POSITION PAPER

Navigating the world with ease and confidence:

Leveraging facial recognition for secure and convenient journeys

IDEMIA PUBLIC SECURITY

Contents

1. **Introduction**
2. **Facial recognition technologies boost border management and strengthen national security**
3. **Facial recognition technologies to secure and streamline the traveler journey, from the couch to the gate**
4. **Face technology**

   How does it work?
   - Image acquisition
   - Image processing
   - Comparison

   Benefits and challenges of facial recognition
   - Benefits of using facial recognition
   - Challenges of using facial recognition

   How to measure the efficiency of facial recognition technology
   - International benchmarks (algorithm transparency)
   - Performance over time across multiple tests
   - Experience and robustness in the field
   - Fair face algorithms
   - Resistance to spoofing attempts

5. **Securing facial biometric data and promoting responsible biometric use**
   - Biometric data security
   - Biometric data privacy
   - IDEMIA Public Security commits to safeguarding personal data

Introduction

After the pandemic, a growing number of people are going back to traveling more frequently and further afield. To accommodate this growth, address post-pandemic challenges, and meet the ever-evolving expectations of travelers, airports must accelerate their digital transformation.

The Airports Council International (ACI) Airport Service Quality (ASQ) 2023 Global Traveller Survey highlighted that 58% of travelers prefer a more technological and automated approach to simplify their journey. Self-service (72%) and off-airport solutions (71%) emerged as the top preferences, with nearly three out of four respondents stating such systems could enhance their travel experience. Biometric solutions, such as facial recognition, were also well received, with 66% favoring contactless journeys and 59% supporting digital identities to replace physical passports. This shift in traveler mindset indicates a desire to have greater control and a more digitalized process.

Governments, port operators, and carriers are progressively leveraging biometric technologies to reliably verify the identity of travelers and secure entry/exit movements. The rising acceptance of biometrics among travelers is key to helping the travel industry's digital transformation. According to the International Air Transport Association (IATA) 2023 Global Passenger Survey, 46% of passengers have used biometrics at the airport in the past 12 months, up from 34% in 2022. Additionally, 75% of passengers now prefer using biometric data over passports or boarding passes, a notable rise from 46% in IATA's 2019 survey.

The widespread adoption of biometrics will boost passenger convenience without compromising security, streamlining processes from check-in to crossing borders at the final destination. With top results in speed and accuracy, facial recognition is commonly used in the travel industry, surpassing fingerprint recognition as the primary method for traveler identity verification.

According to the Biometrics Institute Industry Survey 2024, facial biometrics is predicted to see the greatest increase in use over the next few years, with 46% of respondents favoring its adoption. This trend is primarily driven by the fact that travelers' passports already include photos, simplifying the biometric identity verification process. Along with iris recognition, facial recognition is one of the least intrusive biometric methods, requiring minimal behavioral adaptation.

Over the past decades, numerous use cases have demonstrated how this technology enhances both convenience and security. Today, facial recognition is used to facilitate boarding processes and automate border crossings, such as the Transportation Security Administration PreCheck program in the USA and various initiatives designed to secure Singapore's borders. Within the European Entry/Exit System (EU-EES), facial recognition has been chosen as a key technology to process third country nationals (TCNs) while maintaining high security levels.

IDEMIA Public Security, the global leader in identity and security solutions, has extensive experience in biometrics, particularly facial recognition technologies. Our algorithms, independently recognized as the most accurate and fair in the market, consistently rank in the top tier of evaluations, such as the benchmarking tests conducted by the National Institute of Standards and Technology (NIST). Our facial recognition solutions are field-proven and are already being used around the globe. We are ready to support the travel industry by upgrading and integrating facial recognition technologies into their systems.

58%

of travelers prefer a more technological and automated approach

72%

self-service solutions emerged as the top preference of travelers

75%

of passengers now prefer using biometric data over passports

Facial biometrics

predicted to see the greatest increase in use

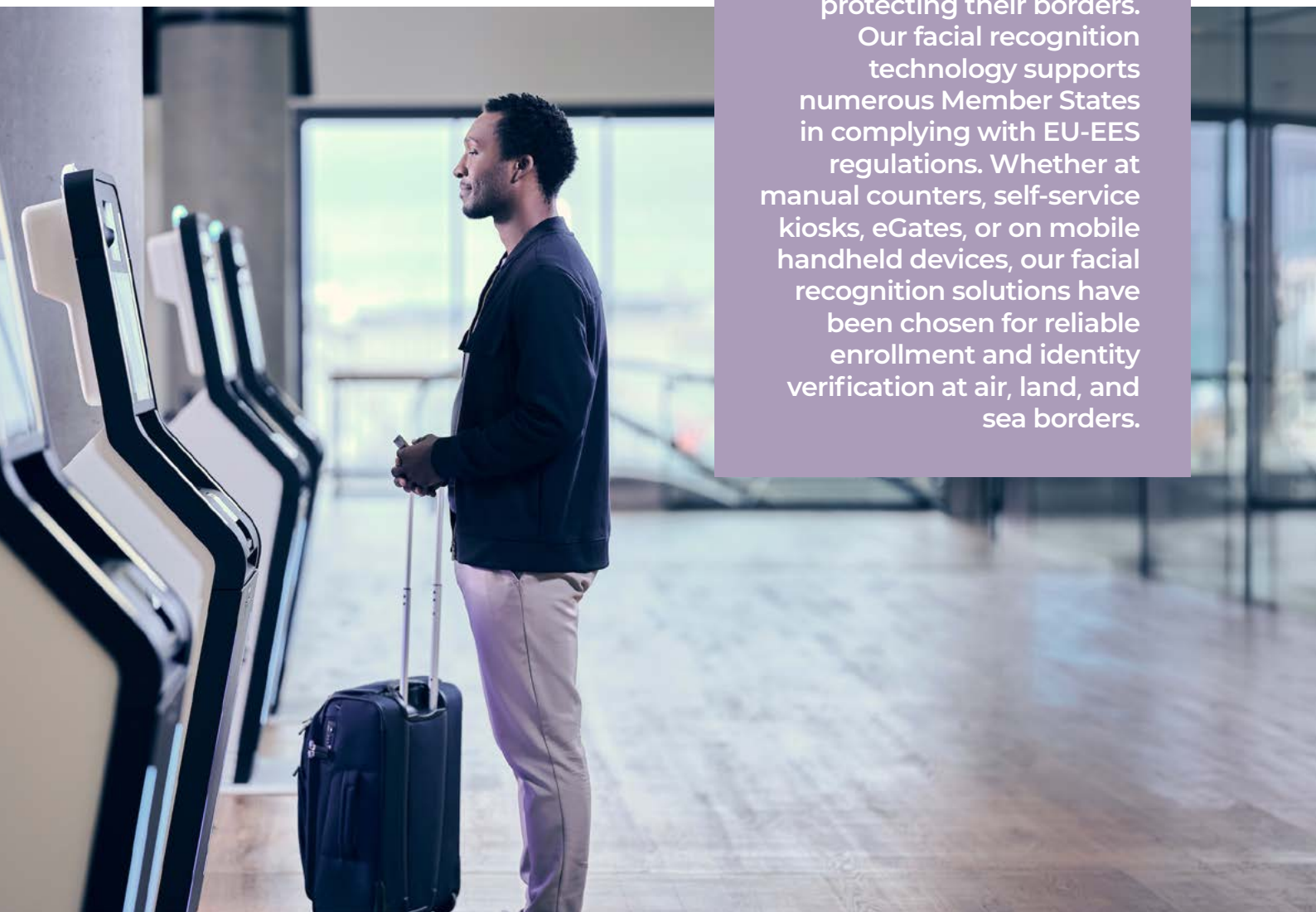
Facial recognition technologies boost border management and strengthen national security

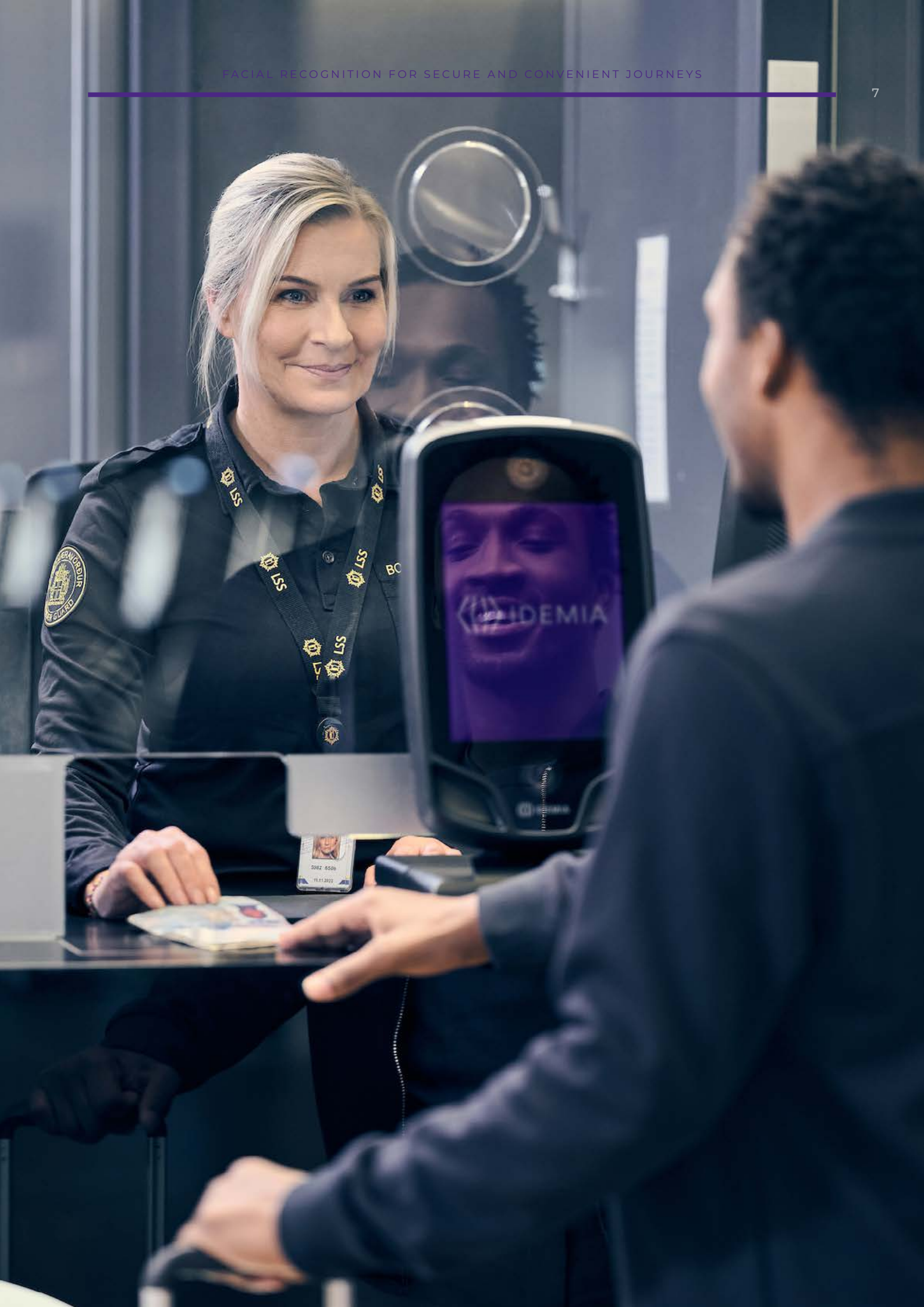
Governments and border control authorities rely on cutting-edge technologies to strengthen security while facilitating the movement of bona fide travelers. Facial recognition technology is essential to accurately verify travelers' identities and efficiently address potential threats, notably in self-service and automated solutions.

Historically, border control authorities have relied primarily on fingerprint matching for passenger clearance and identity verification at Automated Border Control gates or manual counters. However, facial recognition is now gaining traction, either as the primary modality or as a complement to fingerprint and iris recognition, expanding the passenger population eligible for automated checks.

For instance, under the EU-EES, a TCN crossing a Schengen border will need to enroll during their first visit. Member States can implement border clearance processes where travelers start enrollment at a self-service kiosk (passport scan, four-fingerprint capture, and face acquisition) and then present themselves at a manual counter to complete the clearance process.

We assist over 30 governments worldwide in protecting their borders. Our facial recognition technology supports numerous Member States in complying with EU-EES regulations. Whether at manual counters, self-service kiosks, eGates, or on mobile handheld devices, our facial recognition solutions have been chosen for reliable enrollment and identity verification at air, land, and sea borders.




IDEMIA

Facial recognition technologies to secure and streamline the traveler journey, from the couch to the gate

Facial recognition is the go-to technology for passenger flow facilitation, offering port operators and carriers an ergonomic solution to streamline processes and enhance the traveler experience—from the comfort of their home to the departure gate—while maintaining high security levels. It also permits passengers to check in remotely using secure identity verification on their smartphones.

Facial biometrics have been successfully trialed, tested, and implemented by numerous airports and airlines globally. The aim is to increase the processing capacity within existing terminals and reduce queues amid rapidly rising passenger volumes and staffing shortages, which could lower the quality of service. The challenge now is to expand the use of facial biometrics, both on-site and remotely, to limit travel infrastructure congestion, boost non-aeronautical revenues, and enhance airlines' on-time performance.

According to IATA's 2023 report, check-in (33%) and baggage check-in (19%) are among the top processes passengers wish to complete before arriving at the airport. The IATA One ID concept supports this shift by:

. moving processes off-airport and completing them before the trip so passengers arrive ready to fly.

• regulating airport congestion and processing times, which have more than doubled in some cases.

• addressing skilled staff shortages.

Facial biometrics will play a crucial role in ensuring remote processing is secure and reliable. Port operators and carriers can upgrade their apps with biometric capabilities, enabling travelers to remotely create a genuine digital identity from their smartphones. Live face acquisition combined with Presentation Attack Detection (PAD) and matching accuracy will create a unique identifier for each traveler. This will enable them to breeze through touch points using their face and no longer necessitate the need to repeatedly present travel documents.

Implementing and using facial recognition technology at airports presents several challenges before meeting the expected objectives. With over 250 airports utilizing our solutions, IDEMIA Public Security has a deep understanding of these challenges and the requirements for successful deployment.

Face technology

The human face is constantly changing due to factors such as glasses, beards, makeup, age, physical condition, and health, which can even affect its color. These variations make facial images extremely variable. For efficient identification, facial recognition technology must start processing well before comparing images.

How does it work?

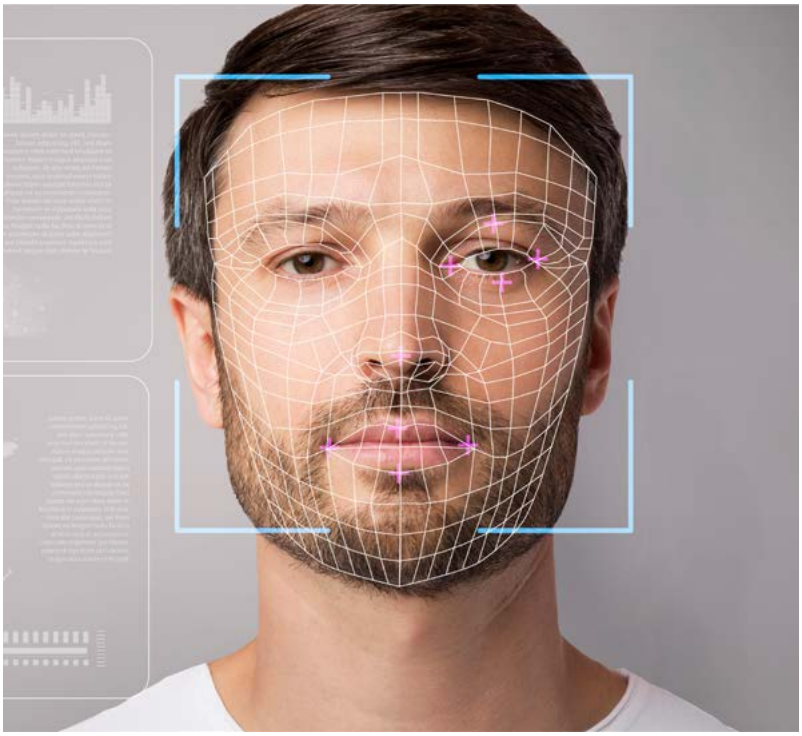
Image acquisition

The capture process for facial recognition is inherently contactless and conducted at a distance: The traveler simply looks straight at the camera. Various technologies are available to acquire the face within a predefined space. Stereovision, for instance, simulates human binocular vision, facilitating depth perception. The complexity lies in ensuring high-quality image capture, which is fundamental to the facial recognition process. Poor image quality results in less accurate matching. Acquisition equipment, distance from the camera, and capture environment must be optimized to achieve the expected resolution. Capturing a face at home with a smartphone versus at an airport with a self-service camera presents different challenges, such as lighting conditions, face position, and background.

Several strategies can be employed to confirm image quality:

- Control lighting to optimize brightness and contrast, either with the camera itself or with an additional light source.
- Take multiple images of the traveler to select the best one.
- Embed quality assessment into the camera.
- Guide the traveler to adopt the correct posture.
- Use automatic face quality assessment to determine if a new image capture is necessary, ensuring matching accuracy and speed.

These measures help retain excellent image quality, which is crucial for the reliability and efficiency of facial recognition technology.



Today, it is possible to capture a face on-the-move as the traveler approaches the device, speeding up the capture and identity verification processes. Additionally, the ability to capture multiple faces simultaneously (for groups or families) makes the travel experience more efficient and user-friendly.

How does it work?

Image processing

Once captured, the image is processed to extract a digital representation of the face, known as a biometric template, which can be matched in milliseconds.

Creating this template from the original face image typically involves deep learning, a technology widely used for over a decade and often called Artificial Intelligence (AI).

This face template serves as the unique digital signature of the individual.

Deep learning in facial recognition involves **two main steps :**

01

effective learning of a face classification model, which is trained in advance using hundreds of thousands of face examples

02

application of the established model to the captured face image to extract the biometric template

The model learning phase is crucial, as the matching accuracy and fairness of the algorithm are greatly dependent on it.

Comparison

Once the face template has been created, it can automatically be compared with others to determine the person's identity.

All biometric modalities, including facial recognition technology, can be used in two modes:

- **Authentication (1:1):** This mode verifies that a person is who they claim to be by comparing one face template (such as a live face capture from a smartphone) to another face template (such as a traveler's photo extracted from their passport).
- **Identification (1:N):** This mode identifies a person by comparing one face template to many others in a database.

Accuracy and speed are crucial for biometric matching. For accuracy, we consider:

- **False acceptance:** This occurs when the system incorrectly declares a match between two face templates that are not from the same person.
- **False rejection:** This happens when the system incorrectly declares no match between two face templates from the same person.

The impact of false acceptance and false rejection depends on the type of system used. There are two types of system:

- **Negative:** The person should be stopped if there is a match (e.g., criminal watchlist).
- **Positive:** The person should be allowed through if there is a match (e.g., frequent traveler program).

A false rejection in a frequent traveler program causes unnecessary stress, while a false acceptance on a criminal watchlist could permit a dangerous person (e.g., a terrorist) to enter the country. Accuracy affects the entire system beyond the biometric comparison result. Even a small difference in accuracy between systems or configurations can significantly influence the efficiency of the overall system and its operational costs. Excessive false negatives or positives can lead to a loss of confidence in the system.

When it comes to speed, it is not just about ease of use. The speed of the capture process also depends on the size of the templates generated by the capture technology. Smaller templates require less processing memory and less network bandwidth for transfers. Essentially, a smaller template does not mean lower accuracy. In real-life scenarios, the balance between accuracy and speed is crucial. A slower algorithm can be more accurate, but the right trade-off is essential for optimal performance.

Benefits and challenges of facial recognition

Face is the easiest and least invasive way to identify someone. Facial recognition technology is now extremely accurate, with error rates decreasing fivefold between 2018 and 2023. Additionally, new generation technology can now complete face capture and recognition on-the-move.

Benefits
of using facial recognition

Available

When traveling, unlike fingerprint or iris recognition, facial recognition may not require specific prior enrollment. This is because all passports include the traveler's photo, and most also have it stored in a chip, which can be used as a biometric reference.

Unique

Every face is unique (except for identical twins) and has many distinguishable traits.

Accurate

Facial recognition technology has advanced significantly and can now achieve superior accuracy levels. Today, facial recognition performance is comparable to that of fingerprint and iris scans.

Convenient

A person simply looks at a camera for a few moments to complete enrollment or verification. The capture process is non-invasive, safe, and compatible with glasses and contact lenses. Additionally, the powerful smartphone cameras of today allow face capture to be performed from the comfort of the user's home. Facial recognition systems are seamlessly interoperable with different hardware vendors and work well with a wide range of applications.

Mitigation of sanitary concerns

Face capture can be conducted at a distance, preventing direct contact with equipment. In case of a health crisis, facial recognition can still be performed with face masks.

Challenges
of using facial recognition

Demographic bias

Algorithmic bias refers to systemic and repeatable errors in a computer system that create unfair outcomes, like favoring one group of users over another. This bias can stem from the composition of the datasets used to train algorithms, the methods used for algorithm training, and the conditions under which images are acquired. The impact of bias includes false matches and denial of access to services.

Partially covered face

Even the most advanced algorithms are less accurate when identifying a partially covered face (e.g., with sunglasses or a facemask).

User behavior

Optimal facial recognition requires the individual's pose to be frontal, with a neutral expression during image capture.

Aging

A person's face changes over time, making it easier to compare two facial images taken two years apart than ten years apart. This issue is more noticeable in children, whose faces change rapidly, especially under the age of 6. Consequently, some countries restrict facial recognition use to children aged 12 and over.

Database size

In authentication use cases (1:1), facial recognition accuracy may exceed that of iris or fingerprint recognition. However, as the database size expands, especially with members of the same family or twins, accuracy can significantly decrease. In cases like these, it is recommended to use multibiometric systems (e.g., face and iris, or face and fingerprint).

Subject to spoofing

Facial recognition can be counterfeited through various means:

- **Presentation attacks:** Defined in ISO/IEC 30107 as «presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system,» this involves impersonating someone else to use their identity document or to conceal one's own identity. Presentation attack instruments can include makeup, masks, and covering the face with a photo or tablet. Detecting these fraudulent attempts is crucial in confirming the authenticity of biometric data. However, while detection methods are effective against known attacks, they may not detect new, emerging threats. Continuous work on PAD is essential.

- **Morphing attacks:** This involves tampering with a reference image by merging two faces into a single image, allowing one genuine passport to be used by two different people.

- **Adversarial attacks:** These attacks trick Machine Learning/Deep Learning (ML/DL) algorithms into making incorrect decisions. For example, high-frequency noise (adversarial noise) can alter the interpretation of an ML/DL algorithm. A fraudster banned from traveling could create a fake travel document using a photo of an accomplice, modified with adversarial noise, to deceive the facial recognition algorithm.

- **Deepfake:** This involves injecting a modified live video stream to replace the existing face with another face, potentially fooling identity verification algorithms on a video stream.

How to measure the efficiency of facial recognition technology

International benchmarks (algorithm transparency)

Biometric matching focuses on both accuracy and speed. Accuracy is measured by examining the False Rejection Rate (FRR) and False Acceptance Rate (FAR). For any given biometric technology, lowering the FRR by adjusting the decision threshold will increase the FAR, and vice versa.
Transparency about where and how an algorithm was tested is critical. Fortunately, customers can rely on independent, trusted, and recognized organizations to test and compare the accuracy and speed of different vendors. One organization that fits this description is NIST, part of the U.S. Department of Commerce, which conducts ongoing biometric benchmarks.
NIST's Information Technology Laboratory (ITL) trust in IT and metrology through research on biometrics. ITL develops biometric data exchange formats, sample quality standards, and acquisition and processing protocols. Additionally, it tests biometric matching algorithms.

The Face Recognition Vendor Test (FRVT) is the largest-scale test of facial recognition technology conducted by NIST. It is an open and independent test, using large, real-world datasets that represent different use cases for facial recognition, such as border control and law enforcement. The FRVT is ongoing, allowing technology providers to submit new algorithms for testing at any time. It is the accepted benchmark for facial recognition today, offering an objective and quantitative comparison between vendors. Recently, the FRVT has evolved to provide greater clarity and precision in the testing process. It is now divided into the Face Recognition Technology Evaluation (FRTE) and the Face Analysis Technology Evaluation (FATE), offering more detailed assessments.

- FRTE focuses on identity verification, measuring algorithm performance in terms of speed, accuracy, scalability, and fairness in 1:1 and 1:N use cases. It also includes specific facial recognition tests, such as the identification of twins.
- FATE focuses on facial image processing and analysis, including image quality assessment, age estimation, PAD, and Morphing Attack Detection (MAD).

Results are publicly available on the website:
Face Technology Evaluations - FRTE/FATE | NIST

Performance over time across multiple tests

As a vendor, achieving top ranking on a technology benchmark like NIST FRTE/FATE is certainly worth celebrating. However, the main challenge lies in demonstrating the ability to sustain ongoing research and continually improving algorithms over time. While AI facilitates rapid initial algorithm development, vendors must also have a record of continuous progress to avoid quickly falling behind competitors. A vendor with a history of continuous improvement enables end users to benefit from subsequent advancements during technology refresh cycles. As NIST advises: «Given the pace of developments associated with the industrial migration to various convolutional neural networks, it is incumbent on end users to establish contractual provisions for technology refreshment, factoring in speed, scalability, stability, and cost.»

Experience and robustness in the field

While third-party benchmark tests provide transparency for algorithm performance, it is crucial to understand how a lab-tested algorithm will be productized and operationalized for real-life use cases. For a product or solution vendor, it is essential to demonstrate the field-readiness and robustness of their algorithm to support operational deployments.

Fair algorithms

The most widely accepted definition of fairness in facial recognition algorithms is when they present the same statistical performance across different user population groups, ensuring the probability of error is not considerably different from one group to another. Achieving this requires intentional efforts to mitigate systemic AI bias during model development. A best-in-class algorithm should perform equally well for all people and under all conditions. Similar to inclusive UX design, which addresses usability and accessibility for diverse user populations, the development of a facial recognition algorithm should account for diversity. Fairness is built into IDEMIA Public Security's identification algorithms by design, as demonstrated by independent public evaluations conducted by NIST.

Resistance to spoofing attempts

Attacks vary in nature and are constantly evolving, requiring a tailored response for each type. Staying up to date with market technology and continuously innovating helps protect against these attacks. Ongoing research into new countermeasures is essential, and we are optimally positioned in this area, with dedicated research scientists, hardware engineers, and data scientists developing advanced capture solutions and optional dedicated hardware.

How does this translate operationally within passenger facilitation and border control?

High level of security:

Enhances confidence in automated/self-service solutions and improves resource management.

Low biometric rejections:

Reduce the number of exceptions that need manual handling, leading to better passenger flow management and shorter queues and waiting times.

Inclusion of all passengers:

Ensures no discrimination or bias between different passenger profiles, resulting in a better travel experience for everyone.

Operationally, efficient facial biometric technology can halve passenger processing time while maintaining a high level of security.

Securing facial biometric data and promoting responsible biometric use

Biometric data security

With the assistance of advanced technologies, identity verification through biometrics is fast and easy. However, biometric data is undeniably one of the most sensitive types of data. Due to increased usage, biometric data can become more exposed to risks such as cyberattacks, which could lead to data breaches or data corruption. This necessitates top-notch technologies and a comprehensive approach that simultaneously secures the biometric capture equipment, the biometric system, and the means of communication.

Here are a few examples of the various data security methods used:

- **Secure multi-party computation:** While securing data at rest and in transit is quite common, the trickiest part is securing data during processing. Traditionally, the processing party needs to 'see' the data to work with it. This method carries considerable risk, which can be mitigated by distributing the data processing workload among different parties. This means there is not one central entity processing all the exposed, vulnerable data, but rather several contributors. Only by breaching the data processed by each party would the data make sense to a malicious perpetrator.

- **Verifiable computing:** Verifiable computing allows a central entity to outsource data computation to another potentially unknown and unverified entity while maintaining verifiable results. In the world of biometrics, this could mean travelers perform the matching of their own data to verify their identity on their smartphone (i.e., the unknown, unverified entity), without anyone doubting the validity of the computation. This means travelers control their biometric data at all times, and it never leaves their device.

- **Homomorphic encryption:** Homomorphic encryption already protects data both at rest and in transit. The final step is to apply this encryption technology to data that is being processed. The goal is simple: Prevent the data processor from deciphering or understanding the data being processed. This method computes operations on encrypted information without decrypting it first. It guarantees end-to-end data privacy is achieved, and that the data is never exposed without protection.

- **Biometric hardware-based security:** The solutions use computing platforms secured at a hardware level, preventing access to data during processing.

On September 15, 2022, the European Commission proposed the Cyber Resilience Act (CRA), which aims to enhance cybersecurity across the EU by establishing common standards for products with digital elements, including mandatory incident reporting and automatic security updates.
The Act was approved by the European Parliament in March 2024 and now awaits formal adoption by the EU Council. Once the CRA enters into force, manufacturers, importers, and distributors will have three years to adapt to the new requirements.

IDEMIA Public Security is actively working to ensure full compliance with the CRA requirements within the specified period.

Biometric data privacy

The general surge in digitalization across various industries means that people are more accustomed to securely providing personal data. Travelers understand that, in order to enjoy more personalized services and access the latest, most accurate information, they must consent to the secure capture of their personal data, including biometrics.
However, there is still some reluctance to share personal and biometric data due to ongoing concerns about data privacy. The key is to reassure travelers that their data will only be used temporarily to make their experience secure, smooth, and stress-free.

Travelers should have the option to choose where their data is stored, with multiple options available. Transparency is fundamental; passengers need to know who will have access to their data and for what purposes

To alleviate any concerns around unauthorized access to confidential data, travelers will have the opportunity to choose between two options:

01

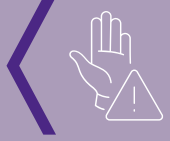
Store their biometric data in their smartphone. In this case, they will have to scan their smartphone at every touch point to authenticate their identity.

OR

02

Temporarily consent to sharing their data with a central database. In this case, their identity will be authenticated using their biometrics at multiple touch points.

In both cases, **consent is mandatory**, which gives the user control of their personal data at all times.



IDEMIA Public Security commits to safeguarding personal data

IDEMIA Public Security is part of international working groups and is compliant with international standards (ISO/IEC). This involvement keeps us well informed of best practices and helps us to develop solutions that adhere to data privacy requirements. Given the risks associated with the deployment of facial recognition, it is important to note that IDEMIA Public Security's export control policy has long followed the most stringent international regulations and recommendations, particularly those concerning human rights, as outlined in UN guidelines.

We are active members of several industry associations, such as the Biometrics Institute and the European Association for Biometrics. Our participation includes frequent presentations on advancements in biometric technologies to promote best practices and emphasize emerging data protection technologies in biometric applications. Our methods for data collection, retention, and management observe the strictest regulations and undergo regular monitoring.

It is important to note that all IDEMIA Public Security's research teams working on facial recognition algorithms are located within France and Germany. This guarantees the entire algorithm development process complies with GDPR regulations and, upon its enactment, with the EU AI Act. We are committed to algorithmic fairness and developer responsibility and strive to meet international and local standards in an exemplary manner.

In conclusion, the post-pandemic era has ushered in a new wave of technological advancements in the travel industry, driven by the growing demand for more seamless, secure, and automated travel experiences. The increasing acceptance and preference for biometric solutions, particularly facial recognition, highlights a significant shift in traveler expectations toward more digitalized processes. As airports and border control agencies continue to modernize, the adoption of biometric technologies will be critical in enhancing passenger convenience while maintaining robust security standards.

IDEMIA Public Security is at the forefront of this transformation, offering industry-leading facial recognition solutions that have been proven to deliver exceptional accuracy and efficiency. As the travel industry accelerates its digital transformation, we are ready to support this evolution, ensuring that the future of travel is not only more secure but also more convenient and user-friendly.

Unlock the world

IDEMIA GROUP

www.idemia.com