VERIDOS
IDENTITY SOLUTIONS
by Giesecke+Devrient
and Bundesdruckerei

White Paper

Biometrics

May 2018

Date: May 18, 2018

VERIDOS
IDENTITY SOLUTIONS
by Giesecke+Devrient
and Bundesdruckerei

Contents

VERIDOS
IDENTITY SOLUTIONS
by Giesecke+Devrient
and Bundesdruckerei

1 Management summary

The deployment of biometric systems has advanced drastically in recent years. The unchangeability and uniqueness of the features used makes them an attractive alternative to PINs and passwords, which are prone to being stolen or forgotten. Automated biometric recognition systems have also improved the speed and accuracy of identity verification.

Unfortunately, there is not one single biometric feature that is consistently the 'best', most practicable, efficient, or cost-effective. The best choice will depend on the individual application. Factors to consider include the availability of required sensors, space requirements, and environmental conditions (e.g. lighting, humidity, user access). A newly proposed modality must be intensively researched as regards its properties, especially uniqueness, to evaluate its quality and appropriateness.

Biometric systems cannot achieve 100% accuracy in identity verification. There will always be a tradeoff between high precision to distinguish between people who are similar but not identical, such as twins, and rejecting the correct person due to poor conditions for data acquisition.

On the technology side, major improvements in deep neural networks have facilitated the development of biometric solutions. The new technology achieves better feature extraction performance and can easily be applied to new biometric modalities. However, big databases of these modalities are required to train the systems. This has opened the market to new players, especially in the field of face recognition.

Biometric technology has great potential to improve public safety and convenience in the years to come. But for this to be realized, special care must be taken to ensure the security and reliability of these systems.

Public discourse has been focused on means to ensure data security and privacy while preventing data abuse. Over recent years, legislators have addressed the biometrics trend with an increasing amount of regulations introduced to control the use of biometrics, and these can vary greatly by jurisdiction. In Europe, the General Data Protection Regulation (GDPR) attempts to define a common standard, whereas each state in the U.S. has its own legislation.

Biometrics is emerging as a promising solution in multiple areas, including mobile payments, online banking, immigration and border control, healthcare and welfare, surveillance, and access management. It is affecting various trends, such as urbanization (maintaining public order), smart homes (automatic adjustment of home environments without interaction), mobility (reliable driver license validation for car sharing, personalized ticketing systems),

payment (replacing card/token-based payment systems), and online authentication (replacing secret-based systems). In turn, the rise of biometrics has increased interest in anti-spoofing technologies and the miniaturization of sensors.

The biometrics market continues to grow apace, with major revenue generated via biometric sensors for smartphones and the internet of things. It is likely that deep neural networks will become the preferred method for extracting features in the years to come, disrupting the existing market for biometric algorithms.

The complexity of biometric systems demands a deep understanding of how biometrics work and extensive practical experience in developing solutions for the scenario at hand. Ensuring the security of these systems poses a particular challenge. G+D has proved its competence across many sophisticated biometric projects in recent years.

2 Introduction to biometrics

The general meaning of biometrics encompasses the counting, measuring and statistical analysis of any kind of data in the biological sciences, including medical sciences (Busch 2017). This white paper addresses biometric methods of recognizing human individuals..

Biometrics is a method to provide reliable identification of individuals. Biometric technology measures physical or behavioral characteristics to determine the true identity of a person. While just a few years ago biometrics were mostly the domain of science fiction, this technology is now mature and used in an increasing number of settings.

Biometric systems can broadly be classified into two categories based on the respective biometric characteristics: biological and behavioral.

- Biological characteristics are the physical characteristics of body parts, such as fingerprints or hand contours, i.e. characteristics that do not change substantially over a person's lifetime.
- Behavioral biometric systems analyze a person's behavior and actions. Examples of monitored behaviors include signature movements or voiceprints. It should be noted that behavioral biometric characteristics also have a physical component, e.g. the articulatory system in the case of speech.

2.1 Methods of authentication

Authentication is the act of "verifying the identity of a user [...], often as a prerequisite to allowing access to resources in an information system" (Kissel 2013). The various authentication methods are usually grouped into three categories:

- Secret Knowledge: "What I know", characterized by secrecy or obscurity. Examples include secret PINs and passwords.
- Personal Possession: "What I have", characterized by physical ownership. Examples include keys, passports, or ID cards.
- Biometrics: "Who I am"" characterized by uniqueness to one person.

All of these methods have their pros and cons, as shown in the following table (++ = pro, – = con, o = can be both a pro and con):

Secret Knowledge or Personal ownership		Biometrics
Authenticators are chosen randomly	o	Characteristics are inherent
Authenticators can be changed	o	Characteristics cannot be changed
Transfer is possible	o	Transfer is impossible
Loss / Forgetting is possible	–	Loss / Forgetting is possible
Theft possible	–	Theft pointless
Security constrains user-friendliness	–	Secure and user-friendly
Impossible to draw conclusions regarding the user from the authenticator	+	Possible to determine the owner
No special hardware required	+	Special hardware required
Secret cannot be reconstructed from stored reference	+	Original can potentially be reconstructed from template
User is responsible for failure	+	System is responsible for failure

The last point in particular requires attention: In biometrics, responsibility for failed authentications is shifted onto the operator of the system. This can be a crucial point when deploying biometric systems.

2.2 Aspects of biometrics to consider

Biometric characteristics are used in a diverse range of scenarios, and current scientific research covers a broad range of future applications. The use of biometric characteristics has a long tradition in forensics. Modern developments expand on automated analysis of biometric characteristics, for example for health applications such as the early identification of disease outbreaks (at an individual level or early identification of pandemic outbreaks). Even correlations between several biometric characteristics and individual traits are again the subject of scientific investigations (Wang and Kosinski 2017).

The examples mentioned above are beyond the scope of this document, which will focus on technical aspects and possible fields of application related to biometric authentication.

In the last few years, the evolution of biometric systems has advanced drastically. The availability of sensors in electronic devices such as mobile phones or wearables enables cost-efficient implementation of biometric systems, bringing them to the mass market.

Many factors influence the applicability of biometric systems. For example, face recognition may be appropriate in surveillance, since it can be used from a larger distance than, for example, a fingerprint. Similarly, voice recognition may be practical in communication and telecommunication, while hidden biometric traits such vascular patterns may provide better resistance to identity theft or spoofing. Even issues of hygiene may influence the choice of biometric trait.

Biometric systems offer the potential to obtain and store individual data for large parts of the population, ensuring data security, data privacy and the risk of data abuse is a hot topic in public discussion. Further, different legal regulations may impact or even restrict the use of biometrics – depending on the country where the biometric system is to be used (e.g. GDPR).

2.3 Identity claims

Biometric recognition traditionally distinguishes between verification and identification:

Verification: In verification systems, a user makes a positive claim to an identity, resulting in a one-to-one comparison of the submitted biometric sample to the stored template of the claimed identity. The claimed identity is submitted to the system in the form of a name or personal identification number.

Identification: In identification systems, a user makes no claim to an identity, and a one-to-many search across the entire biometric database is required.

The result of a verification is always a yes or no binary outcome; whereas the result of an identification is either the identity itself or nothing – in the event no subject in the database is sufficiently similar to the current subject.

2.4 Key components of biometric recognition systems

Broadly speaking, biometrics is a pattern recognition task. A biometric system consists of the following components (cf. Figure 1): signal acquisition, pre-processing, feature extraction, and classification (pattern or model match). For new users, reference templates or models must first be generated (enrollment). The classification is subsequently performed by comparing the new recorded sample with the stored reference template, and calculating a matching score. Identification (one-to-many search) or verification (one-to-one comparison) is achieved by setting a threshold for the matching score to discriminate between accepted and rejected trials.

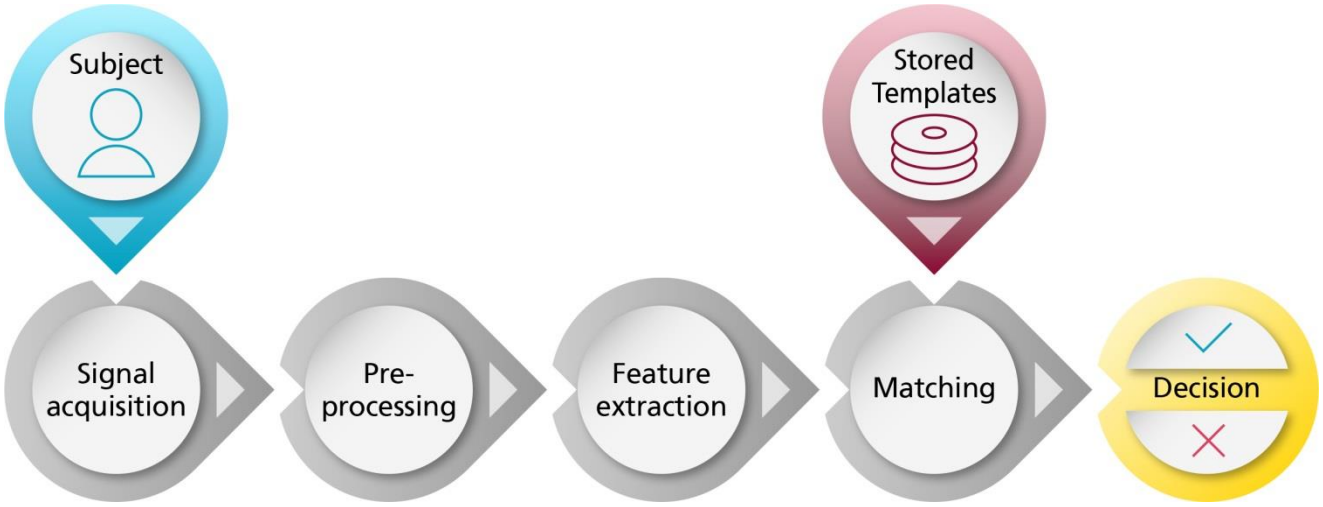


Figure 1: Building blocks of a biometric system

Building blocks

- Signal acquisition: A sensor captures a biometric characteristic presented by a user
- Pre-Processing: In pre-processing, the captured signal is enhanced (e.g. distortions are filtered out), segmented (areas of the signal that do not contain relevant information are removed), and the quality assessed.
- Feature extraction: A mathematical representation of the information is extracted from the pre-processed signal. Examples of extracted features include points of identity in the case of fingerprints, or abstract mathematical representations such as Gaussian mixture model (GMM) parameters in case of speaker recognition.
- Data storage: The data storage contains user models for all enrolled users. A user model consists of all templates of a specific user obtained during one or multiple enrollment sessions. In its most basic form, templates consist solely of the extracted features. More advanced user models store the parameters of the classifier used, for example statistical parameters in case of statistical classifiers, weights in case of neural networks, or the kernel's parameters and the soft margin parameter in the case of a support vector machine.
- Matching: During recognition, the extracted features are compared against one (verification) or multiple (identification) user models. The result is what is called a matching score for each user: a measure of similarity between the current features and each user model.
- Decision: A decision is made based on the matching score. Here, the validity of a user's claim to a specified identity is confirmed or denied in case of verification, or the identity is established in case of identification.

2.5 Performance measures

2.5.1 Decision error rates

The error rate is a particularly interesting factor when evaluating the quality of any given system. In case of biometric systems, the two most common errors that should be considered are the rate at which it falsely accepts an user/an impostor (false acceptance rate or FAR; also called a false match rate or false positive), and the rate at which it falsely rejects a genuine user (false reject rate or FRR; also called false non-match rate or false negative).

- **FRR:** Probability of falsely rejecting an original.
- **FAR:** Probability of falsely accepting an impostor.

A biometric system compares the features of the actual sample and a user model and calculates a matching score. The matching score is compared to a threshold to make a decision to accept or reject. In most systems, the decision threshold can be set by the system administrator. As a consequence, there is not a single FAR/FRR value, but a curve of FAR/FRR value pairs for certain threshold settings.

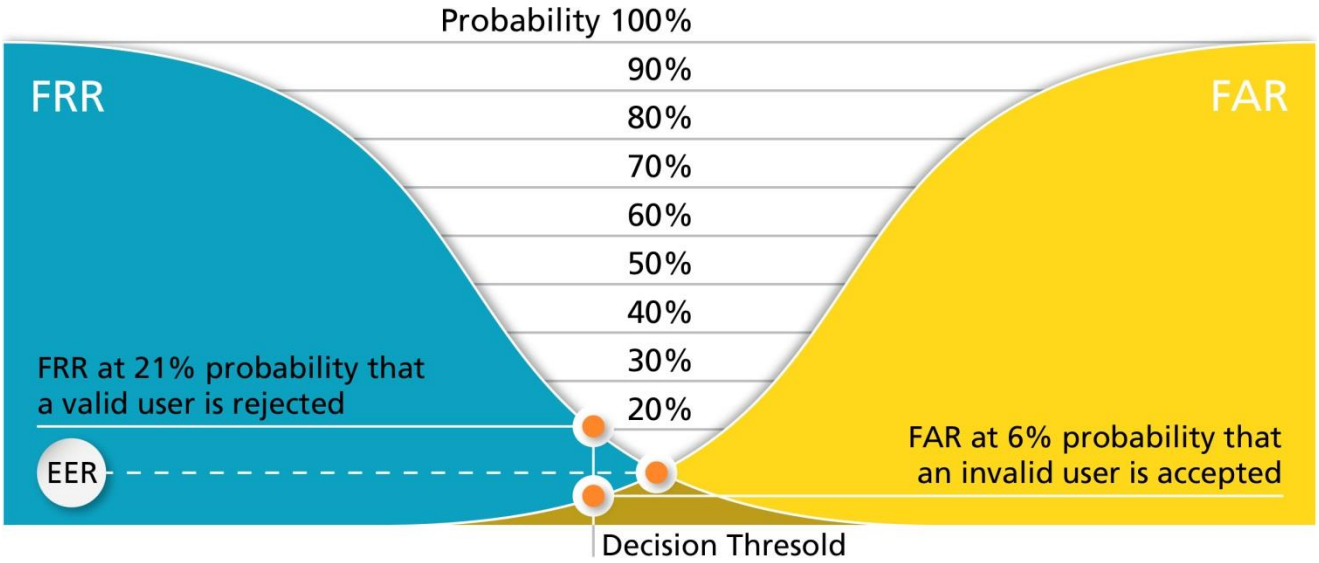


Figure 2: FAR and FRR in relation to the decision threshold

The administrator can choose to have a 'forgiving' system that will 'never' reject genuine attempts, or a high-security system that will 'never' accept anyone but the original user – at the expense that the original user might have to perform a number of attempts to get in.

The point where the FAR and FRR intercept is called the EER (equal error rate). This value is often used in short descriptions of biometric systems in place of FAR and FRR curves.

2.5.2 Other error rates

In addition to decision error rates, there are also two measures for acquisition errors:

- **FTA** (failure-to-acquire rate): Probability of sensor acquisition failures
- **FTE** (failure-to-enroll rate): Probability that a usable template cannot be generated for a user.

The ability-to-verify rate (ATV) is a measure of the system's overall effectiveness. It is a combination of the failure-to-enroll rate and false reject rate:

- **ATV** = (1-FTE)*(1-FRR)

The ATV rate represents the proportion of users which can use the biometric system without any difficulty on a daily basis. No system will have 100% ATV rate, but in general a higher ATV rate represents a more effective system.

3 History of biometrics at G+D

In 1998, G&D started to look at biometrics as a means to replace PIN use in cardholder authentication. The first working prototype was an ATM machine with biometric recognition presented at CeBIT in 1998. Shortly after, the first match-on-card algorithm was developed and released as a product in 2004.

Around the same time, the International Civil Aviation Organization (ICAO) specified requirements for biometric passports. G&D released a card operating system that supports biometrics according to the ICAO specifications in 2003.

The success of the smartphone changed the view on biometrics. It is now common to use a fingerprint sensor to unlock a phone. However, if truly reliable identification of a person is necessary, for example to open a bank account online, official identity documents must be integrated into the process. For this reason, G+D launched a virtual startup in 2017 with the purpose of implementing secure remote identification based on biometric facial recognition and ID cards.

4 Benefits of biometrics in identification and verification systems

As mentioned earlier, biometric systems can be classified as one of two large categories: verification or identification. This chapter presents the benefits of using biometrics in both processes alongside example use cases.

4.1 Verification

Biometric verification is the process of confirming a claimed identity through biometrics. The decision is therefore binary, answering the question: 'Based on the data presented – can it be

assumed that this subject is the rightful owner of the identity claimed?' Depending on the individual use case, this confirmation can be achieved by comparing the biometric trait presented by the subject to a template stored either locally or remotely.

4.1.1 Verification of locally stored identity claims

Biometrics can be used as a second test to confirm the claim of rightful ownership to a token (e.g. ID card or employee pass). This requires the identity token to contain both the personal information and a biometric template which can be read and verified against a live capture. This assures that the token itself is used by the rightful owner and cannot be passed on to someone else. This prevents misuse and can be applied in several different scenarios. For example, it can be used to implement access control in corporate environment. The owner presents their token to a scanner, which reads their personal data plus the associated access rights from the token. They also present one or more biometric traits to a scanner which then, depending on the implementation, are either matched to the token itself or verified on the system reading the data. This mitigates the risk of abuse through stolen or lost access tokens.

This type of biometric verification also has multiple advantages in border control scenarios. Comparing the biometric data stored on a passport to the actual person claiming the identity it represents can ascertain the rightful ownership of the document. This decreases the risk of travelers abusing forged passports. These comparisons can be conducted by autonomous systems with minimal supervision, allowing a reduction to the number of personnel required at border crossings. This both reduces costs and makes personnel available for other important tasks. Passengers also enjoy benefits ranging from faster processing time to easier, automated interactions without a language barrier.

4.1.2 Online authentication schemes using biometric verification

The most common authentication scheme for web services to date is still a combination of a username and a password. This approach has multiple drawbacks. Users or system administrators might disclose the password to an attacker carrying out a social engineering attack, or users may get tricked into using it on a forged website (phishing). Passwords may also be written down by the legitimate owner of an account, and therefore are prone to being lost or stolen. Biometric recognition systems help to address these problems, because the characteristics used in such systems are an inherent part of the person to be authenticated, and cannot be forgotten or lost (except via surgery, injury or rare medical conditions). Users have no control over the biometric comparison data, even though it is locally stored on their devices, which makes it impossible to disclose remotely through social engineering attacks or malicious

websites. The matching of biometric attributes happens on the device itself and is performed by hardware which is not easily accessible, even via manipulations to a phone's regular operating system. This approach protects both the user's template and helps to exclude external influences on the decision process, unless forging artificial biometric traits. Aside from these benefits from a corporate or service perspective, biometric recognition systems also offer advantages to the end users themselves. It is both convenient and fast to unlocking electronic devices such as phones, tablets or laptops using biometrics. Typing long passwords on a touchscreen is cumbersome, time-consuming, and error-prone, whereas modern sensors are fast and reliable.

4.1.3 Biometric verification against central databases

Another way to link an identity to biometrics is to store the template outside of the token itself. The subject presents the token to the system, which in turn reads the personal data contained within and starts the process of confirming the identity via biometrics. Depending on the implementation, the matching itself can be performed either directly on the system or in the backend where the template is stored. In both cases, the proper template is selected according to the personal data provided by the user. An example of such a system is the Schengen Visa Information System (VIS), which uses the number of the visa document or stamp in order to determine the right set of templates to compare against the passenger's live fingerprints. The inherent characteristics of the VIS mean the stored template can be considered highly reliable means to identify the rightful owner of the visa.

This approach can be taken to the extreme by using tokens based on something the user knows – e.g. an identification number not stored on any physical item, but rather provided to the subject by other means.

4.2 Identification

Biometrics are a natural fit for identification scenarios due to the very nature of the process. Much in the same way that people are able to distinguish individuals from one another based on aspects of their appearance, computers can use the people's inherent attributes for the same purpose. This allows the creation of systems and workflows which no longer depend on external proof of identity using some kind of token (e.g. ID card or employee pass), which are prone to being lost, stolen or forgotten. Biometrics remedy all these problems.

Businesses can use biometric identification to implement both physical and IT access control. Depending on the implementation, the same biometric trait could be used, for example, to

access a restricted area without providing any ID token (one-to-many) and as a second test to authenticate a domain account (one-to-one). Employees no longer have to carry tokens with them, nor do they have to remember their login credentials. Both factors have a huge impact on the total cost of ownership. Personalizing tokens for large scale businesses is costly both from a production perspective and, depending on the type of token, in terms of the time required to create them. Biometric enrolments are, in most cases, instantaneous.

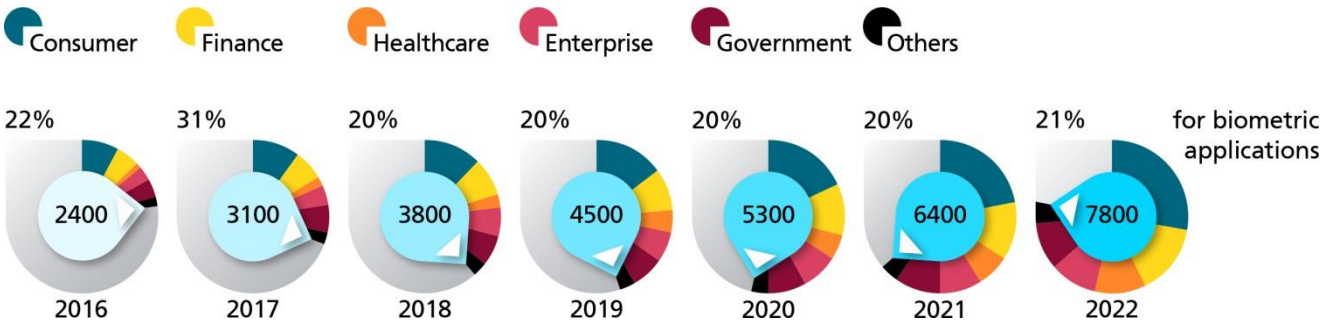
Identification systems can also be used to link biometrics to other parts of the identity, essentially eliminating the necessity to carry any kind of token in order to perform certain interactions, such as payments. This has the potential to dramatically improve convenience for the user. Aside from the benefits of not requiring the user to present a token, another benefit is that the physical presence of a user at the given time may even render traditional means of confirming transactions (for example PINs or TANs) obsolete.

For authorities, biometric identification may also provide information about individuals which could otherwise not be obtained. Their inherent unchangeability means identification schemes could be used to prevent social benefit fraud or allow the deduplication (identification and elimination) of multiple identities, even in cases where no other information is available.

Lastly, biometric identification can also be used in surveillance. Facial recognition or other suitable traits can be used to automatically identify subjects in video sequences. This drastically reduces the effort required for such tasks, thus allowing security forces to effectively monitor larger public or corporate spaces. This in turn allows more thorough coverage, which would not be possibly by other means due to the sheer quantity of data to be processed. An example application would be counter-terrorism, which heavily relies on tracking potential criminals in public spaces in order to prevent them from carrying out their attacks. When taking under consideration that such attacks often occur in crowded places, it is especially evident that automated systems offer substantial advantages over human investigators due to their ability to process a multitude of faces simultaneously. Similarly, automated systems do not suffer symptoms of fatigue during longer surveillance missions, which negatively effects the performance of humans performing the same tasks.

5 Market outlook

Market reports predict an average growth rate of 22% for biometric applications over the next 10 years. The majority of revenue will be generated in the consumer market.



Source (Tractica LLC 2017)

Figure 3: Market forecast in Mio US$

Strong merger and acquisition activities in biometrics-driven companies can be observed. Companies focusing on biometrics and biometric startups are frequent targets of acquisitions. Major security companies are actively broadening their portfolios.

6 Trends

6.1 Urbanization

The trend of urbanization will push the introduction of automated biometric surveillance systems required to maintain public order. An extreme example can be observed in China, where biometric surveillance systems are envisioned to enforce compliance and social behavior of citizens in its cities of the future. In this scenario, total surveillance based on facial recognition could lead to immediate prosecution of every illegal or anti-social behavior. Incidents could be recorded in a scoring system. If a person's score were to fall too low, the individual would have to pay fines or suffer other negative consequences. Positive social

behavior could increase a person's score. People with the highest scores would in this scenario be celebrated as role models.

6.2 Smart homes

Biometric identification is interesting in smart home environments because it makes it possible to control access and set personalized environmental conditions according to the preferences of the individuals present without any need for interaction.

6.3 Mobility

Car sharing introduces the challenge of automating identification of the driver and confirming the validity of their driving license. In public transport, biometrics could support the personalization of tickets, preventing abuse speeding up verification when used without tokens. This would also reduce costs since there would be no need for card or paper tickets.

6.4 Payment

Most current payment systems still require the use of a token, such as smartphone or credit/debit card. There is constant demand to accelerate payment processes. Biometric identification could eliminate the need for tokens, further increasing the speed and convenience of transactions.

6.5 Online authentication

Online authentication processes are increasingly moving away from secret-based systems, e.g. PINs, passwords and TANs, in favor of biometric authentication.

6.6 Anti-spoofing

The rising adoption of biometric authentication systems has led to a parallel increase in spoofing attempts. There will be a trend to develop more advanced sensors or systems to counter that threat.

6.7 Miniaturization of sensors

The ongoing trend in mobile devices, IOT, embedded technologies, and smart gadgets will further drive the miniaturization of sensors.

6.8 Promising biometric characteristics

The current boom in biometric solutions is accompanied by research into new biometric characteristics that might have promising applications in identification or verification scenarios. Several aspects have to be considered when evaluating biological and behavioral biometric characteristics. Inherent requirements that must be met by biometric characteristics are:

- **Uniqueness/Entropy:** Uniqueness: The characteristic should be unique for every person
- **Universality:** Everyone should have the biometric characteristic
- **Permanence:** The characteristic should not change over time
- **Measurability:** It should be easy to acquire and measure the characteristic

In addition to the four characteristics listed above, several aspects dependent on the respective use case must also be taken into account when analyzing new biometric characteristics or solutions. Three additional factors have to be considered:

- **Performance:** The speed, accuracy (e.g. error rates), and robustness of technologies based on a characteristic
- **Acceptance:** The degree to which people accept a given choice of biometric characteristic and their willingness to be measured
- **Circumvention:** The ease with which a characteristic might be spoofed

The availability of certain sensors, the maximum space available for the sensor, the nature of the environment for the specific use case (e.g. lightning conditions, humidity, user access to the sensor) are also factors for consideration when evaluating the appropriateness of a biometric characteristic for a given use. For example, the sensors required to analyze gait are widely available (cameras), and systems based around this biometric characteristic do not demand physical contact (hygienic). However, gait analysis is characterized by low precision and a high dependence on environmental circumstances (e.g. street conditions). For these reasons, an iris scan may be more appropriate in many use cases. Iris scans offer a high degree of uniqueness, supporting systems do not demand physical contact, while the required cameras are widely available but do have to be equipped with infrared lights.

Last but not least, it is important to emphasize that biometrics are not always the most preferable solution for identification/verification systems. The necessary shift of liability from user to provider, the level of security offered by existing non-biometric solutions, or the estimated costs to implement a biometric system can lead decision-makers to decide against such a system.

6.9 Artificial intelligence

Artificial intelligence (AI) usually refers to machines or computer algorithms that demonstrate something comparable to elements of human intelligence. Artificial intelligence comprises many different areas of research, including machine learning, robotics, and natural language processing. Machine learning and pattern recognition techniques are the most promising areas of AI in relation to biometrics.

6.9.1 History

The term AI dates back to the summer of 1956, when scientists and mathematicians came together at Dartmouth College in Hanover, New Hampshire, for a "study of artificial intelligence" (McCarthy, et al. 1955). Referred to as the Dartmouth Workshop, the event is considered the birth of artificial intelligence (AI). Since then, artificial intelligence has experienced various ups and downs. Around ten years ago, deep learning became possible, a concept already proposed in 1998. This led to the current boom in artificial intelligence and applications based around deep learning are now found nearly everywhere: from speech assistants to driverless cars and preventive healthcare – deep learning has left its mark on nearly every field. The main factors that led to the breakthrough in deep learning are the availability of huge amounts of (training) data (commonly referred to as big data), the ever-increasing general computing power, and the use of GPUs (graphics processing units).

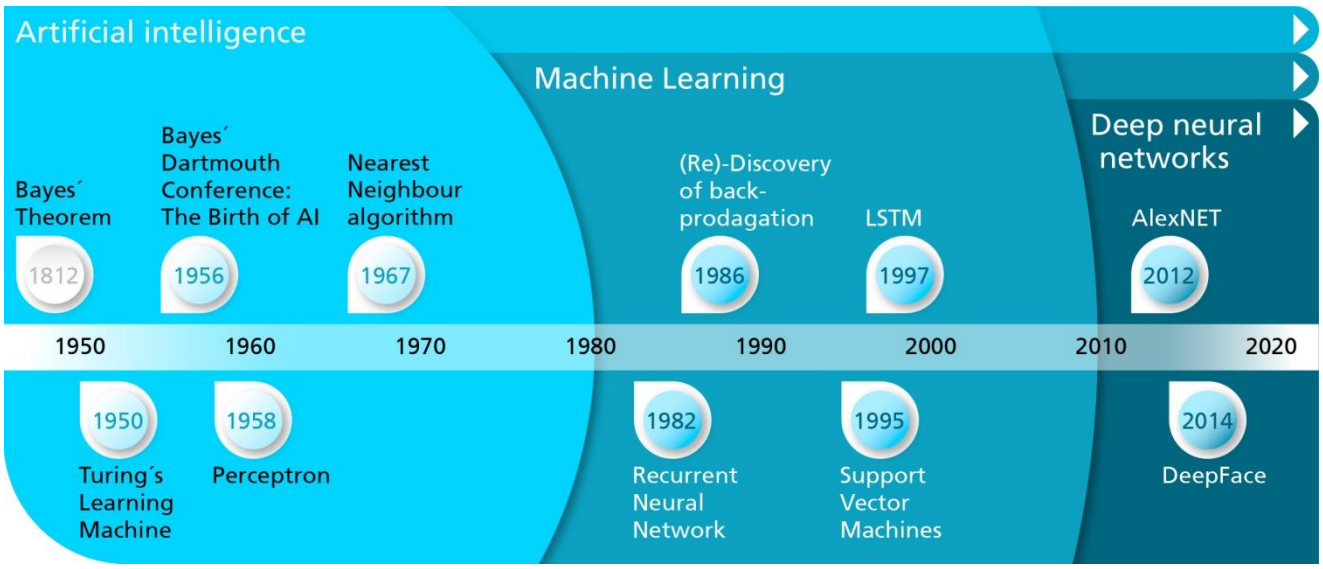


Figure 4: History of artificial intelligence

6.9.2 Deep neural networks

Artificial neural networks (ANNs) try to mimic the biological neural networks which make up human brains. They consist of a collection of connected units called artificial neurons, arranged in two or more layers. Each neuron has a number of inputs quantified based on individual weights. The weighted inputs are added together and then processed by an activation function (e.g. a non-linear threshold function). The output is propagated to all neurons of the next layer.

Learning takes place by presenting a big number of training samples to the network input layer. The network processes each input and the result is compared to the correct (expected) result for that input. Then the weights are modified to slightly reduce the difference between the network result and the correct result (gradient descent approach). The amount of reduction is determined by what is called the learning rate (which must be smaller than 1). After a certain amount of training time and samples, the difference at the output is minimized and the network stabilizes. It can then be used to process unseen (test-) samples.

Deep neural networks (DNNs) are artificial neural networks with *multiple* hidden layers between the input and output. Each of the hidden layers perform a different task: convolutional layers filter their input, activation layers introduce nonlinearities to the system, and pooling layers reduce the spatial dimension (and therefore the number of parameters) and control overfitting. Training a deep neural network requires a huge amount of data. For example, ImageNet, a popular database for training convolutional neural networks (CNNs),

contains more than 14 million labeled images from more than 22,000 categories (Stanford Vision Lab 2017). Accordingly, the training of a deep neural network on such a huge dataset (deep learning) takes a long time, usually several days.

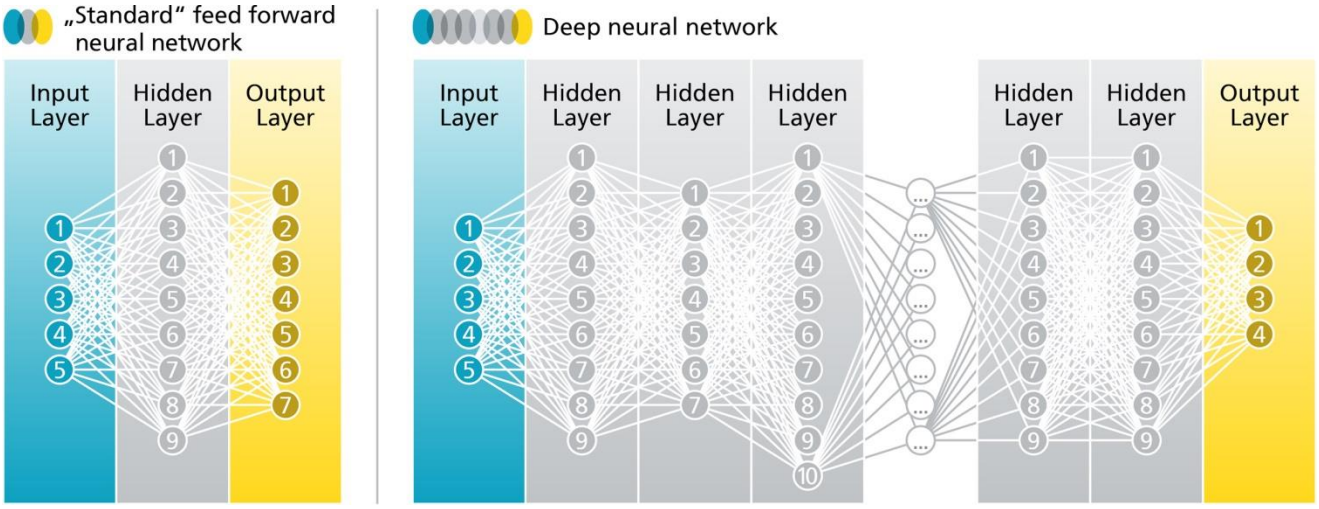


Figure 5: Standard neural network and deep neural network

Dramatic improvements in computing power and the amount of data available have made deep neural networks an increasingly interesting method for extracting features in biometric systems. At the time of writing, the top-rated face recognition algorithms are based on deep neural networks. The straightforward implementation compared to other approaches makes it very likely that deep neural networks will continue to be the preferred method for extracting features in the years to come, disrupting the market for biometric algorithms.

6.10 Legal regulations

In recent years there have been increasing debates on the ethical and societal consequences of using biometrics, and especially the building of large biometric databases. There are three main areas of concern:

1. Biometric data could be abused by oppressive regimes
2. Proliferation could render biometrics useless in forensic investigations
3. Stolen biometric data could be used to enable identity theft

Regulations on biometrics are usually integrated into data protection laws. Looking at trends across different jurisdictions, we can see that the number of new regulative acts concerning the use of biometrics have increased significantly over recent years. Activity has been concentrated in well-developed countries where the digitization of processes is increasing apace and the collection of biometrics for identity verification is becoming increasingly commonplace. In less developed countries, the use of biometrics mostly concerns the registration of the population, elections, and fighting corruption. DLA Piper presented the degree of data protection legislation around the world in the following map:

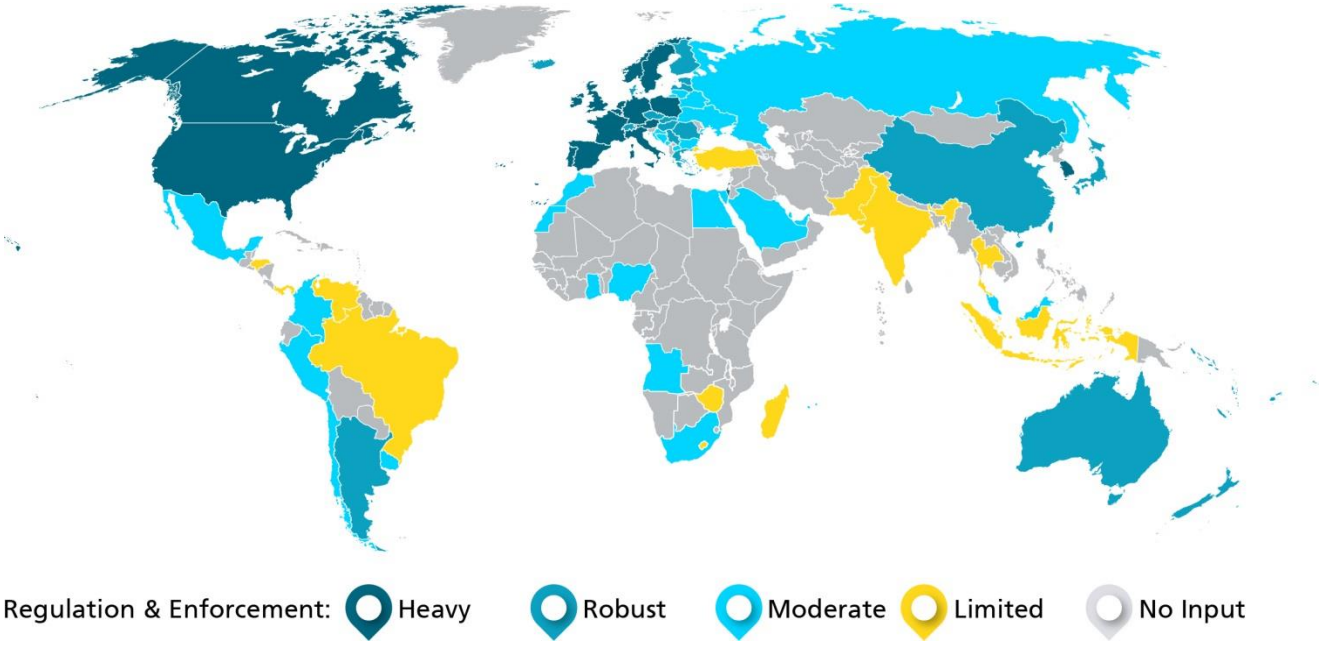


Figure 6: World map of data protection (DLA Piper n.d.)

According to (DLA Piper 2017), 91 countries have enacted or are currently in the process of enacting data protection legislation.

The strongest regulation to date is the EU General Data Protection Regulation (GDPR), which became effective on May 28, 2018.

In the United States, the collection and use of personal data in general and specifically biometric data is not comprehensively regulated by federal law. Instead, this is covered by a mix of federal and state laws and regulations that sometimes overlap or contradict one another.

Most states currently allow the identification of an individual using images taken without consent while they are in public.

7 Proliferation of biometric data

In countries with pre-existing well-developed identity management systems, the proliferation of biometric data is mainly driven by convenience and public security. By contrast, in developing countries, where identity management systems are either unreliable or non-existent, the proliferation is mainly driven by the need for credible population management solutions.

While the proliferation of biometric data in the first case typically drives the storage of biometric data in millions of connected devices and/or connected small systems, the latter case typically drives the storage of a huge amount of biometric data within a single central database.

A prime example of a centrally stored biometric database is India's Unique ID program, where more than a billion citizens are biometrically registered in a single national database. Similar databases have been established in many African, Asian, and Latin American countries to support the modernization of civil services and citizen rights.

Today, biometrics is emerging as a promising solution in multiple areas, including mobile payments, online banking, immigration and border control, workplace access management, healthcare and welfare, retail, wearables, surveillance, and access management for clubs and associations. However, it remains unclear whether biometrics will be universally used as authentication for physical and logical access control. Bojan Cukic, a professor at West Virginia University, said: "In five to ten years, we will not be talking about biometrics because it will be ubiquitous. It will be part of systems and applications which we use every day and we may or may not be aware that it is improving the security of these systems. Computers will monitor our activities and when they become unusual, they will warn us or warn the administrator about it." (Griffin 2012)

Biometric solutions that can continuously learn new biometric patterns and associate data from different data sets are allowing systems to combine information, such as fingerprints, voice, gait, facial features, behavioral patterns, emotions, interests, habits, and routines. This means that psychological, behavioral, and even health data will be combined to develop future biometric systems. This naturally creates huge concerns in terms of how this information can be used against the subjects and for commercial purposes.

Recent history shows that leaked private information has repeatedly been used against individuals and even against society as a whole. Thus, the growing usage and interlinkage of biometric information calls for proper understanding of the technology and its underlying challenges, e.g.:

- Psychological and cultural challenges
- System and technological challenges

8 Challenges relating to the use of biometric systems

Over recent years, we have witnessed a surge in the use of biometrics for logical and physical access control. Many mobile device manufacturers have already adopted biometrics as a tool to unlock their devices. In these use cases, the primary motivation for using biometrics is convenience.

We believe that the success of biometric systems comes hand in hand with their ability to ward off attacks and detect security vulnerabilities.

The biggest vulnerability in biometric systems is that, unlike passwords or pins, biometric information cannot be changed, as it is part of who the person is, and there can only be one biometric. Therefore, the credibility and further development of any individual biometric system or the technology in general will depend on whether it can protect itself from underlying vulnerabilities.

Biometric vulnerabilities can be classified into three categories:

- intrinsic or inherent vulnerabilities
- vulnerabilities due to biometric overtness
- vulnerabilities due to non-secure infrastructure and breaches at the administrative level

Several studies have been conducted to analyze these vulnerabilities and propose methods to address them. A systematic overview of the challenges and related potential solutions is provided in particular detail in Jain, Nandakumar and Nagar 2007,. The diagram below summarizes the attacks that could potentially target the different vulnerabilities of biometric systems.

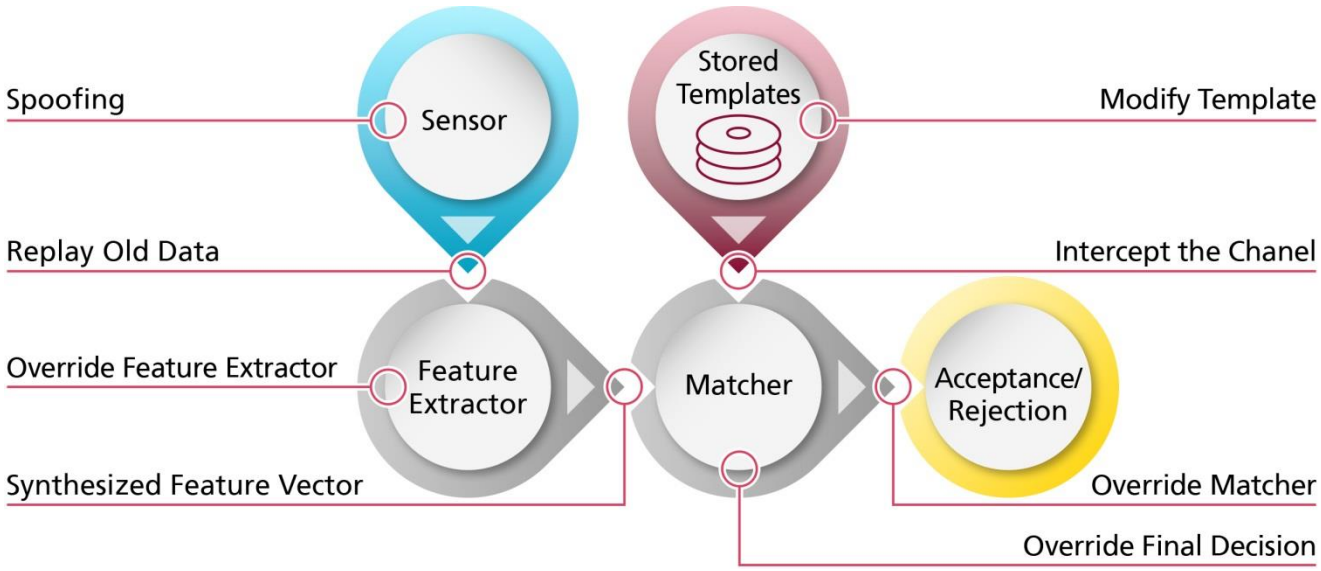


Figure 7: Potential attacks exploiting the vulnerabilities of biometric systems

8.1 Intrinsic vulnerabilities

Intrinsic vulnerabilities refer to inherent characteristics of biometric systems that can lead the biometric system to fail even without an explicit effort from an attacker to circumvent the system. Examples of intrinsic vulnerabilities include false acceptances and false rejections.

Generally speaking, one has to accept the intrinsic vulnerabilities of biometric systems and always take these into consideration when designing systems. The solutions to these weaknesses are evolutionary and need to be looked at from a holistic perspective. Better sensors, robust algorithms, and multi-biometric systems are all part of the solution.

8.2 Non-secure infrastructure and insider attacks

Non-secure infrastructure and insider attacks refer to vulnerabilities that result in data breaches during data processing, transmission, and storage. It is a similar challenge to those faced by any sensitive IT systems, and therefore must be tackled as such. Nevertheless, unlike many secure access control systems where compromised access data can be revoked, biometric traits cannot be replaced at will.

8.3 Spoofing

Of the many ways to attack a biometric system (see Figure 7), attacking the sensor is biometric-specific: The attacker tries to infiltrate a fake biometric sample into the system. The purpose is either to avoid recognition (false negative), or to masquerade as another person (false positive). The latter attack is known as spoofing. As long as biometric systems are in use, there will always be spoofing attacks, just as there will always be attacks on other IT systems.

Ever since the proliferation of biometrics began, many research groups and hackers have been trying to challenge new systems to show the world the limitations of biometrics and push companies to further enhance the security measures used in authentication systems. In recent months, many successful spoofing attacks to biometric systems have come to light – including the attack on Apples Face ID system in November 2017, or the one on the Samsung Galaxy S8 iris scanner, just to name the most well-known examples. This is also based on the fact that successful spoofing attacks are sure to receive high public attention (whereas false non-matches are of no public interest).

As it happens, the successful spoofing attacks revealed to date have turned out in practice to not have been as simple as they might have seemed on first sight (e.g. obtaining a high-resolution image of the iris of an unknown owner of a found smartphone), and many attacks were only possible with the active help of the spoofed party. Nevertheless, biometric traits are not secret, and these attacks show that spoofing is possible in principle. Also, as the images show, using a mask of someone else's face in a public environment would be quite startling, to say the least. Based on current spoofing technologies, only a fingerprint mask could be used discreetly in a public setting. Thus, spoofing attacks are more likely to happen to unattended biometric systems than in a public environment such as access control for a building.

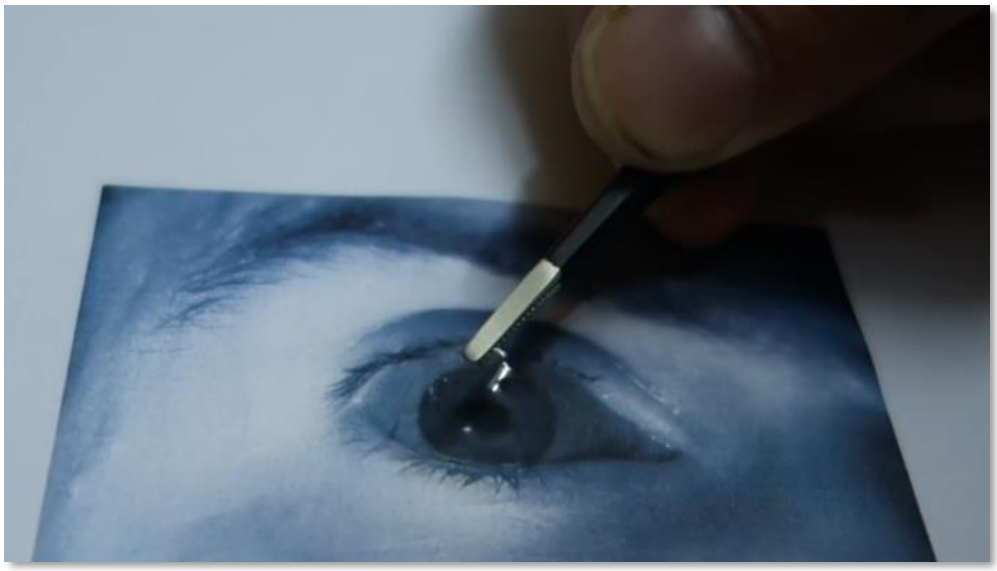


Figure 8: Spoofing the iris recognition of a Samsung Galaxy S8 Smartphone with a printout of the iris and a contact lens. (Chaos Computer Club e.V. 2017)

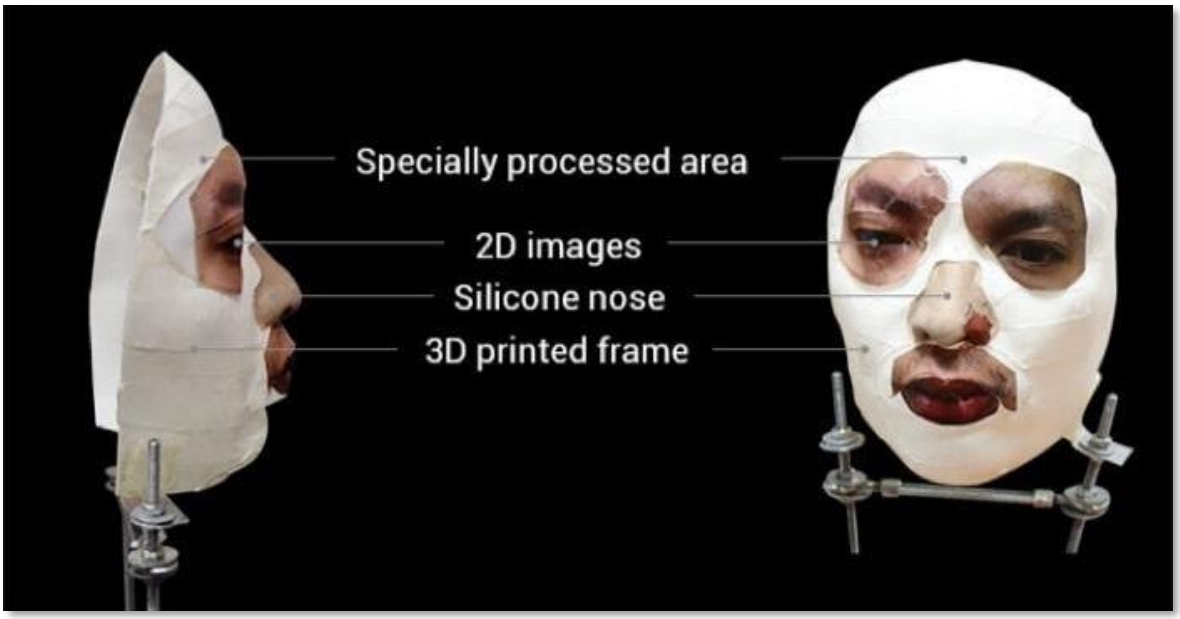


Figure 9: The three dimensional mask used for spoofing Apple's Face ID face recognition software. (© Bkav Corporation 2017)

The consideration of certain factors when designing a biometric system can make such attacks harder to accomplish. The art of distinguishing a genuine biometric characteristic of a living human being from some form of artificial replica is known as spoof or liveness detection. Liveness detection methods vary in maturity and cost, or rather, cost-effectiveness. They can be categorized into a number of different approaches:

- Set up algorithms to only use data already collected via biometric recognition
- Use additional hardware and associated software designed for liveness detection
- Use multi-biometric-systems
- Use a risk management system that contributes additional available information (e.g. location, default user behavior).
- Monitor the recognition process (e.g. border control)

Additional security measures should always be evaluated according to their impact on user convenience and the error rates of the respective biometric system.

9 Privacy and template protection

9.1 Privacy

Privacy means "someone's right to keep their personal matters and relationships secret" (Cambridge University Press 2017).

Biometric data contains identifiable personal information acquired from individuals, which raises privacy concerns. Some of the questions that arise in relation to the use of biometrics include (Jain, Flynn und Ross 2008):

- Will biometrics be used to covertly track people?
- Will the biometric data be used for purposes other than those for which it was originally acquired?
- Can a person's health status be deduced from raw biometric data?
- Will various biometric databases be linked to create a detailed profile of an individual?
- What happens when stored biometric templates are compromised?

These concerns lie at the core of many objections to the use of biometrics. There are some technical measures and codes of practice to address these legitimate concerns and to protect personal data. For example, biometric templates can be stored and processed on personal smartcards instead of a central database. Template protection allows the canceling of a

biometric enrollment and ensures that compromising the templates is ineffective. But, as stated by Jain, Flynn und Ross (2008): "government regulations are required in order to prevent the inappropriate transmission, exchange and processing of biometric data."

9.2 Template Protection

Overview

Biometric templates contain true personal information and the subject cannot change their biometric characteristics. Therefore, gaining access to the templates is one of the most potentially damaging attacks on a biometric system and can result in the following threats:

- The template can be replaced to gain unauthorized access
- The template can be used to create a physical spoof
- The template could be misused for purposes other than the intended purpose

In contrast to PINs and passwords, which can be changed if they are compromised, biometric features cannot be altered. Biometric templates should therefore be protected where they are stored. A common solution is to transform the raw template into a secure template, which should meet the following privacy requirements as defined by the ISO/IEC 24745 standard:

- Irreversibility: To prevent the use of biometric data for any purpose other than originally intended, biometric data shall be processed by irreversible transforms before storage
- Unlinkability: The stored biometric references should not be linkable across applications or databases
- Confidentiality: To protect biometric references against access by an unauthorized entity resulting in a privacy risk, biometric references shall be kept confidential

Further, there needs to be the capacity to revoke/renew a compromised biometric template without necessarily revoking the underlying biometric characteristic.

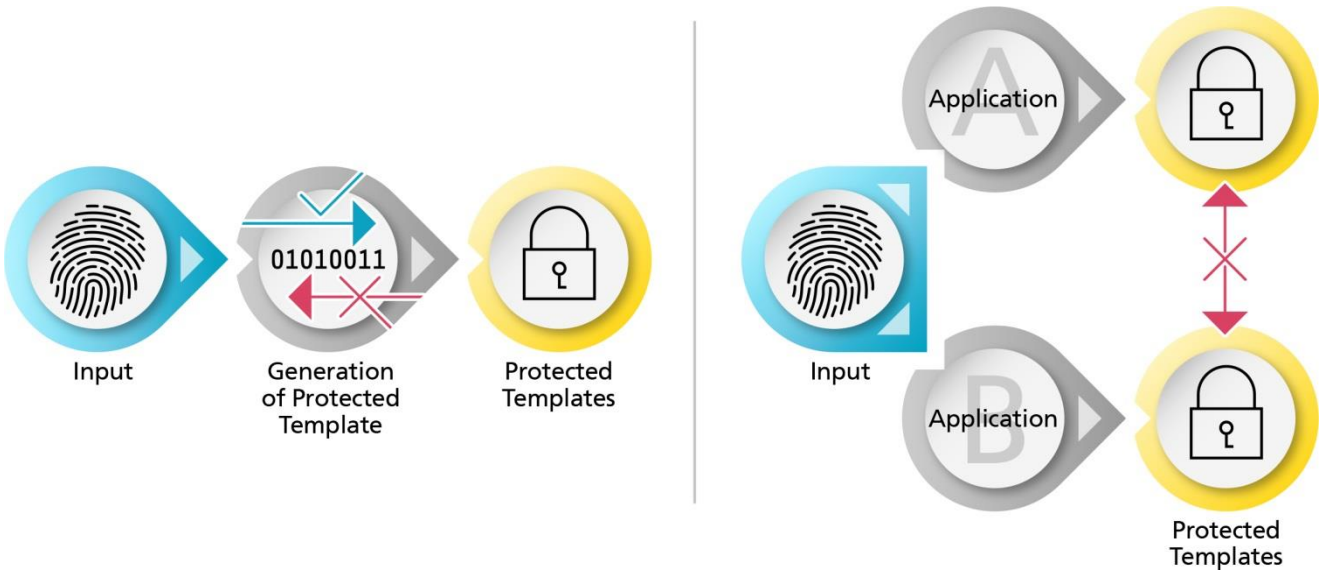


Figure 10: Irreversibility (left) and unlinkability (right)

Approaches to protecting templates can be classified into the following categories (Jain, Nandakumar and Nagar 2007):

- Cancelable biometrics (also referred to as feature transformation)
  - Salting (e.g. encryption)
  - Non-invertible transformation
- Biometric cryptosystems
  - Key-binding biometric cryptosystem
  - Key-generating biometric cryptosystem

In the case of cancelable biometrics, biometric features are transformed based on intentional, repeatable distortions. The biometric templates are then compared in the transformed domain:

- In salting, the challenge is that a secret key must be stored for each biometric record. The implication is that when the key is lost, the biometric trait will be lost – and if the key is known, the original biometric features can be reconstructed. Therefore, this approach cannot be considered a true template protection solution.
- In non-invertible transformation, the biometric data undergoes a noninvertible transformation selected via a secret key from a pool of such transformations. While this seems like a secure solution, the challenge is that a large number of user-dependent transformation functions must be implemented, making the solution unrealistically

complex, or a universal application-related key, which would mean that loss of that key would critically compromise the entire system.

Strictly speaking, only the key-binding biometric cryptosystem and the key-generation cryptosystem can be considered cryptographically sound template protection algorithms:

- Key-binding systems bind a cryptographic key to the biometric template. The result is referred to as helper data. The helper data is subsequently used in conjunction with very similar biometric data to recreate the key.
- Key-generation systems use biometric data to generate a cryptographic key. The key generation is normally dependent on particular parameter settings. Different parameters result in different keys.

Both forms of biometric cryptosystems involve producing a biometric comparison indirectly by comparing the cryptographic keys, resulting in a binary yes/no result without setting any thresholds. Error correction, quantization and so on must be applied to account for the intrinsic variance between biometric features.

However, the main challenge in the use of biometric cryptosystems is the loss of discretionary control due to the underlying error correction schemes.

10 The G+D Group's role in biometrics

The G+D Group has a long history in securing identities, and biometrics has become an important tool to achieve this.

Veridos is building biometric databases for governments all over the world to prevent the acquisition of multiple identities that can be used to commit fraud, corruption and organized crime. We provide all components alongside expertise to create complete custom biometric solutions. As an example of our work, Veridos and secunet are supporting border control agencies with the introduction of automated border control systems based on biometric recognition technologies. These will improve accuracy, speed, and convenience at check points. secunet is consulting governments and private companies on how to successfully implement biometric technologies and supporting related standardization activities. Both companies are involved in active research into the application and security of future biometric systems. Mobile Security provides components and solutions to private businesses, such as financial institutions or mobile network operators, to secure access to privileged systems for customers and employees. Biometric authentication is an important part of these solutions.

Biometric technology has great potential to improve public safety and convenience in the years to come. But for this to be realized, special care must be taken to ensure the security of biometric systems to prevent the abuse of the sensitive data that is naturally generated with the use of the technology.

The G+D Group is a renowned trusted and reliable expert in the field of data security with experience dating back more than 165 years. We have a proven track record of successful projects and long-lasting close partnerships with governments, central banks and private companies all over the world. This experience, our holistic approach to the secure handling of data, and our expertise in secure tokens puts us in a uniquely strong position to designing and secure effective biometric systems.

11 References

© Bkav Corporation. *Bkav's new mask beats Face ID in "twin way": Severity level raised, do not use Face ID in business transactions.* November 27, 2017. http://www.bkav.com/d/top-news/-/view_content/content/103968/bkav%EF%BF%BDs-new-mask-beats-face-id-in-twin-way-severity-level-raised-do-not-use-face-id-in-business-transactions (accessed December 20, 2017).

Busch, Christoph. *Harmonized Biometric Vocabulary.* n.d. http://www.christoph-busch.de/standards.html (accessed November 23, 2017).

Cambridge University Press. *Cambridge Dictonary.* n.d. https://dictionary.cambridge.org/ (accessed November 28, 2017).

Chaos Computer Club e.V. *Hacking the Samsung Galaxy S8 Irisscanner.* May 23, 2017. https://media.ccc.de/v/biometrie-s8-iris-en (accessed December 22, 2017).

DLA Piper. "DATA PROTECTION LAWS OF THE WORLD; Full Handbook." n.d. https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country=all (accessed October 10, 2017).

Griffin, Joel. *Security Info Watch.* 13. July 2012. http://www.securityinfowatch.com/blog/10742129/the-proliferation-of-biometrics (accessed December 22, 2017).

Jain, Anil K. (Editor); Flynn, Patrick (Editor); Ross, Arun A. (Editor). *Handbook of Biometrics.* New York: Springer, 2008.

Jain, Anil K.; Nandakumar, Karthik; Nagar, Abhishek. "Biometric Template Security." *EURASIP Journal on Advances in Signal Processing*, December 4, 2007.

Kissel, Richard (Editor). *Glossary of Key Information Security Terms.* Gaithersburg: National Institute of Standards and Technology, 2013.

McCarthy, John; Minsky, Marvin L., Rochester, Nathaniel; Shannon, Claude E.. "A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence." Dartmouth, 1955.

O'Leary, Dave. *IT World Canada.* October 03, 2016. https://www.itworldcanada.com/blog/the-present-and-future-of-ai-and-deep-learning-featuring-professor-jurgen-schmidhuber/386551 (accessed October 24, 2017).

Stanford Vision Lab. *Summary and Statistics (updated on April 30, 2010).* April 30, 2010. http://www.image-net.org/about-stats (accessed October 24, 2017).

Tractica LLC. *Biometrics Market Forecasts, Global Unit Shipments and Revenue by Biometric, Modality, Technology, Use Case, Industry Segment and World Region: 2016-2025.* Marekt Analysis, Boulder, CO: Tractica LLC, 2017.

Wang, Yilun; Kosinski, Michal. "Deep Neural Networks Can Detect Sexual Orientation From Faces." *Journal of Personality and Social Psychology*, September 7, 2017.