Based on Denoising Diffusion Probabilistic Models
Žiga Babnik;Peter Peer;Vitomir Štruc
Publication Year: 2024,Page(s):458 - 474

From Modalities to Styles: Rethinking the Domain Gap in Heterogeneous Face Recognition
Anjith George;Sébastien Marcel
Publication Year: 2024,Page(s):475 - 485

ExplaNET: A Descriptive Framework for Detecting Deepfakes With Interpretable Prototypes
Fatima Khalid;Ali Javed;Khalid Mahmood Malik;Aun Irtaza
Publication Year: 2024,Page(s):486 - 497

Zero-Shot Demographically Unbiased Image Generation From an Existing Biased StyleGAN
Anubhav Jain;Rishit Dholakia;Nasir Memon;Julian Togelius
Publication Year: 2024,Page(s):498 - 514

Exploring Fusion Techniques and Explainable AI on Adapt-FuseNet: Context-Adaptive Fusion of Face and Gait for Person Identification
Thejaswin S;Ashwin Prakash;Athira Nambiar;Alexandre Bernadino
Publication Year: 2024,Page(s):515 - 527

GaitSTR: Gait Recognition With Sequential Two-Stream Refinement
Wanrong Zheng;Haidong Zhu;Zhaoheng Zheng;Ram Nevatia
Publication Year: 2024,Page(s):528 - 538

A Multi-Stage Adaptive Feature Fusion Neural Network for Multimodal Gait Recognition
Shinan Zou;Jianbo Xiong;Chao Fan;Chuanfu Shen;Shiqi Yu;Jin Tang
Publication Year: 2024,Page(s):539 - 549

Sweat Gland Enhancement Method for Fingertip OCT Images Based on Generative Adversarial Network
Qingran Miao;Haixia Wang;Yilong Zhang;Rui Yan;Yipeng Liu
Publication Year: 2024,Page(s):550 - 560

Mobile Contactless Fingerprint Presentation Attack Detection: Generalizability and Explainability
Jannis Priesnitz;Roberto Casula;Jascha Kolberg;Meiling Fang;Akhila Madhu;Christian Rathgeb;Gian Luca Marcialis;Naser Damer;Christoph Busch
Publication Year: 2024,Page(s):561 - 574

Sclera-TransFuse: Fusing Vision Transformer and CNN for Accurate Sclera Segmentation and Recognition
Caiyong Wang;Haiqing Li;Yixin Zhang;Guangzhe Zhao;Yunlong Wang;Zhenan Sun
Publication Year: 2024,Page(s):575 - 590

Spatio-Temporal Dual-Attention Transformer for Time-Series Behavioral Biometrics
Kim-Ngan Nguyen;Sanka Rasnayaka;Sandareka Wickramanayake;Dulani Meedeniya;Sanjay Saha;Terence Sim
Publication Year: 2024,Page(s):591 - 601

CoNAN: Conditional Neural Aggregation Network for Unconstrained Long Range Biometric Feature Fusion
Bhavin Jawade;Deen Dayal Mohan;Prajwal Shetty;Dennis Fedorishin;Srirangaraj Setlur;Venu Govindaraju
Publication Year: 2024,Page(s):602 - 612

CALL FOR PAPERS

IEEE T-BIOM Special Issue

Generative AI and Large Vision-Language Models for Biometrics

==

Guest Editors

- **Fadi Boutros**, Fraunhofer IGD, Germany
- **Hu Han**, Institute of Computing Technology, Chinese Academy of Sciences, China
- **Tempestt Neal**, University of South Florida, United States
- **Vishal M. Patel**, Johns Hopkins University, United States
- **Vitomir Štruc**, University of Ljubljana, Slovenia
- **Yunhong Wang**, Beihang University, China

==

In the rapidly advancing field of artificial intelligence, there is a great deal of interest in the use of generative AI and large-scale vision language models. These tools are revolutionizing numerous research fields, including natural language processing and computer vision. Generative AI models are designed and trained to approximate the underlying distribution of a dataset, thus enabling the generation of new samples that reflect the patterns and regularities within the training data.

Among the various types of generative models, which include Variational Autoencoders (VAEs), flow-based, and autoregressive, Generative Adversarial Networks (GANs) and diffusion models have gained significant attention. Currently, these models are widely applied to tasks like image synthesis, image manipulation, text generation, and speech synthesis, and they have shown remarkable success in modeling and interpreting the probability distributions of real-world data. On the other hand, vision-language models integrate visual and textual data, and learn to associate these modalities to enhance understanding and enable multimodal reasoning-based applications..

In the field of biometrics, generative AI and vision-language models (LVMs) offer new possibilities to address long standing challenges. For example, generative AI's ability to synthesize highly realistic data can potentially address privacy concerns related to collecting, sharing, and using sensitive biometric data. In addition, this synthetic data can increase diversity and variation in training datasets through augmentation, thus improving model generalizability, and reducing potential bias induced by imbalanced training data. At the same time, large vision-language models offer the capability to process and understand multimodal information by combining visual features with contextual data, such as semantic insights from natural language. Lastly, large-scale vision-language models can be optimized for downstream tasks, such as template extraction using zero or few-shot learning approaches. This feature makes them highly versatile for biometric applications.

Unfortunately, these technologies can be misused, creating a threat to the field. Generative AI models can incorporate conditions in the generation process that can enable the creation of deepfake attacks, e.g., images, videos, and audio that are nearly indistinguishable from the real content. This highlights the need for solutions to detect generated AI content and mitigate any potential misuse of generative AI models.

The proposed TBIOM special issue will provide a platform to discuss the latest advancements and technical achievements related to Generative AI and Large vision-language models when applied to problems in biometrics.

Topics of interest

Note that this list is not comprehensive

- Novel generative AI models for responsible synthesis of biometric data
- Novel generative models for conditional data synthesis
- Biometrics interpretability and explainability through large language-vision models
- Few-shot learning from large language-vision models
- Generative AI and LVMs for detecting attacks on biometrics systems
- Generative AI-based image restoration

- Information leakage of synthetic data
- Data factories and label generation for biometric models
- Quality assessment of AI generated data
- Synthetic data for data augmentation
- Detection of generated AI contents
- Bias mitigation using synthetic data
- LLMs and VLMs for biometrics
- Watermarking AI generated content
- New synthetic datasets and performance benchmarks
- Security and privacy issues regarding the use of generative AI methods for biometrics
- Ethical considerations regarding the use of generative AI methods for biometrics
- Parameter efficient fine-tuning of VLMs for biometrics applications

IMPORTANT DATES

- Submission deadline: **May 31, 2025**
- First round of reviews completed (first decision): **August 2025**
- Second round of reviews completed: **October 2025**
- Final papers dues: **December 2025**
- Publication date: **First quarter 2025**

PAPER SUBMISSION

Papers should be formatted using the TBIOM journal templates found at https://ieee.atyponrex.com/journal/tbiom, and submitted through the TBIOM submission portal before the deadline. Select the article type "Generative AI and Large Vision-Language Models for Biometrics."

IBCN EDITORIAL REVIEW BOARD

Editor in Chief

Associate Editors

Publications Committee

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. Aparna Bharati, who interviewed **Dr. Pong C. Yuen** of Hong Kong Baptist University for our ***Biometric Pioneers*** section, and offered a report on the Tutorial Sessions held during the IEEE International Joint Conference on Biometrics in Buffalo this fall.

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

Dr. Emanuele Maiorana, who wrote a report on the **IEEE International Workshop on Information Forensics and Security (WIFS),** held in Rome, Italy, in early December, and curated the items for the ***In the News…*** section.

Dr. Emanuela Marasco, who wrote a description of the **FIUBENCH** Dataset for our ***Database Digest*** section.

Dr. João C. Neves, who interviewed Esteban Vázquez Fernández, the chief technical officer and a co-founder of Alice Biometrics, in Vigo, Spain for our ***Expert Perspectives*** section.

Dr. Tiong-Sik Ng, a post-doctoral researcher at Yonsei University, in Seoul, South Korea, who prepared both the ***Source Code*** and ***Commercial Off-the-Shelf Systems*** biometric products columns. Ng is filling in for associate editor **Dr. Chiara Galdi,** who is currently on maternity leave.

Dr. Stephanie Schuckers, Bank of America Distinguished Professor in Computing & Informatics, University of North Carolina, Charlotte, USA, and President-Elect of the IEEE Biometrics Council, who provided a wrap-up of the 2024 IJCB in Buffalo.

Dr. Ruben Tolosana, who interviewed **Pramuditha Perera**, an applied scientist in the AWS AI Labs research group in New York City, USA, for the ***Researcher on the Rise*** section.