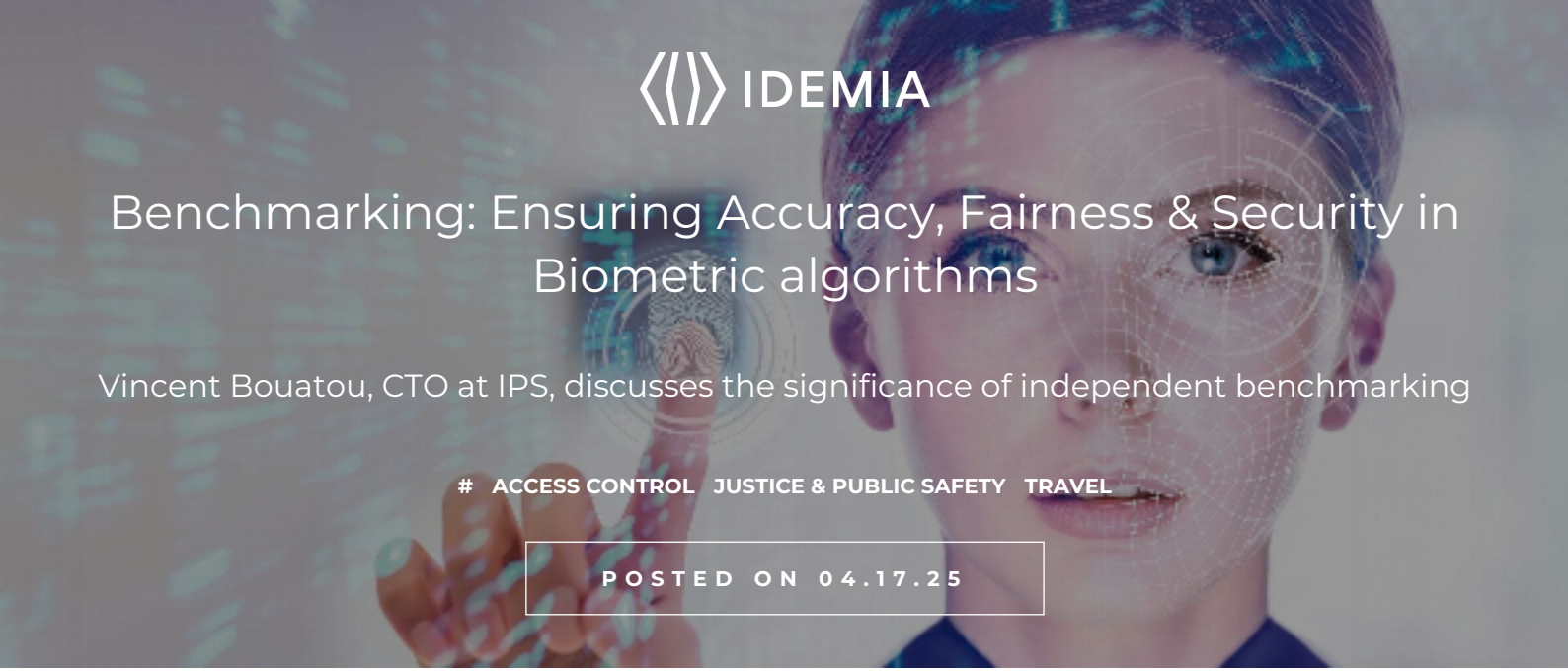

Benchmarking: Ensuring Accuracy, Fairness & Security in Biometric algorithms

Vincent Bouatou, CTO at IPS, discusses the significance of independent benchmarking

ACCESS CONTROL JUSTICE & PUBLIC SAFETY TRAVEL

POSTED ON 04.17.25

Biometric technology is essential for identity verification, security, and fraud prevention. But accuracy and fairness are only part of the challenge—systems must also resist sophisticated threats like spoofing and morphing. Independent benchmarking organizations rigorously test biometric algorithms to assess their performance, helping stakeholders choose the most reliable solutions.

To learn more about the importance of independent benchmarking and how IDEMIA Public Security continues to lead in innovation and security, we spoke with Vincent Bouatou, Chief Technology Officer at IDEMIA Public Security.

Why is independent benchmarking important for biometric technologies?

Independent benchmarking is crucial for assessing the accuracy, fairness, and reliability of biometric technologies. By evaluating systems on sequestered data, these tests provide an unbiased view of performance, confirming that technologies meet high standards. IDEMIA Public Security leads in facial recognition matching accuracy, but we also prioritize fairness and inclusivity. Our facial identification algorithm has reached a level of efficiency where biases are no longer measurable, a claim few can confidently make.
Regular independent testing encourages continuous improvement in the industry. These evaluations highlight areas for refinement, pushing companies to invest in R&D in order to prevent progress from stagnating.

What role do independent benchmarks and compliance play in upholding fair and accurate biometric technology?

Independent benchmarks and compliance are essential for ensuring the ethical performance of biometric technologies. These evaluations provide neutral, unbiased assessments, helping clients select solutions that deliver top performance in accuracy, fairness, and reliability. In automated systems like eGates and kiosks, for example, image quality directly impacts recognition accuracy, and independent testing makes sure systems can handle challenges such as lighting, alignment, and clarity.
Additionally, compliance with national and regional regulations reinforces fairness, guaranteeing that systems not only perform well but also adhere to legal and ethical standards. These independent assessments foster a transparent, responsible ecosystem, building trust and encouraging widespread adoption across industries like security, travel, and physical and logical access control.

How can organizations verify claims of fairness and accuracy in biometric technologies?

Many companies state that their biometric algorithms are the most accurate and unbiased, but independent benchmarking organizations provide the objective validation needed. Establishments like the National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) conduct rigorous testing, evaluating biometric algorithms on their efficiency and accuracy. They then publish results, which are available to the public.
IDEMIA Public Security has continuously participated in NIST benchmarking for iris, face, and fingerprint and palmprint recognition, ranking among the top performers. Our 1:N facial recognition algorithm achieved the highest accuracy and fairness scores in the 2024 Face Recognition Vendor Test (FRVT). In the same year, we also ranked #1 in the NIST Proprietary Fingerprint Template (PFT), Age Evaluation Verification (AEV), and Evaluation of Latent Fingerprint Technologies (ELFT) tests.

What is the Face in Video Evaluation, and why is it important?

The Face in Video Evaluation (FIVE) by NIST is a critical initiative designed to assess the accuracy and robustness of facial recognition algorithms in video sequences. Unlike static images, video presents unique challenges, such as varying angles, lighting conditions, occlusions, and motion blur. FIVE focuses on evaluating the algorithms to verify consistent and accurate identification across these factors, simulating real-world scenarios more effectively than still-image assessments. The importance of FIVE lies in providing objective and standardized performance benchmarks for facial recognition systems, particularly in open-set identification where the goal is to recognize individuals from a pool of unknown subjects. In these settings, the system must identify familiar faces and correctly determine when a face does not belong to any preregistered individuals. FIVE's results are instrumental for sectors like security, law enforcement, and public safety.

What impact do NIST rankings have on law enforcement and public security operations?

Our leading position in ELFT means that forensic investigations can be conducted more efficiently, allowing law enforcement agencies to solve criminal cases faster. Similarly, the #1 ranking in PFT evaluations enables seamless one-to-one fingerprint verification, strengthening national security measures such as border control and secure access management. These advancements enable agencies to operate with greater accuracy and speed, ultimately contributing to public security.

What threats do biometric systems need to guard against?

Biometric systems must withstand sophisticated spoofing attempts. One major threat is presentation attacks, where individuals disguise themselves to impersonate someone else and fraudulently use their identity documents, such as passports. These attacks can take many forms, including makeup, masks, or even holding up a photo or digital display to mislead recognition systems.
Another significant challenge is morphing attacks. This technique blends the digital images of two individuals to create a synthetic hybrid that shares facial features from both original subjects. Because these manipulated images incorporate genuine characteristics from each person, they can deceive both human inspectors and even highly advanced facial recognition algorithms. The complexity of these threats underscores the need for cutting-edge countermeasures to safeguard biometric authentication systems.

Independent benchmarking organizations thoroughly test biometric solutions for their ability to detect presentation attacks (such as the DHS S&T “RIVTD”) and morphing attempts (such as NIST’s FATE MORPH).

What sets IDEMIA Public Security apart in biometric technology?

A biometric system’s performance relies on numerous subcomponents that collectively determine its efficiency. For instance, even the most accurate algorithms can be undermined by a subpar camera, affecting the overall result. At IDEMIA Public Security, we not only develop top-tier matching and detection algorithms but also ensure that every subcomponent in our solutions, such as quality assessment, detection, segmentation—essentially also developed by us—meets the highest standards. We take full responsibility for every element of our solutions, consistently delivering on our promises and prioritizing customer satisfaction.

How does IDEMIA Public Security’s performance in NIST benchmarks reflect its commitment to innovation in biometric solutions?

Our consistent top performance in NIST benchmarks, including ELFT and PFT tests, reflects our dedication to biometric technologies. We continue to demonstrate a commitment to innovation that supports the evolving needs of law enforcement and public security agencies by improving the accuracy and efficiency of our fingerprint recognition algorithms. These achievements reinforce our leadership in the biometric industry and also keep our solutions at the forefront of technological advancements, providing agencies with cutting-edge tools to enhance their operations.