IEEE BIOMETRICS COUNCIL NEWSLETTER

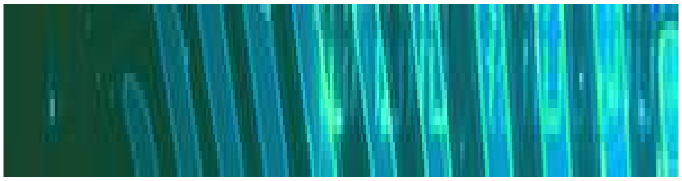
Volume 56, December 2025

BIOMETRICS THAT CAN KEEP A SECRET

Privacy-preserving biometric strategies can enhance identity verification systems by introducing Zero-Knowledge strategies. In an interview in our **Expert Perspectives** section, Keyless Co-founder and CEO Andrea Carmignoni explains how his company is using these concepts to create less vulnerable biometric templates. Also in this issue, meet up and coming biometric researcher Francisco Castro of the University of University of Málaga in Spain, our **Researcher on the Rise.**

GREETINGS FROM THE EIC

ANDREW TEOH BENG JIN
Yonsei University, Korea



Dear Readers of the *Biometric Newsletter,*

Welcome to the December 2025 issue of the *IEEE Biometrics Council* Newsletter. As the year closes, I want to thank our readers, authors, editors, and volunteers for the steady support that keeps this newsletter lively and useful. The community's willingness to share ideas, tools, datasets, as well as hard-earned lessons, is what turns an issue into something more than just a collection of pages.

This issue's theme, *"Biometrics that can keep a secret,"* reflects a simple reality: as biometric systems scale into everyday infrastructure, privacy and template security stop being "features" and become design constraints that determine whether a technology is deployable. A practical demonstration of this principle can be found in the work of our **Expert Perspective** subject, which is described below.

In **Council News**, we congratulate ***Christoph Busch, Davide Maltoni***, and ***Vishal Patel*** on being named 2026 IEEE Fellows. The honor recognizes contributions that span biometric image quality, template protection, morphing attack detection, fingerprint recognition, and biometrics-driven computer vision. We also highlight an important update from *IEEE T-BIOM*, which is **now welcoming position papers** to stimulate forward-looking discussion on the field's technical and societal trajectory.

Our **In the News** column surveys prominent English-language coverage of biometric issues published from April to July 2025. Collectively, the items trace how biometrics are increasingly discussed through the lenses of border operations, consumer authentication, wearable sensing, and regulatory pressure. The recurring tensions illustrated between expanding capability and convenience, and heightened scrutiny around privacy risks, accountability, and the impact of failures, is familiar to researchers and practitioners alike.

The **Profiles** section opens with the aforementioned **Expert Perspectives** interview with ***Andrea Carmignoni,*** co-founder and CEO of Keyless, who explains the logic of zero-knowledge biometrics and how secure multi-party computation enables server-side authentication without exposing a usable biometric template. The interview grounds the cryptographic idea in operational constraints, such as remote onboarding, liveness assurance, certification, and latency. In **Researcher on the Rise**, ***Francisco M. Castro*** reflects on his personal research path, which spans gait biometrics and efficient edge AI. Drawing from this experience, he provides recommendations to current researchers on the importance of persistence, collaboration, and the value of looking beyond a single modality or problem framing.

In **Noted in the Literature**, we feature the **Voice2Visage** technology, which explores voice-to-face generation that aligns vocal and visual signals in a shared embedding space, and then conditions a modern diffusion model to produce identity-consistent faces. Beyond its technical interest, the article also offers a reminder that multimodal learning can infer sensitive correlations that were previously difficult to operationalize, and can sharpen the urgency of privacy-preserving design.

This issue's **Database Digest** focuses on **EyeNavGS**, a dataset for VR-based biometric and navigation research. The dataset captures 6-DoF head pose and eye-gaze traces from Meta Quest Pro headsets across diverse real-world scenes. These scenes are reconstructed via 3D Gaussian Splatting, accompanied by record-and-replay tooling that supports immediate experimentation.

For builders, the **Source Code** column presents 2D-Malafide, an adversarial framework that stresses face deepfake detectors through optimized 2D filtering distortions. The framework exposes failure modes that look visually obvious yet remain effective. Meanwhile, its sister column, **Commercial Off-the-Shelf Systems**, shifts to deployment practice, describing Keesing's biometric identity proofing workflow for KYC that combines document authentication with selfie matching and liveness checks through SDK-based integration.

I hope you enjoy this issue and find ideas worth reusing, debating, and improving. On behalf of the Council, I wish you a restful end to 2025 and a productive, curiosity-driven start to 2026.

Warm regards,

Andrew Teoh

COUNCIL NEWS

BUSCH, MALTONI, & PATEL NAMED IEEE FELLOWS

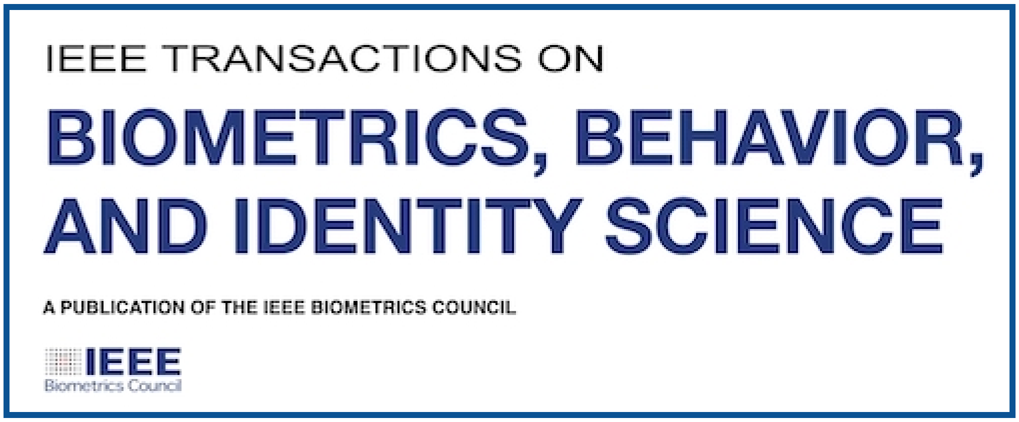
The grade of Fellow in the Institute of Electrical and Electronics Engineers (IEEE) recognizes unusual distinction in the profession. Those elected must currently be an IEEE Senior Member or Life Senior Member, and have 15 years or more of professional experience. Nominees must also be a member in good standing for a minimum of 5 cumulative years.

Three representatives of the emerging fields of biometrics were selected as part of the 300-plus member class of 2026. They are as follows:

- **Christoph Busch** (photo above, left) **,** Professor, Hochschule Darmstadt, Germany. Honored for contributions to biometric image quality, template protection and morphing attack detection.
- **Davide Maltoni,** (photo center) Professor, University of Bologna, Italy. Honored for contributions to fingerprint biometric recognition.
- **Vishal Patel,** (photo, right) Associate Professor, Johns Hopkins University, Maryland, USA. Honored for contributions to image processing, computer vision and biometrics.

To learn how to nominate an IEEE Fellow, go to https://www.ieee.org/membership/fellows/fellows-nomination.

IEEE T-BIOM NOW ACCEPTING POSITION PAPERS


IEEE TRANSACTIONS ON

BIOMETRICS, BEHAVIOR, AND IDENTITY SCIENCE

A PUBLICATION OF THE IEEE BIOMETRICS COUNCIL

IEEE Biometrics Council

With the goal of “stimulating discussion and forward-thinking dialogue about the future trajectory of biometric technology, applications, policy, evaluation, and ethical frameworks,” the flagship publication of the IEEE Biometrics Council is now welcoming submissions of **position papers.** Unlike conventional articles, these papers are shorter in length and present a clear, well-supported argument addressing critical challenges, emerging technologies, or societal implications in the biometrics domain. Authors are encouraged “to advance provocative, well-reasoned stances intended to inspire discussion, guide future research agendas, and inform policymaking and industry practices.”

Potential topics could include, but are not limited to:

- Fundamental Problems;
- Edge Computing and Distributed Systems;
- Active and Passive Threats Against Biometric Systems;
- Fairness, Accessibility, and Inclusion;
- Global-scale Identity Management;
- Ethical, Legal, and Societal Implications;
- Quantum-secure Biometric Systems; and
- Implications and Future of AI in Biometrics.

A more detailed description of position paper topics, along with submission instructions, can be found at https://ieee-biometrics.org/wp-content/uploads/TBIOM-position-papers.pdf.

IN THE NEWS…

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

In a time when digital identity verification and security have become part of daily life, biometric recognition has shifted from a specialized technology to a topic of broad public interest. Whether through facial recognition systems in airports, voice authentication in customer service, or fingerprint sensors in devices, biometric technology is now a common part of many people's lives. As the use of this technology spreads, so do public discussions about it.

Media coverage is vital in shaping how these technologies are understood and evaluated by the general audience, who often lack technical expertise. Thus, the way news stories present developments, successes, risks, and controversies can affect public opinion, influence policy discussions, and shape broader views on privacy, security, and technological advancement.

Below we feature articles related to biometrics that were published between April and July 2025 on prominent English-language news websites.

Long-awaited EU Border System Expected for October (April 15, 2025)
https://www.bbc.com/news/articles/cq678ymylrmo
The article reports on the impending UK introduction of the EU’s Entry/Exit System (EES), which will replace passport stamping with mandatory biometric registration for non-EU travelers. It outlines the expected rollout timeline, the preparations underway at major UK/EU travel hubs, and the concerns about possible delays due to the added checks. Biometric recognition is presented as a security-enhancing requirement, but also as a source of operational challenges. Thus, the article highlights both the perceived necessity of adding

this technology for modern border control, and the public's apprehension about longer processing times.

What Happens If Biometric Data Is Breached (And How To Prevent It) (April 25, 2025)
https://www.forbes.com/councils/forbestechcouncil/2025/04/25/what-happens-if-biometric-data-is-breached-and-how-to-prevent-it/
The article presents biometric recognition as both highly valuable and inherently risky: though a powerful, convenient authentication method, its uniqueness also makes it a prime target for cyberattacks. Biometrics is framed as more sensitive than password methods because it is immutable, and a breach is portrayed as having potentially severe, long-lasting consequences for individuals and organizations. Media treatment here emphasizes the vulnerability of biometric systems, highlighting threats like spoofing, database breaches, and loss of consumer trust, while simultaneously promoting a set of advanced technical safeguards as the path forward. Overall, biometrics is depicted as an indispensable tool, yet still requires sophisticated, privacy-preserving protection to remain trustworthy and secure.

Valuable Tool or Cause for Alarm? Facial ID Quietly Becoming a Part of Police Arsenals (May 14, 2025)
https://www.theguardian.com/technology/2025/may/24/valuable-tool-or-cause-alarm-facial-id-quietly-becoming-part-police-arsenal
The article reports on the rollout of fixed and mobile live facial recognition cameras in London, highlighting both their increasing use by police and the broader expansion of facial biometrics across public spaces. It emphasizes technology's effectiveness in identifying individuals on watchlists and preventing crimes, while also raising concerns about misidentifications, lack of regulation, and potential chilling effects on everyday life.

Biometrics is presented as a powerful but controversial tool: framed as a law-enforcement asset with clear benefits, yet simultaneously generating ethical, legal, and social tensions.

Samsung's Smartphone Palm Print Scanner Revealed (May 26, 2025)
https://www.forbes.com/sites/daveywinder/2025/05/26/samsungs-smartphone-palm-print-scan-is-more-secure-than-fingerprints/
The article portrays biometrics as generally secure and convenient for everyday smartphone authentication, yet not entirely foolproof, noting that fingerprint and facial recognition can theoretically be bypassed through highly specialized attacks—though such methods pose little real-world risk for typical users. Biometric recognition is framed as strong but improvable technology, with the narrative emphasizing ongoing innovation to achieve higher levels of security. The story also presents Samsung's newly patented palm-print recognition system as a more robust alternative, highlighting its deeper and harder-to-spoof biological features compared to fingerprints or facial images.

UK Must Toughen Regulation of Facial Recognition, Say AI Experts (May 29, 2025)
https://www.ft.com/content/09ce1755-554e-43c9-90ad-8e07196763b0

The article discusses concerns over the rapid expansion of facial recognition technology in the UK, highlighting its use by both police forces and private businesses like retailers and sports venues. Privacy campaigners and researchers from the Ada Lovelace Institute emphasize that the lack of clear legislation and oversight creates legal uncertainty and risks for human rights, and calls for a dedicated regulator and updated laws. In general, biometric recognition is presented as a powerful tool for identification and security, but also a technology for which deployment raises serious privacy, ethical, and legal challenges that current governance does not adequately address.

UK Citizens Face Fingerprint Checks each Time they Visit the EU (May 31, 2025)
https://www.theguardian.com/travel/2025/may/31/uk-citizens-face-fingerprint-checks-each-time-they-visit-eu
Because of delays in installing a planned digital verification app, frequent UK travelers will soon face manual fingerprint checks at every entry. The article describes the upcoming shift to EU biometric border controls, and details the extensive infrastructure being built in the port of Dover to manage biometric capture safely while minimizing disruption. Establishing the system will include reclaimed land, new processing hubs, and a "virtual frontier" 1.4 miles from the docks. The authors portray biometric recognition as central to modernizing border management and replacing passport stamping, but also as a logistical hurdle as incomplete digital tools will temporarily impose more friction on travelers.

Sam Altman Brings his Eye-scanning Identity Verification Startup to the UK (June 8, 2025)
https://www.cnbc.com/2025/06/08/sam-altman-world-eye-scanning-uk.html
The article describes the UK rollout of World's iris-scanning identity system, explaining how the project uses Orb devices to create unique biometric codes aimed at distinguishing

humans from AI-generated figures. Covering both the rapid expansion of the system and the concerns raised about privacy, data protection, and large-scale digital identity schemes, the article presents biometrics as a powerful but contentious solution. Though essential for combating AI-driven fraud, it's a system accompanied by significant public, regulatory, and ethical scrutiny.

Here Come the Glassholes (June 13, 2025)
https://www.ft.com/content/9c21af68-28ba-489e-81a6-552aff61ddbb
Covering Meta’s AI-powered Ray-Ban smart glasses, the article highlights their popularity in 2025, and their potential to integrate facial recognition technology in the future. While the glasses currently assist with photos, videos, queries, and object recognition, adding facial recognition—which could identify people in real time—is raising ethical and privacy concerns. Biometric recognition is treated as a powerful convenience feature, but the article emphasizes the regulatory, legal, and societal challenges of deploying it in wearable devices, particularly under the GDPR in the UK.

Facial Recognition Technology Needs Stricter Regulation (June 17, 2025)
https://www.theguardian.com/technology/2025/jun/17/facial-recognition-technology-needs-stricter-regulation
The article discusses the rapid expansion of biometric surveillance in the UK, emphasizing that both police and private-sector uses, including live facial recognition in public spaces and systems that infer emotional states, lack a clear legal framework. It highlights concerns about accuracy, ethics, legality, and public trust, noting that existing guidance is fragmented and insufficient to protect fundamental rights. Biometric recognition is presented as a powerful but largely unregulated technology, one where widespread adoption has outpaced governance and urgently calls for comprehensive legislation and independent oversight**.**

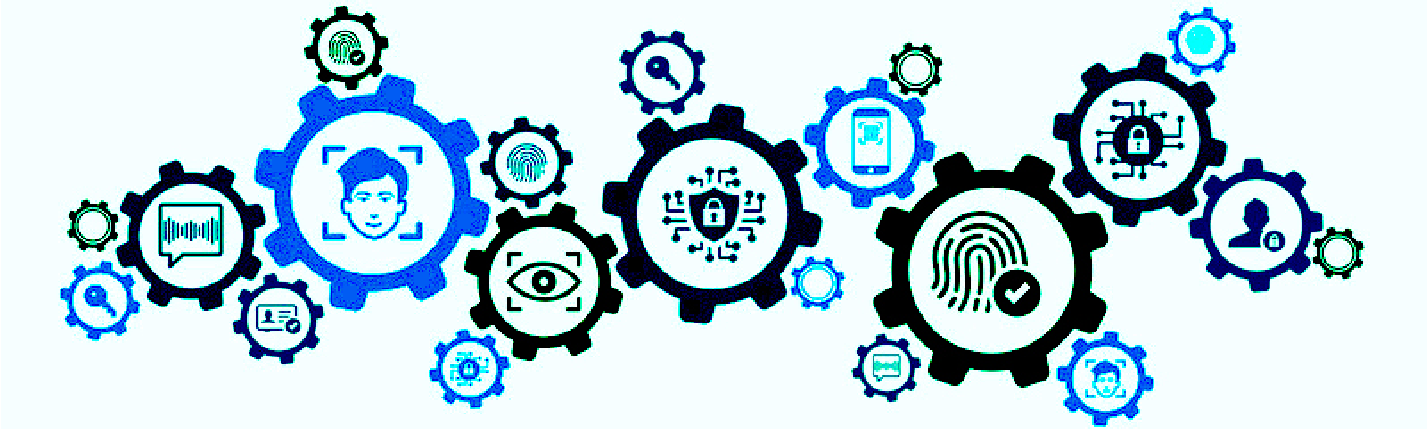
Colorado’s Biometric Privacy Law Takes Effect July 1: Are You Ready? (June 27, 2025)
https://www.forbes.com/sites/alonzomartinez/2025/06/27/colorados-biometric-privacy-law-takes-effect-july-1-are-you-ready/
Treating biometric data as an especially sensitive and high-risk category of personal information, the article emphasizes the data’s permanence and the long-lasting consequences of misuse. Biometrics is framed not primarily as a technological innovation, but as a type of data requiring strict legal safeguards: because traits like fingerprints, faces, and voices cannot be replaced. For this reason, the law imposes detailed obligations on notice, consent, retention, security, and disclosure. The tone underscores that the growing use of biometrics in workplaces and authentication systems demands rigorous, rights-protective regulation to ensure responsible use. Overall, the article presents biometric

technologies as “powerful but inherently vulnerable,” thus justifying stronger privacy protections and signaling a broader national shift toward stricter oversight.

Clear CEO Caryn Seidman Becker on the Future of Identity Verification Technology in Daily Life (July 2, 2025)

https://www.cnbc.com/2025/07/02/clears-identity-verification-journey-beyond-airport-security-line.html

The focus of the article is on Clear’s planned expansion beyond airports into broader identity-verification use cases—including digital document signing, enterprise onboarding, and fraud prevention, even as these scenarios are increasingly threatened by AI-generated identities. The article highlights partnerships with companies like DocuSign, Uber, Okta, and Greenhouse as Clear positions itself as a solution to emerging risks, such as synthetic identities and deepfakes. Biometrics is presented as a trusted, scalable, and necessary layer of modern security—a method more reliable than traditional ID documents and essential to countering sophisticated digital impersonation.



EXPERT PERSPECTIVES: *Andrea Carmignani*

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

Andrea Carmignani is Co-Founder and CEO at Keyless, the leader in privacy-preserving biometric authentication. He founded Keyless alongside world renowned security and privacy experts, and its patented solutions are the first to use privacy-preserving technologies for biometric authentication and identity management. A graduate of INSEAD, a non-profit business school, Carmignani previously worked as a strategy consultant for Accenture and Roland Berger, where he sold and managed multi-million digital transformation projects.

NEVES: Keyless Technologies has become a pioneer in privacy-preserving biometrics by introducing the concept of zero-knowledge biometrics. Could you explain to us how it differs from the way traditional biometric systems handle template storage and matching?

Carmignani: Traditional biometrics store a “template”—a feature vector from a raw signal, be it a face, or a fingerprint—sourced either locally from a tool like FaceId or centrally on a server. Local storage is private but lacks strong, verifiable identity binding for external services, such as a bank. Centralized storage solves the binding issue, but creates a high-value target. If breached, even hashed templates can be misused for surveillance or impersonation.

Zero-Knowledge Biometrics (ZKB) eliminates this trade-off. During enrollment, the user's device creates a privacy-preserving, opaque cryptographic template. The server stores only this non-invertible artifact. Authentication uses a Secure Multi-Party Computation (SMPC) protocol in which the comparison occurs in the encrypted domain. Neither the server nor the device learns the other's secret state. This ensures strong server-side identity verification, while keeping the biometric data exclusively on the user's device. As a result, server breaches yield only useless, non-linkable cryptographic blobs.

NEVES: SMPC is a core technical part of your approach. Could you describe how this protocol operates within the Keyless authentication process. Specifically, how can biometric matching occur without any single party ever accessing or reconstructing the biometric data of the user?

Carmignani: Keyless leverages SMPC to move biometric matching into the encrypted domain, guaranteeing that no party—including the service provider—ever accesses a usable biometric template. The process begins on the user's device, where the raw biometric sample is converted into a feature vector and then encrypted using a mechanism specifically designed for computation, rather than just storage. The server stores only this encrypted representation, which is non-invertible.

During authentication, a fresh sample is similarly processed and encrypted on the device. The server then executes the matching algorithm as an MPC protocol over the two encrypted inputs (the enrollment template and the current sample). This allows the system to determine if the samples match with high probability. But, critically, it does so without ever decrypting the inputs or exposing intermediate values. The "multi-party" aspect ensures that neither the device nor the server holds enough information to reconstruct the underlying biometric data. The only result exposed is the final yes/no decision.

NEVES: While the use of zero-knowledge biometrics already offers a competitive advantage over existing biometric players, what other major technological innovations does Keyless provide?

Carmignani: While privacy is a significant benefit, we’re often chosen over our competitors for other reasons.

For one thing, Keyless is multi-factor by design. During enrollment, we capture not just the user’s face, but their device as well. Authentication can then simultaneously check that the two are the same. This effectively nullifies remote attacks. A fraudster would need access to both the user’s face and the original bound device.

Another key draw is our liveness detection capabilities. We were the first to achieve high-level certification for injection attack detection under the European CEN/TS 18099 standard. This is a vital quality for EUDI Wallets looking to carry out remote onboarding. Our liveness detection is also certified against ISO/IEC 30107-3 for Presentation Attack Detection.

Lastly, Keyless is also fast. The nature of sMPC means the data payload is very small, allowing a server-side response in under 300 milliseconds. This is one of the fastest responses on the market.

NEVES: AI-supported significant performance gains in the biometrics field has also introduced new vulnerabilities, such as deepfake-based spoofing and model bias. How does the Keyless framework integrate liveness detection and bias mitigation while preserving privacy?

Carmignani: Keyless performs consistently in diverse real-world conditions, with ongoing improvements allowing the detection of emerging threats like deepfakes. We see our recent certifications for injection and presentation attack detection (CEN/TS 18099, ISO/IEC 30107-3) as a testament to this.

Doing all this while preserving privacy is key. All liveness detection happens on the device in the secure enclave. Only then is the biometric data cryptographically transformed into a non-biometric payload and sent to the server to confirm identity. This unique approach means Keyless never stores biometric data on the server. This information truly never leaves the device.

NEVES: Given our newsletter's academic readership, we are interested to know how Keyless approaches R&D. Does Keyless primarily focus on in-house, foundational R&D to generate novel knowledge? Or does it integrate into its products advances obtained by the academic community?

Carmignani: Keyless takes a hybrid approach to R&D that is very much rooted in both practice and academia. Our core technology is designed, implemented, and continuously evolved in-house by a team of engineers and researchers whose expertise spans machine learning, biometrics, and cryptography. That means the systems we deploy are not black-box integrations of third-party components, but architectures we developed and understand at a fundamental level. Thus we can adapt, harden, and extend them as requirements change.

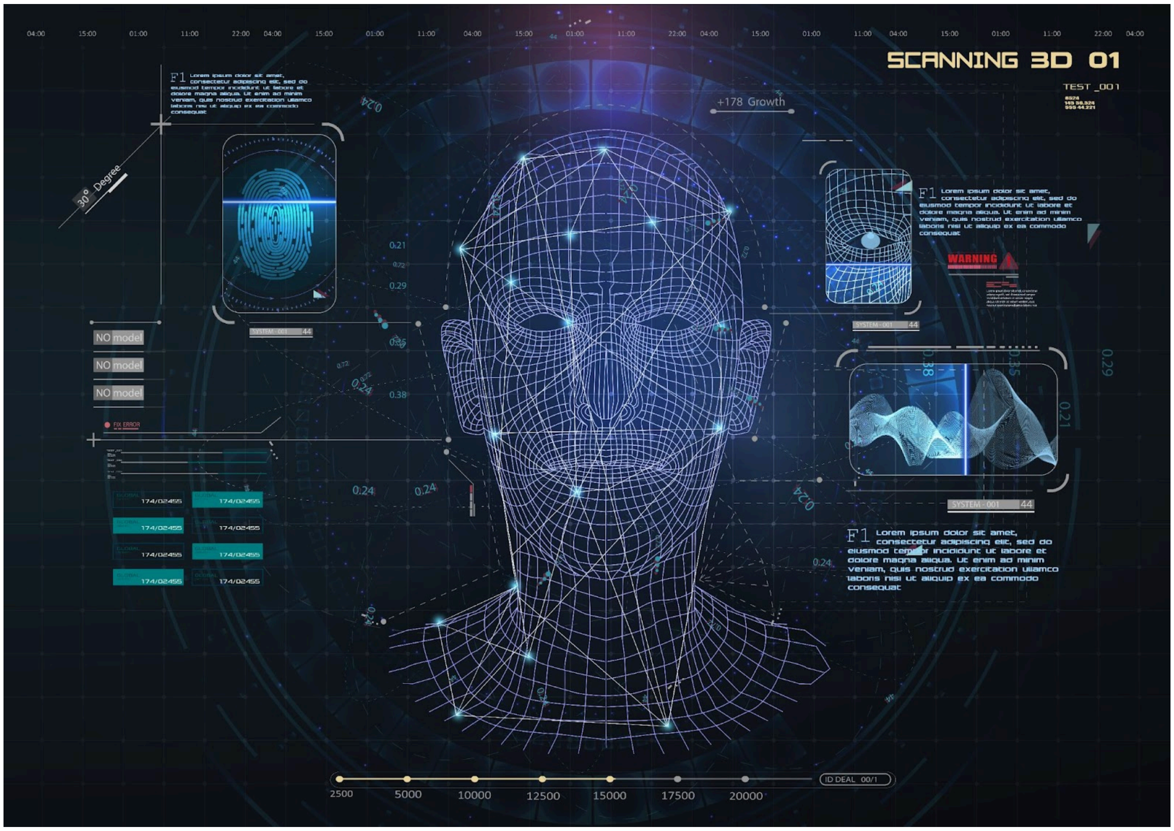
At the same time, we do not try to reinvent what the academic community has already done well. Our work actively builds on state-of-the-art results in biometric recognition, representation learning, privacy-preserving computation, and AI. The team closely follows current research—benchmarking products and systems against new methods, integrating robust advances where they make sense, and stress-testing them in real-world conditions, such as latency, hardware constraints, and adversarial environments. In practice, this gives us the best of both worlds. Our products are grounded in original, in-house applied research, but continuously informed and uplifted by the latest developments in the academic literature.

NEVES: Looking toward the future, do you envision zero-knowledge biometrics and SMPC becoming standard practices in large-scale identity systems? What technical or regulatory milestones must the industry achieve to make this transition a global reality?

Carmignani: We do expect that ZKB and SMPC will become the norm for future large-scale identity systems. This is because traditional designs are unsustainable at the internet scale.

Conventional server-side biometric templates, even if hashed or encrypted, create long-lived, high-risk identifiers prone to breaching and misuse. At the same time, local biometrics offer privacy but are device-bound, easily bypassed, and cannot provide the strong, cryptographically verifiable identity link that remote services demand.

ZKB with MPC eliminates this trade-off by enabling remote services to authenticate users without ever taking custody of their raw biometric data. Keyless has proven this model's viability, security, and scalability in real-world production. For this to become a global standard, technical building blocks, such as efficient MPC protocols and hardware support must be standardized for interoperability. Simultaneously, regulators and policymakers must begin treating centralized biometric storage as a high-risk practice and explicitly mandate privacy-preserving architectures as the preferred method for meeting both security and compliance goals.



RESEARCHER ON THE RISE: *Francisco M. Castro*

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

Francisco M. Castro is an Associate Lecturer at the University of Málaga, Spain, whose research focuses on the field of computer vision, specifically the application of machine learning technologies to person identification based on gait analysis, and the design and optimization of Deep Learning models for embedded systems. After completing his undergraduate work at the University of Córdoba, Castro went on to earn a Master's degree in software engineering and artificial intelligence at the University of Málaga. He would later complete his PhD there with international distinction and a Cum Laude distinction in 2018. In 2019, he received the runner-up prize for Best Thesis from the Spanish Association for Pattern Recognition and Image Analysis.

TOLOSANA: You have worked on several research topics in your career to date, including gait biometrics, people fall detection, anomalous object detection, and efficient training of deep learning models in scenarios with limited labeled data. What is your advice for young Ph.D. students on how to quickly get acquainted with, and contribute scientifically to, new research fields?

Castro: My primary advice is to stay consistently engaged with the current literature. While reading papers can sometimes be tedious, it is the most effective way to understand the state-of-the-art in any field. I recommend setting aside a dedicated block of time each week for reading, and it's crucial not to limit this to just one's immediate research area. Often, breakthroughs in one field, like broader computer vision or machine learning, can inspire novel approaches in another, such as biometrics. Furthermore, it's essential not to be afraid to propose unconventional ideas. What might initially seem like a wild or impractical thought could, upon detailed analysis and development, become a significant scientific contribution.

TOLOSANA: You have also contributed quite a bit of work to top conferences and journals during your research career, publishing more than 40 papers in top journals and conferences, like *IEEE Transactions on Information Forensics and Security*, *Pattern Recognition*, the *European Computer Vision Association* and more. What are the strategies and key factors that have encouraged this level of productivity?

Castro: I do not believe there is a strategy to increase productivity, but I can point to a few key factors. A core element of my productivity has been a strong emphasis on collaboration. I have always been passionate about working with other researchers, which has naturally led to a greater number of shared publications. And, of course, the quality and motivation of our research group are also important. I am fortunate to work with a group of highly driven Ph.D. students, and our joint efforts have been very fruitful.

When I advise my students about productivity, I stress two principles: perseverance and a collaborative spirit. Research is a challenging path, filled with setbacks that include manuscript rejections and difficult reviews. The key is to view this feedback as constructive, use it to strengthen the work, and persist. Success is the inevitable result of this persistence. Furthermore, embracing collaborations and maintaining a constant willingness to learn from others are fundamental drivers that will naturally increase a researcher's output and impact.

TOLOSANA: You have held several different research internships during your career to date, including one with the THOTH group at INRIA-Grenoble in France, and another at the Universidad Católica del Maule in Chile. How do you rate the importance to researchers of internships and collaborations with other institutions? How has this experience impacted the way you conduct research?

Castro: I consider collaboration to be an extremely important part of research. Working with other teams pushes you beyond your comfort zone, and exposes you to new research lines and novel solutions you might not have otherwise considered. In particular, research internships are invaluable. They allow for deep integration into another team's workflow, which can provide fresh perspectives and methodologies that you can then adapt to enhance your own lab's environment.

My time with the THOTH group at INRIA deeply instilled in me the value of perseverance, which is required to publish in top-tier venues. Their practice of holding weekly group-wide presentations was particularly impactful; it fostered a broad awareness of diverse research topics. This is a model we have since adopted in our research group.

Similarly, my stay at the Universidad Católica del Maule was instrumental in launching two new research directions for me: biometrics based on palm vein patterns and Parkinson's detection through voice analysis.

Beyond the scientific benefits, these experiences are personally enriching. Engaging with diverse people and cultures broadens your perspective and contributes significantly to personal growth.

TOLOSANA: Since 2020, you have been an NVIDIA Jetson Ambassador. Could you please tell us a bit more about the mission of this program and your tasks? Also, what changes or improvements in the use of AI on small devices have you noticed in the world, especially for things like real-time video or security cameras?

Castro: As an NVIDIA Jetson Ambassador, my mission is to demonstrate that powerful AI can be accessible and does not require dependence on expensive, high-end hardware for real-world applications. In my courses, I guide participants through the entire workflow. They design, train, and deploy their own models on an NVIDIA Jetson Nano. Seeing their models operate in real-time with a simple camera is often a transformative experience. It shows that compact, low-power devices are capable of running sophisticated models.

The landscape of edge AI has evolved dramatically since 2020. The variety and power of embedded devices have exploded, fostering a robust and competitive ecosystem. Today, platforms like the NVIDIA Jetson family possess significant computational power, making it feasible to deploy complex models for tasks like person re-identification and object detection, and even to perform on-device fine-tuning. This hardware evolution is complemented by new technologies, like M.2 accelerators, which can augment devices like a Raspberry Pi or a standard laptop. This trend is crucial for democratizing AI, moving us away from a reliance on power-hungry, centralized servers. Naturally, these hardware advancements have been paralleled by software improvements. Modern libraries make it easier than ever to optimize and deploy models efficiently on target devices.

TOLOSANA: You are an expert in gait biometrics. What were the major advances your Ph.D. research brought to the field? And, do you think there is still a long way to go in the field?

Castro: My Ph.D. research focused on gait recognition, but shifted the input modality away from traditional silhouettes to more dynamic data, specifically optical flow. I have long been a strong advocate for moving beyond silhouettes in gait analysis. While the goal of avoiding RGB data to protect subject privacy is valid, modalities like optical flow or dense pose representations can preserve that privacy, while providing far richer information for recognition. Consequently, the central thesis of my work was the investigation of optical flow for multi-view gait identification. We also pioneered multimodal approaches that combine different data streams to further enrich the input to our models.

Looking forward, I believe the field of biometrics has significant room for advancement. A primary challenge remaining is the scarcity of large-scale labeled datasets, which has historically constrained the use of the massive models seen in other domains. Despite this, the research community is incredibly innovative. At every top-tier conference, we see creative new architectures and training strategies designed specifically to overcome data limitations and push the state-of-the-art forward. For this reason, I am convinced that biometrics is far from a solved problem. It remains a vibrant and promising area for future research.

TOLOSANA: Today, large multimodal models and self-learning systems are gaining popularity. How do you think this will change the way we train models when we have limited labeled data, such as in gait recognition or on small devices?

Castro: Self-supervised learning and similar strategies that require less labeled data are set to revolutionize how we train models in data-scarce domains. I believe the dominant paradigm will involve a two-step process. First, a large foundation model is pre-trained on vast amounts of unlabeled data using a pretext task that teaches it to understand the fundamental structure of the input data. Second, this pre-trained foundation model is fine-tuned on a small, domain-specific labeled dataset for the target task. It’s an approach that makes it feasible to leverage the power of large architectures, even with limited labeled samples.

As for large multimodal models, this is a concept I explored during my Ph.D. as well. Using multiple input streams is a powerful way to enrich the data and boost model performance. However, it's not a universal solution. The benefits are highly domain-specific and come at the cost of increased model complexity and size. Therefore, it's critical to carefully evaluate the trade-off. Is the resulting gain in accuracy worth the increased computational cost? This question becomes especially pertinent when designing for resource-constrained environments and embedded devices.

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

Castro: Currently our research group is trying to address two topics that, in our opinion, enormously limit the applicability of AI in real-world environments. The first is the amount of labeled data and the computational requirements needed for the proposed solutions. To address this, we are studying solutions that require minimal human supervision in terms of labels, and the use of automatic label discovery techniques to further alleviate this human

dependency. In parallel, the proposed solutions must be optimized to be deployable on cheap, low-power devices.

In this way, we can bring our proposals closer to the real world, where labeled data are few, and buying extremely expensive servers that have to be in cold rooms is not a realistic proposal.

TOLOSANA: Do you have any other suggestions or comments for young researchers or for the biometrics community in general?

Castro: My main advice for young researchers, particularly Ph.D. students, is to cultivate persistence and patience. A Ph.D. is a marathon, not a sprint. It's a challenging journey that often has delayed rewards. It's easy to become discouraged by rejected papers or long review processes, but it's crucial not to fixate on these setbacks. Instead, view research as a long-distance race. The key is to keep learning, keep working, and keep submitting your work. If you remain persistent, all your effort and dedication will be rewarded.

NOTED IN THE LITERATURE

Voice2Visage: Deciphering Faces From Voices

A summary of an article that appeared in the September 2025 issue of* IEEE Transactions on Biometrics, Behavior, and Identity Science*, as prepared by its authors Wuyang Chen, Kele Xu, Yanjie Sun, Yong Dou, and Huaimin Wang

INTRODUCTION

Across decades of research, scientists have uncovered a striking fact: the human face and voice are shaped by the same biological forces. Hormones, like testosterone and estrogen, sculpt not only our jawlines, cheekbones, and brow ridges, but also the thickness and length of our vocal folds, which ultimately determine whether our voice is deep, bright, or resonant. Because these anatomical systems develop together, the voice naturally carries subtle clues about a person’s facial structure. Remarkably, the human brain already exploits these cues. We often form mental images of a speaker’s appearance within seconds of hearing them. This may stem from an innate tendency for multimodal co-perception, or from lifelong exposure to cultural patterns that link local speaking styles with characteristic facial traits.

This raises a captivating question: could a computational model infer someone's facial appearance using only the sound of their voice?

Yet this task is far from straightforward. A single voice clip can correspond to countless visual possibilities—affected by hairstyle, makeup, lighting, expression, and head pose. Similarly, the same face can be associated with many vocal variations depending on content, mood, and speaking style. Moreover, many fine-grained facial attributes simply do not manifest directly in acoustics.

These challenges make voice-to-face prediction an inherently ambiguous and underdetermined problem. Solving the problem calls for demanding models that can extract identity-bearing cues while remaining robust to the rich variability of human appearance and speech.

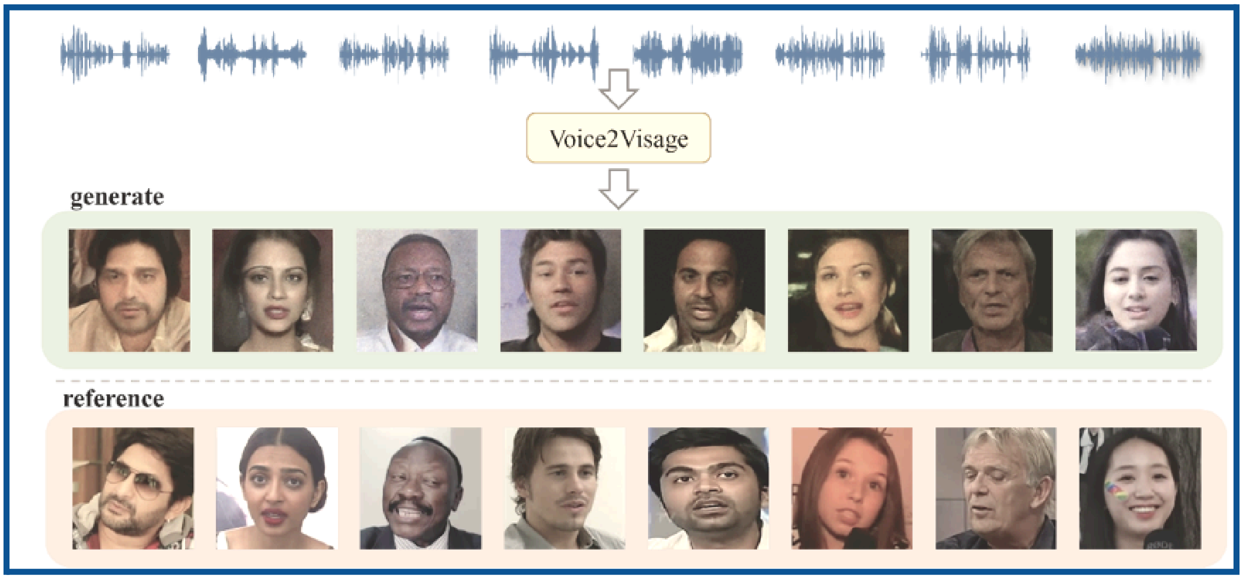


Figure 1. Given unheard voices, Voice2Visage framework can generate a face closely related to the reference.

Technical Perspective

In Voice2Visage, the research team takes a computational step towards addressing these challenges by systematically modeling the association between vocal information and facial appearance. The central idea is to construct a shared multimodal representation space in which the voice and face of the same person naturally align. Within this space, the embedding of a person's voice is encouraged to be close to the embedding of their face. This alignment allows the system to extract identity-related cues, such as timbre, resonance patterns, and formant structure, and connect them to visual traits that tend to co-vary across individuals.

To ensure that these representations are robust, the team trains the model on a newly constructed multilingual and multicultural dataset. This prevents the learned associations from being biased toward a single demographic group or speaking style. By observing diverse linguistic, cultural, and visual patterns, the model learns generalizable voice-face correspondences instead of relying on narrow or culturally-specific stereotypes.

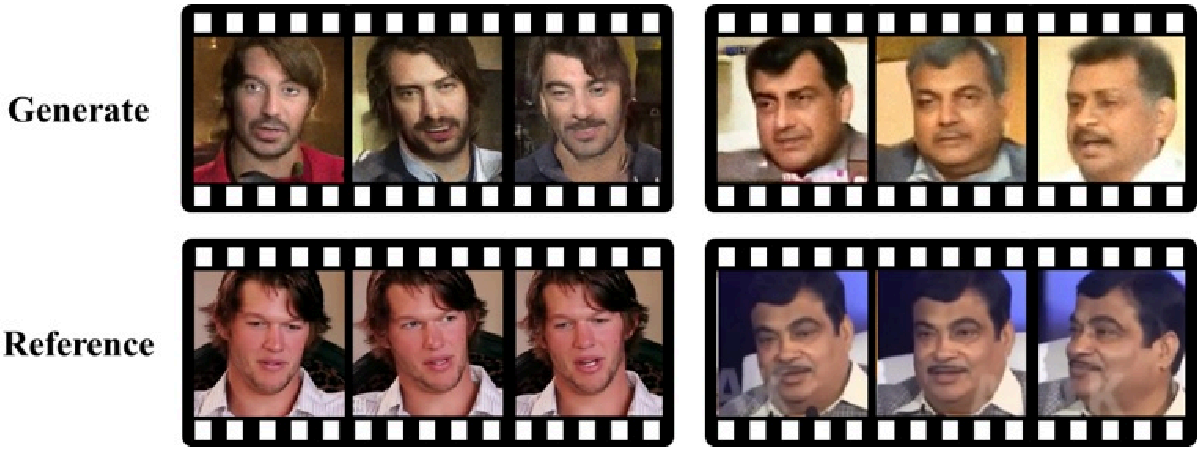


Figure 2. The first row presents the generated results, whereas the second row presents the reference images. These results demonstrate the reliability of the Voice2Visage framework's voice-identity module, which generates diverse facial images while preserving identity consistency across different temporal segments of the input speech.

===

Building on this representation, Voice2Visage employs a conditional generation framework powered by a modern diffusion model. The voice embedding serves as the semantic condition that injects identity-related information into the generation process, while the mask-guided mechanism provides coarse structural guidance. The mask is a binary map that indicates the approximate location and orientation of the face, helping the diffusion model establish consistent geometry without restricting appearance details.

During evaluation, the system is tested by providing different speech segments from the same individual. The generated portraits vary in pose, lighting, or clothing, yet consistently maintain recognizable identity features. This demonstrates that Voice2Visage is not simply memorizing faces but is instead capturing the underlying relationship between how a person sounds and how they tend to look. Additional tests show that modifying the mask during inference may change pose or orientation, but does not break identity consistency. This indicates that identity preservation is driven primarily by the voice representation, rather than the mask.

CONCLUSION

Voice2Visage represents a compelling step forward in the long-standing question of whether machines can approximate a person's appearance from their voice. While the method cannot be expected to reconstruct a face with perfect accuracy, its predictions are nonetheless valuable. In entertainment, gaming, and virtual reality, users who prefer to keep their real identity private can still obtain expressive, voice-driven avatars that feel personally tailored. And, in investigative scenarios when only an audio recording is available, coarse visual approximations may help guide early-stage filtering or narrowing of search efforts. Ultimately, Voice2Visage showcases how the voice can serve as a window into identity, and how multimodal AI can illuminate connections that humans have intuitively sensed for generations.

W. Chen, K. Xu, Y. Sun, Y. Dou and H. Wang, "Voice2Visage: Deciphering Faces From Voices," in *IEEE Transactions on Biometrics, Behavior, and Identity Science*, September 2025, doi: 10.1109/TBIOM.2025.3615961

DATABASE DIGEST

EyeNavGS: Eye-Gaze and Head-Pose Dataset for VR-Based Biometric and Navigation Research

by Emanuela Marasco, Assistant Professor, Information Sciences and Technology (IST) and Center for Secure Information Systems (CSIS), George Mason University, USA

EyeNavGS is the first publicly available dataset to capture full 6-degrees-of-freedom (6-DoF) navigation for users interacting with real-world scenes reconstructed in VR via 3D Gaussian Splatting (3DGS). The dataset, which can encompass head position and orientation, along with detailed eye-gaze data, was collected from 46 participants across two sites—Rutgers University and National Tsing Hua University. Data was gathered using Meta Quest Pro VR headsets in a “free-world standing” mode, within an approximately 3 m × 3 m physical play area. The VR content includes twelve diverse real-world 3DGS scenes in both indoor and outdoor environments. Eight scenes were drawn from pre-trained models named in the original 3DGS paper, while four were newly generated from the ZipNeRF dataset.

For each rendered frame, and for both left and right eyes, EyeNavGS provides head pose data, including 3D position (X, Y, Z) and orientation as quaternions (X, Y, Z, W) in world coordinates. The frames also capture eye-gaze information that specifies the gaze origin position (X, Y, Z) and orientation (quaternion X, Y, Z, W) for each eye, enabling precise 3D gaze direction within the virtual environment. And, the dataset also records field-of-view parameters for each unit of eye (left, right, top, bottom) in radians, and includes timestamps in milliseconds for each

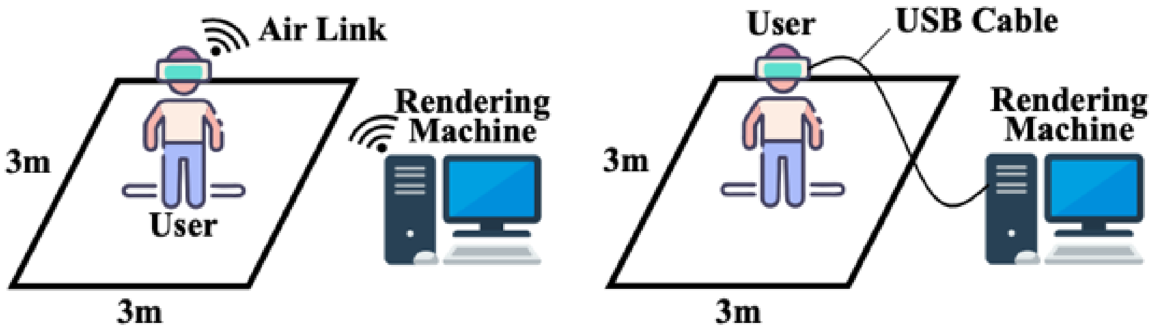


Figure 1. Real-time user trace collection setup showing the tracked space, a user with HMD, the HMD connection, and the rendering machine

==

frame. This allows temporal analysis of gaze and head dynamics. All data is organized into structured CSV files per user and per scene (for example, user1_truck.csv), with each top-level folder corresponding to a specific 3DGS scene. The release includes open-source record-and-replay software and a fork of the SIBR viewer, along with utility tools for data conversion, visualization, and coordinate transformations. These tools facilitate offline replay, analysis, and re-rendering of VR navigation sessions.

EyeNavGS does not provide high-resolution eye-region images and therefore does not include close-up iris or periocular data. Its biometric information is limited to head pose, gaze direction, and field-of-view as captured by the VR headset's eye-tracking system. Thus, it does not directly support iris recognition, periocular feature extraction, or spoof-detection tasks. As a result, the dataset is most suitable for behavioral or gaze-based biometric research, head-gaze dynamics analysis, and VR user behavior modeling, rather than appearance-based recognition. For research on multi-modal biometric authentication in MR/VR headsets, EyeNavGS can serve as a foundation for behavioral- or gaze-based authentication modules. If combined with other datasets containing high-resolution eye or iris data, the dataset can build hybrid systems that leverage both appearance and behavior. Furthermore, since EyeNavGS is publicly accessible with accompanying tools, it can be used immediately for prototyping and analysis.

REFERENCES

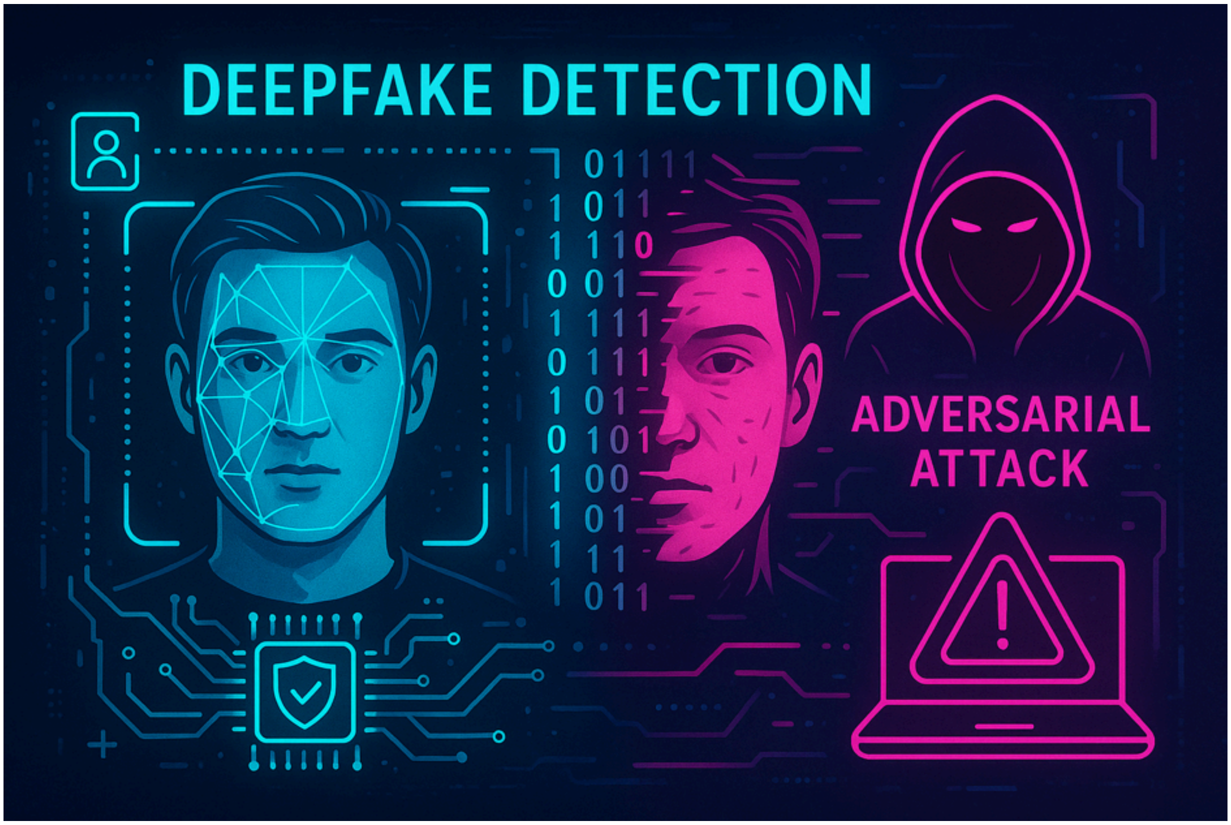
1) Z. Ding, C-T. Lee, M. Zhu, T. Guan, Y-C. Sun, C-H. Hsu, and Y. Liu, "EyeNavGS: A 6-DoF Navigation Dataset and Record-n-Replay Software for Real-World 3DGS Scenes in VR," arXiv preprint, arXiv:2506.02380, 2025.
2) Dataset and software, GitHub, https://symmru.github.io/EyeNavGS/.

SOURCE CODE

By Chiara Galdi, Assistant Professor, Digital Security Department, EURECOM, Biot, France

2D-Malafide: How Adversarial Distortions Reveal Blind Spots in Deepfake Detectors

Image created with ChatGPT 5



Back a few issues ago, we introduced in this newsletter Malafide [1], an adversarial noise-based technique to challenge the robustness of voice spoofing countermeasures in biometric systems. In this issue, we present a follow-up to this work: 2D-Malafide [2], a version of Malafide adapted for image-based biometric systems.

Deepfake detectors are designed to spot manipulated faces, but how resilient are they when confronted with deliberately altered inputs? 2D-Malafide is an adversarial attack framework designed specifically to fool face deepfake detectors. Instead of targeting the deepfake generation process, the authors create carefully crafted perturbations directly on the input data. The method modifies pixels in a way that pushes the detector to misclassify the image. 2D-Malafide shows that even state-of-the-art detectors can be surprisingly fragile, but more importantly, it offers a way to diagnose those weaknesses.

The attacks involve the optimisation of a 2D linear, time-invariant (LTI), non-causal filter. The coefficients are optimised to provoke the misclassification of deepfake images as bona fide. The optimization was not constrained to maintain visual realism. As a result, the adversarial samples often appear clearly distorted to a human observer. Yet, the altered images still fooled the detector.

The fact that the perturbations are visually obvious shows that:

1) The state-of-the-art deepfake detectors tested in the paper lack basic image quality sanity checks;
2) The detectors have dangerous blind spots in their training data; and
3) Even unsophisticated adversarial noise can break a state-of-the-art system.

To enable researchers to replicate the attacks, and thus further investigate deepfake detector vulnerabilities, the authors have also released the full 2D-Malafide implementation as open-source code on GitHub [3].

2D-Malafide serves as a powerful diagnostic tool. The distorted adversarial samples are effectively stress tests, and each successful failure case potentially highlights a missing class of training examples. Consequently, incorporating these cases in the training phase can significantly improve detector robustness.

REFERENCES

1) M. Panariello, W. Ge, H. Tak, M. Todisco, N. Evans,“Malafide: A Novel Adversarial Convolutive Noise Attack Against Deepfake and Spoofing Detection Systems,” 24th Conference of the International Speech Communication Association, 2023. https://www.isca-archive.org/interspeech_2023/panariello23b_interspeech.pdf.
2) C. Galdi, M. Panariello, M. Todisco and N. Evans, "2D-Malafide: Adversarial Attacks Against Face Deepfake Detection Systems," International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, pp. 1-7, 2024.
3) “2D-Malafide” GitHub repository. https://github.com/eurecom-fscv/2D-Malafide.

COMMERCIAL OFF-THE-SHELF SYSTEMS

Keesing’s Approach to Biometric Identity Proofing in KYC Processes

By Chiara Galdi, Assistant Professor, Digital Security Department, EURECOM, Biot, France

Know Your Customer (KYC) procedures have become a central component of modern digital services. They refer to a set of identity verification steps that organisations must perform to ensure that the person on the other side of the screen is truly who they claim to be. KYC is essential for preventing fraud, money laundering, and the use of stolen or synthetic identities.

Illustration of the “Know Your Customer” concept as practiced by Keesing Technologies. Source: https://www.keesingtechnologies.com/blog/keesing-blog/beyond-compliance-kyc-know-your-customer-and-identity-verification/.

As more services transition to digital channels, secure and reliable remote identity verification has become an essential requirement. At the same time, verification systems need to counter increasingly sophisticated forms of identity fraud, including the use of forged documents, stolen identities and presentation attacks. In this context, biometric identity proofing offers an effective way to strengthen security, while maintaining a convenient user experience.

Keesing Technologies is a long-standing provider in the field of document and identity verification. Building on its historical expertise in checking ID documents, Keesing now offers solutions that combine document authentication with biometric verification. Their systems are designed to support remote identity verification, as well as provide on-site checks, by offering organisations a set of flexible tools to establish trust in digital identities.

The identity proofing process typically starts with the capture of an ID document, such as a passport, identity card or driver's licence. The document is analysed to verify its identity using Keesing's extensive reference database, which contains specimen documents issued by authorities from many countries worldwide. Consistency checks between different zones of the document and reference data help to detect tampering or the use of forged documents. Once the document has been validated, AuthentiScan's biometric verification is used to confirm that the person presenting the document is its rightful holder.

The process works as followers. The user is asked to take a selfie, using their phone or webcam, which is compared with the photograph on the ID document. In addition, a liveness check is performed to ensure that the biometric sample originates from a live person rather than from a printed photo, screen replay or other spoofing attempt. Depending on the configuration, this may involve analysing a short video or other evidence of liveness. The identity is considered verified only if the document is proved to be genuine, the face on the selfie matches the document photo, and the liveness check is passed.

From an integration perspective, Keesing's solutions are offered via software development kits, making them suitable for embedding into existing digital customer onboarding or payment services. The generation of an audit trail is also an important feature, as it supports regulatory compliance and provides documentation for risk management and internal controls. Lastly, by employing common devices, such as smartphones and standard cameras, the solution supports remote, user-friendly identity verification without requiring specialised hardware.

REFERENCES

1) Keesing Biometrics, "Biometric Identity Proofing," https://www.keesingtechnologies.com/technologies/biometrics/.
2) Keesing Biometrics, "About Keesing," https://www.keesingtechnologies.com/about-keesing/.

BIOMETRIC ALERT

NOVEMBER 2025

By Dr. Carmen Bisogni, *Assistant Professor, 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 different sub-fields of biometrics that have been accepted by various IEEE journals over the past few months, either via early access or publication.

BEHAVIORAL BIOMETRICS

1. C. Brasile, S. Palese, M. Pazzini, C. Lantieri and V. Vignali, ”Freeways’ Road Safety Analysis Through Accident Database and Human Behavior,” in *IEEE Access*, vol. 13, May 2025.**DOI: 10.1109/ACCESS.2025.3570070**
2. Y. Hao, A. Ojha and Y. Liu, ”LSTM and GRU Based Lightweight Temporal Models for Edge Computing on Real-Time Individual Abnormal Behavior Recognition,” in *IEEE Transactions on Consumer Electronics,* June 2025. **DOI: 10.1109/TCE.2025.3582934**
3. S. Meng et al., ”From FastPoseGait to GPGait++: Bridging the Past and Future for Pose-Based Gait Recognition,” in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 47, no. 9, pp. 8231-8248, September 2025. **DOI: 10.1109/TPAMI.2025.3577594**
4. W. Shwe Sin Khine, P. Siritanawan and K. Kotani, ”Complex Emotion Estimation Using Analysis-by-Synthesis of Facial Expression Images,” in *IEEE Access*, vol. 13, pp. 88731-88746, May 2025. **DOI: 10.1109/ACCESS.2025.3570167**

5. S. Zhao, S. Li, Y. Zhang and S. Liu, ”Channel Self-Attention Residual Network: Learning Micro-Expression Recognition Features from Augmented Motion Flow Images,” in *IEEE Transactions on Affective Computing*, May 2025. **DOI: 10.1109/TAFFC.2025.3568633**

BIOMETRIC DATASETS AND SURVEYS

1. A. Rouco, C. Gouveia, D. Albuquerque, S. Brás, and P. Pinho, ”Biometric Identification via Through-Wall Radar: A Survey on Vital Signs and Gait Analysis,” in *IEEE Access*, vol. 13, June 2025. **DOI: 10.1109/ACCESS.2025.3583831**
2. H.O. Shahreza and S. Marcel, ”Foundation Models and Biometrics: A Survey and Outlook,”in *IEEE Transactions on Information Forensics and Security,* August 2025. **DOI: 10.1109/TIFS.2025.3602233**
3. W. Zhou et al., ”CASIA-PR-V1: A Multi-ethnic, Multi-device and Cross-spectral Dataset and a Multiscale Disentangled Model for Periocular Recognition,” in *IEEE Transactions on Multimedia*, August 2025. **DOI: 10.1109/TMM.2025.3599084**
4. M.A. Farooq, P. Kielty, W. Yao and P. Corcoran, ”SynAdult: Multimodal Synthetic Adult Dataset Generation via Diffusion Models and Neuromorphic Event Simulation for Critical Biometric Applications,” in *IEEE Access*, vol. 13, August 2025. **DOI: 10.1109/ACCESS.2025.3594875**
5. A. Shehata, F.M. Castro, N. Guil, M.J. Marín-Jiménez, and Y. Yagi, ”OUMVLP-OF: Multi-View Large Population Gait Database With Dense Optical Flow and Its Performance Evaluation,” in *IEEE Access,* vol. 13, May 2025. **DOI: 10.1109/ACCESS.2025.3570280**

CONTEXT-AWARE BIOMETRICS

1. J. Sameri et al., ”Physiology-driven User Perception Prediction for Networked Collaborative Virtual Reality,” in *IEEE Access*, November 2025. **DOI: 10.1109/ACCESS.2025.3635298**
2. P. Jonnalagedda and B. Bhanu, ”Novel Unified Body-based Biometric for Clothing Invariant Human Recognition,” in *IEEE Transactions on Biometrics, Behavior, and Identity Science*, November 2025. **DOI: 10.1109/TBIOM.2025.3631607**
3. I. Cho, J.H. Kwak and B.G. Lee, ”Mobile Banking Usage Through Biometric Authentication: Effects of Smartphone Attributes and Privacy Consent Index,” in *IEEE Access,* November 2025. **DOI: 10.1109/ACCESS.2025.3631849**
4. Y. Jiao, Y. Zhang, W. Liu and Z. Jiao, ”Detecting Driver Sleepiness From Physiological Indicators Using a CNN-LSTM Self-Attention Model,” in *IEEE Journal of Biomedical and Health Informatics*, November 2025. **DOI: 10.1109/JBHI.2025.3629974**
5. M.S. Chae et al., ”Eye-Blink and SSVEP-Based Selective Attention Interface for XR User Authentication: An Explainable Neural Decoding and Machine Learning Approach to

Reducing Visual Fatigue,” in *IEEE Access*, vol. 13, pp. 176998-177018, 2025.**DOI: 10.1109/ACCESS.2025.3613355**

FACE RECOGNITION AND ANALYSIS

1. S. Hemalatha et al., ”Security of Sensitive Data in Face Recognition System Applications: A Novel Encryption Approach,” in *IEEE Access*, vol. 13, pp. 169473-169489, 2025. **DOI: 10.1109/ACCESS.2025.3614266**
2. S. Wang, S. Chen, D-H. Wang, Y. Hua and Y. Yan, ”CAMD: Context-Aware Masked Distillation for General Self-Supervised Facial Representation Pre-Training,” in *IEEE Transactions on Circuits and Systems for Video Technology*, November 2025. **DOI: 10.1109/TCSVT.2025.3632418**
3. S. Chhabra, K. Thakral, R. Singh and M. Vatsa, ”PrIdentity: Generalizable Privacy Preserving Adversarial Perturbations for Anonymizing Facial Identity,” in *IEEE Transactions on Biometrics, Behavior, and Identity Science*, October 2025. **DOI: 10.1109/TBIOM.2025.3625986**
4. W. Xiong, M. Zhong, S. Li, G. Huang and L. Zhang, ”RUL: Region Uncertainty Learning for Robust Face Recognition,” in *IEEE Transactions on Multimedia,* September 2025. **DOI: 10.1109/TMM.2025.3613164**
5. J. Moonrinta, M.N. Dailey and M. Ekpanyapong, ”Improving Noisy Face Embeddings Using Time Series Transformers and Adaptive Triplet Loss,” in *IEEE Access,* vol. 13, pp. 174254-174269, 2025. **DOI: 10.1109/ACCESS.2025.3618156**
6. J. Wang, C. Shan, Z. Liu, S. Zhou and M. Shu, ”Facial Privacy Protection for Remote Photoplethysmography,” in *IEEE Journal of Biomedical and Health Informatics,* October 2025. **DOI: 10.1109/JBHI.2025.3624113**
7. J. Dan, Y. Liu, B. Sun, J. Deng and S. Luo, ”TransFace++: Rethinking the Face Recognition Paradigm with a Focus on Accuracy, Efficiency, and Security,” in *IEEE*

Transactions on Pattern Analysis and Machine Intelligence, September 2025. **DOI: 10.1109/TPAMI.2025.3616149**

8. W. Liu et al., ”Hidden Facial Verification Scheme in IoT Cloud Environment Based on Homomorphic Privacy Information Retrieval,” in *IEEE Internet of Things Journal*, November 2025. **DOI: 10.1109/JIOT.2025.3637285**
9. D. DeAlcala, A. Morales, J. Fierrez, G. Mancera, R. Tolosana and J. Ortega-Garcia, ”Is My Data in Your AI? Membership Inference Test (MINT) Applied to Face Biometrics,” in *IEEE Access,* vol. 13, pp. 163805-163819, 2025. **DOI: 10.1109/ACCESS.2025.3608951**
10. Y. Zhang, J. Ji, T. Wang, R. Zhao, W. Wen and Y. Xiang, ”Make Identity Indistinguishable: Utility-Preserving Face Dataset Publication with Provable Privacy Guarantees,” in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, September 2025. **DOI: 10.1109/TPAMI.2025.3605195**
11. H. Wang, W. Luo, X. Xie, P. Zheng, W. Huang and J. Huang, ”Adv-Inversion: Stealthy Adversarial Attacks via GAN-Inversion for Facial Privacy Protection,” in *IEEE Transactions on Information Forensics and Security,* vol. 20, pp. 11892-11906, 2025. **DOI: 10.1109/TIFS.2025.3625635**

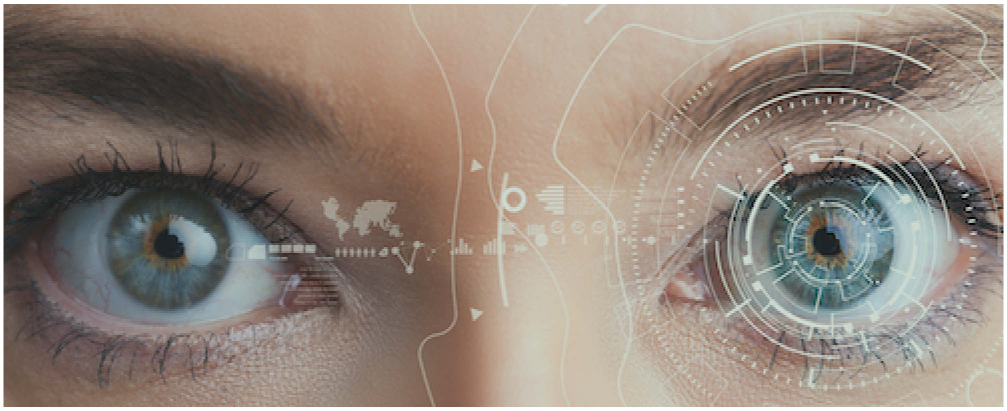
GENERATIVE BIOMETRICS

1. H. Kim and H. Kim, ”Data Reliability Testing Framework for Biometric Datasets Using Synthetic Iris and Fingerprint Images Generated via Deep Generative Models,” in *IEEE Access*, vol. 13, pp. 155084-155095, 2025. **DOI: 10.1109/ACCESS.2025.3604894**
2. L. Ming, P. He, H. Li, S. Wang and X. Jiang, ”Critical Contour Prior-Guided Graph Learning With Pose Calibration for Identity-Aware Deepfake Detection,” in *IEEE Transactions on Multimedia*, September 2025. **DOI: 10.1109/TMM.2025.3613159**
3. L. Cascone, M.D. Maio, V. Loia, M. Maucioni, M. Nappi and C. Pero, ”Synthetic Data for Fairness: Bias Mitigation in Facial Attribute Recognition,” in *IEEE Open Journal of the Computer Society,* vol. 6, pp. 1703-1714, 2025. **DOI: 10.1109/OJCS.2025.3622694**

IRIS AND PERIOCULAR RECOGNITION AND ANALYSIS

1. J.E. Tapia, S. Gonzalez, D. Benalcazar and C. Busch, ”Are Morphed Periocular Iris Images a Threat to Iris Recognition?” in *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 12417-12428, November 2025. **DOI: 10.1109/TIFS.2025.3632231**
2. N.A. Mashudi, N. Ahmad and N.M. Noor, ”Hybrid U-Net with ResNet Iris Segmentation Method for Occlusion by Eyelids and Eyelash in Iris Recognition,” in *IEEE Journal of Selected Topics in Signal Processing,* November 2025. **DOI: 10.1109/JSTSP.2025.3628533**

3. J. Yang et al., ”Enhancing Privacy-Preserved Iris Recognition in Consumer Electronics: A Soft Actor-Critic and GAN-Based Digital Forensic Framework with Bayesian Hyperparameter Optimization,” in *IEEE Transactions on Consumer Electronics*, October 2025. **DOI: 10.1109/TCE.2025.3625642**



MULTI-MODAL BIOMETRICS

1. Z. Zhang, W. Zhang and S. Pan, ”Fault-Tolerant Multibiometric Recognition System Based on Neural Network,” in *IEEE Transactions on Instrumentation and Measurement*, vol. 74, May 2025. **DOI: 10.1109/TIM.2025.356806**
2. R. Ryu, S. Yeom, D. Herbert and J. Dermoudy, ”From Fusion to Adaptation: Investigation on Enhancing Multimodal Biometric Authentication Systems,” in *IEEE Access*, vol. 13. **DOI: 10.1109/ACCESS.2025.3599907**
3. M.A. Farooq, P. Kielty, W. Yao and P. Corcoran, ”SynAdult: Multimodal Synthetic Adult Dataset Generation via Diffusion Models and Neuromorphic Event Simulation for Critical Biometric Applications,” in *IEEE Access*, vol. 13. **DOI: 10.1109/ACCESS.2025.3594875**
4. Y. Qiao, W. Kang, D. Luo and J. Huang, ”Normalized Full-Palmar-Hand: Toward More Accurate Hand-Based Multimodal Biometrics,” in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 47, no. 8. **DOI: 10.1109/TPAMI.2025.3564514**
5. I. Riaz, A.N. Ali, H. Ibrahim and I.A. Huqqani, ”Multimodal Biometric Recognition System Based on Feature-Level Fusion of Dorsal Finger Crease and Finger Knuckle Print,” in *IEEE Transactions on Artificial Intelligence*, April 2025. **DOI: 10.1109/TAI.2025.3563315**

PHYSIOLOGICAL SIGNAL-BASED BIOMETRICS

1. M.G. Preti, D. Van De Ville and E. Amico, ”Brain Fingerprinting: A Signal Processing Perspective,” in *IEEE Signal Processing Magazine*, vol. 42, no. 4, pp. 91-102, July 2025. **DOI: 10.1109/MSP.2025.3615296**

2. H. Guo, B. Wei, W. Fan, S. Liu, F. Jiang and C. Yi, ”PPTP: Performance-Guided Physiological Signal-Based Trust Prediction in Sequential Human-Robot Collaboration,” in *IEEE Robotics and Automation Letters*, vol. 10, no. 12, pp. 13256-13263, December 2025. **DOI: 10.1109/LRA.2025.3629986**
3. R. Yuvaraj, S. Samyuktha, J. Fogarty, J.S. Huang, S. Tan and W.T. Kiong, ”Automated Boredom Recognition Using Multimodal Physiological Signals,” in *IEEE Transactions on Affective Computing*.**DOI: 10.1109/TAFFC.2025.3619979**
4. V. Cipollone, N. Morresi, S. Casaccia and G.M. Revel, ”A Questionnaire-Free Approach for Thermal Comfort Measurement Using Unsupervised Machine Learning on Physiological Signals,” in *IEEE Sensors Journal,* 2025. **DOI: 10.1109/JSEN.2025.3618404**
5. H. Chen et al., ”Quantifying Emotional Patterns for EEG-based Emotion Recognition: An Interpretable Study on EEG Individual Differences,” in *IEEE Transactions on Affective Computing*. **DOI: 10.1109/TAFFC.2025.3614727**
6. K. Cui, J. Li, Y. Liu, X. Zhang, Z. Hu and M. Wang, ”PhysioSync: Temporal and Cross-Modal Contrastive Learning Inspired by Physiological Synchronization for EEG-Based Emotion Recognition,” in *IEEE Transactions on Computational Social Systems*. **DOI: 10.1109/TCSS.2025.3602913**
7. F. Ma, H. Luo, Z. Guo, J. Wang and P. Zhang, ”Multilevel Spatiotemporal Modeling Network for Emotion Recognition With Multimodal Physiological Signals,” in *IEEE Transactions on Instrumentation and Measurement*, vol. 74, pp. 1-14, 2025, Art no. 2548514. **DOI: 10.1109/TIM.2025.3618736**

SECURITY AND ANTI-SPOOFING IN BIOMETRICS

1. A. Susi, V. Akila and V. Govindasamy, ”Utilizing rPPG Signal Synchronization and Deep Learning Techniques for Deepfake Video Detection,” in *IEEE Access*, August 2025. **DOI: 10.1109/ACCESS.2025.3604336**
2. N.G. Venkataswamy, O. Olugbenle, M.K. Banavar and M.H. Imtiaz, ”Descriptor: Contactless Fingerprint Image Streams and Heart Rate (CFISHR),” in *IEEE Data Descriptions*, July 2025. **DOI: 10.1109/IEEEDATA.2025.3592172**
3. J. Su Kim and S. Pan, ”Fake Electrocardiogram Signal Analysis to Detect Spoofing Attacks in Biometrics,” in *IEEE Sensors Journal,* vol. 25, no. 14, June 2025, **DOI: 10.1109/JSEN.2025.3577311.**
4. H. Qin et al., ”WTxGRN: Wavelet Transform-Based Extended Gated Recurrent Network for Palm Vein Recognition,” in *IEEE Transactions on Information Forensics and Security*, vol. 20, July 2025. **DOI: 10.1109/TIFS.2025.3592561**

5. Y. Wang, J. Gui, X. Shi, L. Gui, Y.Y. Tang and J.T.Y. Kwok, ”ColorVein: Colorful Cancelable Vein Biometrics,” in *IEEE Transactions on Information Forensics and Security*, vol. 20. **DOI: 10.1109/TIFS.2025.3562690**
6. T. Xie and W. Kang, ”A Random-Binding-Based Bio-Hashing Template Protection Method for Palm Vein Recognition,” in *IEEE Transactions on Information Forensics and Security*, vol. 20. **DOI: 10.1109/TIFS.2025.3559791**
7. Z. Cheng and X. Zhang, ”Integrating Fine-Grained Classification and Motion Relation Analysis for Face Anti-Spoofing,” in *IEEE Access*, vol. 13, pp. 93649-93660, 2025. **DOI: 110.1109/ACCESS.2025.3573790**
8. R. Akbari, L. Sperling, N.R.A. Ross and V.N. Boddeti, ”Homomorphically Encrypted Biometric Template Fusion and Matching,” in *IEEE Transactions on Biometrics, Behavior, and Identity Science,* August 2025. **DOI: 10.1109/TBIOM.2025.3595438**
9. Y. Lu, S. Wang, G. Zhu, Z. Zhang and J. Huang, ”FGMIA: Feature-Guided Model Inversion Attacks Against Face Recognition Models,” in *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 8465-8480, 2025. **DOI: 10.1109/TIFS.2025.3592542**
10. S. Li, J. Hu, B. Zhang, X. Ning and L. Wu, ”Dynamic Personalized Federated Learning for Cross-Spectral Palmprint Recognition,” *in IEEE Transactions on Image Processing,* vol. 34, pp. 4885-4895, 2025.**DOI: 10.1109/TIP.2025.3592508**

SPEECH BIOMETRICS AND ACOUSTIC ANALYSIS

1. X. Sun et al., ”SCR-Auth: Secure Call Receiver Authentication on Smartphones Using Outer Ear Echoes,” in *IEEE Transactions on Information Forensics and Security*, vol. 20, July 2025, **DOI: 10.1109/TIFS.2025.3584643**
2. S. Gupta et al., ”Neural Forensic Analysis for Privacy and Integrity Protection in Biometric Authentication Systems,” in *IEEE Transactions on Consumer Electronics*, July 2025. **DOI: 10.1109/TCE.2025.3593968**

CALL FOR CONTRIBUTIONS

20th IEEE International Conference on Automatic Face and Gesture Recognition

25-29 May 2026, Istanbul, Türkiye

https://fg2026.ieee-biometrics.org/

FG 2026
KYOTO 京
The 20th IEEE International Conference on Automatic Face and Gesture Recognition
May 25-29, 2026, Kyoto Research Park (KRP), Kyoto, Japan

The IEEE conference series on Automatic Face and Gesture Recognition is the premier international forum for research in image and video-based face, gesture, and body movement recognition. Its broad scope includes advances in fundamental computer vision, pattern recognition, computer graphics, and machine learning techniques relevant to face, gesture, and body action, as well as innovative algorithms and analyses of specific applications.

Though the initial deadline for paper submissions has passed, Round 2 paper submissions, as well as submissions for tutorial and demonstration proposals, are still open. Note the relevant deadlines below.

IMPORTANT DATES

Abstract submission deadline (new Round 2 paper submissions only): **January 9, 2026**
Tutorial proposals due: **January 13, 2026**
Paper submission deadline (all papers): **January 15, 2026**
Notification of acceptance (tutorials**): January 27, 2026**
Notifications to authors (papers): **April 2, 2026**

Demonstration one-page proposal and supplementary material: **April 9, 2026**
Notification of acceptance (demonstrations): **April 16th, 2026**
Camera Ready (for papers from both submission round): **April 21, 2026**
Camera Ready (demonstrations): **April 21, 2026**

Main Session Papers

FG 2026 uses a two-round reviewing procedure, and the deadline is approaching for Round 2 paper submissions. Unlike papers submitted in Round 1, the final decision will be made without an opportunity for a rebuttal. Submissions to Round 2 may be either new papers or revised papers from Round 1. Revised papers from Round 1 are re-evaluated based on the original reviews and the authors' response.

Topics of interest include, but are not limited to:

- Face, gesture, and body detection and tracking
- Robust recognition under varying conditions (pose, occlusion, illumination)
- Generative modelling and neural rendering (e.g., deepfakes, AR/VR)
- Advanced learning paradigms (self-supervised, few-shot, foundation models)
- Soft biometrics and behavioural analysis (emotion, personality, demographics)
- Multimodal fusion and cross-modal analysis
- Benchmark development and dataset creation
- Cognitive and bio-inspired vision systems
- Bias mitigation, interpretability, and ethical considerations
- Real-world applications and deployment studies

Call for Workshop Proposals

Accepted workshops will be held on either May 25 or May 29, 2026, in the same venue as the FG 2026 main conference. Complementary to the main proceedings, we especially encourage workshop proposals relating to emerging new fields or new application domains of face and gesture analysis and synthesis. For the submission procedure and contact details, go to https://fg2026.ieee-biometrics.org/workshops/.

Call for Tutorial Proposals

We solicit proposals on any topic of interest to the FG community. Interdisciplinary topics that could attract a significant cross-section of the community are highly encouraged. Tutorials should complement and enhance the scientific program of FG 2026 by providing authoritative and comprehensive overviews of growing themes that are of sufficient relevance with respect to the state-of-the-art and the conference topics.

We particularly welcome tutorials that address advances in emerging areas not previously covered in an FG related tutorial. Accepted tutorials will be held on either May 25 or May 29, 2026, in the same venue as the FG main conference.

For submission and review procedure and contact details, go to https://fg2026.ieee-biometrics.org/tutorials/

Call for Proposals for Demonstration Sessions

The conference organizers invite researchers from academia and industry to present live demonstrations of their research findings and face/gesture recognition systems to conference participants. These demonstrations aim to provide tangible, practical, and interactive validation of the presenters' research concepts and scientific or engineering contributions. The primary objective is to offer researchers and practitioners a platform for discussing operational face/gesture recognition systems, applications, prototypes, or proof-of-concepts. Such a setting enables conference attendees to witness cutting-edge research in action.

Demos are NOT restricted solely to the papers accepted by FG 2026 or its associated workshops. We encourage the submission of any demo that demonstrates the effectiveness of face and gesture recognition methods. These demos may originate from papers accepted at other venues (e.g., extended works), such as peer-reviewed conferences or journals. However, it is expected that these demos present innovative and novel research outcomes.

We strongly encourage submissions in all areas related to face and gesture analysis and synthesis, as outlined in the general call for papers for IEEE FG 2026, which can be found at https://fg2026.ieee-biometrics.org/

CALL FOR PAPERS AND PROPOSALS

IEEE INTERNATIONAL JOINT CONFERENCE ON BIOMETRICS
(IJCB 2026)
1-4 September 2026, Rome, Italy
Full paper submission: April 10, 2026
IEEE
Biometrics Council

https://ijcb2026.ieee-biometrics.org

The **IEEE International Joint Conference on Biometrics (IJCB 2026)** is the premier international forum for cutting-edge research in biometrics and related areas. IJCB brings together two major conferences — the IEEE Biometrics Theory, Applications, and Systems (BTAS) and the IAPR International Conference on Biometrics (ICB) — and is sponsored by the **IEEE Biometrics Council** and the **IAPR Technical Committee on Biometrics (TC-4)**.

The **2026 IJCB** will be held in **Rome, Italy,** from **1-4 September.** Organizers are now soliciting proposals for papers, special sessions, and competitions. Below are the specific submission details for each category.

CALL FOR PAPERS

Important Dates

Full paper submission	**April 10, 2026**
Notification of acceptance	**June 10, 2026**
Camera-ready submission date	**July 10, 2026**

We invite submissions of **original and unpublished research papers** addressing theoretical advances, applications, and interdisciplinary developments in biometrics. Submissions under review elsewhere will **not** be considered.

Topics of Interest

Topics may include, but are not limited to, the following areas:

- Biometric modalities: face, fingerprint, iris, palmprint, vein, periocular, ear, voice, gait, signature, touch dynamics, behavioral biometrics
- Deepfake detection and AI-generated content verification
- Multimodal and multispectral biometric systems
- Presentation Attack Detection (PAD) and anti-spoofing techniques
- Template security and privacy protection: encryption, secure storage, anonymization, differential privacy
- Bias, fairness, explainability, and transparency in biometric systems
- Machine learning for biometrics: deep learning, transfer learning, continual learning, efficient/compact models, transformers
- Evaluation protocols and benchmarking, performance modeling, new datasets and large-scale studies
- Biometrics in forensics and law enforcement, large-scale identification, and border control
- Emerging applications: IoT, wearable devices, mobile biometrics, healthcare, human-computer interaction
- Ethical, legal, and societal implications: compliance with regulations (GDPR, AI Act), human rights, societal acceptance

Submission Guidelines

- Manuscripts must be in **English,** and be formatted according to the **IEEE conference template**.
- Maximum length: 8 pages (excluding references).
- The review process will be **double-blind**. Authors must remove all personally identifying information, including names and affiliations.
- Submissions must be made electronically via the conference submission portal, which will be available on the official IJCB 2026 website.

Accepted papers will be published in ***IEEE Xplore****,* provided they meet IEEE's publication and quality standards.

CALL FOR SPECIAL SESSION PROPOSALS

Important Dates

Special Session proposals due	**January 31, 2026**
Notification of acceptance	**February 15, 2026**
Paper submission date	**April 10, 2026**
Decision deadline:	**June 10, 2026**
Camera-ready submission date	**July 10, 2026**

The IJCB 2026 technical program will include a limited number of Special Sessions that enrich the regular conference program by introducing new or emerging topics of particular interest to the biometrics community. In particular, the organizers welcome areas of research that are not yet consolidated, as long as the organizers can provide a thorough and scientifically convincing rationale for their interest.

Special Session organizers should submit proposals containing the following information:

- Special session title
- A clear description/list of the addressed topic and the subjects that fall within its scope
- A description of the significance and novelty of the topic and the scientific motivation for the proposed session. The presence of possible interdisciplinary aspects is also welcome, and the proposal should include an overall answer to the question: "Why should the topic of the special session be considered in a separate combined session, rather than the main track of the conference?"

- Names, affiliations, and short biographies of the organizers that highlight their expertise in the area of the Special Session. The organizer's expertise in the proposed topical areas is of paramount importance, and represents a core selection criterion. Providing a relevant publication list helps to satisfy this criterion.
- A list of research groups currently active in the designated area, and potential contributors
- A list of up to six (6) potential contributed papers for the session. For each paper, the organizers should list the title, authors, contact information for each corresponding author, and a short abstract.

Upon acceptance of the Special Session proposal, a Call for Papers will be publicized via the IJCB 2026 website and mailing lists. The contributed papers will be submitted in the same format as regular papers. **Organizers should contribute only one paper.**

Proposals will be evaluated on the timeliness of the topic and the organizers' qualifications. Papers in each accepted Special Session will undergo a review process similar to the one employed for regular papers.

Inquiries and completed submissions should be sent to the Special Sessions chairs listed below as a PDF attachment to an email. The chairs are:

- Maria de Marsico (maria.demarsico@uniroma1.it)
- Andreas Uhl (uhl@cs.sbg.ac.at)
- P.C. Yuen (pcyuen@comp.hkbu.edu.hk)
- Clinton Fookes (c.fookes@qut.edu.au)

CALL FOR COMPETITION PROPOSALS

IMPORTANT DATES

Competition proposals due	**January 31, 2026**
Acceptance decisions to organizers	**February 15, 2026**
Summary paper submission date	**May 30, 2026**
Acceptance notification to authors of summary papers	**June 14, 2026**
Camera-ready submission date	**June 23, 2026**

The main goals of the IJCB competitions are to:

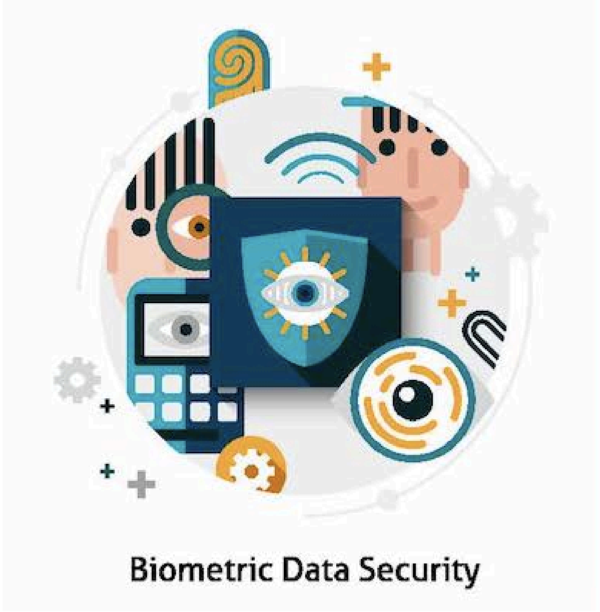
- provide a common ground for benchmarking,
- push the boundaries of state-of-the-art algorithms,
- consolidate research, and
- identify open problems in biometrics-related research areas.

Competition proposals on any topic of interest to the broader biometric community are welcome, and we strongly encourage proposals that focus on emerging fields, and open research questions that will attract a significant number of participants. Competition organizers with a strong track record in the field are particularly valued.

The principal selection criteria for competitions will be:

- Novelty
- Relevance and timeliness of the problem explored
- Importance of the research questions investigated
- Potential to attract a large number of competitors
- Impact of the competition, and,
- Track record of the organizers.

The deadline for submitting competition proposals is **January 31, 2026**. Decisions will be made by **February 15, 2026.**



Submission Criteria

Proposals should be sent to the **IJCB 2026 COMPETITION** co-chairs Abhijit Das, Marija Ivanovska, Daniel Moreira, and Massimiliano Todisco with the email subject: *IJCB 2026 Competition Proposal: [title of your competition]* All emails are listed below.

To facilitate the decision process, proposals should include the following information:

- Title
- Names, affiliations, contact information, and a brief CV of the competition organizers
- A list of the three most relevant publications related to the competition for each organizer
- A justification for the competition that includes:
    - Motivation for the competition, expected outcomes and anticipated impact
    - Relevance to IJCB 2026
    - Relationship to previous competitions (if any)
    - Description of the novelty of the competition
- Execution:
    - Description of the dataset(s) used for the competition and the available annotations
    - Details on the experimental protocol and result generation/submission procedure
    - Information on the platform used (for data sharing, submission, and verification of the results, if any)
    - Description of the evaluation criteria (performance metrics) and available baseline implementations/code (e.g., a starter kit).
- Organization:
    - Expected minimum number of external participants, other than the organizers
    - Plan for promoting the competition and attracting participants
    - Description of the planned coordination activities
    - A detailed timeline for the competition

Schedule

The competitions should start by the beginning of March 2026 and be completed by the summary paper submission deadline of May 2026. Competition organizers will also be requested to prepare a web page that will be linked to the conference web site. The website should be online 7 days after the competition proposal has been accepted.

Proceedings and Presentations

Competition organizers will be invited to submit a summary paper discussing organization, datasets, and results **by May 30, 2026.** Summary papers will be considered for inclusion in the IJCB 2026 conference program. These papers should follow the same formatting and presentation rules as regular papers, and will undergo the same review process. The presentation format (if accepted) will be determined based on the quality of the submission and reviewer feedback received. Accepted summary papers will be included in the proceedings of IJCB 2026 and sent for inclusion in *IEEE Xplore.* **NOTE:** Summary papers should not be anonymized.

For any additional information, please contact the IJCB 2026 Competition Co-Chairs as follows:

- Abhijit Das (abhijit.das@hyderabad.bits-pilani.ac.in)
- Marija Ivanovska (marija.ivanovska@fe.uni-lj.si)
- Daniel Moreira (dmoreira1@luc.edu)
- **Mas**similiano Todisco (todisco@eurecom.fr)

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 paper selected for this issue's ***Noted in the Literature*** section.

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

Dr. Chiara Galdi, who prepared both the ***Source Code*** and ***Commercial Off-the-Shelf Systems*** biometric products columns.

Dr. Emanuele Maiorana, who curated the items for the ***In the News*** section.

Dr. Emanuela Marasco, who wrote the ***Database Digest*** report on EyeNavGS, the first publicly available dataset to capture full 6-degrees-of-freedom (6-DoF) navigation for users interacting with real-world scenes reconstructed in VR via 3D Gaussian Splatting (3DGS).

Dr. João C. Neves, who interviewed **Andrea Carmignani,** co-founder and CEO of Keyless, for our ***Expert Perspectives*** section.

Dr. Ruben Tolosana, who interviewed **Francisco M. Castro**, an Associate Lecturer at the University of Málaga, Spain, for the ***Researcher on the Rise*** section.