thalesgroup.com

THALES
Building a future we can all trust

Designing an ethical, socially accountable facial recognition system

A vision from Thales

Editorial

The ability to identify someone's face is a talent we all rely on, both for our social interactions, as well as for our own safety and protection. This is an innate ability, but we don't all possess it at the same degree. According to research made by the University of York, humans can recognise 5,000 faces[1]. A super-recogniser may be able to memorise and recall 10,000. But when asked to match a face and a picture, even the best-trained are accurate only 80% of the time.

As we look for secure and convenient ways to identify people, **facial recognition is the least intrusive and most accessible form of biometric identification**: contactless, fast and reliable. When asked to match a face and a picture, the top performing 100 Facial Recognition algorithms tested by the United States NIST agency in 2020 are accurate 95% of the time.

Facial recognition technologies are still making headway, and identity applications are constantly being improved. The industry's R&D teams are blending their expertise in identity technology, biometrics and cybersecurity to design better performing solutions. Continuous improvements are being made regarding accuracy, speed, privacy best practices, security issues, standards and user experience.

This e-book explores the different aspects of this fascinating emerging technology.

[1] Humans can recognize 5,000 faces on average, according to a study from the University of York, 2018. *https://royalsocietypublishing.org/doi/full/10.1098/rspb.2018.1319*

All you need to know about facial recognition

What is facial recognition?

Facial recognition is a technology designed to **automatically identify a person using their face if they are previously known to the system. If the system does not have a reference image available of the individual, the technology is not capable of identifying the individual**. Its first steps date back to the 1970s, but it has made considerable headway in recent years thanks to increasing computer processing power, machine learning and the development of Artificial Intelligence (AI).

Facial recognition is a **biometric technology** which uses different scientific methods to identify and verify individuals through analysis of their specific physical characteristics. Other common biometric modalities include fingerprints, palm geometry, voice, Iris and DNA.

How does a computer recognize a face?

Facial recognition solutions do not compare a person's face to an actual photo: they rely on extracting key features, called "vectors," from a photo, or specific data points on the face, such as the spacing of the eyes, the bridge of the nose, the base of the ears, the space between chin and mouth to create a unique template for each face which is then encrypted. This encrypted template data obtained during enrolment of the individual is then stored digitally in a reference file or database. Once the person's live face is then presented after enrolment, the facial recognition system will be able to match the live face with the one previously provided by scoring the match as a high probability of it being the same person.

The initial facial images must be of a certain quality and resolution to be enrolled. Facial images can be obtained and enrolled one by one, or from a gallery of faces. The templates stored in the reference database cannot be used to recreate the face as they are essentially a one-way mathematical interpretation of the original facial image.

Several steps are required for making a facial match:

- First, a reference digital facial template is created, incorporating all the key facial characteristics from a photo or image of the individual. This is the **biometric data acquisition phase** or enrolment phase.
- Subsequently, when attempting to verify or identify an individual, **a photo or a video of them is captured or obtained**. The facial recognition system then uses the same mechanism on the new facial image to create a new template to compare against the reference template database. In cases where an individual is submitting their own facial image remotely, a selfie image can be submitted via a mobile app. The capture of their photo or video should include liveness detection, to prevent spoofing by presenting just a photo at the time of remote capture.
- The facial recognition system then **compares the newly collected facial image to the reference template**. If a sufficiently high comparison score is obtained between the face presented to a reference template, the individual is determined to be "recognized". In some situations more than one 'match' may be obtained from comparing against a gallery of templates. The facial recognition system will present the matching candidates for an authorized person to adjudicate the actual match, if any.

Authentication vs. identification: what's the difference and how are they used?

Two types of facial recognition can be done: authentication and identification.

Authentication (also called verification) seeks to prove someone's identity – are you really who you say you are? Authentication consists of performing a one-to-one (or 1:1) comparison of the newly presented image of an individual, against their own reference template – the one they claim to be. This requires prior enrolment and consent from the person who is to be verified. The aim is to confirm that the live face being presented is the same as the one previously enrolled. Authentication is quite notably used by many to unlock their smartphones on a daily basis.

Identification is the process of finding out someone's identity – who are you? When seeking to identify an individual, their captured image or video is compared to a database of facial templates to see if there is a match. This is referred to as a one-to-n (or 1:N) matching, with N representing the total number of templates in the database.

Distinct ways of using facial recognition

Facial recognition – whether authentication, identification or a mix of both – may be used in a variety of ways, and offer many advantages to the organizations and companies deploying it, as well as to the people benefitting from this non-invasive, contactless technology.

- Physical access control: allows for an easier and more secure access to restricted areas (e.g. office buildings, sporting events, warehouses...).
- Airport boarding / passenger journey: when used for check-in, baggage drop, border check, gate access... facial recognition makes it easier to cross borders and board planes.
- ID verification: facial recognition provides a more secure way to sign up for digital services, with reduced risk of fraud or identity theft (e.g. remote ID check when registering for online services, onboarding customers remotely...)
- Law Enforcement (lead generation after an incident). Similar to DNA and fingerprint evidence, some law enforcement agencies are using facial recognition to generate leads after a crime has been committed if there is video evidence of the incidence. Unlike DNA and fingerprints, facial recognition cannot be used to convict anyone. It can only be used to provide leads that allow law enforcement to narrow their search and solve crimes faster. In many jurisdictions, new or updated regulations may be required to ensure that civil liberties are not violated.
- Surveillance (locating, potentially identifying someone and tracking their movements in real-time). With the explosion of video cameras throughout the world, the possibility exists for government entities to identify and track people as they navigate throughout the day. This application, rightly so, has civil liberty and privacy concerns. This application should only be done when appropriate regulations are in place that balance an individual's rights against the common good. Facial recognition for this purpose provides enormous benefits when used by authorities to help find missing children and those with limited cognitive capacities, abducted individuals, etc.

When facial recognition is used for either real-time surveillance purposes or law enforcement lead generation, a regulatory framework may be required to be put in place to ensure respect for individual privacy and civil liberties, however this may vary for each situation, country or jurisdiction.

Less waiting time, better security: facial recognition at airports and company sites

Facial recognition is useful in a wide area of contexts and applications, especially when massive crowd movements are involved, with safety and control issues.

Illustration? Paris Airports recently decided to move from fingerprint to facial recognition technology. When fully implemented, it will allow for 45% of Paris Airports' 100 million yearly passengers to benefit from fast-track control – up from the current 10%. Passengers with electronic passports present it at the eGate, to be automatically scanned. A first door opens, the passenger shows their face at the camera. The image is compared to the data in the passport's chip. In a few seconds, the passenger has crossed the border, authorities are warned if anything is wrong, and the whole airport user experience is improved.

Facial recognition can thus contribute to everybody's safety and comfort. It allows for:

- **Simpler and faster site access control.** Facial recognition is safer than the usual security badges, which may be stolen or lost, and faster, less intrusive than other biometrics technology such as fingerprint analysis or iris recognition;
- **More efficient boarding process in transportation,** through automatic control and screening of unwanted individuals posing a security risk by using the traveller's face as their 'ticket';
- **Automatized access to services or equipment,** in the way smartphones are unlocked by using facial recognition of its user;
- **Real-time site monitoring** to identify and locate people in a crowd (wanted individual, missing child, etc.);
- **Reliable identity control,** when combined with the use of electronic passports, which also store facial data: identity theft is made virtually impossible;
- **An alternative solution to badge or fingerprint control,** with enhanced efficiency: no badge needed, no physical control by a security guard or an automatic terminal, no badge lending possible...;
- **Commercial applications** (purchase, payment, etc.)...

Airport facial recognition technology can be usefully applied to other contexts: access to sensitive locations, large events entry, ID control at large company buildings. Corporations can make sure only authorized workers are allowed in some areas, check arrivals and departure from work, and smoothen the security process for everyone. Data need not leave the control device, but encryption can further enhance data security and privacy, to placate legitimate concerns about civil liberties.

Border control checks takes just 10 to 15 seconds in airports equipped with facial recognition! [1]

[1] La Tribune

Performance and comfort combined

Nowadays, facial recognition has become **a mature, reliable, very accurate, fast matching technology.**

- It is **free from most of the physical interaction required with other biometric technologies**. Unlike fingerprints recognition, it raises no health concerns, as it does not involve **any physical contact** with a sensor. Unlike DNA analysis, it is **non-intrusive** and requires no sampling. It is **ergonomic**, **user-friendly**, with optimal user experience: unlike iris recognition, it does not require the individual to take position precisely in front of a sensor; unlike other technologies, such as signature recognition, it does not imply any particular action on the part of the person controlled.

- **It eliminates most risk of fraud or identity theft,** unlike systems based on security badges, for instance.

- **It is simple and easy to set up**, both for the IT team and for the site security staff. It can be integrated and deployed easily in either green field locations or existing video surveillance infrastructures.

  Last, but not least, the technology is improving as it is more widely used: thanks to machine learning, facial recognition gains accuracy as the data grows. The top ten algorithms tested by the United States NIST agency in 2020 showed 1 to 1 accuracy above 98%, where the top five are above 99%.

Roadblocks on the way !

Facial Recognition is already much more accurate than humans and it is much more technically efficient and reliable. And it continues to get better: experts expect it to improve by a factor of 2 within 4 years! While the technology is already deployed with important benefits in a number of applications, we will see more of its adoption in the future. Still, fears and concerns, some of which are very legitimate, may explain that the development of facial recognition is not as fast as could be expected, considering the technology's manifest performance and strength.

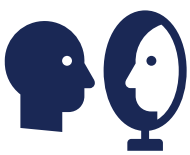
General public mistrust

People are often hesitant about new technology – and even more so if they don't understand how it works. So while on the one hand, many persons have already adopted the ease and efficiency of facial technology for unlocking their smartphone, on the other hand, they are concerned about matters relating to their privacy. More specifically, they fear a potential unauthorised collection and utilisation of their biometric data.

Wider communication on how facial recognition works might allay some of these fears. It should be pointed out that biometric technologies do not necessarily imply a centralized database. For instance, a facial photo is **stored locally on an electronic passport**, to allow for its bearer's authentication using facial recognition. When identifying electronically when crossing border control at the airport, the data doesn't leave the local system.
But to a greater extent, these concerns highlight the need for well-defined **legal frameworks** and for facial recognition solutions to be used in strict compliance with these.

Concerns of «statistical differences»

Objection to facial recognition is rooted primarily in concerns surrounding violation of civil liberties and privacy. However, the technology itself is not the risk – its inappropriate use is. This makes the development of laws and rules that balance the protection of civil liberties and privacy against the common good a priority.
And, as previously stated in this paper, a framework of laws and regulations surrounding the surveillance and law enforcement applications is under consideration in many countries to protect individual rights.



Another top concern revolves around questions of ethics and equity, specifically:

- Concerns of bias, where opponents say technology may not be as reliable depending on a person's gender or ethnicity
- Concerns of misidentification (False Match) and their potential unqualified consequences.

Many of these claims are based on the performance and results of older tests that used limited and unrepresentative datasets. However, the latest developments in facial recognition technologies have significantly lowered the scope of these "statistical differences". As datasets get bigger and bigger, the technology learns and gets more precise. Face templates are also getting more efficient: the features and angles chosen are more neutral. According to the December 2019 NIST Face Recognition Vendor Test: Part 3: Demographics Effect, the performance of the algorithms are a direct correlation to the data included in the database.

To minimize statistical differences, databases require a diverse and representative dataset. A study led by the National Institute of Standards and Technology shows that performance results are very consistent when a candidate's face is compared to a set of data from the same country, sex, ethnicity and age. It compares facial recognition performance whether the person is from Russia, Somalia or Vietnam, and shows that if a Russian woman of older age is matched through an algorithm that is seeded predominately by a country other than Russia, the results decrease significantly. The key to consistent performance across ethnicity, age, and sex is to ensure that the system used is seeded with a robust, diverse database.

To know more about about this study, please consult the following publication from the National Institute of Standards and Technology : *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*

Lack of transparency

Another concern is the technical possibility of deploying a facial recognition solution without people being aware of it, whether in a public or a private place. It's important to note that video surveillance is already common place in both public and private environments today. Adding real-time facial recognition to these applications is where transparency becomes an issue.

In matters of surveillance, **Thales supports the legislator's role in protecting individual freedoms** by setting the laws and regulations applying to security solutions, and providing public information about where and when these same solutions are effectively deployed.

What legal framework for facial recognition ?

In Europe, Asia and the United States, facial recognition technology is developing under very different legal frameworks. And these are still changing.

In Europe, a common framework for 500 million citizens

Since 2018, in the whole European Union, The GDPR (General Data Protection Regulation) sets the guidelines for country legislations on the protection of personal data – which include biometric data. It applies to **500 million European citizens in 28 countries** (Great Britain has retained it despite «Brexit»). It implies:

- **«Free, specific, informed and unambiguous» consent** from the user when processing their personal data ;
- **The «right to be forgotten»**, meaning any individual has a right to request an organization to delete their personal data,
- **Several security obligations**, among which systematic information of concerned users if a security breach is discovered in the database.

However, digital technology watchdogs in several countries are suggesting the possibility of specific regulations for facial recognition solutions that may go beyond the legal framework for collecting personal information. In France, the CNIL (National Commission on Informatics and Liberty) thus comments, «facial recognition calls for political choices: on the role of technology, on its impact on the fundamental freedoms of individuals, on humanity in the digital age."

In the United States, a patchwork of laws and differences between states

In the United States, different states or localities have passed specific legislation to regulate or prohibit the use of biometrics in general, or the sole use of facial recognition technologies, by government agencies and / or private companies.

- Several local jurisdictions and States have legislation on the use of biometric data.
- In all other States, you can lawfully use software that identifies a person using images captured without their consent in public space.
- Several cities in the USA have banned the use of facial recognition technology by law enforcement agencies, whether public or private.

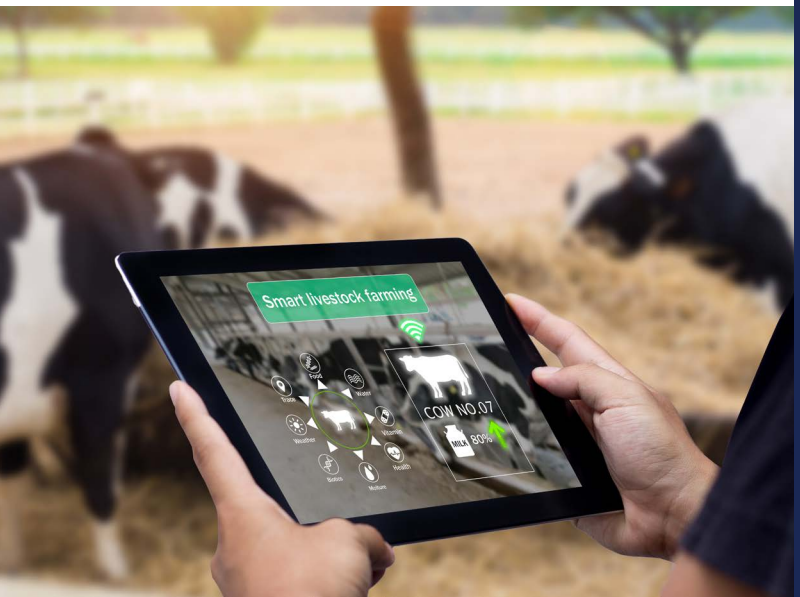
Many of the involved players (suppliers and users of facial recognition systems, local or federal organizations, etc.) are now calling on the Federal government to define a clear policy line, allowing States and local jurisdictions to rely on a definite and common framework to design their own legislation.

Using facial recognition in a socially responsible way

Facial recognition is part of our future. Still, some fear abuses in the use of facial recognition: we are aware of this. Thales's solutions are designed with **strict ethical principles** in mind. We not only master biometrics: we are cybersecurity experts as well. Coupled with our TrUE AI approach (2) , our range of expertise allows us to **build end-to-end solutions that are safe, ensuring data confidentiality and integrity, as well as secure storage of biometric data**.

Wider use of facial recognition seems inevitable because it is reliable, efficient, easy to deploy and does not require specific sensors. Most of all, it can be of great help to humans in many ways. Let's ensure that it happens under the best possible conditions, especially in sensitive sectors such as safety, health and commerce. New applications may emerge that are yet to imagine: a few years ago, **who would have thought facial recognition technology would be applied to agriculture, to improve identification of cows or pigs?**

(2) The Thales TrUE AI approach stands for Transparent, Understandable and Ethical artificial intelligence. *Transparent AI*, where users can see the data used to arrive at a conclusion. *Understandable AI*, that can explain and justify the results and finally an *Ethical AI*, that follows objective standards protocols, laws, and human rights.
https://www.thalesgroup.com/en/journalist/thales-podcasts



We design all our solutions in accordance to strict ethical rules

For us, at Thales, facial recognition solutions must be designed in accordance to a few essential rules.

- **Confidentiality and consent.** Setting up a facial recognition solution involves the collection of biometric data from people. This process must be carried out with the explicit consent of all concerned. Confidentiality of data must be guaranteed and protected from any use not initially intended and agreed upon.
- **Transparency.** Any facial recognition solution must be deployed in total transparency. Data subjects must have access to a description of how biometric data is collected, stored and used and for how long their information will be retained.
- **Precision and reliability.** Facial recognition solutions must ensure maximum precision and reliability. They must be based on algorithms processing a very diverse set of data and sensitive to all the specifics of the captured image (glasses, hat , scarf...).
- **Security.** Facial recognition systems should by design ensure total security of the personal and biometric data collected and stored. Data should be encrypted both at rest and in motion.
- **Ethics & Compliance.** Facial recognition solutions must be designed and implemented in full **compliance with market standards, regulatory and legal obligations.** They must respect standardized and objective protocols, legislation and human rights.
- **Accountability.** Technology providers must support customers over the long term, offering sustainable technical solutions, adapted to their present and future needs.

Thales is a member of several biometric industry associations and groups, among which are the Biometrics Institute and the International Biometric and Identity Association.

Biometrics Institute

International Biometric and Identity Association

To know more about Facial Recognition at Thales
please get in touch with Kadie-Ann Fyffe
Communications Specialist, Identity & Biometric Solutions

E-mail: kadie-ann.fyffe@thalesgroup.com

THALES
Building a future we can all trust

thalesgroup.com