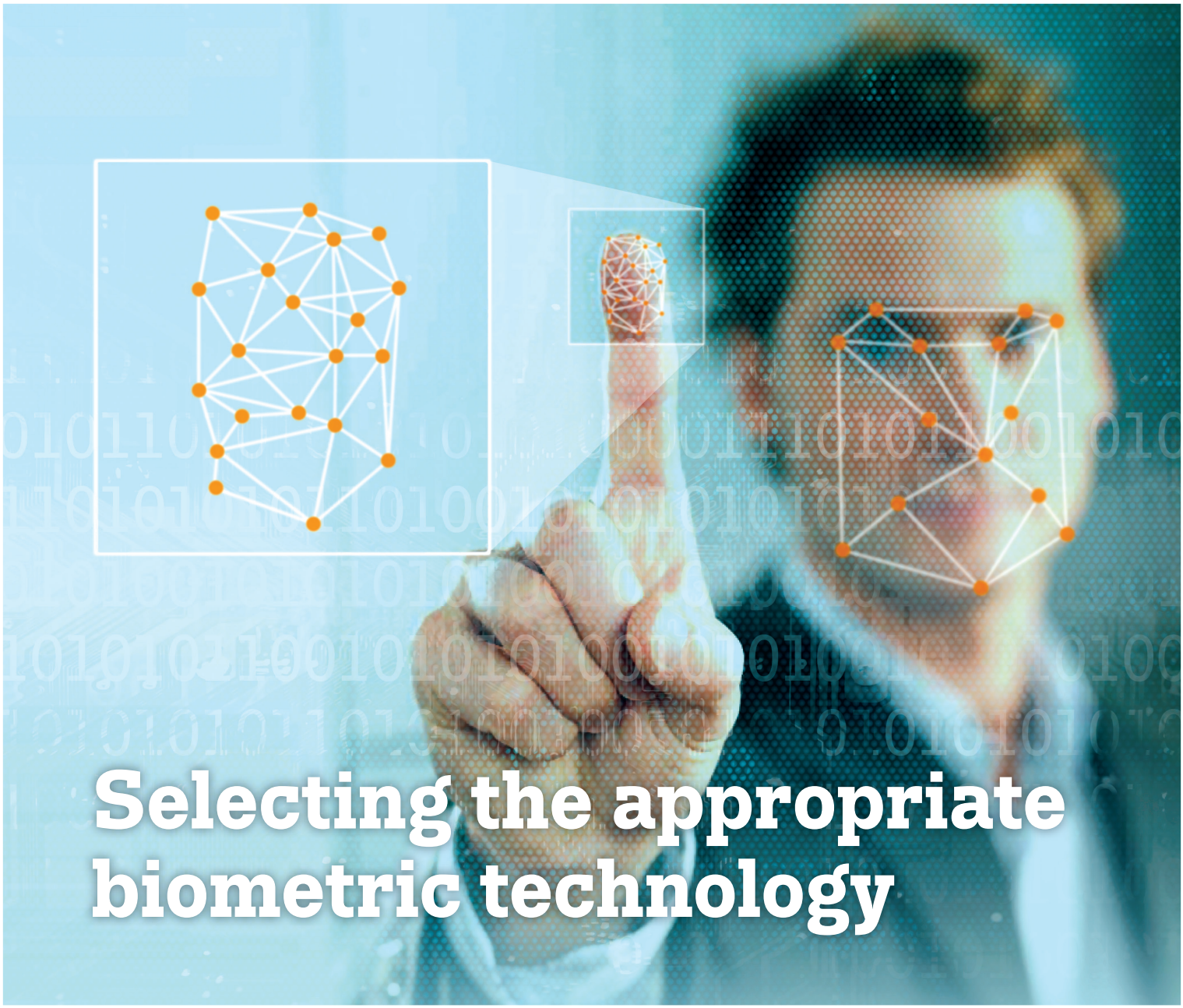


Selecting the appropriate biometric technology

It's crucial that physical access control systems identify and verify people reliably. This article covers the most common ways for identification and verification via biometric technology. Biometrics have grown in maturity, and many systems based on fingerprint, face, hand and eye recognition are performing well with physical access control systems. To select the right biometric solution criteria such as accuracy, fraud and user friendliness need to be considered. Here, we provide an overview of technologies currently available and their typical properties, plus guidelines you can use when selecting identification and verification options for your organisation.

What are biometric technologies?

Biometric identification refers to the automated recognition of individuals based on their behavioural or biological characteristics. Biometric technologies are concerned with either physical aspects of the human body, for example the face or fingerprints, or the personal traits of human beings, for example a signature or voice pattern. To be useful, biometric technologies must recognise or verify these physical aspects or human traits quickly and automatically, in real time.

There are two different ways to recognise a person via biometric technology: identification and verification. When applying biometrics for identification purposes, the system has to recognise a person from a list of users in a database. Verification, on the other hand, involves confirming or denying a person's claimed identity, for example the user presents an ID card and is then asked to present a finger or face to verify his or her identity. Biometric technologies enable organisations to identify or verify the identity of individuals with a high degree of certainty. For that reason, it was first used in high-security environments. With the arrival of user-friendly and affordable systems, however, biometric technologies began being applied in a variety of systems and environments.

Biometric characteristics

Biometric technologies have specific characteristics that help you to determine their benefits and shortcomings and enable you to select the most suitable technology for your organisation. The most important characteristics are discussed below.

Accuracy: acceptance level versus error rate

A biometric system should not reject authorised users (FRR, False Rejection Rate) or provide fraudulent access (FAR, False Acceptance Rate). Comparing the EER (Equal Error Rates where FRR = FAR) of the different systems available can be instructive as it demonstrates the relative strength of various biometric systems.

Fraud

All systems are susceptible to fraud, but defrauding modern systems takes significant knowledge and skills. The many differences in the various technologies make fraud even harder. Copying biometric characteristics is more difficult for some systems than others. Copying a fingerprint, for example, is easier than presenting a forged iris. Another threat relating to fraud involves sniffing data from the sensor and playing it back to the biometric system. Encrypting the data coming from the sensor can prevent this, as can changing the biometric data on a card or database.

Stability

Biometric characteristics like faces and fingerprints can change over time causing errors in recognition performance. Hands and fingers can change due to fluctuations in weight, for example, and age can influence face recognition. While damage or illness can change fingerprints or the iris, even though these are usually more stable. Some biometric systems can overcome these changes by automatically storing updated templates.

Usability

The system should be easy to learn and simple to use in everyday practice. Particularly in situations where user training isn't possible, the system should be intuitive to ensure that authorised people are being correctly recognised. Irritating lighting or an inconvenient location of biometric readers, for example, can also have a negative influence on practical use.

Speed

For convenient access control the decision to grant or deny access must be given within seconds, especially at places where many people require access, or where people pass through several times a day.

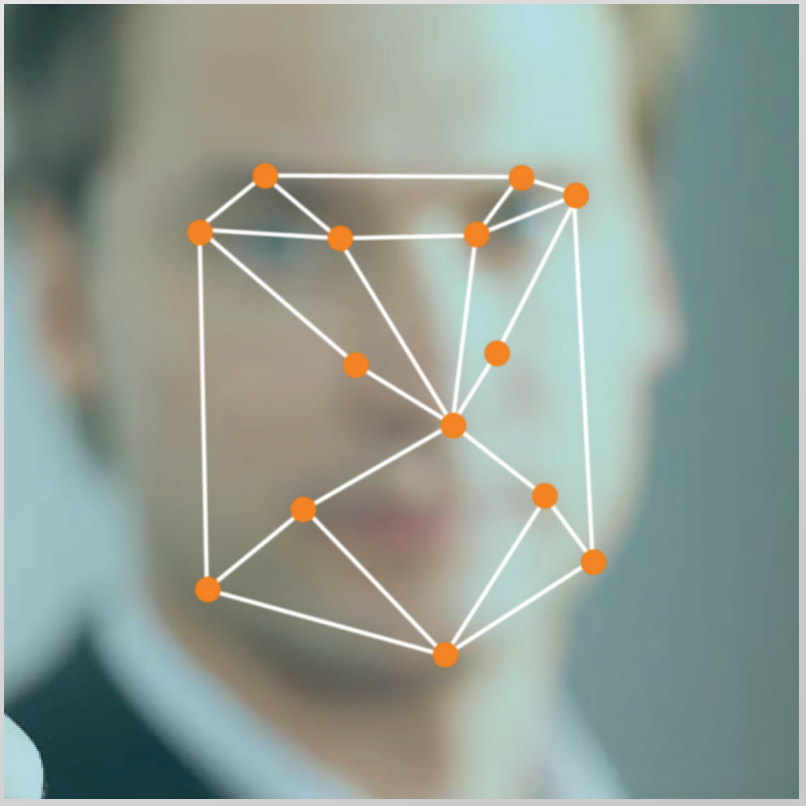
Enrolment

The majority of recognition failures in a biometric system are caused by improper enrolment. Good performance and accuracy can only be achieved when people's characteristics are enrolled properly. For all systems, this starts with clear user information and guidance on how to enrol people and use the system. Vein, retina and iris systems demand extra effort as they're less commonly used than fingerprint and face recognition solutions.

Modern biometric technologies for access control

2D face recognition

When applying 2D face recognition, an image of the face is captured by a camera and converted into a unique mathematical code. This code is stored as a template and used as a biometric reference to which the image of the person requesting access will be compared. 2D face recognition can also be used in video surveillance systems to track people based on a black or white list. It's easy to use and the technology has a high recognition speed. Accuracy, however, is not as high, so we recommend only using 2D face recognition for additional identification or verification measures.



3D face recognition

With 3D face recognition, a three-dimensional map of the face is created through infrared grids or the merging of multiple images. As with 2D face recognition, it's very user friendly and people are identified quickly. 3D images contain more unique characteristics, so recognition accuracy is higher than with 2D face recognition. The drawback is that glasses and beards can have a negative effect on accuracy. Accuracy for face recognition is not as high as it is for eye or fingerprint recognition, but has been improved in the last few years and is expected to improve further.

Iris recognition

When using iris recognition, unique features of the iris are extracted from a captured sample, converted into a unique mathematical code and stored as a template. An image of the iris needs to be created in a well-lit environment, as the pupil needs to be small for the optimal amount of iris to show. Glasses need to be removed when capturing an image of the iris, but they don't cause problems during recognition at the door. These aspects have a slightly negative effect on user-friendliness. Recent developments, though, have improved convenience of use, as the recognition distance for identification or verification has increased to approximately two metres. Moreover, the accuracy of iris identification is high, making iris recognition an attractive option in high-security applications.

Fingerprint recognition

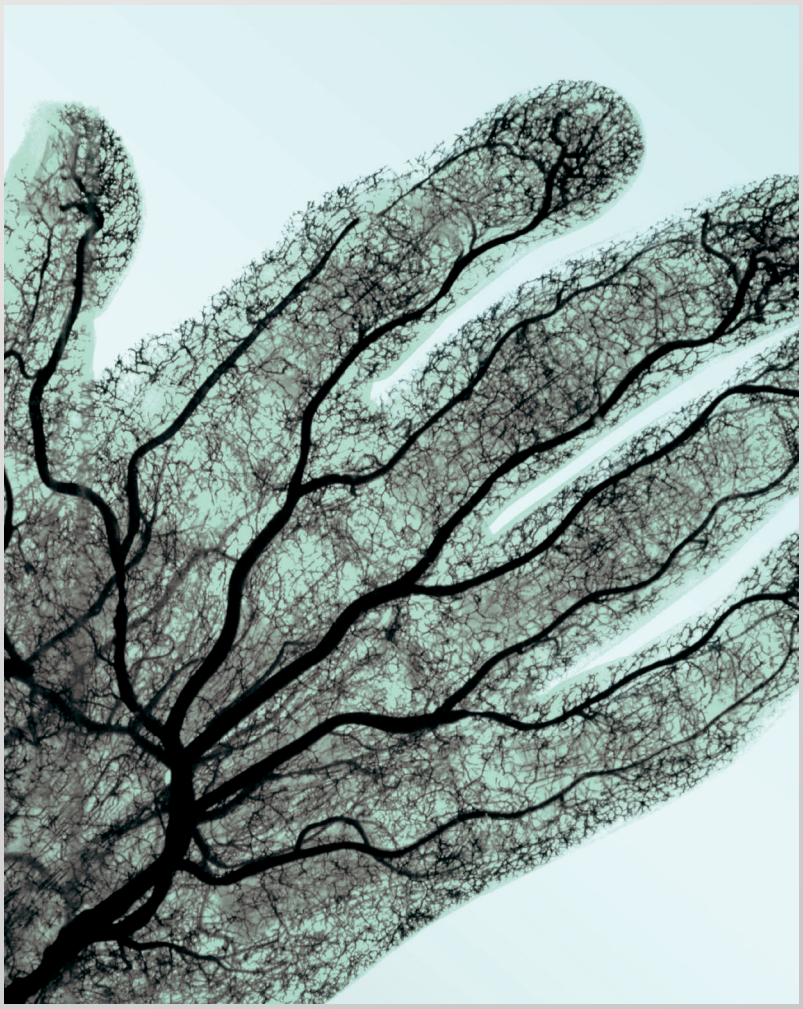
Fingerprint recognition compares a template consisting of fingerprint characteristics with the finger presented. A template is generated from an enhanced picture of grid lines taken with a fingerprint scanner. The characteristics are then computed, including ridge endings, bifurcations, position and direction. Accuracy of fingerprint recognition is good, but dirt or wetness can cause problems. These problems have been solved in contactless or multi-spectral fingerprint technologies. As damaged fingers may also affect the accuracy of recognition, it is preferable to enrol at least two or three fingers per person. The relatively low price and high accuracy make fingerprint recognition a good choice in many access control applications, especially those where fewer people need access.

Hand geometry

Hand geometry takes a three-dimensional image of the hand via a hand reader and measures the shape and length of fingers and knuckles. The 3D measurement is then converted into a unique mathematical identifier and a template is created for that person. Hand geometry does not achieve the highest levels of accuracy, but it is convenient to use and the primary advantage is that large volumes of people can be processed quickly. Hand geometry is predominantly used for one-to-one verification and is very suitable in harsh environments, as wet or dirty hands barely affect the hand reader's performance.

Hand and finger vein recognition

Veins form a unique pattern for each person and can be captured using infrared light. The unique vein patterns in either a finger or the hand can be recognised by vein readers. When using a hand palm vein reader, the infrared light is reflected by the hand surface and creates a good picture of the vein pattern. Biometric technologies that analyse vein patterns are considered to offer high authentication accuracy, with surface dirt or damage having little influence on the reading. Vein recognition is suitable for high-security environments, as the correct person must be physically present with blood flowing through their veins. For both types of vein recognition, the positioning of the finger or hand has to be so precise that user friendliness is reduced. Cold temperatures can also affect the recognition of finger veins as it reduces the flow of blood to the veins.



DNA

Human DNA can now be analysed within ten minutes, but it's not yet sufficiently automatic to rank DNA as a biometric technology for security purposes. When technology advances so DNA can be matched automatically, in real time, it may emerge as a significant contender in the biometric security industry.

Semi biometrics

Semi biometrics are often used for verification purposes, especially in high-security environments. There are several ways to ensure that only the person positively identified gains access and no one else tries to access the area with them, for example. Measurement of weight, the body and video surveillance are three examples:

- By placing a weighing scale in front of a door, it can be verified that only one person is trying to gain access if the weight is correct (allowing a small margin).
- Body measurement also provides information on how many people are trying to access a certain area. This is done using several light beams and detecting if one or more of them are interrupted.
- Installing a video camera at the door can be used for the same function. An intelligent image-processing algorithm will determine if more than one person is present.

Bio Characteristics

	2D Face	3D Face	Iris	Finger-prnti	Hand geometry	Retine vein	Hand vein	Palm vein	Finger vein
Accuracy	✗	●	✓✓	✓	✗	✓✓	✓	✓	●
Fraud	✗	●	✓	●	●	✓✓	✓	✓	✓
Stability	✗	✗	✓✓	✓	●	✓✓	✓	✓✓	✓
Usability	✓✓	✓	●	✓	✓	✗	●	✓	●
Speed	✓	✓	●	✓✓	✓✓	✗	✓	✓	✓

Key	Significance
✓✓	Excellent
✓	Good
●	Sufficient
✗	Not recommended
✗✗	Insufficient