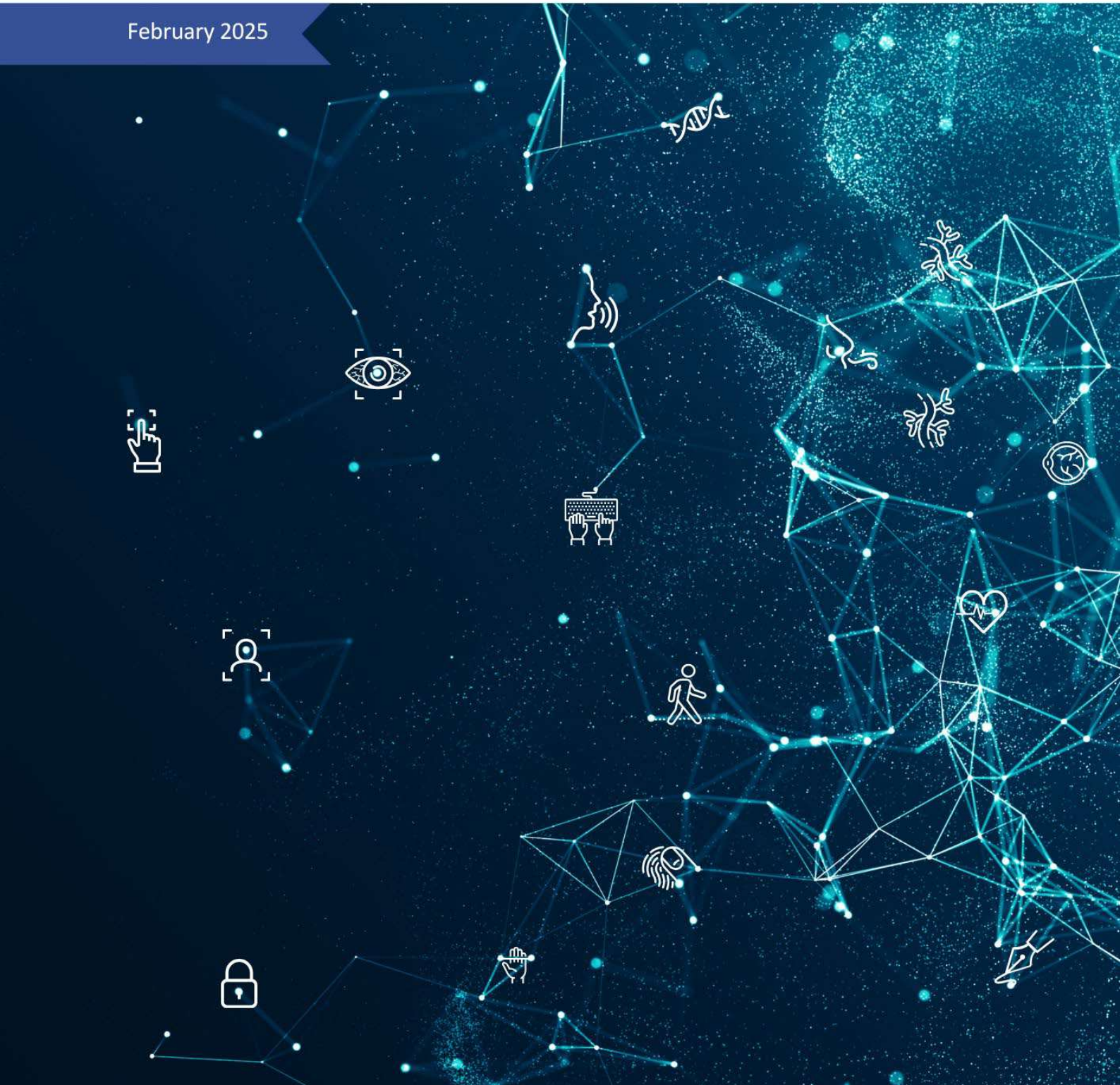
Biometrics Institute Concepts and Solutions Report

The future of responsible biometrics

February 2025



Contents

1. Introduction

This edition of the *Biometrics Institute Concepts and Solutions Report* focuses **on the future of responsible biometrics – what trends we are seeing and solutions that are available,** from Biometrics Institute members. Building upon the success of our previous reports, which have been downloaded over 16,000 times, this 2025 edition aims to provide valuable insights and guidance as biometrics continue to permeate every aspect of our lives.

The public increasingly demands **transparency and accountability** regarding biometric systems, emphasising the need for trust and public confidence. Ensuring impartiality, clearly defined usage, and robust controls is paramount. This report focuses on these aspects, exploring how to achieve responsible biometric implementations in systems that interact with the public.

The submissions within this report offer valuable thought leadership from industry experts who are members of the Biometrics Institute. They present real-world insights, lessons learnt, and tested solutions, addressing the ethical and responsible use of biometrics both today and in the future.

This report addresses several key themes, including:

- Challenges the world is facing and potential solutions for responsible biometrics
- How privacy is changing and how biometrics respond to it
- Impacts of governance and new legislation
- Is AI outsmarting us: Deepfakes – how to detect them and prevent their use
- Communicating biometrics: How to improve public education on biometrics
- Responsible biometric data-sharing (e.g., for re-use, interoperability or specific use cases like counter-terrorism)
- Different use cases for the future of responsible biometrics (e.g., behavioural biometrics)
- Is multimodal the next wave and why? Mitigating risk with a multi technology approach
- Biometrics and AI – friend or foe?
- Remote identity verification – good practices and solutions
- Preventing and recovering from account takeover and the role of biometrics
- Digital passports – what is available and what will come next?
- Biometrics, borders, and travel – future trends and available solutions
- Migration challenges and the role of biometrics
- DNA – How we use it and what comes next
- Biometrics and vulnerable people – creating greater inclusion and safety

Please note that the Biometrics Institute does not endorse any of the submissions or products featured in this report and the adverts. This compilation aims to facilitate discussion and knowledge sharing within the biometric community as we collectively navigate the challenges and opportunities presented by this rapidly evolving field.

For any questions regarding the content of specific submissions, please contact the respective authors directly. For anything else relating to the work that the Biometrics Institute does, please contact me

Many thanks

Isabelle Moeller
Chief Executive
Biometrics Institute
manager@biometricsinstitute.org

2. Auraya: Responsible Biometrics in a Changing World

The world stands at the intersection of unprecedented technological innovation and increasing societal challenges. From privacy concerns to governance changes, the rapid evolution of artificial intelligence (AI) and biometrics has transformed how we authenticate identity, secure sensitive information, and enable digital interactions.

Challenges the World Is Facing and the Role of Voice Biometrics

The digital world is scary. Challenges such as data breaches, identity theft, deepfake fraud, and exclusion of vulnerable populations, or frustrating interactions with service providers call for innovative solutions. Take remote identity verification, for example. With so many of us now working from home or managing our lives online, proving who we are, has never been more important—or more challenging. Voice biometrics changes all that. By analysing the unique characteristics of your voice, it provides a secure, seamless way to confirm who you are, without the hassle or risk of old-school methods.

Evolving Privacy Concerns

One of the primary hurdles to biometric adoption is public scepticism, fuelled by misconceptions about data privacy and misuse. Voice biometrics offers an opportunity to reshape this narrative by emphasising transparency, simplicity, and user empowerment. Voice biometrics offers real-time fraud detection, empowering organisations to meet stringent compliance standards in regulated sectors such as finance, healthcare, and government.
Educational campaigns can demystify voice biometrics, highlighting its privacy-focused design and practical use cases. For example, showcasing applications in contact centres, digital banking, and applications can illustrate how voice biometrics simplifies processes while safeguarding data. Collaboration with advocacy groups and regulators can further enhance public understanding and trust.

AI Deepfakes and Synthetic Voices

If you've heard a synthetically generated audio, you know how unsettling it can be, with the potential to disrupt trust and security across domains. AI-generated deepfake audio and synthetic voices are becoming increasingly sophisticated, posing significant threats to trust and security. These technologies can mimic individuals with uncanny accuracy, leading to scenarios where malicious actors can impersonate voices to deceive, defraud, or manipulate.
Voice biometrics serves as a critical countermeasure by accurately distinguishing between genuine and synthetic voice inputs. Advanced algorithms analyse degrees like vocal tone, pitch, and speech patterns to detect deepfake-generated voices, providing a superior level of protection against malicious actors. By integrating advanced AI and deep machine learning, voice biometric systems can continuously adapt to evolving threats, ensuring robustness and reliability.

What's Next? A Multimodal Future

The future of biometrics lies in multimodal approaches that combine multiple authentication methods for enhanced security and inclusivity. Voice biometrics plays a pivotal role in this ecosystem, complementing other modalities like facial recognition and fingerprint scanning. By integrating voice biometrics into multimodal systems, organisations can mitigate risks associated with individual modalities, such as spoofing or environmental limitations. Voice biometrics plays a crucial role in this ecosystem. For instance, in low-light conditions where facial recognition systems struggle, voice biometrics provides a reliable alternative. Similarly, in environments where fingerprint scanning may not be feasible due to hygiene concerns or physical limitations, voice biometrics ensures accessibility and security.

Inclusion and Empowerment

Biometric solutions must prioritise inclusivity to ensure that security and convenience are accessible to all, regardless of physical ability, age, or socioeconomic status. Voice biometrics exemplifies this human-centric approach by enabling secure and dignified interactions for marginalised and vulnerable populations.
For elderly individuals, voice biometrics provides a user-friendly alternative to complex passwords or physical authentication devices. Persons with disabilities benefit from voice-based authentication systems that require no

physical interaction. Similarly, individuals without access to traditional identification documents can use voice biometrics to access essential services like banking, healthcare, and social welfare programs.
Voice biometrics is already making an impact in areas such as telemedicine, where secure voice verification enables patients to access remote consultations without compromising privacy. In social welfare disbursements, voice biometrics ensures that benefits reach the intended recipients, reducing fraud and administrative inefficiencies.

Biometrics and AI: Friend or Foe?

The convergence of biometrics and artificial intelligence (AI) presents both groundbreaking opportunities and pressing challenges, particularly in the fight against bad AI. As AI technologies enable the creation of highly convincing deepfake voices, the risks of identity fraud, misinformation, and security breaches escalate. This makes the role of good AI, such as voice biometrics, even more critical. By using ethical AI to counteract malicious uses, voice biometrics not only restores trust but also strengthens security in a world increasingly threatened by deepfake manipulation. The path forward demands innovation rooted in responsibility, where technologies like voice biometrics serve as essential tools to safeguard identity and rebuild confidence in digital interactions.

Voice biometrics is redefining security and trust in a rapidly evolving digital world, addressing challenges like identity fraud, deepfakes, and inclusivity gaps. With its ability to enhance security, empower marginalised populations, and integrate seamlessly into multimodal systems, voice biometrics is a vital tool for the future. Responsible innovation, ethical practices, and collaboration will ensure biometrics and AI serve as forces for good, creating a safer and more equitable digital landscape.

Organisation: Auraya
Name: Aayush Kamora
Contact: info@aurayasystems.com

3. Biometix: Why Human Expertise Remains Critical in Identity Recognition

In a world increasingly reliant on biometrics, artificial intelligence (AI) and automation, it's tempting to assume that machines are poised to dominate every facet of our lives. Yet, in identity recognition, human expertise remains irreplaceable. Despite remarkable advancements in biometric technology, the human-in-the-loop (HITL) approach, where human judgment complements AI decision-making, is our best safeguard against errors, system failures, biases, and unforeseen complexities. This balance is vital for ensuring ethical and responsible use of biometrics, particularly in systems that directly impact the public.

The Case for Human Expertise

Human oversight in identity recognition is indispensable across industries. In the financial sector, for example, bank personnel routinely resolve identity conflicts and detect fraud—tasks that often require nuanced judgment beyond the capabilities of machines. Similarly, at airports, frontline staff validate identities, enforce security protocols, and navigate complex cultural, legal, and ethical considerations. These roles extend beyond operational functions to strategic responsibilities.

Humans excel at identifying anomalies, adapting to unexpected situations, and ensuring fairness and inclusivity. While AI systems are exceptional at analysing patterns, they struggle in nuanced contexts where outliers or subtle indicators of fraud require human intuition and contextual understanding.

Lessons from Research

Research underscores the importance of human involvement in identity recognition:

- Mitigating Bias: AI systems, despite their sophistication, can unintentionally perpetuate biases in biometric recognition. Human oversight is crucial for identifying and addressing these biases, thereby ensuring that systems promote fairness and equity.
- Improving Accuracy: Machines thrive on patterns but falter with outliers. For instance, facial recognition systems can perform poorly with people with certain medical conditions, from certain demographics, or even those using older devices. Human expertise bridges these gaps, enhancing the reliability of automated systems.
- Offline Capabilities: There are many circumstances where people who are verifying people will need to fall back to the manual assessment of biometric identity. This includes where hardware systems fail, where additional manual verification is mandated, or if a person has deliberately created a denial of service (i.e. by destroying the chip on a passport).
- Identifying New Vulnerabilities: Where there is no human in the loop any unknown vulnerabilities might slip through undetected. Having humans review some selection of verifications provides the chance for a human operator to spot such vulnerabilities. before they become a problem.

These insights emphasise the importance of a collaborative approach to identity recognition, where humans and AI work in tandem to achieve ethical and effective outcomes.

The Role of Training

To fully realize the potential of human expertise, continuous training is paramount. The fast-evolving landscape of identity recognition demands that professionals stay ahead of emerging technologies and methodologies. Without regular upskilling, even the most experienced personnel risk falling behind.

Training platforms designed to address this need offer immersive, real-world scenarios that replicate the challenges faced by frontline and back-office personnel. These include:

- One-to-Many Facial Recognition Scenarios: Training professionals to handle high-stakes environments with accuracy and speed.
- Biometric Document Verification: Enhancing the ability to identify forged or tampered documents.
- CCTV Footage Review: Building precision in identifying individuals in surveillance footage.
- Deepfake Assessment: Determining if an image of a person is likely to be real or generated by AI.

Detailed progress tracking and customisable configurations should allow organisations to tailor training to their specific needs. Airport staff, for example, might focus on real-time passenger verification, while bank personnel might concentrate on resolving complex identity fraud cases. This adaptability ensures that training remains relevant and effective.

Building the Workforce of the Future

As identity recognition becomes increasingly critical in our digital and interconnected world, organisations must invest in tools and training that empower both backend and frontline professionals. Such platforms should enable professionals to:

- Develop expertise in a range of realistic identity scenarios.
- Build confidence in high-pressure environments.
- Identify fraudulent or suspicious biometrics.
- Adapt to the ethical, legal, and operational challenges of identity recognition.

These investments not only enhance workforce capabilities but also strengthen public trust in biometric systems.

A Balanced Future

The future of identity recognition lies in collaboration, not replacement. Machines bring efficiency, scalability, and consistency, while humans bring judgment, empathy, and adaptability. Together, they form a formidable partnership capable of navigating the complexities of modern identity verification.
By adopting training platforms, organizations can bridge the gap between technology and human expertise, creating a balanced approach to identity recognition. This not only ensures the ethical and effective use of biometrics but also prepares organisations for the challenges of tomorrow.

Final Thoughts

As the role of biometrics expands, so too does the responsibility to use these technologies responsibly. Human expertise is not a backup — it is an essential component of any robust identity recognition system. By investing in training and fostering collaboration between humans and AI, we can build systems that are not only efficient but also fair, inclusive, and trustworthy.

We believe the path forward is clear: reinforce, don't replace. By equipping the workforce with the right tools and skills, we can build a future where human expertise and biometrics/AI collaborate seamlessly to create a safer, more secure world.

Organisation: Biometix
Name: Ted Dunstone
Email: info@biometix.com

4. BixeLab: Beyond the Benchmark: Why General Biometric Testing Alone Falls Short

If you have been involved with or spoken to someone responsible for deploying a new biometric system, you'll likely recognise the frustrations that come with ensuring the system operates optimally in real-world conditions. Common issues include determining the best threshold or quality parameters, identifying the environmental conditions where the system might struggle, and evaluating how difficult it will be for users to provide a good biometric sample.
In many cases, systems arrive preconfigured with default parameters based on generic, large-scale, standardised testing. While these benchmarks provide insights into baseline performance, they are far from sufficient to guarantee ideal operation in diverse, real-world scenarios. Localised and tailored testing approaches (to appropriate international standards) are essential to address demographic biases, unique vulnerabilities, and the evolving regulatory landscape.

The Role of Standardized Testing

Standardised testing frameworks, such as those provided by NIST, FIDO, and MOSIP, serve as the foundation for the assurance of accuracy in the biometric industry. They establish industry-wide benchmarks to measure system accuracy, reliability, and compliance with global standards. However, these frameworks often overlook the nuances of specific deployments, which are critical to project success.
For example, a biometric system might perform well in controlled environments but fail to meet expectations when in diverse lighting conditions, by specific types of users, age, gender or ethnicity, or even with unique cultural practices. Standardized tests also tend to focus on matching accuracy, leaving gaps in other areas like bias detection, attack resilience, and usability under real-world conditions.

Bridging the Gap with Tailored Testing

To address these limitations, tailored testing must complement standardised frameworks. Tailored testing ensures that biometric systems meet the unique requirements of specific demographics, devices, environments, and use cases. This holistic approach encompasses:

- Diversity in Demographics: Ensuring inclusivity by testing with underrepresented groups minimises biases that can erode trust and efficacy. For example, certain facial recognition systems have been shown to perform poorly on darker skin tones due to limited diversity in training datasets. Even neurodiversity can be factor in the usability of some biometric systems.
- Device-Specific Performance: Evaluating systems across a full range of devices—including low-cost or legacy hardware—ensures consistent performance regardless of the technology used by end-users.
- Real-World Conditions: Assessing performance under varied environmental factors such as lighting, humidity, and background noise reflects actual usage scenarios, revealing vulnerabilities that might not be apparent in controlled settings.
- Attack Resilience: Testing for resistance to specific threats, including spoofing, adversarial AI attacks, and physical tampering, ensures that the system is robust against malicious attempts to compromise its integrity.

The Importance of Localized Testing

Localized testing is particularly vital in addressing issues like demographic bias and environmental challenges. Biometric systems often interact with diverse populations and operate in varied conditions. Without localized testing, organizations risk deploying systems that inadvertently exclude certain groups or fail to perform reliably in specific regions.

This type of testing also plays a critical role in meeting regulatory requirements. Frameworks such as the European Union's Artificial Intelligence Act, GDPR, and Australia's Privacy Act emphasize fairness, transparency, and demonstrable protections against vulnerabilities. Tailored testing methodologies allow organizations to meet these demands, ensuring compliance while fostering trust and confidence among users.

The Role of Regulation in Driving Responsible Testing

As biometric systems become more integrated into daily life, the regulatory landscape is evolving to ensure responsible use. Regulations now extend beyond accuracy to include:

- Bias Detection: Identifying and mitigating biases that could result in unfair treatment of certain groups.
- Transparency: Demonstrating how biometric data is collected, processed, and secured.
- Vulnerability Protections: Proving ongoing resilience against attacks such as spoofing and adversarial manipulations.

These requirements necessitate a shift from reliance on generic benchmarks to more nuanced testing approaches that address specific operational challenges. By incorporating tailored testing, organizations can proactively identify and address potential risks, ensuring compliance with regulatory standards while safeguarding user trust.

Building a Holistic Testing Framework

To achieve the goals of accuracy, fairness, and security, organisations should adopt a comprehensive testing framework that integrates both standardised and tailored methodologies. This approach includes:

1. Baseline Assessments: Leveraging standardised benchmarks to establish a foundation for performance and reliability.
2. Demographic-Specific Testing: Conducting targeted evaluations to ensure inclusivity and minimise biases. For example, testing facial recognition systems on diverse skin tones, ages, and facial structures.
3. Device and Environmental Testing: Evaluating performance across different devices and under varied environmental conditions to simulate real-world scenarios.
4. Vulnerability Assessments: Testing for resilience against specific threats, such as spoofing attacks, adversarial AI, and physical tampering.
5. Regulatory Compliance Audits: Aligning testing methodologies with relevant regulations to demonstrate fairness, transparency, and security.
6. Continuous Monitoring: Measuring and managing performance as the threat landscape changes, and software and hardware systems are updated, to ensure that business and performance objectives continue to be met.

Organizations that embrace a comprehensive testing framework stand to gain multiple benefits, including:

- Enhanced Accuracy: Tailored testing ensures that systems perform reliably over time across diverse scenarios and user groups.
- Improved User Trust: Addressing biases and vulnerabilities fosters confidence in biometric systems.
- Regulatory Compliance: Proactive testing methodologies help organisations meet evolving regulatory demands.
- Cost Savings: Identifying and addressing potential issues during pre-deployment reduces the likelihood of costly system rework and user friction.

Conclusion

As the digital identity landscape evolves, the importance of biometric testing will only grow. While standardised testing provides a critical foundation, it must be complemented by localised and tailored approaches to address the unique challenges of each deployment. By integrating these methodologies, organisations can deliver biometric systems that are accurate, inclusive, secure, and aligned with regulatory expectations. This holistic approach not only ensures compliance but also builds trust, fosters innovation, and paves the way for a responsible digital future.

Organisation: BixeLab
Name: Somya Singh
Email: info@bixelab.com

5. Corsound AI: Biometrics in the Era of Generative AI: Biometric Deepfake Challenges and Next Gen solutions

Biometrics, leveraging unique physical or behavioural traits such as voice, face, or fingerprints, has become a cornerstone of modern identity verification. However, the rise of Generative AI (GenAI) and deepfake technologies introduces unprecedented threats, challenging the reliability and security of these systems.

The Deepfake Threat and Responsible Biometric Adoption

GenAI enables fraudsters to create hyper-realistic synthetic voices and faces, bypassing traditional biometric systems. These deepfakes erode trust in authentication processes, increasing the risk of fraud. For example, speaker recognition systems can be fooled by synthetic voices cloned with remarkable precision.

To combat these threats, innovative approaches are required to "beat AI with AI." By embedding intelligent technologies that detect and alert against deepfakes, biometric systems can be fortified without compromising privacy or introducing biases.

Below are key pillars for responsible biometric adoption in identity authentication and verification:

1. Privacy-Centric Biometric Processing

Avoid creating centralized biometric databases. Instead, encrypt biometric data into non-reversible numeric vectors, which cannot be reconstructed into the original traits. This ensures that even in the event of a data breach, sensitive information remains protected.

2. Inclusive Design Principles

Incorporate diverse datasets and adaptive algorithms to improve system accuracy across various demographics. This approach ensures equitable access and fosters trust while addressing biases.

3. Deepfake Detection Technologies

As deepfakes proliferate, specialized tools that identify subtle inconsistencies in synthetic voices or faces are essential. These technologies can reliably distinguish between genuine and manipulated biometric inputs, maintaining trust in voice and facial recognition systems.

Multimodal and Cross-Modality Biometrics: The Next-Gen Solution

Given the rapidly evolving threat landscape, relying on a single biometric modality is no longer sufficient. Multimodal and cross-modality approaches represent the future of secure and resilient biometric systems.

Multimodality: Combining Layers of Security

Multimodal biometric systems utilize multiple traits, such as voice and face, to create a layered security approach. This redundancy ensures that even if one modality is compromised or unavailable, the system remains reliable.

Cross-Modality: A Sophisticated Identity Solution

Cross-modality takes security a step further by integrating two or more modalities into a single cohesive identity check.

As an example, an identity could be represented with both voice and its correlated face. This is a unique representation that is based on a proven correlation between voice biometric to a matching face biometric.

Correlating a given voice with a corresponding face ensures that the two match, providing an additional layer of verification. This method not only enhances security but also mitigates deepfake risks. By requiring fraudsters to

simultaneously spoof multiple modalities, cross-modality systems make it exceedingly difficult—if not impossible—for adversaries to succeed. This approach restores trust in biometrics as a reliable authentication tool.

Advantages of Multimodal and Cross-Modality Biometrics

Mitigating Deepfake Risks

Deepfake tools are increasingly capable of replicating single modalities but cloning a voice and simultaneously fabricating a matching face is significantly more challenging. Multimodal and cross-modality systems reduce the likelihood of successful attacks, reinforcing security in critical applications.

Enhancing Accessibility and Inclusion

Multimodal systems improve accessibility by offering alternative options for identity verification. For instance, facial recognition can serve as a fallback when voice input is unavailable due to temporary constraints, and vice versa. This adaptability enhances user experience while ensuring inclusivity.

Real-World Applications

Multimodal and cross-modality biometric systems offer versatile solutions across various industries:

- **Financial Services:** Combining voice and facial recognition adds layers of protection for high-value transactions, minimizing fraud.
- **Remote Work and Verification:** Multimodal solutions enable secure identity checks in remote settings, such as video communication, by analysing voice and face both independently and together.
- **Law Enforcement:** Cross-modality tools enhance forensic investigations by correlating existing biometric data (e.g., a suspect's photo) with additional inputs (e.g., voice samples). For example, correlating a suspect's image with a voice sample from a phone call or social media can validate their identity at a specific time and place.

Adapting to a GenAI-Driven World

The integration of multimodal and cross-modality biometrics addresses current challenges while preparing for future threats. By combining modalities and leveraging their correlation, biometric systems enhance security, uphold privacy, and promote inclusivity.

These approaches exemplify how advanced technologies can adapt to the complexities of a GenAI-driven world, providing a secure and reliable foundation for digital identity. Multimodal and cross-modality systems not only meet today's challenges but also offer scalable and robust solutions for the future of biometric authentication.

Organisation: Corsound AI
Name: Orly Shechtman, Director of Product Management
Contact: orly.shechtman@corsound.ai

6. Daon: The Passport-less Era: How Digital Wallets & Biometrics Are Simplifying Cross-Border Travel

Passports have been the cornerstone of international travel for centuries but may soon become relics of the past. Biometrics and digital wallets are leading the next frontier in travel technology, streamlining cross-border travel and transforming identity verification. By integrating tools like facial recognition and fingerprint scanning, these advancements promise to reshape the global travel ecosystem.

Biometrics at the Forefront

Biometric technology's potential lies in its ability to provide a faster, more secure, and more convenient alternative to traditional travel documentation. Unlike passports, which can be lost, stolen, or forged, biometric data is unique to each individual and far more difficult to compromise. Imagine passing through an airport where your face, fingerprint, or iris scan replaces the need to fumble through a bag for your boarding pass. The concept isn't merely futuristic; it's already becoming a reality in select locations.

There has been a natural progression toward the use of automated kiosks in places like airports, stadiums, cruise ship embarkation points, and other high-traffic, high-security travel areas. Even at airports without biometric capabilities (the ability to scan a traveller's face, iris, or fingerprint) built into their kiosks, automated checkpoints like these have allowed travellers to scan travel documents for years. These innovations represent the first steps toward full biometric automation—the kind that would create a truly seamless travel experience for people around the world.

Airports in countries like Singapore, the Netherlands, and the United States have already adopted biometric screening systems for check-in, security, and boarding. For example, Singapore's Changi Airport, known for its technological advancements, integrates facial recognition technology into its passenger journey. Travelers can move from check-in to boarding with minimal human intervention, cutting down wait times while ensuring security standards remain uncompromised.

Similarly, U.S. Customs and Border Protection (CBP) has rolled out biometric entry and exit programs at several major airports. These programs use facial recognition technology to verify a traveller's identity against their passport photo, stored in a secure database. The process not only accelerates screening but also adds an extra layer of security, making it harder for fraudulent identities to slip through.

Digital Wallets: The New Travel Companion

Digital wallets, which securely store digital versions of identification documents, payment methods, and other credentials, are seen as a natural complement to biometric technology. Companies like Apple, Google, and Samsung have pioneered digital wallets for payments and loyalty programs, but their potential in the travel sector is vast.

Imagine a scenario where your digital wallet contains a secure, government-issued digital passport. Upon arriving at the airport, you pass through biometric scanners that verify your identity and match it to your digital passport in seconds. This seamless process eliminates the need to present physical documents, reducing friction at every stage of the journey.

Beyond passports, these wallets can also store other travel documents like boarding passes, and each document is made accessible through a traveller's smartphone. Some systems are now integrating biometric verification into these wallets, allowing travellers to authenticate their identity with a fingerprint or face scan. The combination of digital and biometric technologies creates a comprehensive, seamless travel experience that extends beyond airports to include hotels, rental cars, and even border crossings.

The benefits of biometrics and digital wallets extend beyond convenience. For governments and security agencies, these technologies offer enhanced tools for combating identity fraud and tracking potential security threats. By

creating a more reliable way to verify identities, biometrics reduce the reliance on paper-based documents that can be manipulated or forged. This dual benefit—greater efficiency for travellers and improved security for nations—is a significant driver behind the push for these technologies.

Simplifying Modern Travel with Innovative Digital Technology

Though it may be a while before every airport offers the convenience of Singapore Changi, the technology exists today to reduce the stress of international travel without compromising border or traveller security.

A document validation service pre-processes travel documents to reduce time spent standing in line and streamlines pre- and post-boarding. For example, customers using an industry-leading travel document validation solution, have enjoyed 45 percent faster queuing and check-in processing times at the airport, simplifying their travel day. At the same time, the businesses implementing the solution have reduced operating costs by up to 30 percent.

The RFID chip in modern passports includes a digital version of the traveller's photo that is compared to the live customer standing in front of the automatic reader (whether at an airport, stadium, or border control area), which uses facial recognition software to capture an image. This is driven by artificial intelligence (AI) and machine learning (ML) technologies to help organizations ensure that travellers are truly who they claim to be and maintain the strictest security, all while still making the face scan process simple and fast.

A New Era of Travel

In the long term, the shift to biometrics and digital wallets could fundamentally change the way we think about travel. The elimination of traditional passports could pave the way for a more interconnected world, where identity verification is seamless and instantaneous. Yet, this vision depends on overcoming current challenges, from privacy concerns to ensuring equitable access for all travellers. Restrictions remain in place on where and how biometrics can be used in aviation. For example, the European Data Protection Board rightly insists that "individuals have maximum control over their biometrics". Defined data protection measures like this create a useful framework for enabling adoption, as demonstrated by the impact of GDPR.

For now, passports remain a travel necessity, but the growing adoption of biometrics suggests that their days may be numbered. As these technologies and standards continue to evolve, the dream of a truly seamless travel experience edges closer to reality. The International Air Transport Association's (IATA) focus on automating traveller experiences, including using digital identity to facilitate contactless travel, is a great example. Travelers, governments, and industries must work together to navigate this transition, ensuring that the benefits of innovation are shared widely and responsibly.

Organisation: Daon
Name: Clive Bourke, EMEA & APAC President
Contact: cbourke@daon.com

7. Entrust: Frequent flyers send a clear message: We're ready for fully digitalised contactless travel

The proliferation of digital identity systems highlights the critical need for interoperable biometrics

In November 2024, Entrust published the results of our Seamless Travel Experience Survey, which aimed to understand international travellers' expectations for a smoother, more efficient travel experience. Surveying over 2,000 frequent international flyers across the G20, the study highlights the increasing acceptance of biometrics to facilitate frictionless border control processes. 66% of travellers surveyed preferred biometric corridors and remote identity verification over traditional checkpoints for traveler identification when applying for visas and during customs and immigration.

Key insights from the survey emerged about the types of innovations these frequent flyers wanted to see made available soon and how they might positively affect the traveler's journey. The top three responses were:

1. Fully digitalized visa and electronic travel authorization applications

Frequent international travellers do not want to spend time filling out paper forms and they certainly do not want to attend in-person appointments when applying for visas or travel authorizations. Where these are required, the expectation from travellers in 2025 is that the process should be easy, quick and digital.

2. Remote digital identity verification

Frequent flyers have become familiar with remote, digital identity verification in various aspects of life, from banking to airline check-in. They are comfortable with sending both biographic and biometric information electronically or via an app, in exchange for easier, faster processing, and have even come to expect it for most interactions during travel.

3. ePassports & Digital Travel Credentials

Our respondents welcomed innovations in passport technology, including chipped ePassports and the advent of Digital Travel Credentials (DTCs), in anticipation of more seamless border experiences and accelerated check-in for flights.

Globally, few countries have taken the leap of faith and listened to travellers' demands by implementing programs and pilots that bring biometrics-based seamless travel to life, while protecting their borders. Let us explore some of these initiatives to see how purpose-built technology is shaping the future of seamless travel.

Seamless Air Travel with the Curaçao Express Pass: Expedited immigration on arrival

The government of Curaçao recently launched Express Pass, an innovative new program designed to enhance traveller satisfaction and to encourage repeat visitors. When considering how to improve its immigration process, the vision of the Government of Curaçao was simple but compelling: how to reduce to a minimum the time from the plane to the beach?

Curaçao Express Pass is the first of its kind mobile-based, pre-processing border crossing system, using innovative traveller-controlled, contactless technologies, allowing visitors to complete border control and immigration requirements for their journey, from home, up to seven days in advance of arrival. Then, upon arrival at Curaçao International Airport (CUR), passengers pass through dedicated, contactless biometric e-gates, bypassing the need for slower, in-person interactions. The result is a true seamless walk-through experience, made possible with the intelligent use of interoperable technologies that the Government of Curacao and its technology partners built collaboratively to meet the needs of the 21st century traveller.

Seamless Land/Sea travel for UK-EU maritime borders: Expedited border crossings

The UK Border Force is in the process of applying similar innovations to their maritime borders. The aim of the developing program in the UK is to create expedited vehicle lanes at ports of entry based on instant facial matching

that can be performed through the vehicle's windshield. This technological automation of an otherwise manual process holds the promise of accelerating the flow of vehicles upon arrival and reducing friction at vital ports of entry.

Cameras in new, dedicated vehicle lanes at border crossing points capture photos of each individual inside the vehicle as it approaches the border. These images are then verified against a reference image already held by the government, such as a visa, ETA or passport. This instant verification allows for verified travellers to cross the border in an expedited manner, perhaps without being stopped by a border officer at all, subject to policy. Throughout the process, the transmission and storage of data are secured with strong encryption to protect traveller privacy.

Crossing times for authorized travellers could potentially be further reduced by implementing a pre-registration process, which would enable the government to establish a limited gallery of passengers expected to arrive within a specific time window. In the future, this new process could be expedited even further for any cohorts allowed to proceed without stopping, subject to a successful identity verification, possibly establishing *fully automated lanes* for certain qualified passengers.

The result: an innovative border control system with future paths for automation that allows for the rapid movement of people while keeping the UK's borders secure.

New UK Electronic Travel Authorization: improving border security with seamless identity verification

At the time of writing in early 2025, the UK Home Office is rolling out an innovative program to establish an Electronic Travel Authorization (ETA) system for all non-visa visitors to the UK. This massive program needed to be simple for travellers to use while also safeguarding UK's borders. Conceptually, it is similar to the US ESTA and the Canadian and Australian ETA systems. But it is the *first ETA program to be biometrically secured from day one*, requiring applicants to submit a contemporaneous photograph which is matched instantly with the reference image in the traveller's passport.

Once fully rolled out, later in 2025, the UK ETA is expected to handle over 30 million applicants per year and is rapidly becoming a core pillar in the wider UK border control system, providing both a boost to national security and a quick, easy, welcoming system for travellers. This program is a notable example of emerging biometric technologies integrating with existing systems to reduce travel friction and pave the way for innovation.

Interoperable Biometrics are the way forward

The success of these programs lies in the interoperability of biometric identity systems. Interoperability is especially critical for international travel, where multiple stakeholders—airlines, airports, border agencies, and governments—must collaborate to provide seamless, secure, and efficient experiences while protecting individual privacy and ensuring data accuracy.

Globally, biometrics are enhancing travel in innovative and responsible ways. However, programs lacking the right technology for seamless integration with existing systems risk creating unnecessary friction or risk exposing travellers' Personally Identifiable Information (PII) to greater vulnerabilities. Travellers are more likely to embrace these innovations when the benefits are clear, tangible, and consistently delivered. Improved interoperability between systems will amplify these advantages, fostering higher acceptance and satisfaction among travellers worldwide.

Organisation: Entrust
Name: Jon Payne, Government Relations
Email: jon.payne@entrust.com

8. ezPassport: The Responsible Use of Photographic Biometrics: A Vision for the Future

The world is changing rapidly, and the way we confirm our identities is evolving too. Biometric technologies, such as facial recognition and facial landmark analysis, are helping to make identity verification faster and more secure. However, as these tools become more common, we must ensure they are used responsibly and fairly.

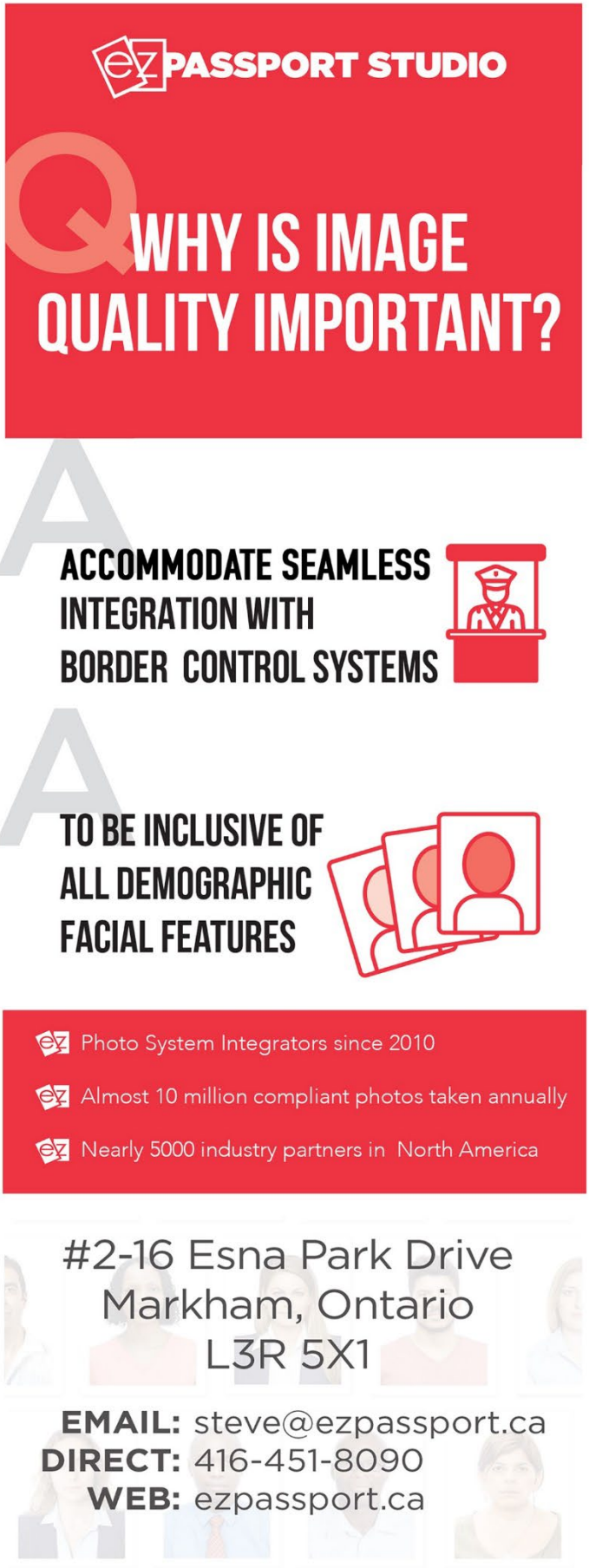
Challenges in Biometric Use

While biometrics have great potential, they also face challenges. For example, these systems work best with high-quality photos. Poor lighting, blurry images, or awkward angles can reduce accuracy. Studies, such as those by the National Institute of Standards and Technology (NIST), show that poor-quality images can lead to errors, especially in critical areas like border crossings.

Privacy is another major concern. Biometric data, such as facial images, must be handled carefully to prevent misuse or unauthorized access. If people lose trust in how their data is managed, they may hesitate to use these systems. Additionally, some biometric algorithms work better for certain groups of people, which can lead to fairness issues. For instance, failures in recognizing individuals with darker skin tones have been noted, often due to poor exposure and inadequate training data. These challenges highlight the need for improving both the image capture process and dataset diversity. Finally, because biometric data is permanent, it requires strong protection from hackers and misuse.

The Importance of Image Capture Methods

A crucial yet often overlooked aspect of biometric systems is the method used to capture images. The procedures and equipment employed during this process play a significant role in ensuring the quality and reliability of the captured data. High-quality cameras and standardized practices help eliminate common errors caused by poor lighting, incorrect positioning, or substandard image resolution. These improvements are especially critical in addressing biases related to skin tone and ensuring fairness. Organizations that prioritize proper image capture methods ensure the foundation of their biometric systems is robust and dependable, reducing the likelihood of downstream issues.



Moving Towards Responsible Biometrics

To address these issues, it is essential to use thoughtful approaches. High-quality photo capture and advanced image processing can improve accuracy. Processing biometric data locally, rather than in the cloud, can reduce privacy risks. Ensuring algorithms are trained on diverse datasets helps avoid bias, and encryption can protect sensitive data from security threats.

Innovations in Biometrics

Facial landmark analysis, which identifies specific points on a person's face, is one way to make biometric systems more reliable. This technology works well even with less-than-perfect photos, making it ideal for real-world applications. Organizations with experience in passport photo compliance demonstrate how innovations like these can meet practical needs while addressing concerns about fairness, accuracy, and privacy.

Building Trust in Biometrics

Biometric technologies, when used responsibly, can make everyday tasks—like crossing borders—faster and safer. However, trust is essential. To earn and keep that trust, biometric systems must be accurate, fair, secure, and respectful of privacy.

By focusing on these principles, we can ensure biometrics continue to improve lives responsibly. While no single solution fits all situations, thoughtful innovation, like facial landmark technology, shows how we can address today's challenges and build a better future for biometric use.

Organization: ezPassport
Name: Steve Lim
Email: steve@ezpassport.ca

9. Facephi: The future of responsible biometrics: Trends and solutions

Biometrics have transformed the way in which we interact with digital technologies, allowing speedy, accurate identity verification. However, as its adoption expands, key questions are emerging about how to ensure its ethical and responsible use. Aspects such as privacy, data security, equity and inclusivity are the main focus of the debate.

Current trends in responsible biometrics

Privacy as a priority

Regulations like the General Data Protection Regulation (GDPR) in Europe and growing interest in similar laws in other regions have led companies to adopt privacy-first approaches by design. The use of anonymisation techniques, advanced encryption and secure storage of biometric data is now standard practice.
Solutions based on the "on-device" model (processing on the user's device) are gaining ground. This approach minimises the transfer of sensitive data, reducing risks and aligning with user demand to allow greater control over their personal information.

Bias mitigation in biometric algorithms

Bias in biometric algorithms has been widely documented, especially in facial recognition technologies. Institutions and developers are working to create more inclusive models, trained with data sets representative of global diversity. Generative AI is taking on a crucial role in this area, facilitating the creation of synthetic identities and the augmentation of images in underrepresented groups. Furthermore, certification and validation by bodies such as the National Institute of Standards and Technology (NIST) have established themselves as guarantors of the standardisation and robustness of these technologies. What's more, practices such as continuous auditing and inclusive design are crucial in order to minimise any discrepancies in error rates between different demographic groups and to promote the responsible adoption of biometrics.

Transparency and explainability

The rise of AI in biometric systems has generated the need to promote an understanding of how these systems work and about how they impact users.
Transparency in biometric processes allows users to trust the technology and understand how their data are processed. Furthermore, compliance with regulations such as the European Union Artificial Intelligence Act (AI Act) is crucial for building trust in these solutions.

Focus on accessibility and inclusive design

Ensuring that biometric technologies are accessible to all users, regardless of their skills, age or level of technological experience, is a challenge that has become a priority. This includes the design of intuitive interfaces, the reduction of technical complexity and the incorporation of visual and tactile elements adapted to different needs.

Emerging solutions for a responsible future

Decentralised processing and data protection

Decentralised biometric processing can mitigate certain cybersecurity risks, such as attacks on centralised databases, and strengthen user privacy. This falls in line with the trend towards self-sovereign identity, allowing sensitive data to remain under the control of the users themselves.

On-device biometrics also contribute to this aim, although it is essential to strengthen security measures on the devices themselves. It is not always feasible to delegate full responsibility for protection to users, as many are not aware of the threats.

Significant advances are being made in hashing and cryptography techniques, including solutions such as homomorphic encryption, allowing operations to be performed on data without the need for decryption. However, their adoption still faces technical challenges.
Concurrently with the advancement of Synthetic Data techniques and generative AI, it is crucial in sectors that handle sensitive data, such as healthcare or identity verification, to explore Federated Learning techniques that allow the training of algorithms without centralising information.

Continuous audit and ethical standards
Algorithm auditing is essential for detecting and correcting any potential biases. These evaluations include demographic impact analyses and periodic reviews of the algorithms to adapt them to new data.
Assessments such as those performed by the NIST (Facial Recognition, Presentation Attacks etc.), are commonplace in the industry, but it is crucial to add new standards and assessments for new challenges such as Deepfakes or Injection Attacks.

Informed consent and user education
Ensuring informed consent is a mainstay of responsible biometrics. This includes providing users with clear information about how their data are collected and processed, as well as consent withdrawal options.
Concurrently, education plays a key role in training users in how to interact with biometric technologies safely and consciously.

Responsible and ethical use cases
The design and implementation of biometric solutions must always consider their impact on real life, especially in sensitive sectors.

Key examples of responsible apps include:

- Banking and digital payments: Biometric systems in banking allow for faster and more secure processes, but they must ensure that they do not exclude vulnerable populations
- Border control and security: Biometric technologies used at airports and border crossings must strike a balance between security and privacy. The use of bias-free algorithms reduces discrimination risks and ensures fair treatment for all travellers.
- Medical care: Biometrics in the healthcare sector can facilitate secure access to medical records and protect sensitive patient information.

The future of responsible biometrics

The future of biometrics lies not only in its expansion, but also in the way it is adopted ethically and transparently. Organisations have the responsibility to align their technological developments with the principles of privacy, security and equity.

To ensure responsible and sustainable solutions, it is essential for there to be a continued commitment to audit, regulation and inclusive design, balancing technological innovation with ethics to deliver fair and equitable benefits to all users.

Organisation: Facephi
Name: Mayte Hernández
Contact: Javier Barrachina, R&D Director, jbarrachina@facephi.com

10. FaceTec: Digitally Signed Biometric QR-Codes - Solving the Human-to-Identity-to-Privilege Binding Problem

The Last Remaining Gap in Identity Management

The 2024 Verizon Enterprise Security Report, among many others from the last decade, states the transfer of legitimate credentials to an unauthorized user represents the attack vector in up to 75% of breaches, hacks, frauds, and identity crimes. And, potentially, trillions of dollars annually in damages and losses.

This, the last remaining issue in identity management, exploits the analogue "gap" between a physical human and the devices used for digital access. Because they are not permanently, physically connected, we cannot guarantee which human controls a device and the credentials cryptographically bound to that device. This gap allows bad actors to control a valid credential or device to misrepresent themselves for access to privileges they are not entitled to. Attackers are not "hacking in", but "logging in."

The Problem: A Lack of Binding Between a Living Human and Their Identity

According to Merriam-Webster, a credential "warrants credit or confidence." Effectively, a credential represents proof of deserving higher trust. Theoretically, a credential contains legitimate identity data describing a person, typically including a face image, but potentially also their entitled privileges. Central to that trust is an implied binding between physical humans, their identity, and their privileges. However, while cryptography provides irrefutable binding between trusted identity data and privileges, it cannot provide irrefutable binding between identity data and the human it describes. If there is any possibility identity data or credentials can be controlled by someone other than the legitimate owner, their use as a trust factor can only provide probabilistic evidence. Given this, the goal of any identity security system must be to raise the probability of correct verification and authentication as close to 100% as possible.

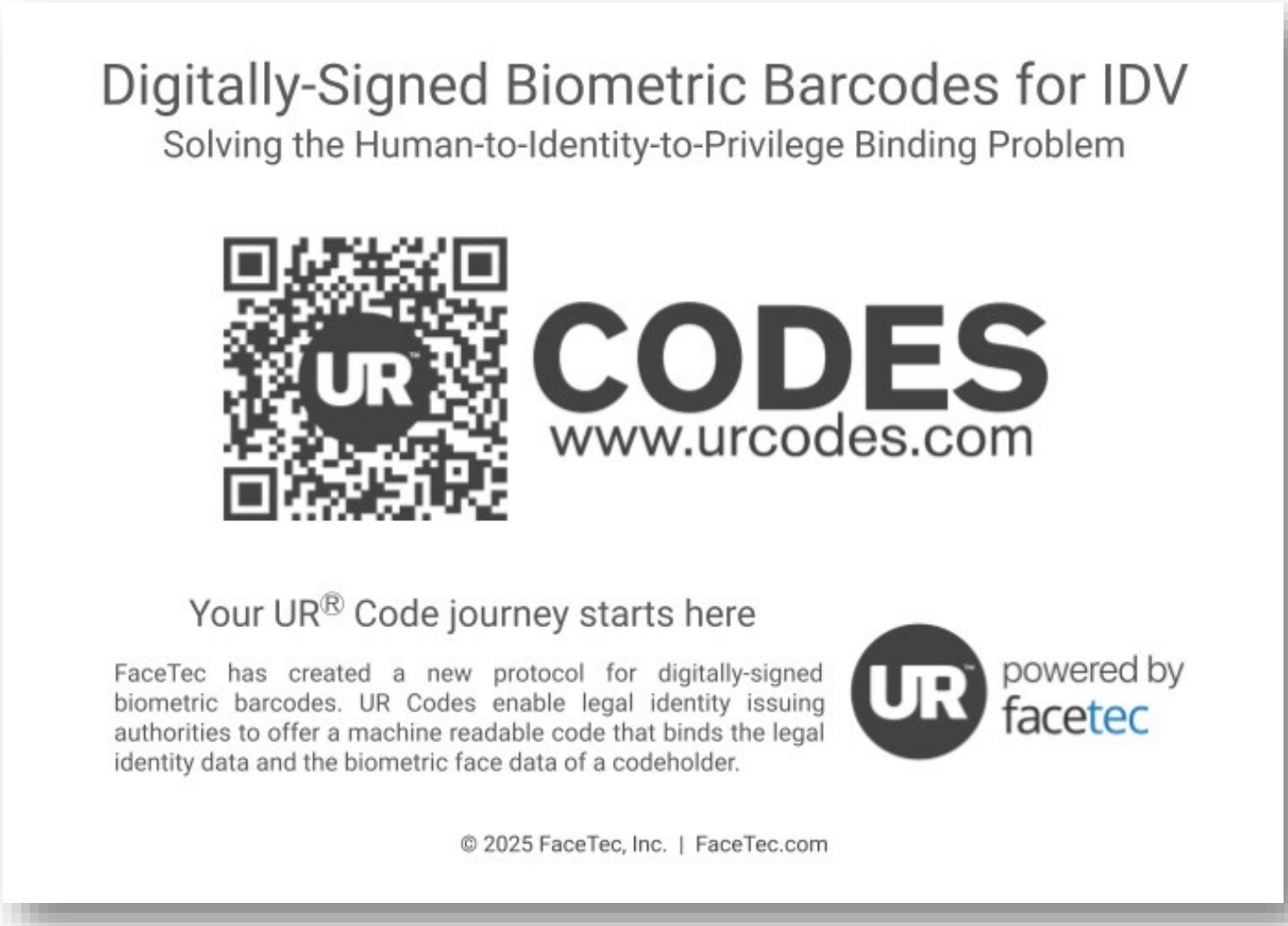
PKI Validates Data and Devices. Biometrics Provides the Highest Confidence Human Trust Factor

The identity security system that provides the highest potential confidence in outcomes utilizes cryptography to validate identity data, devices, and the relationship between them. It must also use strong, Liveness-proven biometric data to verify and authenticate humans. While there are seemingly countless identity trust factors, biometrics are the only trust factor derived exclusively from the physical human described by the verified identity data. Therefore, it is essential to utilize the strongest cryptographic systems and the strongest biometric systems - together- to raise probability confidence in identity verification and authentication outcomes as high as possible.

The Only Identity Data We Can Trust is Source Data Residing at the Official Issuing Authority

Certainly most, and potentially all, identity data has been leaked or stolen and is available for sale on the Dark Web. Foundational identity data describing anyone can be acquired, manipulated, and presented by anyone else in any context, including a false context. While the identity data may be provably legitimate, our confidence in knowing who presented it can only be low. In effect, there is no longer provable binding between foundational identity data *in the field* and the human it describes. However, legal issuing authorities collecting the foundational identity data, including a face photo, maintain that data and relationship between the photo and identity data, in perpetuity. Both identity data and its binding to a trusted face photo retain their integrity within the issuing authority's database. Therefore, the strongest potential identity verification and authentication utilizes verified identity data bound to biometric photo data, directly and immutably sourced from the legal issuing authority.

This can be accomplished in two different locations: within the issuing authority firewall or outside those protections. Within the issuing authority's confines, it can pose a privacy threat, as the issuing authority could gain understanding of an individual's personal life from data in identity verification submissions. Therefore, performing such comparisons outside the government's purview is preferable. This requires the secure transfer of immutable foundational identity data from the issuing authority to somewhere else, preferably into the control of its owner. This is what PKI is designed for and performs well at.



Today, three encrypted delivery mechanisms, standards, or protocols, securely transport trusted legal identity data to rightful owners: e-Passports, mobile driver licenses (mDL), and digitally-signed biometric QR codes. They provide truly strong, cryptographically secured data and data transport directly from the legal issuing authority to the human described by the data. However, while PKI guarantees data integrity, it cannot prove who controls it.

Strong, Liveness-proven biometric face matching ensures the person described by the data is controlling the data; e-Passports and mDLs provide only a face image (a picture) to demonstrate binding between the identity data, the credential and the described human. Both require a manual comparison of the digital photo and the presenting human, and are vulnerable to human errors. Further, both e-Passports and mDLs are logistically difficult to manage on large scales. e-Passports are physical documents carried by individuals, while mDLs are fully digital, but highly complex and challenging to manage.

Enter Digitally-signed Biometric QR Codes

Digitally signed biometric QR codes are currently the only easily deployable, cost-effect mechanism that provides a cryptographically secured biometric binding between a verified legal identity and the human described by the legal identity, without querying a government resource. They are issued to, held, controlled, and presented by the legitimate person, providing absolute privacy and portability.

These QR codes, like e-Passports and mDLs, source legal identity data directly from issuing authorities. However, rather than manual photo verification, these QR codes contain biometric vector data that can be matched on a secured server or the identity owner's mobile device. These codes include the same data and binding integrity as the source data itself, and can be printed onto physical credentials, providing quick, efficient biometric identity verification. Or,

they can be distributed electronically and saved as a verifiable credential in a mobile wallet, or embedded as an mDL feature, confirming the legitimate identity owner controls the device and any credentials bound to it.

Organisation: FaceTec, Inc.
Name: Jay Meier, SVP of NA Operations
Contact: jay@facetec.com

11. Facia: Is AI Outsmarting Us: Deepfakes – How to Detect Them and Prevent Their Use

Deepfakes–AI-generated visuals and audio are specifically designed to deceive industries and individuals. As the creation of deepfake content exponentially grows, it presents serious challenges to society. However, the latest potentiality of Generative Adversarial Networks has improved the creation of hyper-realistic fabricated content, influencing trust, privacy, and global safety. Responsible biometric systems are important against the new deepfake threats while facilitating technologies to recognize and reduce the exploitation of AI technologies. This piece of content highlights the important challenges presented due to the deepfakes, figuring out the best detection mechanisms, and emphasizing the calculated solutions to protect their expansion.

Rising Trends of Deepfakes

AI such as Generative Adversarial Networks has fuelled the deepfake technology that now has grown more than entertainment purposes. This technology can generate highly convincing fabricated images, videos, and audio. Unfortunately, this material is being used as a weapon against individuals and industries to initiate disinformation campaigns and social engineering attacks. From fake celebrity promotions to AI-generated fraud, deepfake expanded wrong information that seems real comes from trusted sources, diminishing public trust. As the dangers are important, deepfake technology also has legal applications, for instance, enabling video game realism, increasing customer support systems, and computation of call forwarding. So, such multipurpose emphasizes the need for strong deepfake detection techniques and preventive planning to maintain innovations with responsibility.

Challenges & Threats

The rapid advancement of AI has made deepfake detection difficult, which is becoming a significant challenge. Tools like GANs allow the creators to exploit the content with exceptional realism, making it hard to differentiate the fake from the real. Accessibility to free, user-friendly software further worsens this problem, as it democratizes the creation of deepfakes, even for individuals with minimal technical expertise. Detection tools are often behind these innovations, which means there is a pressing need for robust, adaptive technologies. The emergence of hyper-realistic deepfakes underlines the need for continuous research and investment in AI-driven solutions to address this growing challenge effectively.

Societal and Ethical Implications

Deepfakes ruin the trust in digital content and provoke the information’s authenticity. This technology is usually used to spread misinformation, public opinion exploitation, someone’s defamation, and threaten democracy, alongside social stability. Moreover, the illegal use of personal data to generate deepfakes elevates important ethical concerns, from identity theft to privacy breaches. Because more sophisticated deepfakes imply dangers to both reputations at individual and institutional levels, these demand ethical controls and rules underpinning better standards of conduct regulating the connected world's uses of AI.

Detection Mechanisms

The latest solutions utilized the neural networks competent on large datasets to increase the detection authority. Rising mechanisms like forensic analysis and blockchain-based content authentication are integrated into the detection structures. Such tools, assembled with the artificial intelligence’s analytical power are important to moving forward with rapidly complex deepfake generation methods. The constant developments in detection algorithms are important to balance the dependability and confidence in the online landscape.

Recognizing AI-Generated Content

AI-generated content has telltale signs, such as distorted reflections, mismatched shadows, and pixelation. Experts use these indicators to distinguish genuine content from deepfakes. Tools like reverse image searches and metadata analysis also help verify authenticity. Automated systems powered by AI analyse patterns to detect subtle

inconsistencies in texture and motion. However, the evolving sophistication of deepfake technologies necessitates ongoing innovation in detection mechanisms to ensure their reliability and effectiveness against emerging threats.

Prevention Strategies

Biometric systems facilitate strong protection against deepfake misuse. Facial recognition technologies verify the identities, confirming that illegal exploitation of visual data is exposed. Biometric authentication has a progressive method, providing real-time verification of online content.

Multimodal Approaches

Assembling such technologies, for instance, behavioural biometrics, voice recognition, and facial analysis increases the detection capacities. However, the multifaceted method confirms the high precision by cross-indexing various data points. The integration of AI-driven models with conventional verification systems serves to fortify the defence against deepfake misuse. By having a broad strategy, industries are protected against the vulnerabilities of single-point verification, thus forming a robust framework against deepfakes.

Financial Losses from Deepfakes

Deepfakes are fuelling a peak in financial fraud, with incidents in fintech increasing by 700% in 2023. The generative AI tools make criminals capable of creating artificial voices, videos, and documents that can bypass today's fraud protection systems. Business email compromise, enhanced by deepfakes, caused $2.7 billion in losses in 2022, with projected losses reaching $11.5 billion by 2027. Despite advancements, banks struggle to adapt existing risk frameworks to emerging AI threats, highlighting the need for robust detection and response tools.

Future Prospects

Advancements in deepfake detection solutions surely lead to a safer future. Future innovations might include AI-based algorithms that could identify deepfakes in real-time, which would further improve security in digital communication. Detection tools will enable industries and governments to respond better to the threats posed by deepfakes as they become more sophisticated.

Governance and Legislation

Governments around the world are developing policies to control the creation and dissemination of deepfakes. Drafted laws include transparency, accountability, and punishments for the abuse of AI. Policymakers, researchers, and technology providers should collaborate to create ethical frameworks and compliance. Promoting responsible use of AI-driven tools and innovation will be key to deepfake challenges at scale.

Final Words

Deepfakes pose an increasing threat to trust and security in the digital world. They are highly sophisticated and easily accessible, which creates a challenge for detection and prevention. Nevertheless, advancements in AI-powered tools, biometric solutions, and multimodal approaches provide a path forward. The collaboration of governments, industries, and researchers is critical in keeping ahead of deepfake threats. With the nurturing of innovation, ethical standards set, and the public informed, society will mitigate the dangers deepfakes present and usher in a safer, more secure digital future.

Organisation: Facia
Name: Daniyal Chughtai, CTO
Contact: daniyal@facia.ai

12. Fime: Identifying and addressing bias in biometric systems

Biometric systems are becoming increasingly prevalent in today's interconnected world. These technologies compare biometric data provided during verification with a previously stored template to allow authentication or identification of the person. They represent a unique innovation capable of simultaneously enhancing security and user experience. This makes biometric systems an attractive choice for key applications such as Remote Identity Proofing solutions, secure access control with passport eGates or unlocking personal devices as smartphones.

However, the speed at which the ecosystem has grown has brought challenges. The fragmented development of various components, coupled with the limited sharing of information about the internal mechanisms of systems, has meant that in certain scenarios, the performance of some solutions is limited by a notable issue: biases. If left unchecked, biases can result in differential performances and security issues for some demographics groups when deployed in real life.

Bias in biometrics

The algorithms and software that power biometric systems are built using artificial intelligence (AI). For example, most facial recognition systems are built on Convolutional Neural Networks (CNNs) such as ArcFace architecture, which allows for deep machine learning based on the templates presented. There is now consensus that an AI model is only as good as the data that trained it. With biometrics, algorithms are trained using genuine and spoofed image datasets. If the data is not diverse then the algorithm’s performance will be inadequate. This is bias. It is not necessarily malicious, but it is a reality.

Such biases, if not addressed, can lead to unequal performance across demographic groups. If a certain group has a poorer experience due to their biological characteristics this might result in lower adoption, and a facial recognition technology that cannot perceive between individuals of any given demographic presents a security risk. Not only does lower adoption risk the financial viability of a product, it risks reputational damage if a product is perceived to have a racist, sexist, ageist or other bias.
This needs urgent attention across the biometric value chain; from software and sensor developers to device OEMs and standardization bodies and governments.

Test bias to address bias

The performance of a biometric system is evaluated against two primary parameters; False Accept Rate (FAR) is where impostors are mistakenly accepted as genuine users; and False Reject Rate (FRR) is where genuine users are wrongly denied. The challenge for biometric system providers is to keep these rates as low as possible for all demographic groups, ensuring inclusive biometric solution with high security and convenience for all. Biases in these systems can be detected by the disparities in FAR and FRR when evaluating different demographic groups. This bias has been traditionally measured by biometric fairness metrics such as Fairness Discrepancy Rate (FDR), Inequality Rate (IR), Gini Aggregation Rate for Biometric Equitability (GARBE) or Separation Fairness Index (SFI).

To know the best metric for evaluating the potential bias of a biometric system, it is important to measure the effectiveness of each metric on the specificity and accuracy of the system. With this in mind, leading biometrics experts have created an innovative method to inject bias on biometric systems and evaluate the effectiveness of each metric. This system allows experts to inject selective biases for specific demographic sub-groups, with control over the

strength of each bias. Exercising direct control over the strength of each bias allowed the expert to monitor the effectiveness of each metric against known variables.

Each sample was tested under two distinct testing scenarios; one with no modifications to the presented sample, and one with a progressively modified variant on a specific demographic characteristic to cause a variation in performance and create bias. This variation of the demographic characteristic allowed the experts to measure the sensitivity of the metric to each bias; if the value of a metric correlates with the change in bias, it indicates that the metric could be used to investigate bias in the industry.

Key findings

Once the fairness metrics on the data sets for both the unbiased and the synthetically biased scenarios had been computed, using the Pearson Correlation Coefficient allowed the experts to visualize the linear relationships between the metrics and the bias introduced. They could then compare how the fairness metrics responded to each of the synthetic alterations. Metrics controlled by an alpha parameter – a variable value used in FDR, IR, and GARBE to achieve equity between security and the user experience – are less stable than those without one.

The findings propose a new fairness index in the form of the Area Max Differential Rate (AMDR), which identifies the differential between False Match Rate and False Non-Match Rate as the hallmark of an unfair system and does not rely on an alpha parameter. This is better suited for detecting variations across the three types of systems with different loss functions. Each system manufacturer uses its own model based on a specific type of loss function, so identifying the most appropriate metric, or combination of metrics, to apply in each specific case is a significant step toward achieving fairness.

Raising the bar for biometrics

This examination of bias in facial recognition systems underscores the need for stringent requirements regarding the accuracy and fairness of all biometric solutions. It demonstrates that, while biometric systems have developed rapidly over the past decade, work is still to be done to enhance their security, practicality, and inclusivity.

Introducing new methodologies to evaluate the effectiveness of bias detection with different metrics, allows vendors to better train their solutions to account for biases and elevate real-world solutions. In doing so, solution providers can enhance their offer to ensure that both they and the OEMs that use their products do not jeopardise user data or risk the reputational damage of uncontrolled bias. Standardization and certification bodies can also use this research to augment requirements, standards and test plans.

By striving towards benchmarks for security and performance, solution providers and device manufacturers can raise the bar for biometric security. Through testing and evaluation with a trusted lab partner, those looking to augment their biometric offer can create inclusive solutions that provide equitable security and performance for all.

Organisation: Fime
Names: Joël Di Manno, Manager, Authentication & Biometry & Neily Sanon, PhD student and Test Analyst
Contact: shirley.yeh@fime.com & stephanie.pietri@fime.com

13. HID: Facial Recognition for Borders and Travel: 2025 Trends and Insights

The world of biometrics is constantly evolving, and 2024 was a transformative year as people continued to embrace the technology's value. The use of facial recognition for border control and travel has grown rapidly, bringing new opportunities and critical discussions about its future role in society.

Key Biometric Trends in Border Control for 2025:

1. **Frictionless Authentication in Public Spaces**: Airports and border crossings are adopting easy-to-use and self-service biometric solutions for faster and more convenient identification to elevate the user experience. Envision walking through checkpoints without needing to show physical documents, all while maintaining layers of digital protection based on biometric credentials.

2. **Ethical Considerations Take Priority**: As biometrics become more ingrained in society, discussions around data privacy, matching bias in algorithms, and potential misuse will continue. Expect stricter regulations and more responsible development practices as leading biometric providers express commitments to data diversity to help reduce AI matching bias and foster inclusivity and fairness in applications.

3. **Data Security and Transparency**: Concerns about data privacy and security will remain a major focus, with regulations like GDPR, BIPA and CCPA shaping how biometric data is collected, stored, and used. Expect increased transparency and user control over biometric data.

4. **AI-Powered Biometrics**: Artificial intelligence will play a crucial role in enhancing biometric accuracy, detecting spoofing attempts, and identifying emerging threats. Expect to see AI-driven algorithms continuously learn and adapt, making biometric systems even more robust and reliable.

5. **Bolstering Border Control**: At immigration checkpoints, biometric technology empowers border authorities to verify passenger identities swiftly and accurately, helping to zero in on potential threats and prevent unauthorized entry. With irrefutable identity verification powered by unique biometric traits, border security is heightened by the ability to better detect fraudulent activity, safeguarding national interests.

Seamless and Secure Border Crossings

Seamless and secure border crossings are crucial for a thriving travel industry. However, border control processes that still rely on manual document checks pose unnecessary risks to both national security and a positive traveller experience. Slow and cumbersome identity verification conducted by humans leads to long lines and frustrated travellers. This is where biometrics come in.

Biometric technologies are revolutionizing border security by providing a faster, more secure, and more efficient approach to verifying traveller identities. As passenger volumes continue to rise globally, transportation authorities and immigration agencies are quickly realizing the value of onboarding facial recognition technology to streamline busy and mission-critical border crossings.

Case Study: Friction-free Passage at a Southeast Asian Seaport

One of the busiest border spots in Southeast Asia is an international seaport with over 8 million people moving through arrivals and departures each year. Slow manual processes resulted in extremely long wait times, leading to irritation, frustration and missed connections. In partnership with government entities and system integrators, a facial recognition solution was incorporated into the automated border control (ABC) gates. The ABC gates were installed throughout the centre and immediately transformed the border crossing experience,

thanks to the layers of engineering excellence built into the AI-powered facial recognition camera.
Now, travellers can experience a hassle-free journey. They simply approach the self-service ABC gate and place their passport on the document reader. Once their information is confirmed, they move through the first gate and step in front of the facial recognition camera for a quick face scan and a match against their ID document photo. The visitor then moves through the second gate. The entire process is done within seconds.

Benefits of Facial Recognition Solutions

These intuitive facial recognition solutions benefit both travellers and authorities:

- Fast and Accurate: On-the-spot verification validates a traveller's identity in seconds.
- Easy to Use: One look is all that's required for secure, frictionless identity verification.
- Secure: Biometric traits provide irrefutable proof of identity to prevent spoofs and enhance border security.
- No Human Intervention: This seamless, automated technology requires no dedicated staff to check travel documents and IDs, freeing up resources to focus on other tasks and priorities.
- Contactless and Hygienic: Touchless authentication minimizes exposure to health risks by reducing shared touchpoints.

A Model for Modernization: Frictionless Security with Facial Recognition: Integrating best-in-class facial recognition cameras into the ABC gates enables immigration entities to:

- Improve the Traveler Experience: The biometric-based gate system provides passengers with a satisfying experience via convenient, self-service authentication that shortens wait times.
- Deliver Fast and Reliable Authentication: The entire process to authenticate an individual is now accomplished in seconds.
- Enhanced Border Security: The ABC gate system can be connected with Interpol and other deterrence databases to prevent foreign travellers involved in unlawful activities from entering.

People moving through borders appreciate the efficiency provided by ABC gate systems with facial recognition. "Wait queues are now drastically decreased and passengers are empowered by the fast and convenient self-service process that has them on their way in a matter of seconds," commented one government official after implementation.

The use of facial recognition at border checkpoints is fast becoming a public expectation and a significant advantage for security operations. The success of these projects sets a precedent and paves the way for broader adoption of facial recognition technology across the country.

Organisation: HID
Name: Vito Fabbrizio
Email: vito.fabbrizio@hidglobal.com

14. IDEMIA: Unlocking the Future of Travel: How Biometrics Ensure Security and Simplicity

As global travel evolves, the demand for secure, and frictionless journeys continues to grow. To meet rising traveler expectations and address industry challenges, the travel sector is embracing advanced digital technologies. The widespread acceptance of biometric solutions is driving governments, port operators, and carriers to adopt these technologies, enhancing operational efficiency, security, and the overall travel experience.

Why biometrics are critical in the traveler's journey

According to the Airports Council International (ACI) Airport Service Quality (ASQ) 2023 Global Traveller Survey, 58% of travelers favor a more technological and streamlined journey. Biometric technologies address two vital needs: strengthening security and optimizing operations. Governments seek to enhance border controls amidst growing security concerns, while carriers and port operators face the challenge of managing rising passenger volumes with finite resources. Biometrics simplify processes across the travel continuum—from check-in to boarding and departure to arrival—delivering convenience while maintaining robust security.

In this digital era, manual processes alone are no longer sufficient for managing millions of daily travelers. Automated, self-service solutions like eGates process travelers in seconds, cutting wait times and improving throughput. Powered by facial, iris, or fingerprint recognition, these solutions optimize resources, accelerate clearance, and boost security through reliable identity verification.

Facial recognition is here to stay

Facial recognition, with its superior speed and accuracy, has become the leading modality for traveler identity verification, surpassing fingerprint recognition. The ACI 2023 Global Traveller Survey found that 66% of respondents are in favor of using biometric solutions such as facial recognition to make the journey contactless, while the Biometrics Institute Industry Survey 2024 predicts that facial biometrics will see the highest adoption growth, with 46% supporting its increased use.

Unlike other biometric recognition, facial recognition is contactless and non-intrusive, offering a hygienic and convenient experience—an appealing factor in the post-pandemic era. Automated checkpoints eliminate the need for repeated document presentation, aligning with traveler expectations and establishing facial recognition as a cornerstone of the future of travel.

The European Entry/Exit System (EU-EES) highlights this trend, selecting facial recognition alongside fingerprints to process third-country nationals. Similarly, Singapore's immigration system leverages multi-modal biometrics, including facial recognition, to enable a passport-less experience.

Key challenges in adopting biometric solutions

While biometric technologies, including facial recognition, offer significant benefits, their adoption also presents several challenges:

- Data privacy concerns: Travelers may hesitate to share personal data, including biometrics, due to privacy concerns. Earning their trust requires demonstrating that their data is secure, used solely to enhance their travel experience, and retained only temporarily. Clear transparency about who can access the data and for what purpose is essential.
- Algorithmic bias: Systemic errors in algorithms can create unfair outcomes, such as false matches or denied access. Addressing bias is vital to ensure equitable treatment for all travelers.
- Changes in physical appearance: Aging or health conditions can affect biometric matching accuracy, posing challenges for reliable identification.

- Spoofing and fraud: Biometric data can be counterfeited through presentation or morphing attacks. Robust detection systems are essential to prevent identity theft and secure passenger clearance.

- System interoperability: Seamless integration of biometric systems into existing IT ecosystems is critical for scalability, operational continuity, and system effectiveness.

Solutions to address challenges

To overcome these obstacles, the travel industry can adopt several strategies:

1. Increased data protection: Deploying cutting-edge technologies to secure biometric capture equipment, systems, and communication channels ensures data safety. Compliance with international regulations like General Data Protection Regulation promotes trust.

2. Fair and transparent algorithms: High-quality algorithms should perform reliably across diverse populations and conditions with notably a focus on fairness, a commitment consistently reaffirmed by top rankings in NIST evaluations.

3. Spoofing resistance: Staying ahead of evolving threats requires continuous innovation in countermeasures. Developing advanced capture solutions to combat spoofing as well as combining multiple biometric modalities can further improve robustness.

4. System interoperability and integration: with various stakeholders and systems involved, standardized protocols and collaborative efforts can encourage cohesive travel ecosystems. In parallel, developing a strong partnership between vendors will be key in making the various systems interoperable while delivering a convenient traveler experience along their entire journey.

5. Biometric data privacy: Travelers should have the assurance that their data is used temporarily to ensure a secure and smooth journey. Providing flexible storage options and maintaining full transparency about data access and usage are critical to fostering trust.

Shaping the future of travel with biometrics

Facial recognition has become a foundation for secure and seamless travel. Alongside other biometric technologies such as iris and fingerprint recognition, it plays a crucial role in building a travel ecosystem where borders are secure, operations run efficiently, and journeys are effortless. Biometrics, particularly facial recognition, are here to stay and will redefine industry standards, shaping a future of travel that is safe, efficient, and inspiring.

Organisation: IDEMIA Public Security
Name: Nicolas Phan
Contact: nicolas.phan@idemia.com

15. Ingenium: The future of responsible biometrics: Ensuring security and performance through testing

Introduction

Biometric technology has seen significant development in recent years, offering enhanced levels of security, convenience, and accuracy in identity authentication and verification applications across a wide range of industries. From fingerprint scanning to facial recognition, biometrics is now deeply integrated into everyday life, influencing sectors such as law enforcement, healthcare, finance, government, travel and the use of mobile devices. However, with these advancements come critical ethical, security, and performance concerns. The responsible use of biometrics must ensure fairness, privacy, and accuracy through rigorous testing, including independent laboratory evaluations and real-world performance assessments.

The growing importance of biometrics

Biometric authentication is becoming the preferred method for identity authentication due to its robustness and convenience. Unlike passwords or PINs, biometric data is unique to each individual, making unauthorised access more difficult. Governments, corporations, and consumers rely on these technologies for secure access control, fraud prevention, and identity verification.

However, the increasing adoption of biometrics also raises concerns about data privacy, bias, and security vulnerabilities. Issues such as racial bias in facial recognition and spoofing attacks on fingerprint sensors highlight the need for responsible biometric development and testing. In addition, rapidly emerging threats from injection attacks and deep fakes need to be evaluated by competent test laboratories in order to demonstrate systems' resilience to a range of threats.

Challenges in biometric implementation

Assurance in any technology, and biometric technology in particular, depends on reliable and robust testing. Despite its potential, biometric technology faces significant challenges that must be addressed by appropriate evaluation to ensure responsible deployment:

1. Privacy concerns: Biometric data, once compromised, cannot be changed like passwords. Protecting this sensitive information from misuse or breaches is paramount.

2. Bias and fairness: In the past, a number of biometric systems have demonstrated racial, gender, and age biases, leading to unfair treatment and misidentifications.
3. Security vulnerabilities: Spoofing attacks, deepfake-based impersonation, injection attacks and database breaches can compromise biometric systems.
4. Performance variability: Biometrics must work accurately across diverse conditions, such as lighting changes, aging, and different demographic groups.
5. Regulatory compliance: Countries are implementing stricter data protection laws, requiring biometric systems to adhere to ethical standards and transparency.

The role of rigorous testing in responsible biometrics

To address these challenges, biometric technologies must undergo extensive testing to ensure they are reliable, fair, and secure. Testing plays a crucial role in evaluating system performance under different conditions, identifying vulnerabilities, and improving algorithm accuracy.

Performance testing

Performance testing measures how well a biometric system functions in real-world scenarios. This includes:

- False Acceptance Rate (FAR) & False Rejection Rate (FRR): These metrics indicate how often a system mistakenly accepts an imposter or rejects a legitimate user.

- Environmental Testing: Assessing system performance under various conditions, such as different lighting, angles, and obstructions (e.g., masks, glasses).

Security testing

Security testing is essential to identifying vulnerabilities in biometric systems and protecting against malicious attacks. This includes:

- Spoofing and Presentation Attack Detection (PAD): Evaluating how well a biometric system can detect fake fingerprints, 3D-printed faces, or voice mimicry.

- Database Security: Ensuring biometric databases are encrypted, protected against breaches, and comply with global privacy regulations.

- Adversarial Testing: Simulating real-world hacking attempts to identify and patch security weaknesses before deployment.

- Deepfake and Synthetic Media Detection: With the rise of AI-generated deepfakes, biometric systems must be tested against sophisticated impersonation threats.

- Evaluating the performance of injection attack detection (IAD) capability

Bias and fairness testing

Ensuring that biometric systems work equally well for all demographic groups is crucial for ethical implementation. Bias and fairness testing involve:

- Diversity assessments: Testing algorithms with datasets that represent different ethnicities, genders, and age groups.

- Error rate analysis across demographics: Identifying disparities in recognition accuracy between different population groups.

- Algorithmic audits: Regularly reviewing biometric AI models for unintentional biases and retraining them with more inclusive datasets.

Regulatory and compliance testing

Governments and regulatory bodies are enforcing stricter compliance standards for biometric technologies. Compliance testing ensures:

- Adherence to data protection laws: Systems must comply with regulations such as GDPR (Europe), CCPA (California), and the Biometric Information Privacy Act (BIPA) in Illinois.

- User consent and transparency: Users should have clear information about how their biometric data is collected, stored, and used.

- Ethical AI practices: Ensuring that biometric algorithms align with ethical guidelines and do not reinforce discriminatory practices.

The role of laboratories in biometric testing

Independent laboratories and testing facilities play a crucial role in evaluating biometric systems before they reach the market. These facilities provide unbiased assessments and certify technologies based on industry standards.

NIST evaluations

The National Institute of Standards and Technology (NIST) conducts rigorous biometric testing programs, such as the Face Recognition Vendor Test (FRVT) and the MINEX evaluation for fingerprint systems. NIST assessments help identify the best-performing algorithms and expose biases in facial recognition technology.

ISO standards and certification

The International Organisation for Standardisation (ISO) provides biometric testing standards, such as:

- ISO/IEC 19795: Performance testing framework for biometric systems.

- ISO/IEC 30107: Presentation attack detection (PAD) standards.

Industry body evaluations

- FIDO Alliance biometric and remote identity verification certification programmes

- Android biometric unlock security assessment

Conclusion

The future of responsible biometrics hinges on rigorous testing, ethical considerations, and compliance with security and privacy standards. By investing in robust performance and security testing, organisations can ensure that biometric systems are fair, reliable, and resistant to evolving threats. As technology advances, prioritising responsible biometric practices will be essential for maintaining public trust and ensuring a safer digital future.

Organisation: Ingenium Biometric Laboratories
Name: Alastair Treharne
Contact: alastair.treharne@ingeniumbiometrics.com

16. Innovatrics: Multimodal approach to remote identity verification- combining face and palm recognition for increased security

Remote identity verification using facial recognition in combination with other technologies (e.g. OCR of identity documents, liveness detection) has become a standard for many verified registration processes. It is even being adopted in high-security applications such as finance and telecommunications, which have high standards for the so-called know-your-customer (KYC) process.

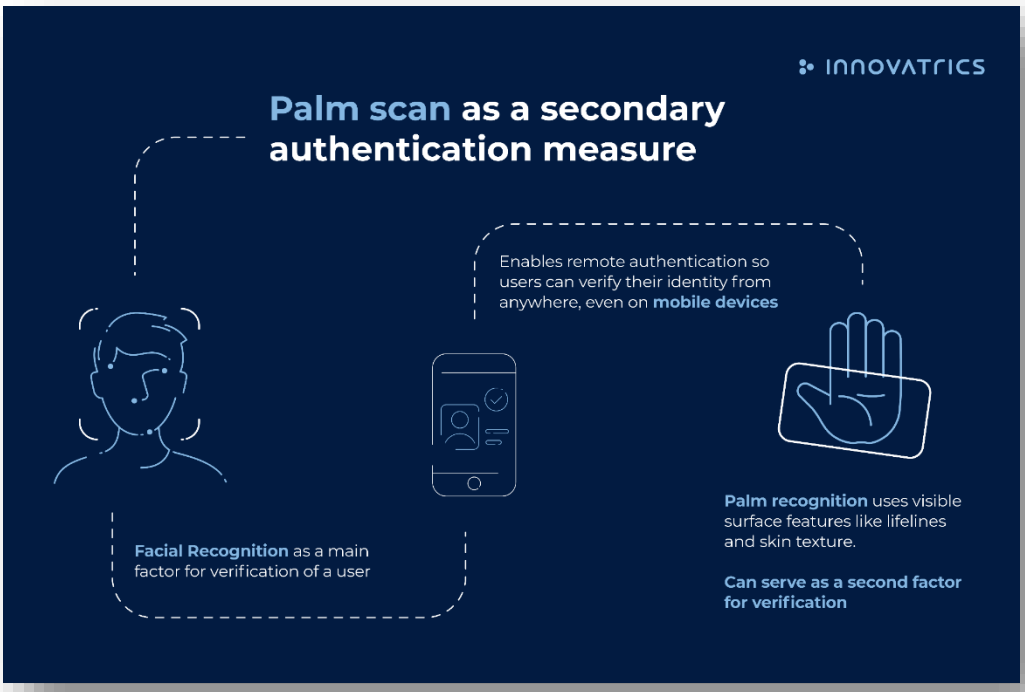
The fact that the onboarding is done on a device that's completely under user's control has its risks. The situation provides many vectors for spoofing and fraud attempts and technology has to be prepared for them. One part is liveness detection, a constantly improving technique of detecting whether a person is genuine or an impostor (video, synthetic face, photograph etc.). Moreover, the standardization and benchmarking of presentation attack detection (PAD) approaches is still underway.

Palm recognition as a second factor

When looking at possibilities to further improve security of the KYC processes, the better approach would have common features with facial recognition- it can be carried out with a standard smartphone and it has to be unique and accurate enough to serve as a reliable way of identity verification.

A solution has been introduced: a palm verification algorithm that's highly accurate and the verification can be done via smartphone, very much the same way as verification of the face or fingerprints. The human palm exhibits a high degree of uniqueness, similar to fingerprints. The patterns formed by the lines, ridges, and creases on the palm surface are unique to each individual, even among identical twins. The probability of two individuals having identical palm prints is extremely low, making palm print recognition a reliable biometric modality for identification and authentication purposes. Furthermore, they can serve as a second factor when using facial recognition as the main one.

Combining the two modalities automatically increases the security of the solution. Having two modalities for verification instead of one increases accuracy. Unless both modalities are verified, the access is not permitted. This keeps fraudsters at bay, because spoofing both modalities is much more difficult. Getting a hold of a specific face in picture or video form is relatively easy even without the person knowing due to social media and widespread use of photo sharing. Unlike faces, however, specific palms in high quality are difficult to find online to be printed and used for fraud.



Use case scenarios

The combination of modalities allows for more granular identity verification. Depending on the security threshold of a given operation or transaction, a person may use either or both modalities to verify their identity. A higher security operation- such as large bank transfer or an electronic signature of a document- may need both modalities. To check for presence, just a face scan may be needed.

This approach may be fully customised for each specific use case, providing a choice between convenience and security. By using palm as a second modality, no additional hardware, physical token or other proof of identity is necessary when interacting with an app.

The palm can also be used in access control scenarios, as it can use the same camera which is used for facial recognition-enabled access. The addition of palm, apart from increased security, adds an element of consent to the scenario, allowing e.g. for biometric payment in grocery stores, where consent is given by showing a palm rather than just looking into the camera. This gives customers more control over the automated solutions. In pure access control, palm can be an alternative to enrolment with face, because some people find face a very sensitive modality and don't want to consent to sharing it. Palm may be a replacement that provides the same level of convenience without opting into facial recognition.

Organisation: Innovatrics, s.r.o.
Name: Jakub Sochor, CTO of Innovatrics
Contact: jakub.sochor@innovatrics.com

17. Inverid: Border Queue Busting Through Secure Pre-Registration

The challenge

Since the terrorist attacks of 9-11, a global shift in immigration control has spurred additional security measures within border management processes. These controls have applied to both travel documentation and associated identity verification (biometrics).

Simultaneously, additional security controls are often at odds with the travel industry's traveller satisfaction expectations given a digital service-on-demand culture we find ourselves in.

Background

The EU Entry/Exit System (EES) serves as an excellent example of the challenge of introducing additional security measures. EES was conceptualised in the early 2000s to modernise border control for the Schengen Area, addressing concerns about illegal immigration, overstays, and terrorism. The EES will work alongside the European Travel Information and Authorisation System (ETIAS) to strengthen border security and migration management.

Despite the understandable rationale the introduction of EES does not come without concerns, primarily related to the travel and tourism sectors, which are expected to bear the brunt of disruptions during the transition:

- Potential for Travel Disruptions: Airlines, airports, and travel organisations have raised concerns that the introduction of biometric checks at border crossings could result in significant delays at airports and other entry points. They fear that the additional time needed to capture biometric data (fingerprints and facial scans) will slow down traveller flow, especially during peak travel seasons.
- Readiness of Border Infrastructure: This is especially pertinent for land and sea borders, where implementing the required biometric capture technologies may be more challenging than at large, established international airports. Many have warned that insufficient testing and the complexity of setting up the new technology could lead to delays.
- Economic and Cost Burdens: Airlines, travel companies, transport operators and governments will need to invest heavily in upgrading systems and infrastructure to comply with EES standards. This is exacerbated by the strain the COVID-19 pandemic has already placed on these sectors.

The Solution

In recent years the capability and availability of core technology to support an increase in the type of data (biographic and biometric) that can be provided prior to arrival at a BCP has improved dramatically. This is in line with the availability of personal technology devices and in particular, smartphones, such as their ability to capture high-quality images and their integrated NFC chip reading.

Modern passports are equipped with a chip that adheres to the ICAO 9303 standard. This means that all information is digitally signed and encrypted and cannot be manipulated. Also, the face image is available at a high resolution, without any additional watermarks. Therefore, they are much more suitable for face matching than the printed face image. Finally, a copied chip can be easily detected.

All modern smartphones are equipped with NFC and can be used to read and verify the chips in identity documents, without the need for expensive bespoke hardware, such as kiosks.

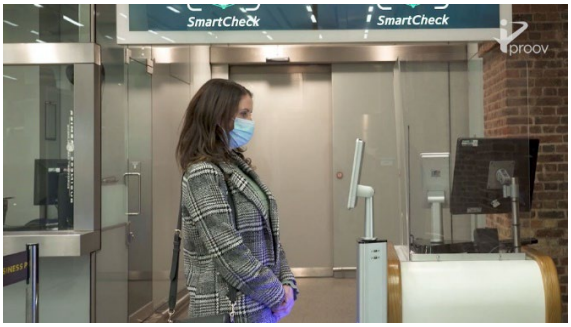
Reading the chip digitally allows the user to verify the authenticity of the identity document and read the customer information without the risk of any OCR or typing mistake. In an identity proofing or preregistration process we can also verify via face matching that the rightful owner of the passport is currently holding the passport (holder verification).

Pre-registration of traveller details is not new and has been operating at the highest level of technology readiness for ten years. ICAO Doc 9303 chipped document and identity verification has been proven in multiple global deliveries, at scale, including Australian Advanced Passenger Processing, EU Settlement Scheme and the UK Immigration Electronic Travel Authorisation.

Case Studies

Frontex and border stakeholders through a project called AP4EES developed an initial trial smartphone app for EES pre-registration. The pilot app, called QuickBorder, was tested by Frontex, the Swedish Police, Arlanda Airport, and airline stakeholders in summer 2024. Third-Country Nationals (TCN) have been used to registering for travel well in advance of arrival at a different country, perhaps through the need to apply for a valid Visa. NFC technology is used to verify the data at their server and sends the validated information to the Member State, who would then send it to the Entry/Exit System.

SmartCheck, which was created to combat a 30% reduction in efficiency at St Pancras, where long-lasting effects from the COVID 19 pandemic, Brexit, and station bottlenecks meant inefficient and labour-intensive pre-boarding checks reduced the number of passengers able to board Eurostar trains successfully. The passenger downloads an app before they arrive at the station, where they read the chip of their passport and take a selfie for facial verification. On arrival at St Pancras, instead of queuing to show their ticket and passport for manual inspection, they simply walk through a SmartCheck biometric gate which scans their face using data collected in the app and proceed to the luggage security area.



The Way Forward

From a security perspective, NFC-based remote identity verification coupled with face verification of the holder is a mature, proven technology. The authenticity of passports can be established with 100% certainty, based on country certificates. This covers both the data inside the chip as well as the fact that it is an original passport. All fully automated and at the highest security level, as proven by case studies.

Mobile pre-registration allows border forces to streamline processes at BCPs by early screening against watch lists, reduces border congestion and streamlines low-risk traveller flow, border control agents can then focus on persons-of-interest.

With the enhanced “Travel to Europe” mobile application now announced by Frontex with Sweden and two other states already implementing the app, Member States can utilise remote registration to reduce the steps and ease the burden and impact at BCPs once EES goes live. Successful implementation of EES can now be greatly assisted by the speedy adoption of the “Travel to Europe” app by Member States.

This approach can and will continue to be adopted globally to improve security of external borders without creating economic barriers to legitimate travel.

Organisation: Inverid
Name: Jim Slevin
Contact: jim.slevin@inverid.com

18. iProov: The Importance of Inclusion and Accessibility in Biometrics

Inclusivity is no longer a "nice-to-have", but a business imperative driven by ethical considerations, growth opportunities, and legal compliance. Despite efforts to standardize accessibility by organizations like WCAG, lawsuits running into millions of dollars due to non-conformance are commonplace. High-profile cases include Facebook's significant $650 million settlement and Uber's lawsuits related to biometric verification systems for drivers – both involving discrimination or bias in their systems.

Unfortunately, even a seemingly low 0.5% false rejection rate – often owing to algorithms performing less accurately for specific demographic groups – can result in hundreds of thousands of new users being denied access due to bias.

As services digitize, we face new opportunities and challenges. Biometric technologies can deliver genuinely convenient and secure identity verification – however, not all biometric technologies perform consistently for inclusivity, accessibility, and bias mitigation.

Oversights around inclusivity and bias can have severe consequences, excluding users from accessing essential services. As regulations tighten and user expectations evolve, organizations must critically evaluate how they integrate biometrics into their processes to ensure equitable access for all. Here, we highlight the tangible benefits of embracing inclusivity and showcase real-world case studies.

Considering Real-World Impact

In particular, facial biometrics have the potential to enhance inclusivity by providing secure, efficient, and accessible means of identity verification that can overcome traditional barriers and expand access to essential services for diverse user groups. The right biometric solution can be used by anyone, on any device with a user-facing camera. Key impacted areas include:

- Finance and Banking: Major institutions have increased financial inclusion rates due to digitization, which often leverages biometric verification technologies to onboard and authenticate the new era of online bankers.
- Public Services: Government agencies are enabling more equitable access to education, medical, and other vital digital services. For example, in the rapidly growing telehealth market, expected to reach $455.3 billion by 2030, facial biometric verification has become essential for improving access to care.

Key Inclusivity & Accessibility Differentiators to Look For

When selecting an inclusive and accessible identity verification and authentication solution, consider the following key differentiators:

1. Compliance With Accessibility Guidelines: Look for solutions that follow the latest web accessibility standards. WCAG 2.2 AA and Section 508 are two leading standards for digital accessibility. WCAG 2.2 prohibits using cognitive function tests (e.g., passwords, puzzles) during authentication ensuring high usability for all. More generally, prioritize solutions that provide detailed bias performance reporting, including third-party audit results and industry certifications.
2. Proven Inclusivity: Request comprehensive testing data showcasing equitable performance across diverse demographics, including socio-economic group, age, gender, skin tone, and cognitive abilities. This transparency ensures the solution does not discriminate against any user group. Inclusivity reports should be available on a regular bias.
3. Proactive Approach: Look for solutions that provide an active inclusion roadmap, continuously working to identify and mitigate potential biases through regular testing, diverse training data, and algorithm adjustments.

Recommended Approach

Building facial biometrics that are both inclusive and ethical requires a dedicated and multifaceted approach. To ensure fairness and accuracy for all users, the following practices are recommended:

1. **Diverse Training Data**: Use AI models that learn from ethically sourced, diverse datasets representing a global user base to mitigate demographic skews.
2. **Continuous Bias Testing**: Conduct regular comprehensive bias testing across age, gender, and ethnicity and analyse for new emerging biases.
3. **Transparent Performance Reporting**: Ensure test insights are transparently shared to build trust via third-party audits and create detailed bias mitigation roadmaps.
4. **Human-AI Collaboration**: Continuous monitoring by expert analysts for novel attacks/biases, and adjusting of algorithms to enhance accuracy and inclusion.

The Decision Framework

When deciding on a biometric identity solution, apply this rigorous framework covering critical factors:

- Accuracy: Insist on comprehensive performance data across global demographics to ensure equitable service delivery.
- Inclusivity and Accessibility: Evaluate training data diversity, WCAG 2.2 conformance, and accessibility for users with disabilities.
- Bias Mitigation: Assess processes like continuous testing, algorithm refinement, and oversight by biometric science experts to identify/address emerging biases proactively.
- Compliance: Verify the solutions meet current and upcoming regulations regarding inclusivity and ethics in your regions/industries.
- Transparency and Ethical AI Principles: Prioritize solutions with public accountability via third-party audits, performance reporting, and ethical AI oversight boards. Ensure alignment with globally recognized tenets like fairness, accountability, privacy protection, and human oversight.

Beyond ethics, there are serious legal impacts of biased biometrics like lawsuits, lost revenue, and reputation damage For example, NIST found higher error rates for ethnic minorities due to biased datasets, prompting Congressional scrutiny.

The Benefits of Inclusive Face Biometrics

In contrast, inclusive and unbiased facial verification unlocks powerful advantages:

- Expanded Market Reach: Remove barriers to access new demographics and build a more extensive customer base across diverse communities.
- Improved CX: Smooth onboarding raises conversion rates and brand satisfaction, reducing support costs from exclusionary friction.
- Competitive Edge: Position your brand as ethical and socially responsible, attracting values-aligned consumers.

The Business Imperative of Trusted Inclusive Face Biometrics

In today's digital-first climate, inclusive and ethical identity verification is a strategic imperative, not an optional consideration. By selecting solutions that prioritize accuracy, inclusivity, bias mitigation, and globally recognized standards, organizations can create a competitive edge while avoiding costly discrimination pitfalls.

Organisation: iProov
Contact: enquiries@iproov.com

19. Jumio: The Future of Biometrics: Enhancing Security with a Multimodal Approach

As biometrics play an increasingly pivotal role in digital interactions, the demand for responsible, transparent, and secure biometric solutions is higher than ever. With applications spanning financial services, healthcare, border control, and more, biometric technology touches nearly every aspect of our daily lives. Yet, as its use proliferates, concerns about accuracy, inclusiveness, and ethical deployment have come to the forefront. Multimodal biometrics – systems that combine multiple forms of biometric recognition, such as facial recognition, fingerprinting, and voice authentication – emerge as a compelling answer to these challenges. A multi-technology approach not only strengthens security but also ensures greater accessibility and minimizes bias, setting the stage for the future of responsible biometrics.

The Need for Multimodal Biometrics

Single-mode biometrics, while effective, have limitations that can impact the accuracy, security, and inclusivity of verification processes. Multimodal biometrics address these limitations by leveraging multiple biometric indicators, making systems both more robust and user-friendly.

Increasing Accuracy

In high-stakes sectors, such as financial services and healthcare, the risk of a false positive or false negative can have significant consequences. By combining multiple biometric inputs – for example, verifying both face and behavior such as location and device – a multimodal system can cross-reference data points to improve the accuracy of identity verification. This redundancy reduces the likelihood of error and ensures that only the correct individuals can gain access.

Enhanced Security

Multimodal systems create an extra layer of security, as each biometric mode serves as an independent verification step. For a fraudster to successfully breach a multimodal biometric system, they would need to replicate each biometric mode accurately, which is far more challenging than circumventing a single-mode system. This added complexity is critical for protecting sensitive data, especially as fraud tactics grow more sophisticated.

Practical Applications and Case Studies

Several industries have already begun deploying multimodal biometric systems to enhance both security and user experience. Below are some examples of how a multi-technology approach is making a difference across sectors:

Financial Services

In banking, multimodal biometrics are used to secure access to accounts and authorize transactions. A system that combines facial recognition with voice authentication, for instance, creates a seamless yet secure experience for customers, who can verify their identity quickly without compromising security. This dual-layered approach helps financial institutions reduce fraud and build customer trust, all while enhancing the user experience.

Healthcare

In healthcare environments, patient identification must be both accurate and efficient, especially in emergency situations. Multimodal biometrics, like combining fingerprint and iris scans, enable rapid and accurate identification of patients, minimizing errors in patient data and medication management. By verifying identity through multiple modes, healthcare providers can prevent costly mistakes and ensure that patients receive the correct treatment.

Retail and E-commerce

Retailers are increasingly adopting multimodal biometrics to enhance security and customer experience, particularly in online shopping and self-checkout. By combining facial recognition with behavioral biometrics (e.g., typing patterns), retailers can verify customer identities more effectively during purchases and login sessions. This approach reduces

fraud risk in e-commerce, where identity theft is common, and streamlines in-store checkout, creating a secure, convenient experience that fosters customer trust.

Future Trends and Technological Considerations

As biometrics continue to evolve, several trends and considerations will shape the adoption and effectiveness of multimodal approaches:

Data Privacy and Security

With multimodal biometrics generating more data, ensuring robust data protection practices is crucial. Users demand transparency and assurance that their data is handled securely and ethically. Organizations implementing multimodal biometrics should adopt data minimization practices, encrypt sensitive data, and provide clear information about data usage to foster trust and compliance with privacy regulations.

Interoperability and Integration

Multimodal biometrics must operate across various devices and platforms, particularly as organizations deploy biometrics at scale. Ensuring that multimodal systems are compatible with different hardware and software systems enhances accessibility and user convenience. The next wave of multimodal biometrics will likely prioritize interoperability, making it easier for organizations to integrate biometric solutions into existing systems.

Ethical Use

As biometrics become more ingrained in our daily lives, ethical considerations must guide their deployment. Transparency, user consent, and responsible data management are essential to maintaining public trust in biometrics. Organizations adopting multimodal approaches should set a precedent by implementing clear ethical guidelines that govern data collection, usage, and storage. Ethical practices ensure that biometric systems are not only effective but also socially responsible.

As multimodal biometrics continue to redefine identity verification, it offers a path toward enhanced security, accessibility, and public trust. By combining technologies like facial recognition and behavioral biometrics, organizations across various sectors can address the pressing demands for accurate, inclusive, and ethically sound verification processes. However, the journey to responsible and scalable biometric solutions requires an industry-wide commitment to data privacy, ethical deployment, and seamless integration.

Organisation: Jumio
Name: Abby Messier
Contact: abby.messier@jumio.com; anna.convery@jumio.com

20. Keyless: Privacy-Preserving Biometrics: The Emergence of Decentralised Systems

Biometric authentication has become an essential part of modern security systems. Its ability to verify individuals based on unique physical traits offers the strongest connection between a user's digital and physical identity. However, since biometric data cannot be changed or revoked, and because it serves as a strong proof of identity, it must be kept private and protected from authorized access. To address these concerns, privacy regulations like GDPR, PDPA, and CCPA have evolved to enforce strict data protection standards. Consequently, biometric systems must adapt to incorporate strong privacy-preserving capabilities. This paper explores how privacy concerns have reshaped biometrics, focusing on the difference between the three biometric systems and how advanced cryptographic methods can address existing challenges.

The Challenges of Biometric Authentication

Biometric systems must keep biometric data private at all stages: when it is stored, transmitted, and matched. Several approaches to managing data exist, each with its own strengths and weaknesses.

Local Biometric Matching

In local systems, biometric data is stored on the user's device, and matching occurs locally. Most commonly seen with the use of FaceID and Samsung ID, this method is widely used in consumer devices like smartphones. It ensures biometric data is kept private, as it never leaves the device when stored, transmitted, or matched.
However, while it is private, it has limitations. Only local applications can trust that biometric authentication took place. In other words, a consumer app must trust that the biometric template used to access their service belongs to the person that originally enrolled in it. It is also not portable, as it does not allow for cross-device authentication—an iPhone user cannot use the same biometrics to authenticate on a Windows computer; they must create a separate biometric template. Also, as biometrics are tied to the device, if a device is lost and an account recovery must be performed, a user has to undergo re-enrolment to prove they are who they claim to be.

Server-Side Matching

Server-side systems store biometric data centrally and match it against user-provided samples. This approach allows for cross-device authentication and simplifies recovery, conveniently addressing the main usability and security concerns associated with local biometrics.

But where local biometrics are private, server-side matching raises significant privacy concerns. A server breach could expose biometric templates for millions of users, and privacy laws impose strict requirements on how biometric data is stored and processed, making compliance costly and complex.

Decentralized Biometrics

The decentralized approach to biometrics has emerged as a way to address the privacy issues associated with server-side biometric authentication. In its 2023 Innovation Insight for Biometric Authentication, Gartner defines decentralized systems as biometric authentication systems that are neither local nor centralized. This approach is still nascent and its exact definition within the biometric authentication space is yet to be fully agreed on.

But there is a notable irony in the commercial implementation of this approach. The vendors offering decentralized solutions today do so in a manner that fails to preserve privacy, contradicting the very principle they aim to uphold.

Existing decentralized systems today aim to split biometric data across multiple servers, storing fragments (or "shares") that individually do not reveal the complete biometric information. While this approach appears to enhance privacy by reducing reliance on a single point of failure, it has critical flaws:

- **Reconstruction Risks**: If enough shares are compromised, attackers can reconstruct the entire biometric template.
- **Collusion Threats**: If entities managing the shares collude, privacy is compromised.
- **Partial Data Vulnerability**: Even a single compromised share can allow attackers to perform partial matches, de-anonymizing users through publicly available data like social media photos.

These limitations show that decentralized systems, as implemented today, fail to fully preserve biometric privacy. To overcome these shortcomings, more advanced methods are required.

Secure Multi-Party Computation as the Solution

Secure Multi-Party Computation (SMPC) is an advanced cryptographic technique that enables multiple parties to perform computations on encrypted data without revealing the underlying data to any party. A common example used to explain SMPC is the "millionaire's problem," where two or more individuals would like to see who is richer without disclosing how much they have. SMPC can be used to address this problem by allowing the parties to learn the output of the protocol (which of the individual is the richest) without disclosing the protocol inputs (how rich is each participant). Used for biometric authentication, SMPC is able to offer the privacy benefits of local biometrics and the usability and security advantages of server-side systems; in other words, the best of both worlds.

In an SMPC-based system, biometric data is transformed into an encrypted template during enrolment and then stored, in encrypted format, in the cloud. During authentication, a fresh authentication template is taken, transformed, and compared with the encrypted enrolment one. Both enrolment and authentication templates are compared while in encrypted form.

Advantages of SMPC in Biometric Authentication

This method has several advantages:

- At no point does the cloud service provider—or the vendor using it—access the actual biometric data, ensuring complete privacy.
- Unlike traditional decentralized systems, SMPC ensures that neither individual servers nor attackers who compromise them can access biometric data.
- Because SMPC prevents the reconstruction of biometric data, it has the privacy capabilities of local biometrics and aligns more closely with existing laws.
- Like centralized biometrics, SMPC systems can operate across devices without requiring users to re-enrol.

Conclusion

Privacy is no longer just a regulatory requirement; it is a fundamental user expectation. By storing only privacy-preserving user profiles—which are not considered biometric data under GDPR and similar regulations—SMPC eliminates biometric honeypots. Among existing centralized and decentralized systems, SMPC is the only technology that provides complete biometric privacy, even in case of vendor breaches.

Biometrics must adapt to meet this demand by adopting technologies that sit within the golden triangle of security, usability, and privacy, and SMPC represents a marked shift in how biometric authentication providers can achieve this.

Organisation: Keyless
Name: Paolo Gasti
Contact: info@keyless.io

21. NEC Australia: Responsible Use of Biometrics in Digital Identity

Emerging Trends in Responsible Biometrics

Biometrics will be instrumental in shaping the future of identity solutions, including decentralized identity systems and the digital integration of physical identity cards. By enhancing security, safeguarding privacy, and fostering user confidence, biometrics will drive the evolution of next generation identity solutions.

Decentralised Identity Credentials

Decentralised identity credentials, such as verifiable credentials and mobile driver's licenses, are rapidly gaining traction. These credentials can be issued directly to a holder's app or digital wallet, installed on the person's mobile device. Both verifiable credentials and mobile driver's licenses include face biometric data as one of their key attributes.

To ensure security, these credentials must be linked to the holder app through biometrics, such as their face. When a user shares their credentials with digital services, the face biometric data within the credential should be verified against the user's live face. The holder app must utilise advanced biometric techniques, such as face verification, presentation attack detection, and injection attack detection, to ensure that the credentials are being shared by their rightful owner. By leveraging "Biometrics as a Service" (BaaS), biometrics providers can deliver tailored solutions for digital credential issuers, holder app providers and users.

QR-Enabled Physical Identity Cards

For underserved populations and environments with limited digital access, QR-enabled physical ID cards bridge traditional and digital systems. These cards embed biometric data within QR codes, offering seamless and secure identity verification. Compliance with global standards, such as ISO/IEC 18013-5 (mDL/mdoc), ensures security and interoperability.

The data in mdoc is typically encoded as CBOR (Concise Binary Object Representation) tokens, chosen for their compactness and efficiency. CBOR tokens are structured data objects encoded in a lightweight format, making them ideal for use in constrained environments where size and processing efficiency are critical, offering an advantage. Since CBOR tokens are lightweight, they are well-suited for generating QR codes on physical identity cards. The CBOR token encapsulates identity data, a biometric template, and the issuer's digital signature, secured with advanced signing methods. This ensures data integrity and facilitates trusted interactions.

Users can use their QR enabled physical identity card to access digital services. By incorporating biometric verification, digital service can match the facial data stored in the QR code on the card with the individual attempting to use the application service, ensuring secure and reliable access.

By leveraging "Biometrics as a Service" (BaaS), biometrics providers can deliver tailored solutions for digital service providers, physical identity card issuers and users.

Ethical and Security Considerations

As reliance on biometrics grows, addressing ethical and security challenges is vital to maintain user trust. Key measures include:

- Explicit User Consent: Ensure transparency by obtaining informed consent before collecting biometric data.
- Encryption: Always protect data, whether in transit or storage, using robust encryption techniques.
- Continuous Improvement: Regularly update systems to counter evolving threats, such as deepfakes and spoofing.

- Biometric Reset: Enable periodic updates to biometric templates to enhance security and mitigate risks.
- Auditing and Monitoring: Implement consistent audits to detect and address unauthorised access or misuse.
- User-Centred Design: Prioritise usability to encourage adoption, testing solutions with real users and incorporating their feedback.
- Unbiased Biometrics: Regular audits and testing should ensure equitable performance regardless of age, gender, or ethnicity.
- Policy Frameworks: Develop comprehensive guidelines for data collection, storage, and disposal to ensure accountability and compliance.

Practical Applications & Case Studies

Decentralised Identity in Action

A national e-passport programme demonstrates the potential of decentralised identity systems. By incorporating facial biometrics and on-device verification, the programme enabled secure, contactless border control, reducing wait times while safeguarding privacy.

QR-Enabled ID for Healthcare Access

In healthcare initiatives where mobile phone use is not possible, QR-enabled ID cards facilitated seamless patient identification and access to medical records. Biometrics ensured the authenticity of user identities, enhancing service delivery while maintaining data security.

QR-Enabled Student ID for Social Media Ban

Schools are seeking limit mobile phone usage to effectively support and enforce a social media ban. Schools can issue QR-enabled ID cards to students which provides a convenient and efficient way to verify student identities and grant access to essential digital services without requiring mobile devices. Biometrics ensured the authenticity of student identities, enhancing service delivery while maintaining data security.

Conclusion

Biometrics are transforming digital identity, offering enhanced security, accessibility, and convenience. However, their potential can only be realised through responsible implementation. By prioritising ethics, transparency, and user trust, the industry can create systems that are secure, inclusive, and aligned with societal expectations. Collaboration across sectors is essential to shape a future where biometrics are not only effective but also equitable and trusted.

Organisation: NEC Australia
Contact: Steven Graham – NEC Head of Biometrics (ANZ) & Innovation - Steven.Graham@nec.co.nz
Venkat Maddali - Principal Architect - Digital Identity & Biometrics - venkat.maddali@nec.com.au

22. OVD Kinegram: How Chip-Based Biometrics Prevent Deep Fakes in Remote Identity Verification

The Evolving Threat Landscape: Identity Theft and Fraud

Fraud and identity theft, are escalating threats to national security and integrity, undermining financial systems and eroding trust.
As digital identities gain popularity for their convenience, their secure implementation is under scrutiny. This leaves physical credentials – such as electronic Machine-Readable Travel Documents (eMRTDs) like passports or other chipped identity documents – as the primary means of and most trusted foundation for establishing identities.

Identity verification methods that rely on visual inspections by camera or the naked eye are particularly vulnerable to sophisticated forgeries. High-quality counterfeit digital images of identity documents or optical security features may deceive even trained inspectors or automated systems. The acquisition of the holders facial image from a non-chipped identity document can be compromised by deepfake technology by manipulating the presented information in real time. This exposes significant security gaps in remote scenarios.
eMRTDs with their embedded chips and sophisticated physical security features like Diffractive Optically Variable Image Devices (DOVIDs) bridge the gap between physical and digital realms, enhancing security and facilitating identity verification. Supported by international standards developed by ICAO or ISO, eMRTDs offer unparalleled reliability in combating fraud and verifying identities, particularly in remote scenarios. By leveraging the encrypted chip data, eMRTDs allow for highly secure and efficient remote identity verification processes. Their adherence to international standards and seamless integration into verification workflows make them indispensable tools for government agencies, businesses and individuals seeking robust identity authentication solutions.

Why the Source Matters: Biometric Data From eMRTDs

The reliability of biometric authentication depends on the integrity of its data source. This makes the chip embedded in eMRTDs – which securely stores biometric and personal data – a critical component of identity verification. It establishes a reliable, direct link between the document and its holder, whilst also ensuring interoperability and compatibility across international borders.
Compared to visual biometric verification, which depends on factors such as video recordings, camera performance, lighting conditions and optical level 1 security features, chip-based identity verification offers numerous advantages. These include reliability, traceability, consistent performance and enhanced resistance to manipulation.
Chip-based identity verification enhances security through:

- **Private-Public Key Security Certificates**
  Chip-enabled identity documents use private-public key certificates to ensure data integrity and authenticity. This cryptographic approach makes electronic verification both simple and reliable. The certificates confirm that the data has not been altered and that it originates from a legitimate source. The method also effectively prevents cloning, as the chip's cryptographic keys are unique and cannot be duplicated without detection.

- **Real-Time Verification**
  Chip verification supports real-time checks, providing immediate liveness assurance that the document is present at a specific time and location. This significantly reduces the risks of fraud and unauthorized use while enhancing the trustworthiness of remote processes.

- **Elimination of Optical Variability Issues**
  Chip-based verification methods are unaffected by issues such as camera quality and resolution, poor lighting or the need for tilting the document to inspect different security features. This makes the process quicker and less prone to human error.

- **Secure Storage of Personal Information**
  One of the most significant benefits of chip verification is the access to the holder's biometric data, such as facial

image, that can be directly matched to the document holder. This ensures accurate identification and minimizes the risk of impersonation. As all personal data is stored electronically, the security and reliability of the information is increased- data cannot be tampered with or altered without detection, be it attempts of deepfakes or other sophisticated digital manipulations.

The Role of Biometric and eMRTD-Based Identity Verification

ICAO 9303 and ISO/IEC 7816 establish international standards for eMRTDs, including foundational specifications for chip-based applications. This ensures security and integrity, consistency, and global interoperability. While these ISO standards enhance the secure organization and protection of sensitive data, they enable quick and accurate verification using automated systems, minimize human error, and enhance onboarding efficiency.
Biometric identifiers like the facial image in eMRTD chips provide a secure method to confirm the rightful document holder. Advanced encryption and digital signatures protect data from unauthorized access and manipulation, thereby reinforcing the overall security of travel document verification.

Modern solutions for eMRTD verification integrate seamlessly into identity verification workflows and are designed for compliance with ICAO and ISO requirements. These solutions support real-time chip verification, providing immediate confirmation of data authenticity and biometric matches. They often emphasize:

- **On-Premise Deployment**: Ensuring full control by operating within the customer's environment, particularly critical for organizations prioritizing data privacy and compliance.
- **Rapid Integration**: Deployable and fully functional in minimal time, enabling organizations to quickly respond to workflow demands.
- **Uncompromising Data Security**: Keeping all data under the customer's control to ensure safety, confidentiality, and compliance.

As digital identity solutions continue to evolve, leveraging eMRTD chips for remote identity verification serves as the standard for high-assurance scenarios. This approach not only upholds the highest security standards but also fosters trust in remote onboarding and digital identity processes. By maximizing the use of biometric data securely stored on chips, organizations can achieve the highest level of reliability in identity verification, strengthen fraud prevention, and enhance user trust.
As digital identity verification becomes an integral part of modern life, adopting chip-based verification methods contributes to a safe, seamless and trustworthy future to prevent deep fakes on identity documents. An advanced chip verification solution empowers governments and organizations to embrace this future with confidence.

Organisation: OVD Kinegram AG
Name: Stefan Gabriel – Expert for ID Chip Verification
Email: Stefan.gabriel@kinegram.com

REFERENCES

- Avoine, G., Beaujeant, A., Hernandez-Castro, J., Demay, L., Teuwen, P. (2016). A survey of security and privacy issues in ePassport protocols. ACM Computing Surveys, Vol. 48, No. 3, Article 47. URL: http://dx.doi.org/10.1145/2825026
- International Civil Aviation Organization. (2021). Doc 9303 Machine Readable Travel Documents. Eighth Edition. Part 1: Introduction. URL: Microsoft Word - Doc.9303.Pt.01.8th.Ed.alltext.en.INPROGRESS.CC.docx (icao.int)
- International Civil Aviation Organization. (2015). Doc 9303 Machine Readable Travel Documents. Seventh Edition. Part 11: Security Mechanisms for MRTDs.URL: Doc 9303 7th Part11.pdf (icao.int)
- Obiora Nweke, L. (2023). National Identification Systems as Enablers of Online Identity. URL: National Identification Systems As Enablers of Online Identity | IntechOpen
- OVD Kinegram AG (2024). Customer Onboarding: Optical vs. Chip Identity Document Verification. URL: Customer Onboarding through Identity Document Verification
- OVD Kinegram AG (2024). Decision Guide: 4 Steps you Should Take Before Buying an Identity Document Verification Solution. URL: Steps before buying an identity document verification solution
- Pagano, S. (2022). Digital Identity: The international landscape of active systems. Politecnico di Milano. URL: Pagano Simone- 952848.pdf (polimi.it)

23. Paravision: Advancing Responsible Biometrics: Achieving Inclusion in Face Recognition Technology

The rapid advancement of face recognition technology offers unprecedented potential for secure identification across sectors such as financial services, government, and border control. However, this promise is shadowed by significant challenges, including the need to address demographic disparities that can lead to biased outcomes and ethical breaches. As the industry progresses, prioritizing inclusion is not merely a technical necessity but an ethical and strategic imperative for responsible biometrics.

Why Inclusion Matters

Failure to prioritize inclusion in face recognition systems carries profound risks:

- **Ethical Failures**: Biased algorithms disproportionately affect marginalized communities, perpetuating discrimination and inequity.
- **Legal Consequences**: Stricter regulations, such as the EU AI Act, demand adherence to anti-bias standards, with severe penalties for non-compliance.
- **Operational Risks**: High demographic differentials can result in increased error rates, leading to identity fraud, unauthorized access, and poor customer experiences.
- **Financial Risks:** Errors stemming from bias can result in costly fraud, fines due to regulatory non-compliance, and operational inefficiencies that strain resources and hinder profitability.
- **Innovation Stagnation**: A lack of trust in biometrics can stifle innovation, as public skepticism and regulatory scrutiny discourage investment and slow the adoption of new technologies.
- **Reputational Damage**: Organizations exposed for discriminatory practices face public backlash and loss of trust.

In high-stakes applications like financial transactions or border security, these risks escalate, making demographic inclusivity a cornerstone of responsible biometrics as well as overall security and reliability.

The Role of Standardized Evaluations

The National Institute of Standards and Technology (NIST) plays a pivotal role in guiding the biometrics industry toward inclusivity. Through its Face Recognition Technology Evaluation (FRTE) 1:1 Verification tests, NIST benchmarks algorithmic performance across demographic groups, highlighting disparities and driving improvements. Metrics such as the False Non-Match Rate (FNMR) and False Match Rate (FMR) offer critical insights, but the Maximum False Match Rate (FMR Max) is particularly significant. This metric reflects the worst-case performance for false positives when viewed across specific demographic groups, which is frequently noted as the biggest risk in biometric identity.

FMR Max is a crucial measure because it highlights the highest likelihood of a false match occurring within a single demographic group. While reducing bias is vital, the ultimate aim should be inclusion through minimizing overall error rates. By striving to eliminate errors altogether, biometrics systems can empower individuals universally, enhancing access and opportunities without compromising accuracy or fairness. The fence metaphor, often used in Diversity, Equity, and Inclusion discussions, illustrates different approaches to inclusion in face recognition systems:

- On the left, the fence represents systems with high demographic differentials, performing better for some groups than others. This approach is inherently biased and creates significant risks.

- In the middle, the fence symbolizes systems that minimize demographic differentials, delivering equal performance across groups but with higher overall error rates. While this approach is fair and equal, it creates barriers for users and operational risks for companies.

- On the right, the fence is removed entirely, representing systems that achieve low error rates across all groups. This approach reduces friction and ensures excellent performance for all demographics, mitigating organizational risks and enhancing trust.

To demystify the impact of FMR Max, consider a system operating at an overall FMR threshold of 0.03% (3 false matches per 10,000 verifications across a mix of all demographic groups). The leading technology by FMR Max globally delivers an FMR Max of 0.00086, meaning the worst-performing demographic group experiences fewer than 9 false matches per 10,000 verifications. In contrast, the current NIST-leading technology in terms of overall FNMR delivers an FMR Max of 0.02020, meaning over 200 false matches per 10,000 verifications, 23X worse than the best demographic performer. Such a technology would substantially amplify risks and operational inefficiencies.

Strategies for Responsible Biometrics

Achieving inclusivity in face recognition technology requires a multifaceted approach:

1. **Rigorous Benchmarking**: Vendors must participate in standardized evaluations like NIST FRTE to demonstrate demographic performance and address disparities. Benchmarking fosters transparency and continuous improvement.
2. **Minimizing FMR Max**: Reducing FMR Max ensures that all demographic groups receive equitable treatment. This metric is especially crucial for high-stakes scenarios where false matches can result in grave consequences.
3. **Adopting Ethical AI Principles**: Organizations must prioritize fairness, accountability, and transparency in algorithm development. Ethical frameworks should guide every stage, from research to deployment.
4. **Emphasizing Diverse Teams**: Including varied perspectives in algorithm development enhances fairness and inclusivity, reducing the risk of demographic bias.
5. **Educating Stakeholders**: Clear communication about performance metrics and inclusivity fosters trust among customers, regulators, and the public. Translating technical metrics into real-world implications makes technology more accessible and understandable.

Critical Questions for Vendors

To ensure responsible biometrics, stakeholders must demand transparency and accountability from technology providers. Key questions include:

- What benchmarks has your algorithm been tested against for demographic performance?
- Is the software tested with NIST FRTE the same as what you make available in production? If so, which production software versions align with which NIST submissions?
- What is your worst-case FMR Max, and on which population?
- How does your organization integrate inclusivity into algorithm design and testing?

Conclusion: A Path to Inclusive Biometrics

The future of biometrics lies in creating systems that work equitably for all individuals. By addressing demographic disparities, prioritizing ethical development, and demanding rigorous benchmarking, the industry can deliver on its promise of secure, fair, and inclusive identification systems. Responsible biometrics is not just a technological challenge—it is an ethical and societal mandate. By prioritizing inclusion, the industry can build a future where biometric technologies enhance security and access for everyone, without compromise.

Organisation: Paravision
Name: Ella Nuutinen, Director of Marketing
Contact: info@paravision.ai

24. Proline: Next-Generation Security Solutions: Integration of Quantum Computing, AI, and Blockchain in Border Control

As global security challenges continue to evolve, the integration of advanced technologies has become crucial in developing robust border control and identity verification systems. This paper examines how the combination of quantum computing, artificial intelligence, and blockchain technology is revolutionizing security solutions.

Current Security Landscape

Modern security systems face unprecedented challenges in an increasingly interconnected world. These include sophisticated security threats, growing traveller volumes, and rising incidents of identity fraud. Traditional systems struggle with digital verification limitations and vulnerability to tampering, highlighting the need for more advanced solutions.

Advanced Technology Integration

Contemporary security solutions leverage three key technologies:

Quantum Computing Capabilities

- Real-time processing of massive biometric datasets
- Quantum-resistant encryption for sensitive data
- Advanced pattern matching and risk assessment algorithms

Artificial Intelligence Implementation

- Sophisticated spoofing detection through pattern recognition
- Continuous learning and security protocol optimization
- Advanced 2D-3D biometric passive liveness analysis

Blockchain Infrastructure

- Immutable record-keeping of authentication attempts
- Decentralized verification of traveler credentials
- Transparent yet secure audit trails

Enhanced Security Features

The integration of these technologies enables:

- Multi-factor biometric authentication
- Real-time threat detection and response
- Quantum-encrypted data transmission
- Blockchain-verified identity management

Future Developments

Ongoing system enhancements focus on:

- Expanded quantum processing capabilities
- Enhanced AI-driven threat detection
- Advanced biometric modalities
- Improved cross-border system integration

Operational Benefits

- Comprehensive security for high-risk areas
- Reduced unauthorized access risks
- Enhanced operational efficiency
- Flexible scalability
- Seamless infrastructure integration

Conclusion

The convergence of quantum computing, AI, and blockchain technology represents a transformative advancement in security systems, as evidenced by recent developments and evaluations. The NIST FATE Part 10 report's assessment of 81 passive face presentation attack detection algorithms demonstrates the rapid evolution of these technologies.

While the integration of quantum computing with face liveness detection systems promises enhanced security and efficiency, it requires careful consideration of implementation challenges and ethical implications. As security threats evolve, the adoption of these integrated technologies becomes increasingly critical, necessitating continued development of standards and frameworks to ensure secure, ethical, and equitable implementation across border control and identity verification systems.

Organisation : Proline
Name: ÖZGÜR DOĞAN
Contact: ozgur.dogan@pro-line.com.tr

25. Resaro: Evaluating and benchmarking deepfake detectors

Humans seem innately wired to detect even the slightest imperfections in human likeness, a phenomenon known as the 'uncanny valley.' Put simply, we trust our own perception and intuition from experience to guide us and decipher what is real and what is not. This explains why *early* deepfakes—glitchy and riddled with errors like mismatched lip-syncing or jerky movements—were easily dismissed as harmless novelties.

Today, generative AI technologies have blurred the line between real and synthetic media. We may well have crossed the 'uncanny valley', reaching an unsettling level of realism where seeing is no longer believing.

Compared to a decade ago, creating or manipulating digital content is now far cheaper, faster, and easier. Social media platforms continue to provide a ripe environment for viral content sharing. The speed, scale, and breadth at which deepfake content can be created and shared have raised concerns about the spread of misinformation, disinformation, and malinformation online.

Fast forward a decade or two—could we find ourselves in a world where citizens no longer share a common reality? A world where an 'information apocalypse' breeds widespread societal confusion about which sources are trustworthy? Or perhaps a reality where 'truth apathy' prevails, and what is true or real no longer matters?

The deepfake arms race

To counter this threat, researchers and enterprises have developed deepfake detectors with widely published claims of 99%+ accuracy rates to help humans discern between real and manipulated or synthesised content.
The core of deepfake technology relies on deep learning algorithms, particularly Generative Adversarial Networks (GANs) and autoencoders.

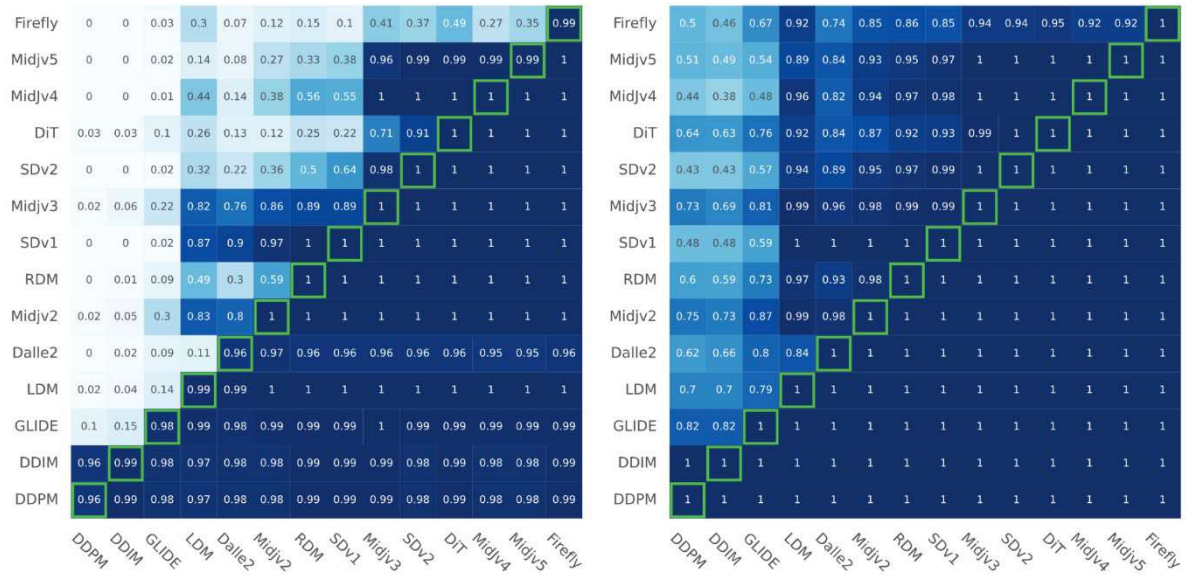
To illustrate the importance of evaluating deepfake detectors, we will focus on GANs as an example. GANs comprise two neural networks working in opposition: (1) the generator, which creates fake content, and (2) the discriminator, which attempts to distinguish between real and fake content. These networks compete and improve each other iteratively, with the generator producing increasingly convincing fakes based on the discriminator's feedback.

However, this space evolves at an astonishing pace, with new and more realistic generation algorithms being released almost weekly. The discriminator must rapidly adapt and improve to detect fake content generated by the generation algorithms. This cycle continually repeats, with each side trying to outmanoeuvre the other—mirroring an ongoing meta-game of deepfakes whack-a-mole.

Rigorous evaluation of deepfake detection tools is critical

As deepfake threats evolve in lockstep with new detection technologies designed to counter them, there is a need for continuous and rigorous evaluation at scale to ensure deepfake detector efficacy.

Firstly, detection technologies are less effective with newer generation algorithms. The figure below illustrates the performance of an online detector trained sequentially to distinguish real images from those generated by AI.



(a) Accuracy (b) Area under Curve (AuC)

Reference: https://openaccess.thecvf.com/content/ICCV2023W/DFAD/papers/Epstein_Online_Detection_of_AI-Generated_Images__ICCVW_2023_paper.pdf#page=0.04

The sequential training simulates the real-world chronological release of the generative models indicated by their order in the x-axis. The y-axis shows the algorithms against which the detector is tested after each training cycle. The diagonal values indicate near-perfect performance on a given algorithm directly after adding data generated by it to the training set. The bottom right triangle shows that the detector achieves good performance across datasets seen previously, indicating its capacity to generalise across various generators that it is trained on. However, performance on unseen models in the upper left triangle shows degradation, emphasising the need for ongoing updates to the detector as new generative models emerge.

Secondly, through our benchmarking and evaluation of deepfake detection tools, we found that deepfake detectors are sensitive towards the generation algorithms they are trained on. This means that they tend not to translate well in real-world scenarios, where deepfake content is generated by algorithms the detector was not trained on.

We used the newly released 2024 DeepAction deepfake dataset to evaluate three open-source deepfake detectors.

When fine-tuned on new data, deepfake detectors can perform well even outside their original training domain (such as faces), achieving 95%+ Area Under the Curve (AUC) scores on the videos. This suggests that the underlying architectures are capable of adapting to new types of deepfakes when properly trained.

However, pre-trained models perform poorly when tested on new types of deepfakes without fine-tuning—even for models designed to be more generalisable and pre-trained on large datasets. In these cases, AUC scores drop to 67-71%, which highlights the challenge of building truly generalisable detectors.

As we move toward an AI-driven world, we need to shape a new model of trust. Testing the performance and quality of deepfake detectors against real-world datasets is becoming ever more crucial. Only through rigorous evaluation can we ensure these tools remain fit-for-purpose and capable of keeping pace with the deepfakes arms race.

Organisation: Resaro
Name: Oliver Salzmann
Contact: oliver.salzmann@resaro.eu

26. Secure Logistics: Enhancing Safety in the Transport Chain with Biometric Verification

Why protect the transport chain?

The global freight and logistics market is a vast and rapidly evolving sector, integral to the movement of goods worldwide. The **transport chain** refers to the sequence of activities and processes involved in moving goods from their origin (e.g., production or supplier) to their final destination (e.g., customers or retail stores). It's a critical part of the supply chain that ensures efficient, cost-effective, and timely delivery of goods. In 2023, the total freight volume was approximately **24.4 trillion tonne-kilometres**, with projections indicating an increase to about **26.5 trillion tonne-kilometres by 2028.**

The logistics transport chain is vital for global trade, connecting manufacturers, suppliers, and customers across various regions and ensuring the smooth flow of goods in the economy. Moreover, millions of people earn their income directly or indirectly within the transport chain.

Current challenges

Disruption by criminals in the transport chain can have significant consequences across multiple levels - from delay and loss of goods, huge cost increases due to the shutdown of transfer points during police investigations and risks with regard to cargo integrity if it concerns food or medicines. Repeated thefts of cargo can have an impact on the carriers involved and damage their business. In Europe alone, **the transport chain yearly suffers more than € 8,2 billion from crime every year.** With the growth of intermodal transport, crime in this sector is expected to increase.

Last but not least, the violence that is regularly used can have an impact on the attractiveness of companies in the chain as employers. The transport chain employs many individuals who face risks due to the misuse of the systems they operate in. For example, in seaports, businesses and resources are often exploited for smuggling people, weapons, and drugs. Organised crime targets access to sensitive information, such as loading and unloading sites, destinations, and schedules. Since this system information is recognised as vulnerable and thus is protected with cybersecurity technologies and not publicly accessible, criminals often target the weakest link in chain – the employees.

Breach methods

The most common methods to take advantage of this employee vulnerability include bribery and coercion. Misuse often involves exploiting “secure” access cards or authorised vehicles. Literally “opening the door” to fraud. In some cases, criminals use stolen or purchased credentials to collect cargo or containers intended for legitimate transporters.

A joint analysis report **‘Criminal Networks in EU Ports – Risks & Challenges for Law Enforcement’** produced by Europol, the European Union Agency for Law Enforcement Cooperation, and the Security Steering Committee of the ports of Antwerp, Hamburg/Bremerhaven, and Rotterdam says, "the specific technique to misappropriate container reference codes – or so-called PIN code fraud – which the importer, their representative, or transporter can use to pick up a container from the destination terminal – requires the corruption of just one individual, along with either the corruption or a Trojan horse style infiltration of extraction teams, who are then paid between 7% and 15% of the value of the illegal shipment.

The logistical processes carried out in ports entail participation from various actors that can be targeted for corruption, all providing targets for corruption. Bribery fees may reach hundreds of thousands of euros. The highest fees are paid to essential links in the extraction chain, often crane operators, planners or employees providing access to information via IT systems." (source TAPAEMEA)

Biometrics as a added layer of protection

At a time when digitalisation and globalisation are making the transport chain increasingly complex, security is crucial. Biometrics provide an additional layer of security by integrating physical and behavioral characteristics into access and authentication processes. Specifically, biometrics because they are always personal and in addition to regulated access, traceability is also improved. Together, this raises the threshold for cooperating with malicious practices or not reporting them if they have not been cooperated with voluntarily. This technology goes beyond traditional methods

such as PINs or passwords, which are vulnerable to fraud and misuse. For example: Implementing facial recognition at port access can prevent unauthorized persons from retrieving containers or approaching sensitive loads, or implementing trusted identities authenticated by fingerprint can regulate access to digital environments connected with and supporting the transport chain and keep classified information secret from malicious parties. In both examples, it is always visible afterwards who has committed an action, which makes detection easier.

Building a trusted identity ecosystem

Port companies could address this potential risk, with their technology partners, by collaboratively issuing trusted identities following thorough screenings. Both companies and their employees could then receive secure identities, which should include biometric features for risk mitigation. This would mean only registered individuals gain access to critical processes and premises after biometrically verifying their identity. Then any misuse of an issued identity can be quickly detected, leading to immediate central blocking, and excluding offenders from the ecosystem.

This type of approach uniquely improves safety for all stakeholders. Employees operate using an alias, ensuring their national identity documents cannot be misused after enrollment. Organisations have absolute certainty about the identity and qualifications of individuals because the identification tools are personal and non-transferable. Implementation on existing operating systems (e.g. Gate, terminal or warehouse and Yard systems) should be very easy through APIs. Employers should be able to leverage these secure and authenticated identities for various functions, such as signing cargo documents and authorising payments, gaining confidence in the integrity of their staff.

Moreover, this type of ecosystem helps eliminates the possibility of identity misuse, as the credentials are non-exchangeable.

Conclusion

The entire transport logistics chain needs to be strong, secure, with complete integrity and organised on a continental scale to prevent maleficence, loss of property, and loss of trust. Trusted Identities in combination with biometrics is a crucial part of that chain. As is choosing a trusted and experienced transport technology partner with a growing ecosystem – it multiplies the benefits for all participants while significantly enhancing security.

Organisation: Secure Logistics B.V.

Name: Cor Stolk

Contact: cor.stolk@secure-logistics.nl

27. SITA: Biometrics for Better Borders and Beyond!

Let's be honest, for all the talk of improving travel, today's biometric systems often add steps instead of making things easy. Sure, the technology has delivered significant benefits over the past decade. Linking your face to your passport and boarding pass, then moving quickly through touchpoints, has simplified the journey for some. Automated border control gates – or eGates – have enhanced security and reduced immigration queues. With over 5,600 eGates deployed worldwide, their impact is clear.

But here's the catch: for many travellers, biometrics still feel like *just another step* in an already complicated process. Despite major advancements – biometric algorithms improving 30x in just two years – the adoption rates remain low. Why? Because the current systems often force travellers into unnecessary steps, like queuing at kiosks to enrol their face. If we're striving to make travel easier, this isn't it.

So, what's the solution? It's quite literally in the palm of your hand – your smartphone.

Why Your Airport Experience Still Feels Like a Hassle

Imagine this: you've checked in at home, your boarding pass is on your phone, and you're traveling light. In theory, you should sail through the airport. But instead, you're asked to scan your boarding pass multiple times – at security, the duty-free shop, the lounge, and the boarding gate. If you want to use biometrics to make the process smoother, you'll have to stop at a kiosk or stand in line to register your face. That extra step makes things harder, not easier, especially when you've done everything else digitally.

This inconvenience isn't just frustrating for travellers – it's a missed opportunity for airports and airlines too. Low adoption rates mean poor returns on their biometric investments and continued inefficiencies. The message is clear: the process needs to be easier and more intuitive for everyone involved.

Your Smartphone: The Key to Easier Travel

What if your phone could act as a kiosk in your pocket? Instead of queuing at the airport to enrol your face, you could complete the process from the comfort of your home. Thanks to advancements in smartphone cameras and biometric algorithms, this is no longer a nice dream – it's happening now.

Enter the Digital Travel Credential (DTC). The International Civil Aviation Organization (ICAO) has introduced standards for turning the data on your passport chip into a secure, digital credential stored on your phone. By creating a verified digital copy of your passport and linking it to your image, governments, airports, and airlines can trust your identity as if they had scanned the physical document themselves.

Here's what that means for travellers: no more kiosk stops. You can choose to share your image with airport systems in advance, gaining all the benefits of using your face to move through checkpoints quickly and effortlessly.

For businesses, this is a game-changer. Governments gain greater confidence in border security, with more accurate and reliable data enabling faster, more informed decisions about travellers – before they even arrive. Airports benefit from improved passenger flows, avoiding bottlenecks and reducing congestion, leading to higher efficiency and cost savings. Airlines gain happier customers who spend less time waiting and more time engaging with ancillary services, improving both customer loyalty and revenue opportunities. By making the process easier, the entire travel ecosystem stands to gain.

Whether it's passing through eGates, accessing the lounge, or boarding your flight, your journey becomes easier and faster.

Trust in the Digital Age: The Role of ICAO Standards

Why is the DTC so important? It's all about trust. Governments have long relied on physical passport checks for security. But the new ICAO standards provide a level of assurance for digital credentials that wasn't possible before. By extracting and verifying data directly from the passport chip, the DTC ensures the authenticity of your identity.

For governments, this means they can confidently make decisions about travellers before they even arrive at the border, avoiding potential security or health threats from entering their country. For airports and airlines, it means faster passenger flows, happier customers, and better utilization of biometric systems. It's an easy way to improve operational efficiency and customer satisfaction.

Biometrics Beyond Borders: Opening New Doors

And it doesn't stop there. The possibilities for digital identities powered by biometrics extend far beyond airports. Hotels, car rental companies, and even event organizers are exploring ways to use this technology to make life easier for their customers.

Imagine bypassing the hotel reception desk entirely – your phone delivers a digital key straight to your room. Or envision unlocking a rental car with just a scan of your face. No more photocopying passports or fumbling with paperwork. The opportunities to simplify and streamline are endless.

With the right standards and secure biometrics, industries can reimagine how they interact with customers. And at the centre of this transformation is SITA, helping to shape and deliver this exciting new world.

Industry's Vision: Making Travel Easier

All stakeholders: governments, airlines, airports, and other industries, are working together, more aligned than we've seen before, to make secure, reliable, and ethical biometrics a practical reality.

And this is just the beginning. With global travel surging post-pandemic, the time to act is now. Organisations that embrace these innovations will lead the way in making travel easier, faster, and more secure for their customers.

Organisation: SITA
Name: Andy Smith
Contact: nick.stephenson@sita.aero

28. Speed Identity: The importance of live enrolment for identity documents

As a response to the increased threat in terrorism, problems related to identity theft, and national security concerns, many governments have introduced biometrics in the process for identity documents issuance. Biometrics help ensure that the person applying for a new identity document is the person they say they are, and that the resulting identity document is secure and trustworthy. These secure identity documents come equipped with a chip which contains biometric data that can be used to authenticate the identity of the document holder at a later stage.

To date, many countries still allow their citizens to supply face images during the enrolment of biometrics, whether they submit digitally or in a printed form. This poses significant security and operational issues:

1. Risk of image manipulation – images can be manipulated before submission to the authority, whether it's by morphing, deepfake, or some other manipulation. Morphing is a form of manipulation in which two or more images are merged and may allow multiple individuals to share the identity document. AI supported manipulation of biometrics is advancing and developing fast while protective software algorithms tend to be a few steps behind. The issuing authority can only check to a certain extent whether an image submitted by an applicant has been manipulated or not.

2. Low biometric quality – the biometric quality of images is crucial. When an image is printed and then scanned at the issuing authority, resolution is lost. When an image is captured from a mobile phone and submitted online, biometric data quality is low and inconsistent because of variations in camera sensors, environmental conditions, and radial distortion. Lower biometric data quality will result in higher false match and false non-match rates during identity verification, whether it is for forensics or for border control.

3. Low efficiency of the application process – the application process is unnecessarily complicated and expensive for the citizen. The issuing authority's employee may have to reject the image because it does not meet the minimum requirements and guidelines, forcing the citizen to retake it and to rebook an appointment at the issuing authority.

Secure identity documents play a core role in identity management and the data they contain must be trustworthy. If it is not, how can one verify or authenticate the identity of the document holder?

To minimize the risk of image manipulation, biometrics experts recommend implementing live enrolment of biometrics. Live enrolment is the process of recording biometric data directly at the application location, whether at a governmental office or at a 24/7 service point. Physical appearance at the counter is required so that it can be determined with certainty that the biometric data belongs to the applicant and that it has not been manipulated. The issuing authority has full control over the data chain, from the sensor to the issued secure document and, with the proper cryptographic measures in place, the biometric data placed in the identity document becomes reliable and trustworthy.

Nevertheless, many live enrolment devices on the market use low-optical-resolution sensors, which compromise the quality of the captured biometric data. This often results in subpar data being stored in databases, making it challenging to use effectively for identity verification. High-quality image capture is essential, particularly when issuing secure documents, as it enhances algorithmic accuracy during biometric matching. This requires purpose-built hardware that implements best practices as required by industry standards, i.e. high optical resolution, low radial distortion, proper illumination with multiple light sources from above and below the face, and optimized face cropping combined with the correct set of compliance verification algorithms. By ensuring better image quality, biometric databases remain reliable and serve their intended purpose – enabling accurate identity verification.

Live enrolment not only improves security and lowers risk but also reduces operational costs and time spent on identity verification. The need for additional software to detect manipulated or morphed images is minimized, allowing authorities to confidently trust the data in the documents for consistent identity verification. Automated identity verification during the enrolment process is also possible, as the live image from the applicant can be used to verify their identity even before their application is processed, and before the new document is issued.

With live enrolment, citizens not only benefit from a secure and reliable process, ensuring their security, but they also benefit from an easy and convenient application process where only one stop is required at the application location for their application to be processed.

Organisation: Speed Identity AB
Name: Thomas Gaudy
Contact: thomas.gaudy@speed-identity.com

29. Trust Stamp: Revolutionizing Security with Biometric-Bound Credentials: A New Era in Digital Identity

Passwords, once the cornerstone of online security, are increasingly proving inadequate in the face of advanced cyber threats and usability challenges. In this landscape, hardware-based authentication methods like passkeys offer a promising alternative. However, they are not without their limitations. The pressing need for more versatile and secure solutions has led to the emergence of biometric-bound credentials—an innovative approach that promises to reshape digital identity management.

The Case for Biometric-Bound Credentials

Passkeys, primarily supported by FIDO (Fast Identity Online) protocols, function as secure hardware tokens designed to eliminate the vulnerabilities of traditional passwords. However, these tokens pose significant challenges in account recovery. When users are tied to their devices—literally and figuratively—loss, damage, or theft of a device can lead to irrevocable access issues. Imagine dropping your phone into water or losing it during travel; with hardware-bound authentication, your digital identity may sink with it. To address these challenges, biometric-bound credentials have been proposed as a transformative solution, offering enhanced security while preserving user convenience.

Understanding Biometric-Bound Credentials

A Biometric-bound Credential refers to a digital credential that is linked directly to a person's unique biological characteristics, like their fingerprint or facial features, essentially using their biometrics as the primary means of verification for accessing systems or services, offering a more secure and convenient way to authenticate identity compared to traditional passwords or PINs.

There are several ways to create biometric-bound credentials. Biometric cryptosystems [1] work by creating a stable key from biometrics; whereas encrypted biometrics simply encrypts biometric templates which must be decrypted during comparison, therefore offering no protection during the comparison phrase. This weakness is addressed by Homomorphic-Encryption biometrics albeit at the cost of higher computation. Finally, SMPC proposes to distribute biometric templates into multiple compute nodes, but it incurs the highest computation cost, not to mention that the biometric comparison must be done online; so not suitable for time-critical applications such as border controls. As shown in the table below, the biometric cryptosystem stands out in terms of template protection, online/offline and low computational requirements.

Feature	Biometric Cryptosystem	Encrypted Biometrics	HE Biometrics	Secure Multi-Party Computation (SMPC)
Template Protection	Yes	Yes	Yes	Yes
Protection of External Secrets	Yes	No	No	No
Protection of Comparison Function	Yes	No	Yes	Yes
Offline Comparison	Yes	Yes	Yes	No
Online Comparison	Yes	Yes	Yes	Yes
Computational Requirements	Low	Low	High	Extremely High

A biometric cryptosystem uses biometrics to encrypt a cryptographic secret. The auxiliary data it generates during registration does not reveal the biometric nor the secret. Therefore, even if the server is hacked, no secret is compromised.

An implementation can go further to incorporate such advanced techniques such:

- **Cancellable biometrics**: Transforming biometric templates into a secure, cancellable format.
- **High entropy key extraction**: Extracting a stable key with more than 235 bits of entropy (or randomness that is independent of the biometric sample) thanks to a highly efficient key-decoding scheme.
- **Secret splitting (sharding)**: Distributing the registration artifact across multiple nodes for secure storage.
- **Encryption**: Safeguarding any data through cryptographic encryption.
- **Liveness detection**: Ensuring that the biometric input is from a live individual rather than a spoof or artifact.

Key Advantages and Applications

Biometric-bound credentials are gaining traction across various domains, offering unique advantages over traditional methods:

1. Enhanced Security
   Unlike hardware tokens, where private keys are stored on the device, biometric cryptosystems like Trust Stamp's stable IT2 [2] reconstruct keys from biometric data. This eliminates the risk of key theft and provides a robust defence against unauthorized access.
2. Account Recovery
   Consequently, biometric cryptosystems are ideally suited to enable account recovery without compromising security. Users can regain access to their account by providing their biometrics, even if they lose their primary authentication device, without the server withholding any sensitive information.
3. Multi-Factor Authentication (MFA)
   By design, biometric-bound credentials comply with high-security standards such as NIST AAL2 and AAL3, ensuring robust multi-factor authentication.
4. Versatile Applications
   The potential use cases for biometric-bound credentials are vast, including:
   - Digital wallets: Securely managing financial transactions.
   - Remote identity proofing: Verifying identity for online services.
   - Digital travel credentials: Streamlining border control processes.
   - Biometric-enabled passes: Facilitating secure access through a QR code, which is a physical manifestation of a biometric bound credential.

Overcoming Challenges

While biometric-bound credentials offer significant promise, they also face challenges. Traditionally, a biometric cryptosystem can only extract some 30+ and certainly no more than 60 bits of entropy per biometric sample of the same modality. Innovations such as Trust Stamp's solution represent a significant advancement is this field, making the solution quantum-ready and practical.

Additionally, public understanding of key concepts remains limited. For instance:

- Credentials should not be confused with tokens.
- Identity proofing differs from authentication.
- Biometric identification is not the same as identity proofing.
- Robustness of offline biometric comparison against the disruption of internet connectivity is often underappreciated.
- Clear communication and education are essential to bridge these gaps and drive adoption.

Looking Ahead

The shift from traditional security methods to biometric-bound credentials marks a transformative change in digital identity management. By overcoming the limitations of hardware tokens, next-generation biometric cryptosystems—characterized by high entropy and modality agnosticism—pave the way for downstream applications that are not only secure, robust, and quantum-ready but also user-friendly, as they free individuals from reliance on specific devices.

As the adoption of biometric-bound credentials grows among organizations and governments, collaboration will be crucial to maximizing their potential. Trust Stamp is actively seeking partnerships with digital identity service providers and biometric vendors to integrate and scale these advanced systems.

Reference

[1] ISO/IEC 24745:2022, Information security, cybersecurity and privacy protection — Biometric information protection.

[2] Trust Stamp's Biometric Authentication with Stable IT2- A Path from Passwords to FIDO, Passkeys and Beyond, Future-Proof Digital Identity Whitepaper Series, 2024, https://resources.truststamp.ai/trust-stamps-ai-powered-stable-it2-technology-whitepaper.

Organisation: Trust Stamp
Name: Norman Poh
Contact: npoh@truststamp.net

30. Veridos: The future of Secure Identities starts with Biometrics

In an increasingly connected and digitized world, it is critical not only to protect identities, but also to ensure that their verification is both efficient and secure. This can only be achieved through biometric solutions - and by advancing research into technologies that go beyond fingerprint recognition.

On the user side, expectations are clear: citizens want government-issued documents to finally make the leap into the digital age- fully. Passports, driver's licenses and ID cards should not only be digitized but also work seamlessly on mobile devices and integrate efficiently with systems such as border control. Imagine a smartphone that acts as a digital passport. Such a solution would not only make life easier for citizens and travelers: it would be much more than merely a convenience feature. Digital and mobile identity solutions are key technologies for streamlining complex processes and enhancing security, whether in government or at international borders.

Biometrics: A Cornerstone of Next-Generation Identity Solutions

Airports illustrate the potential of biometric systems to process and verify large groups of people in record time, setting new standards for efficiency and security.

While governments and operators today rely on eGates that combine document scanning with image verification, border management will increasingly benefit from breakthroughs in artificial intelligence (AI) and machine learning (ML). These technologies are already improving real-time biometric authentication and identifying counterfeit documents with much greater accuracy. In addition, AI is minimizing manual errors, identifying duplicate database entries, and ensuring the highest quality identification documents.

In the future, emerging technologies and innovative use cases will further strengthen ID document security and streamline verification processes. As passenger volumes increase, especially in confined environments such as airports and cruise terminals, innovation in identity management is essential to meet these challenges and move to the next level.

The Efficiency of Biometrics

Initiatives such as D4FLY or EINSTEIN (EU funded research projects) aim to advance technologies in identity verification, particularly for border management. Biometric methods are at the heart of these efforts, and promising approaches such as face recognition continue to emerge. By comparing previously stored data, including features such as the distance between the eyes or the length of the nose, algorithms and deep learning models can identify individuals in real time with remarkable accuracy. Recent advances in AI, particularly through machine learning techniques, have revolutionized facial recognition by significantly improving accuracy and overcoming the limitations of traditional algorithmic methods.

Iris scans also represent an innovative approach to personal identification. By utilizing the unique and unchanging pattern of a person's iris, these biometric technologies offer an exceptionally secure method of verification. Unlike other forms of identification that can be lost, stolen, or altered, iris scans provide a consistent and highly reliable way to confirm an individual's identity. The intricate and distinctive characteristics of each person's iris make this method remarkably tamper-resistant, ensuring a robust solution for security and authentication needs. Taking it a step further, "on-the-move" iris scanning enables identity verification as individuals simply pass through a defined space. In these biometric corridors, travelers of the future would no longer have to wait in long lines for security checks. Instead, a combination of biometric technologies – such as facial recognition and iris verification – will handle identification and verification.

While biometric corridors remain a vision of the future, research advances offer hope that new methods will transform the future of travel and identity verification.

A Game-Changing Future for Biometrics

The next generation of biometric solutions for identity management is already on the horizon, accelerated by the rapid rise of AI as a true game-changer. However, the successful implementation of these new technologies will require close collaboration between industry, research, and policymakers to deliver trusted and legally compliant solutions to the masses.

At the same time, continued research will be essential to realize the full potential of technological advances. This includes research into identification methods based on contactless fingerprints and DNA.

Marc-Julian Siewert is the CEO of Veridos. (Source: Veridos)

Organisation: Veridos
Name: Marc-Julian Siewert, CEO
Contact: info@veridos.com

31. X Infotech: Is Multimodal the Next Wave and Why? Mitigating Risk with a Multi-Technology Approach

General Introduction

Multimodal biometrics refers to the use of multiple biometric modalities to identify or verify an individual. Unlike simple unimodal systems that rely on a single modality (like a face), multimodal systems combine two or more modalities, such as fingerprints, face, iris, palms, voice, etc., to enhance accuracy, security, robustness, and user convenience.

Almost all government ABIS systems use a multimodal approach because the number of enrolled applicants is large, and one modality (for example, face) is not able to provide the required identification (1:N) accuracy.

Accuracy Improvements

It's officially confirmed by algorithm vendors and independent tests: each additional biometric element (especially another modality) in a probe record significantly increases the accuracy of the verification/ identification result.

The largest Automated Biometric Identification System (ABIS) in the world is the Unique Identification Authority of India (UIDAI), which manages the Aadhaar program. Aadhaar is the world's largest biometric ID system, with over 1.3 billion enrolled individuals. It uses multiple biometric modalities, including face, fingerprints, and iris scans, to provide a unique identification record to each resident of India. This system is used for various purposes, such as verifying identities for government services, financial transactions, and more, making it a cornerstone of India's digital infrastructure.

Handling Exceptions

Multimodal systems are indeed effective in overcoming challenges posed by single-modality identification, especially in cases where injuries or surgeries might impair one form of identification. If one biometric modality is unavailable or capture fails, the system can still function using the other modalities.

The simplest example is African countries, where it is often very difficult to capture fingerprints from farmers because their fingers are damaged. In this case, the face or iris modality can be considered a serious alternative.

There are many biometric vendors in the industry that provide algorithms for multimodal verification and identification. This significantly simplifies the development of multimodal solutions and reduces their cost. In cases where different algorithms are used, all decision-making logic and integration of algorithms are provided by the solution developers. Typically, such solutions are not as fast and efficient. In addition, they are more difficult to integrate and support.

Mitigating Risks and Enhancing Security

There are a lot of PAD (Presentation Attack Detection) algorithms for different modalities. It's harder to spoof multiple biometric modalities simultaneously, making the system more secure against fraud.

The twins' faces are too similar. The system can rely on other modalities to make a more accurate identification. This redundancy ensures that the system remains robust even when the faces are not distinct enough. The multimodal approach will not allow a twin to authenticate as their sibling.

Identification systems can employ a multimodal approach to counteract face morphing attacks, which are a form of identity fraud where two or more faces are blended to create a new, non-existent face. Combining facial recognition with other biometric modalities such as fingerprints, iris scans, or voice recognition can enhance security. Additional identification may also be used: candidates (non-twins) found with a very high "face matching score," but with mismatched demographic data and mismatched other biometric modalities, may come under suspicion.

Implementation and what should be taken into account

Biometric algorithms vendors

- It is necessary to always keep your finger on the pulse of modern technologies, analysing independent tests, attending biometric conferences. The cost and results of independent tests are not always the main criteria for choosing. Convenience of integration, stability of work, high-quality support are also very important when

choosing a partner. Internal testing and previous project experience can help. The same is about biometric capture devices.

Correct matching algorithms thresholds (FAR, FPIR, etc,) and quality thresholds

- It is very important to set up the correct matching and quality thresholds, which may depend on biometric algorithms, geographical region, number of biometric modalities, biometric hardware, and database size.

Legislation

- Different countries have different legislation and requirements for storing and processing citizens' biometric data. In most cases, all infrastructure must be located on client local premises, clouds are not allowed.

Region and purchasing power

- Depending on the region and purchasing power, it is necessary to select the optimal vendors of biometric algorithms based not only on cost, but also on the results of independent tests. The same is about biometric capture devices. For example, cheap biometric scanners can negatively affect the quality of biometrics. This should be taken into account when planning.

Pricing model

- Very often, biometric algorithms vendors prefer transaction-based models that are not an option for government orders, the budget of which is fixed.

Broader Implications

Additional modalities certainly complicate and lengthen the process of collecting biometric information, which can affect user experience in terms of speed and convenience. At the same time, it adds new possibilities; for example, users can have multiple options for authentication, which can be more convenient in different scenarios.
The development of artificial intelligence will pose a major challenge to ensuring security. A multimodal approach is one of the ways to enhance security because it's much harder to spoof multiple biometric modalities. According to Biometrics Institute "Industry Insights," multimodal approach popularity will grow in 2025.

Practical Insights

Multimodal systems are more complex and expensive. Development and support require more resources. Such systems are also less convenient for users because they require more cooperation. Legislation in some countries may also complicate development and implementation.
Multimodal biometrics is becoming indispensable in sectors such as government services, financial institutions, and border control. These sectors demand high security and accuracy, making multimodal systems a preferred choice.

Conclusion

If there’s one key message to understand about multimodal biometrics, it is that they provide unparalleled accuracy and security by leveraging multiple biometric modalities. This approach ensures robust identification and verification, even in challenging scenarios. As technology advances and threats evolve, multimodal biometrics will remain a cornerstone of secure and efficient identity management systems.

Organisation: X Infotech
Name: Andrejs Katakins, Biometric Solutions Architect
Contact: roberts.sinicins@x-infotech.com

With thanks to all our contributors

For further thought leadership and deeper insights into biometrics trends, we encourage you to explore other resources available from the Biometrics Institute. These include the *State of Biometrics Report*, which provides a comprehensive overview of the current landscape and future directions of the industry. And our *Annual Industry Survey* which offers valuable data and analysis on key trends and challenges shaping the biometrics landscape.