POSITION PAPER

Use of Facial Recognition Technology for Law Enforcement Investigations

IDEMIA
PUBLIC SECURITY

How is facial recognition technology used for law enforcement investigations?

Use case: Best practices in police FRT deployment—a four-step process

How does facial recognition work?

International working groups

Commitment to compliance with EU regulations

What does fairness in AI mean?

Introducing measures for responsible facial recognition

Introduction

Facial recognition technology (FRT) is playing an increasingly vital role across various sectors, including public safety, law enforcement, and commercial enterprise. As this technology advances, it is crucial to engage in informed discussions that involve all societal stakeholders. By focusing on factual and constructive dialogue, we can ensure that FRT applications are developed and implemented responsibly.

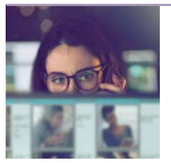
Facial recognition

Facial recognition is a software application that compares an image of a face against an image or database containing multiple images of faces. To conduct the comparison, FRT uses artificial intelligence (AI), which has significantly improved the accuracy and performance of facial recognition systems.

Notably, modern AI techniques, such as deep learning, rely on extensive datasets during algorithm development. This data is essential for training algorithms to recognize faces effectively and minimize biases, ensuring fair and reliable outcomes.

Facial recognition is used for various applications. Depending on a country's legislation, it may be used in the government or commercial sector for:

Immigration border checks



Investigation assistance in post-crime/ terrorist investigations

Creation and use of a digital identity, particularly for online public services

Facilitation of user authentication when using smartphone applications

This paper will focus on FRT's investigative use cases and IDEMIA Public Security's development and application for the law enforcement market.

1 How is facial recognition technology used for law enforcement investigations?

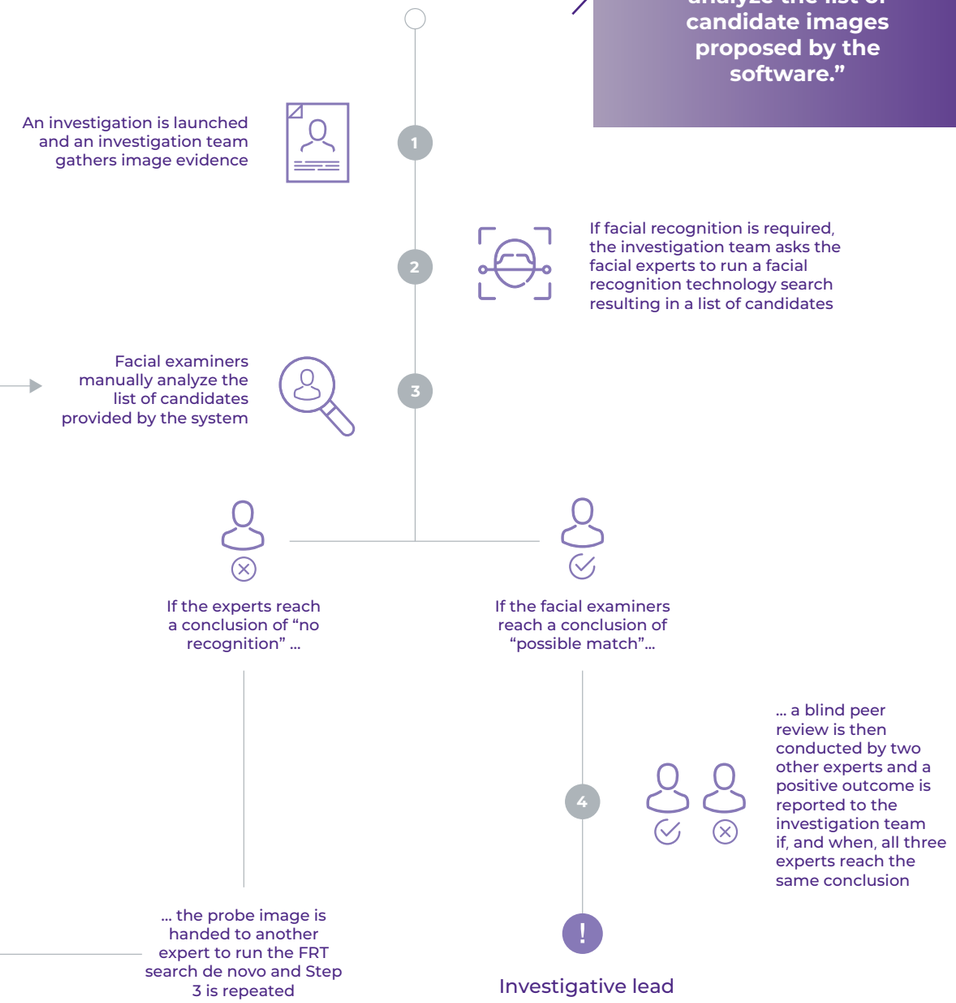
Best practices to enhance forensic efficiency using facial recognition technology

FRT is usually invoked when investigators have an image of the potential perpetrator's face but have not been able to determine the person's identity. The FRT system compares this image to a database of faces of people known to the police. This database is typically composed of portraits (also known as “mugshots”) of people who have been, for example, previously arrested or involved in a criminal investigation for an offense serious enough to warrant the acquisition of their biometric traits, including fingerprints and face.

The system provides a list of potential candidates, which the forensic examiner evaluates to determine if a match exists. This evaluation is conducted in accordance with the standard operating procedures of the local police organization, ensuring consistency and adherence to established protocols.

2 Use case: Best practices in police FRT deployment—a four-step process

“After the search, facial examiners analyze the list of candidate images proposed by the software.”



Source: The World Economic Forum's governance framework report for the responsible use of facial recognition in law enforcement investigations[1]

3 How does facial recognition work?

Algorithm development

Most characteristics of an FRT system are related to the algorithms used. For the sake of simplicity, we will focus on the biometric comparison algorithm. However, one must keep in mind that other factors play a key role, such as acquisition devices (e.g., cameras) and/or detection algorithms, which determine where the face is located in a photograph or whether there is an actual face in the photograph.

Most modern FRT approaches involve deep learning technology, which has been widely used for the last five to ten years, for many different applications, and is often referred to as artificial intelligence. IDEMIA Public Security's FRT, like most other high performers, relies considerably on deep learning techniques.

In deep learning, the developer combines different elements to produce an algorithm:

› **Training dataset development:** Developers compile a training dataset consisting of multiple images of the same individual, alongside images of various other individuals. This dataset enables the algorithm to statistically learn the common features that define the same person across different images, as well as to distinguish between images of different people.

› **Testing dataset:** This dataset is used to evaluate the performance of the algorithm. It is a completely different dataset to the training dataset but is labeled in terms of pictures of the same person or different people. This prevents over-adaptation of the algorithm to the training dataset and enforces performance across a larger variety of operational situations.

› **Cost function:** The infamous "cost function" is a mathematical procedure by which the developer specifies which metrics they want the algorithm to optimize while learning. This procedure is not standardized. It is based on the developer's expertise and the objectives for the algorithm. In many ways, it is the "secret ingredient" of an algorithm's performance.

Algorithm control and traceability

Once IDEMIA Public Security's algorithm has been trained, evaluated, and found compliant with internal criteria, it can be implemented in operational systems. After the algorithm is released by R&D and becomes operational, it remains unchanged, ensuring its integrity throughout its lifecycle. Existing products are upgraded with newer versions, which have also been certified and released by our internal R&D department. IDEMIA Public Security does not use continuous learning or adaptation of algorithms in production systems (i.e., those used by clients). Consequently, we ensure traceability and guarantee the performance of our released algorithms, which remain solely under our control. This approach assures clients and users that the performance of our algorithms in real-world applications matches the results observed during testing.

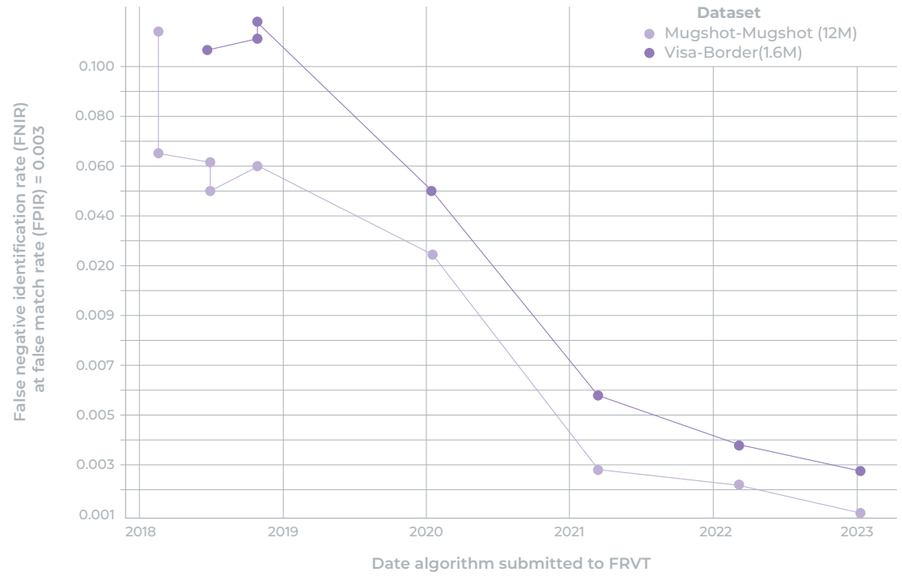
Relentless commitment to the improvement of technology

IDEMIA Public Security continuously invests in R&D and improves its state-of-the-art technology, be it algorithms, devices, or business processes. A core focus of this commitment is the persistent reduction of error rates in FRT, as measured by the independent National Institute of Standards and Technology (NIST) over several years.[2] This ongoing investment in research and development ensures that IDEMIA Public Security remains at the forefront of technological innovation.

Between 2018 and 2023, the accuracy of IDEMIA Public Security's algorithm improved by a factor of ten in a test that compares a picture against a database of pictures, as illustrated below.

Accuracy improved tenfold in the last three years.

Evolution of accuracy for IDEMIA algorithms on two datasets 2018—present



Source: NIST FRVT 1:N Identification. NB: the lower the rate is the better the performance.

4 International working groups

To enhance transparency and ensure ethical use of FRT, IDEMIA Public Security is part of several working groups and participates in developing industry standards. This allows IDEMIA Public Security to promote transparent communications about our technology.

Compliant with international standards pertaining to biometric technology

ISO/IEC 19795-1—Information Technology—Biometric performance testing and reporting

This standard defines methods and metrics to test the performance of biometric systems and algorithms through analysis of comparison scores and decisions output by the system, without requiring detailed knowledge of the system's algorithms or of the underlying distribution of biometric characteristics in the population of interest.

Industry associations

IDEMIA is an active member of several industry associations, such as **Biometrics Institute** and **European Association for Biometrics.** IDEMIA Public Security frequently presents advances in biometric technologies to raise awareness about best practices and emerging technologies that help protect personal data in biometric applications.[3] We also facilitate discussions around fairness in biometric systems with major actors, including NIST and the UN Office of Counter Terrorism.[4]

5 Commitment to compliance with EU regulations

IDEMIA Public Security's research teams, specializing in facial recognition technology algorithms, are based in the EU (France and Germany). This strategic positioning ensures full compliance with the General Data Protection Regulation (GDPR) and positions us to adhere rigorously to the forthcoming EU AI Act. As active contributors to the development of these regulatory frameworks, including our participation in the EU AI Pact, we are committed to shaping and aligning with evolving regulations that emphasize algorithmic fairness and developer accountability. IDEMIA Public Security is dedicated to upholding these standards, setting a benchmark for compliance and ethical responsibility.

GDPR compliance and collaboration

Our longstanding collaboration with French administrative authorities, notably through regular consultations with the Commission Nationale de l'Informatique et des Libertés (CNIL), underscores our proactive approach to regulatory compliance. This engagement includes prelaunch consultations for internal research programs, ensuring transparency and adherence to GDPR requirements.

Ethical oversight and data security

IDEMIA Public Security adheres to stringent ethical guidelines concerning data collection and usage:

- Data is collected exclusively for research purposes, ensuring voluntary participation, providing rights to access and rectify data, and limiting data retention periods, all in compliance with GDPR.
- Data access is restricted to authorized research staff, governed by processes certified under ISO 27001, and subject to regular audits to maintain security and integrity.
- Our intellectual property is safeguarded under French and German regulations, reinforcing our commitment to legal compliance and innovation within Europe.

Innovative approaches to data challenges

To address the challenges posed by limited data availability, we are pioneering the use of synthetic data for training purposes. While current synthetic data yields high performance in specific areas, such as inanimate objects or optical document recognition, it lacks the diversity required for effective facial recognition training. IDEMIA Public Security is actively refining this approach, aiming to overcome data volume constraints and enhance algorithmic performance.

Our continuous efforts in research and development, alongside our proactive engagement in shaping regulatory standards, reflect our commitment to ethical innovation and regulatory excellence.

6 What does fairness in AI mean?

Given the sensitive nature of applications such as criminal identification, it is imperative to ensure that facial recognition algorithms do not exhibit significant disparities in performance across different population groups. While the final decision in criminal identification rests with a human forensic examiner, the algorithm must not introduce bias that could lead to unequal error rates.

Key population categories, such as ethnic groups, age, gender, and physical attributes like glasses or facial hair, must be considered to ensure equitable performance. The widely accepted definition of fairness in FRT is achieving consistent statistical performance across these groups, minimizing the likelihood of error disparities.

False Positive Identification (FPI) happens when an FRT system erroneously presents, to the forensic examiner, one face as extremely similar to the searched face. This can potentially result in an individual being investigated even though they had nothing to do with the crime/incident. Although this can be cleared first and foremost by the expert decision of the face examiner and, later, by the investigative process, it is still an undesired outcome which should not bear the mark of statistical inequity. In the case of criminal identification, FPI is the type of error that needs to be limited, and stability across the different groups is necessary.

How does IDEMIA Public Security ensure fairness in AI?

IDEMIA Public Security applies cutting-edge techniques to the algorithm development process. The current public discourse on facial recognition and AI in general is that any disproportion in the training dataset (with underrepresented categories of population) will prevent fairness. The distribution of the training dataset is not the only factor influencing fairness. The cost function, and, therefore, the expertise of the developer, will also have a significant impact on performance. By carefully building the training dataset and the cost function simultaneously, a developer can greatly influence the performance of the resulting algorithm.

The testing dataset must be:

- representative of the type of data that the algorithm will face in the field.
- representative of all population groups that the algorithm may face in the field.

This comprehensive approach ensures that internal performance assessments accurately mirror the algorithm's real-world behavior. IDEMIA Public Security selects algorithms for release based not only on identification accuracy but also on their fairness across different demographic groups.

Importantly, IDEMIA Public Security's commitment to fairness extends beyond internal assessments and vendor claims, reinforcing trust through transparency and rigorous external validation.

Third-party testing for more transparency

IDEMIA Public Security consistently submits its facial recognition, fingerprint, and iris recognition algorithms to independent third-party testing organizations, reinforcing our commitment to transparency and reliability. Among these evaluations, the most comprehensive is conducted by NIST. Recently, NIST divided its Face Recognition Vendor Test (FRVT) into two distinct programs: the Face Recognition Technology Evaluation (FRTE) and the Face Analysis Technology Evaluation (FATE).[5] FRTE focuses on the performance and accuracy of facial recognition technologies, while FATE assesses aspects such as image quality and morphing detection.

IDEMIA Public Security's algorithms have consistently had results among the best, despite the huge number of submissions. So far, NIST has evaluated more than 570 algorithms by 172 unique developers over the course of the FRVT/FRTE 1:N program, and 1,260 algorithms by 395 unique developers in 1:1.

Focus on "demographic effects"

NIST has been studying FRT demographic effects extensively and went as far as publishing a dedicated report about it.[6] Within this report, NIST studies error rates for a variety of vendor-submitted algorithms and reports performance in terms of fairness. The use case we are interested in is Criminal Identification, where consistency of the FPI rate across different population groups is the desired situation. On page 8 of the report, within the technical summary, in a section focusing on false positive error rates of identification algorithms, the author writes that it is noted:

"The presence of an enrollment database affords one-to-many algorithms a resource for mitigation of demographic effects that purely one-to-one verification systems do not have. We note that demographic differentials present in one-to-one verification algorithms are usually, but not always, present in one-to-many search algorithms… **One important exception is that some developers supplied identification algorithms for which false positive differentials are undetectable. Among those is IDEMIA, who publicly described how this was achieved."**[7]

IDEMIA Public Security's strong performance in mitigating demographic differentials reflects its longstanding expertise in biometric technology. In the August 2024 NIST FRTE 1:1 benchmark, IDEMIA Public Security's algorithm was recognized for achieving the best balance between fairness and accuracy.

7 Introducing measures for responsible facial recognition

The World Economic Forum, the International Criminal Police Organization (INTERPOL), the United Nations Interregional Crime and Justice Research Institute (UNICRI), and the Netherlands Police convened a multi-stakeholder community centered on co-designing a set of principles that outline what constitutes the responsible use of FRT for law enforcement investigations. Among these principles is the respect for human and fundamental rights; human oversight and accountability; optimization of system performance; and mitigation of error and bias.

Assessing your technology provider for responsible facial recognition

These principles are accompanied by a self-assessment questionnaire to support law enforcement agencies with design policies surrounding the use of FRT and to ensure that the technology provider is in line with the proposed principles.

- What existing or forthcoming standards do you ask your vendor to follow to evaluate the performance of your FRT system?
- Have you introduced procurement rules to select providers who comply with these standards of performance?
- Have you introduced procurement rules to select providers who have submitted their FRT system to an independent evaluation such as that organized by NIST?
- Have you selected the technology provider who presented the best results?
- Are the independent lab tests of performance designed to model, as closely as possible, real-world objectives and conditions in which the FRT is applied?
- Do you notify the technology provider when you identify relevant errors in the use of the FRT system?
- What procurement rules have you introduced to ensure the regular upgrades or replacement of the FRT?

Key takeaways

IDEMIA Public Security promotes technological improvement by participating in public, third-party evaluations, which show the transparency of technology capabilities through international standards.

IDEMIA Public Security's FRT is exclusively developed in Europe and complies with all privacy standards and regulations, including GDPR. Export Control applies to all our commercial activities inside and outside of Europe.

FRT is used as a tool for investigators—decisions that may impact citizens' privacy and fundamental rights are always made by a human examiner.

FRT has rapidly improved in accuracy, with error rates decreasing fivefold between 2018 and 2023.

Fairness is provided by design in IDEMIA Public Security's identification algorithms, as has been demonstrated by independent public evaluation of their performance by NIST.

Endnotes

1 **The World Economic Forum:** A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations (Revised 2022).

WEF_Facial_Recognition_for_Law_Enforcement_Investigations_2022.pdf (weforum.org)

2 The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the USA's oldest physical science laboratories.

3 **Biometrics Institute** Congress 2021 – October 13 2021, IDEMIA delivered a presentation entitled *How to enhance biometric applications to protect privacy.*

https://www.biometricsinstitute.org/event/biometrics-institute-congress-2021/

4 **EAB (European Association for Biometrics) Virtual Events Series** Demographic Fairness in Biometric Systems—March 2021, IDEMIA presented a lecture about *Fairness for Face Recognition* and participated in a panel discussion with major actors including NIST and the UN Office of Counter Terrorism.

https://eab.org/events/program/237

5 NIST Face Recognition Vendor Test.

https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

6 NIST Face Recognition Vendor Test, Part 3: Demographic Effects.

https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

7 Stephane Gentric, IDEMIA's Head of Artificial Intelligence Research. Face recognition evaluation @IDEMIA. In Proc. International Face Performance Conference, National Institute of Standards and Technology NIST, Gaithersburg, MD, November 2018. Page 8,

https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

8 Ongoing Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. Annex 17: Candidate list score magnitudes by sex and race. Page 24, figure 21.

https://pages.nist.gov/frvt/reports/demographics/annexes/annex_17.pdf

About IDEMIA Public Security

Justice and Public Safety is the business line of IDEMIA Public Security dedicated to applying our biometric technology excellence to helping law enforcement agencies prevent more offenses, solve more crimes, and protect more people.

With over 50 years of experience and a global team of nearly 600 experts, we focus on developing biometric-based technologies and solutions that enhance the efficiency and effectiveness of justice and public safety efforts. Our solutions, ranging from fingerprint matching through facial recognition to investigative data analytics, are designed to meet the unique needs of law enforcement agencies worldwide.

Over 85 governments in 55 countries trust us to handle and match millions of fingerprints, portraits and latent print records, as well as structured and unstructured data. Enabling a more efficient policing process, we also develop cutting-edge proprietary tools like LiveScan and mobile fingerprint devices. Our goal is to support law enforcement professionals with state-of-the-art resources evolved to meet their changing requirements, ensuring they have the tools they need to protect and serve their communities.

At IDEMIA Public Security, we prioritize fairness, accuracy, and reliability in all our solutions. We work closely with our customers, responding to their specific needs and challenges, to create a safer and more secure world for everyone.

For more information, visit **www.idemia.com**

Follow **@IdemiaGroup** on LinkedIn

Unlock the world, **make it safer.**

IDEMIA GROUP

www.idemia.com