FINGERPRINTS

BIOMETRIC TECHNOLOGIES

FINGERPRINTS WHITE PAPER, *2020*

CONTENT

1 Introduction ... 3
2 Biometric Authentiction ... 4
2.1 User Authentication and Identification ... 4
2.2 Authentication Factors ... 4
2.3 Security and Convenience ... 5
2.3.1 False Acceptance Rate (FAR) ... 6
2.3.2 False Rejection Rate (FRR) ... 6
3 Biometric Technologies ... 8
3.1 Biometric Identifiers and Biometric Systems ... 8
3.2 Fingerprint Recognition ... 9
3.3 Eye Recognition ... 10
3.3.1 Retina ... 10
3.3.2 Iris ... 11
3.3.3 Scleral Vein (Eyeprint) ... 11
3.4 Face Recognition ... 12
3.5 Voice Recognition ... 12
3.6 Vein Recognition ... 12
3.7 Behavioral Biometrics: Gait and Gesture Recognition ... 13
3.8 Comparing Biometric Technologies ... 14
4 Fingerprint Recognition ... 15
4.1 The Fingerprint ... 16
4.2 Fingerprint Sensors ... 17
4.2.1 Optical Sensors ... 18
4.2.2 Capacitive Sensors ... 19
4.2.3 Ultrasonic Sensors ... 23
4.2.4 Thermal and Active Thermal Sensors ... 23
4.2.5 Pressure Sensitive Sensors ... 24
4.3 Comparing Fingerprint Sensor Technologies ... 25
4.3.1 Image quality and Resolution ... 25
4.3.2 Speed ... 25
4.3.3 Power Consumption ... 26
4.3.4 Size ... 26
4.3.5 Cost ... 27
4.3.6 Packaging and other Design Options ... 27
4.3.7 Security and Convenience ... 27
4.3.8 Conclusions ... 28
4.4 Fingerprint Extraction and Matching ... 29
4.4.1 Preprocessing, Feature Extraction and Template ... 29
4.4.2 Matching ... 30
4.4.3 Biometric Processors ... 31
5 Summary ... 32

1. INTRODUCTION

Fingerprint recognition enables an easy to use, reliable and cost efficient way to authenticate an individual. The advantages of the technology have already led to the wide spread use of fingerprint sensors in mobile devices such as smartphones and tablets. But the future holds many more attractive applications of biometrics and fingerprint recognition, for example in payments, access, automotive, wearables and home appliances.

This white paper ***Biometric Technologies*** has been written by Fingerprints™ to help device makers, customers, partners and anyone else who needs a better understanding of the biometric world. The contents draw on the extensive experience of biometric systems within Fingerprints™ and has its focus on fingerprint recognition, being the dominant biometric technology used for authentication and identification. This white paper deals with authentication and identification in general, the various biometric modalities currently used for authentication and includes a detailed explanation of fingerprint recognition.

Biometric Technologies can be read from start to end for those wanting an overview of the whole biometrics field, but also used as a reference, thanks to the index at the back.

All statements and information in this white paper are believed to be accurate at the time being but are presented without warranty of any kind.

2. BIOMETRIC AUTHENTICATION

Our lives are filled with situations where you need to prove who you are; may it be for personal reasons or as part of your profession. Locks are to be opened, e-mail accounts are to be accessed and purchases are to be made – but only by the person correctly authorized to do so. It is not hard to list a wide range of activities, including everything from bank transactions to starting your car, that require fast, reliable and convenient authentication of the user. Thus, identification and authentication of us as individuals have become a cornerstone in today's society, enabling secure interactions while preventing fraud and criminality.

Figure 1. Who are you?

2.1 User Authentication and Identification

To prove your identity, you need to prove that you are the person you claim to be. The process of verifying that an identity claim is true is formally referred to as ***user authentication****, and if the process is more or less automated we have created an automated authentication system. Given the demand for speed and convenience today, ***automated user authentication*** is a given requirement in many applications, for example when opening your phone or logging in to your email.

A related process is user identification, the act of determining the identity of a person. Identification selects one individual out of many in a given population, but the term does not normally imply verification of that persons claimed identity, essential for ***user authentication.*** While user authentication implies a one-to-one relationship ("I am the one I claim to be.") identification is a many-to-one mapping ("I am Mr. X in the US population."). Just as authentication can be automated there are many examples of automated identification systems in use, for example by the police scanning for suspects.

2.2 Authentication Factors

The ways in which someone can be authenticated may be grouped in three basic categories, based on what are known as the factors of authentication: something the user ***knows***, something the user ***has***, or something the user ***is***. Each ***authentication factor*** covers a range of elements used to authenticate or verify a person's identity prior to being granted access, approving a transaction request, signing a document, granting authority to others, etc.

INHERENCE

Something the user is or does, for example a fingerprint, signature, voice etc. Biometric authentication leverages various inherence factors to validate the identity of a user.

OWNERSHIP

Something the user has, for example an ID-card, security token, mobile phone, physical key etc.

KNOWLEDGE

Something the user knows and hopefully remembers, such as a password, PIN-code, answer to a security question etc.

* From the Greek word for "real, genuine"

A complete authorization process may include more than one of the above factors since security research has determined that for a positive authentication, elements from at least two, and preferably all three, categories should be verified. This is then referred to as two-factor and multi-factor authentication respectively. It is of course also possible to use several factors from the same category, such as a PIN-code and a security question, but that will not give the same extended level of security as "true" multi-factor authentication.

We can now define what we mean by biometric authentication a bit more formally:

Biometric authentication – The automated use of behavioral and physiological characteristics to verify someone's identity.

When comparing biometric authentication with other authentication factors, several aspects come into play. Authentication based on knowledge factors, e.g. a password, is technically easy to implement in software but also relatively easy to break with computerized algorithms or by spyware in the user's device. Also, users tend to select simple and common passwords, even sharing them with others and thus making reliable authentication impossible.

Authentication based on ownership factors is generally more safe but relies upon a physical key/card/phone etc. that may be stolen, lost or just forgotten at home when needed. There is also a cost related to the manufacture of any dedicated physical device for ownership authentication.

With correctly implemented biometric authentication the information used is unique for each individual, always stays with the individual, and normally stays invariant over time. These are key advantages making biometric authentication the preferred authentication factor in many applications. On the other hand, there are convenience and social acceptability aspects relating to biometric authentication that must be considered. Also, depending on type of biometrics used, the cost, size and power requirements of the sensor and the processing logic may be a potential drawback.

2.3 Security and Convenience

Security is obviously one of the most fundamental factors to discuss when comparing biometric authentication systems. As always, there is a tradeoff between high security and user convenience which needs to be considered. Assessing a system's security does not stop with how well the biometric identifier can be read and matched. We also have to include possible illegal access to the processing engine – hacking – and if it can be fooled by someone simulating the biometric identifier – spoofing.

As an example of an anti-hacking measure used in today's modern consumer devices, a mathematical representation of the fingerprint is stored as a template, instead of the image itself. Storing the representation reduces hacking risks, since it cannot be used to re-create the original fingerprint image. Furthermore, the template is not stored just anywhere on the device. In mobile devices, the template is stored, and the algorithms involved in the authentication process are run in a Trusted Execution Environment (TEE). This further enhances security as it keeps the biometric data, as well as the processes, away from potential hackers and viruses.

Similarly, payment cards are equipped with a Secure Element, i.e. a chip that offers a dynamic environment to store, process and communicate biometric information securely. If you try to tamper with the chip in any way, it may self-destruct, but will not allow you to gain unauthorized access.

Spoofing involves the forgery of faces, voices, fingerprints etc. in an attempt to authenticate fraudulently. Many advanced technologies have been developed to minimize the risk of spoofing. In fingerprint recognition, for example, spoofing risks can be reduced by increasing the image quality and by using sophisticated matching algorithms. Additional security can be achieved by various anti-spoofing schemes and use of more than one biometric identifier to authenticate the user.

No system can be made absolutely secure – with unlimited time (and money) you can hack and spoof anything. Liveness detection and other advanced biometric techniques however makes such malicious attacks extremely expensive.

To properly quantify the security and convenience characteristics for different biometric systems we need a general model of how such systems work and a set of appropriate metrics to use. Hence, this section also defines some of the general metrics used in the industry of biometric authentication systems.

All biometric authentication systems are designed to perform the following general operations:

- **Data capture** – A sensor of some kind captures data from the biometric identifier used.
- **Enrollment** – The captured data is analyzed and its unique features are stored as a digital template.
- **Authentication** – When the enrolled user wants to authenticate himself/herself, his/her biometric data is captured once again and compared against the template generated by the enrollment.
- **Matching** – An algorithm is used to compare if there is a match between the stored template or not. If there is a match the user has been authenticated, otherwise access is denied.

2.3.1 FALSE ACCEPTANCE RATE (FAR)

A metric frequently used in assessing the security of biometric systems is the ***False Acceptance Rate, FAR*** (sometimes called FMR, False Match Rate). The FAR number tells you how often the sensor will statistically provide a positive match without the right biometric data. The FAR ratio is dependent on the hardware as well as the software (algorithm) of the sensor system. The typical FAR of the fingerprint sensors that are used in today's smartphones is somewhere around 1/100,000, which essentially means that if you let randomly selected persons try to log into your phone using the fingerprint sensor, on average, one in 100,000 persons would succeed.

2.3.2 FALSE REJECTION RATE (FRR)

A metric often used to gauge the convenience of biometric sensors is the sensor's ***False Rejection Rate, FRR*** (also called FNMR, False Non-Match Rate). The FRR tells you how often the sensor will wrongfully reject the valid biometric in the matching algorithm. Convenience is also related to other attributes of the sensor, such as how intuitive it is to use, how quickly it wakes up/what operation is required to wake the sensor as well as how the sensor is incorporated in the end-product, though that is more a consequence of size and design flexibility of the sensor. Plotting the FRR ratio versus the FAR ratio for various types of biometric authentication systems gives an interesting insight into the trade-offs between security and convenience. The ideal sensor has minimal FAR as well as FRR, but in reality, biometric authentication systems are somewhere on a curve where you either have high convenience (low FRR) but lower security (high FAR) or vice versa, see *Figure 4.*

$$FAR = \frac{\text{Total False Acceptances}}{\text{Total False Attempts}}$$

Figure 2. Definition of False Acceptance Rate (FAR)

$$FRR = \frac{\text{Total False Rejections}}{\text{Total True Attempts}}$$

Figure 3. Definition of False Rejection Rate (FRR)

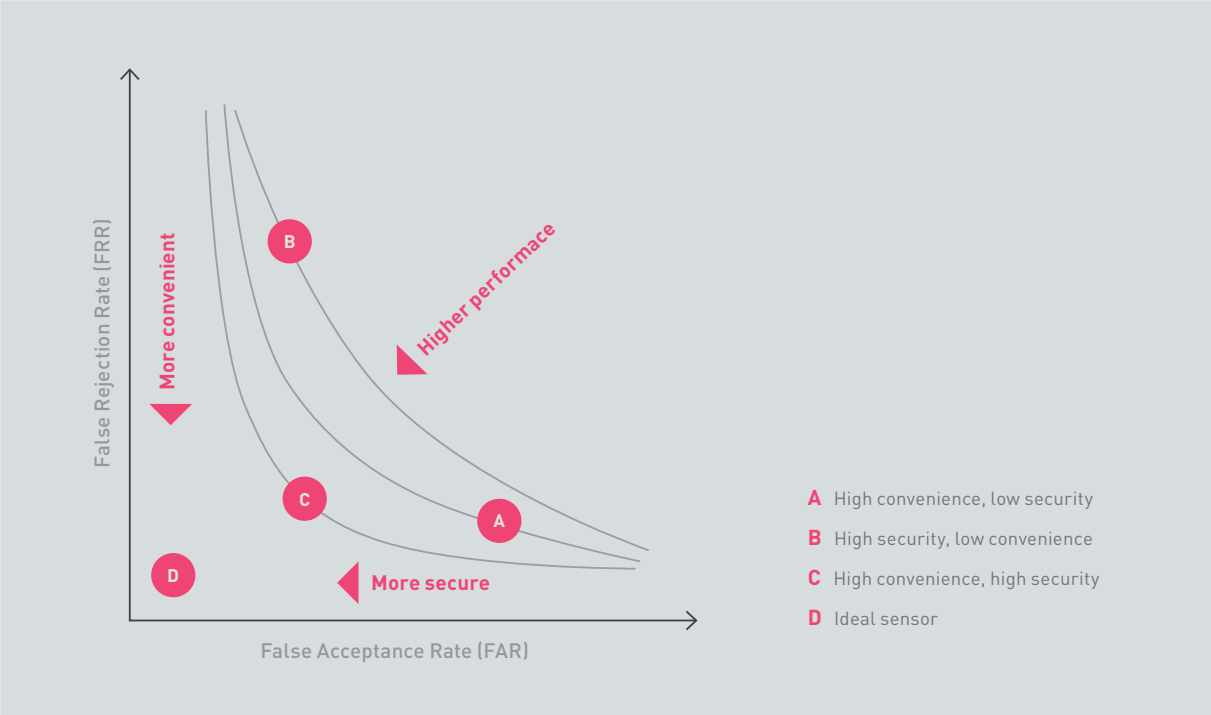

Figure 4. Illustration of the trade-off between security and convenience

3. BIOMETRIC TECHNOLOGIES

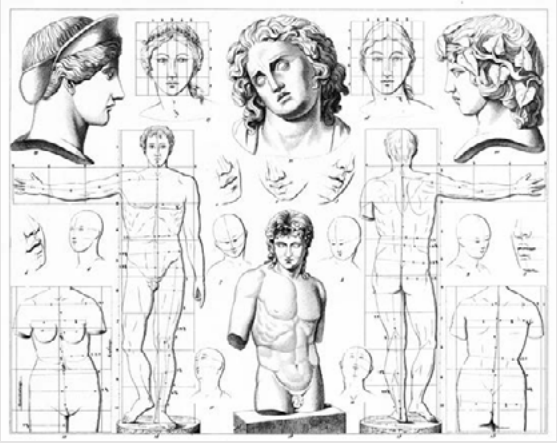

Figure 5. Biometrics

The word ***biometric*** derives from the Greek words"bio" (life) and "metrics" (to measure). Biometrics allow authentication based on something you are rather than something you know (for example a PIN code or password) or something you have (for example a key or passport). The concept of biometrics has been around for hundreds or even thousands of years. One of the oldest and most basic examples of a characteristic that is used for recognition by humans is the face. Since the beginning of civilization, humans have used faces to identify known and unknown individuals. The concept of human-to-human recognition is also seen in behavioral-predominant biometrics such as voice and gait recognition. We use these characteristics, somewhat unconsciously, to recognize known individuals on a day-to-day basis. It is only in the last few decades that it has become possible to replace the biometric recognition we perform every day with automated processes. The enabler has been advances in computer processing driven by the development of increasingly efficient integrated circuits. Today there is a broad variety of biometric technologies available, with fingerprint recognition being the most widely used.

3.1 Biometric Identifiers and Biometric Systems

Given the multitude of characteristics that is coupled to a human being, we need some way of classifying the different biometric identifiers, also called the biometric ***modalities***. A first step is to group them as either behavioral or physiological. ***Behavioral identifiers*** are measurable traits that are acquired over time. The traits can then be used for authentication of a person's identity by using pattern recognition techniques. Behavioral identifiers include for example signature recognition, voice recognition and keystroke dynamics. ***Physiological identifiers*** are something you are rather than something you do or know. There are many types of physiological identifiers, including fingerprint, handprint, iris and retina, face, DNA and many more.

EXAMPLES OF **PHYSIOLOGICAL IDENTIFIERS**	EXAMPLES OF **BEHAVIORAL IDENTIFIERS**
Fingerprint, handprint, footprint	Voice
Iris and retina of the eye	Signature
Face, ear	Gestures
Vein and vascular patterns	Gait

Figure 6. Examples of biometric identifiers (modalities)

Biometric systems are automated systems designed to employ biometric data derived from biometric identifiers (modalities). On a very high level all biometric systems can be described as an automated process that:

- Captures biometric data via a biometric identification device, e.g. a fingerprint sensor and associated circuitry
- Extracts the relevant data from the actual submitted sample
- Compares the scanned data with data captured for reference
- Matches the submitted sample with templates
- Determines whether the identity of the biometric data holder is authentic

Biometric systems consist of both hardware and software. A ***biometric identification device*** gathers, reads and compares the biometric data. The ***biometric data*** is the sample taken from the individual and which must be unique to the person. ***Embedded software*** within the biometric system includes a ***biometric engine*** that processes the gathered biometric data.

The software typically works in tandem with the hardware to operate the biometric data capture process, extract the data, and undertake comparison, including data matching. The most common biometric identifiers used in biometric authentication systems today are fingerprint, face, voice vein and signature. Many variations exist within each basic identifier category and there are also systems on the market combining several identifiers, i.e. performing ***multimodal authenticati***.

The market shares of the different biometrics systems shown above are a compound of both ***stand-alone biometric*** systems and ***client-server biometric systems***, given that most biometric systems belong to either of these two categories. The following sections give a brief overview of each major type of biometric identifier and its key characteristics.

Market shares by Biometric Type – 2019

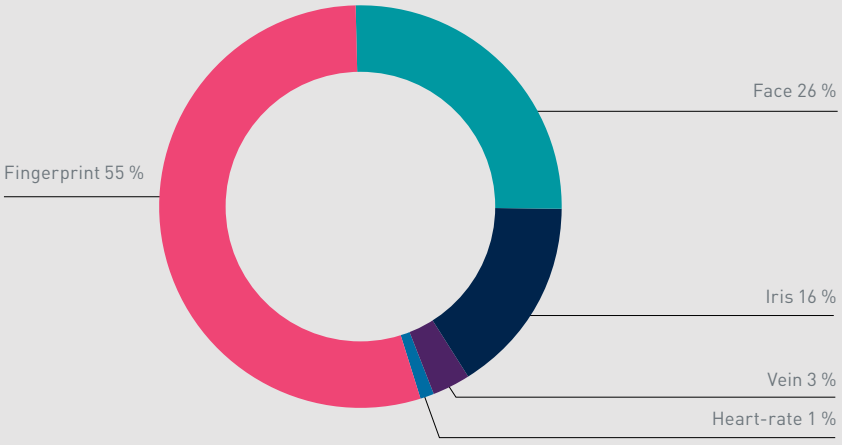

Figure 7. Biometric devices & sensors Revenues market share per type. Including Consumer, Enterprise, Banking, Financial Services & Insurance, Healthcare and Government & Security markets. Source: ABI Research 2019

3.2 Fingerprint Recognition

Fingerprint recognition, being the major biometric identifier in use, will be treated in much greater detail in chapter 4. However, to enable a comparison with other identifiers, a brief overview of fingerprint recognition principles and features is given here. The ridges on the skin of our fingertips form unique patterns shown in our fingerprints. In biometrics, the patterns that are formed by the ridges are called ***minutiae****.

* Minutiae is a Latin word for trifles and minor details.

Examples of minutiae are ridge endings, crossovers, cores and bifurcations, see *Figure 8*. Several different technologies are available to capture fingerprints – from manual methods traditionally used in forensic science to the advanced active capacitive technology used in the sensors from Fingerprints, Apple Touch ID and others. The unique characteristics of a fingerprint can for example be read by optical, capacitive, ultrasonic, thermal or piezo-electrical sensors types, each type having its own benefits and drawbacks as described in chapter 4.

Figure 8. Fingerprint formation

Looking at fingerprint recognition as such it comes out as a very attractive biometric identifier, when compared to other modalities. The main reasons why fingerprint recognition is the dominant biometric modality used in commercial applications today can be summarized as:

- Each fingerprint has a very high level of uniqueness, i.e. authentication is ***definite***.
- The fingerprint normally stays ***permanent*** during the whole lifespan of a person.
- Existing technologies allows for a ***cost efficient*** sensing and measurement of the fingerprint.
- The sensed parameters of the fingerprint can easily be quantified and allows for creation of ***efficient algorithms*** identifying the owner.
- A number of ***standards*** relating to fingerprint recognition are already in place and have created the basis for an economy of scale, i.e. have lowered the cost of fingerprint hardware and software.

Fingerprint recognition also gets high performance scores in terms of ease of use, processing speed and general security. Hence fingerprint recognition comes out as an excellent biometric identifier in most situations, and especially for high volume applications where cost and standardization are of particular importance. Typically, other biometric identifiers can be used as complements, either in special applications or when security requirements demand multimodal authentication of a person's identity. No technology is perfect, and one drawback with fingerprint recognition sometimes mentioned is the social acceptability aspect: Some users regard fingerprint recognition intrusive because of its historic aspect of criminal identification and association with large, governmental registers of citizens. Also dirty or dry fingers may affect the sensing of the fingerprint, causing the recognition process to fail for some sensor types.

3.3 Eye Recognition

Biometric recognition based on features of the eye is compelling as several of the features of our eyes have high uniqueness, including the iris, retina and blood vessel pattern in the whites of our eyes – scleral vasculature recognition. Systems using eye biometrics are therefore common for both identification and verification in law enforcement and government settings. Recently eye recognition has started to make its way into mobile biometric authentication.

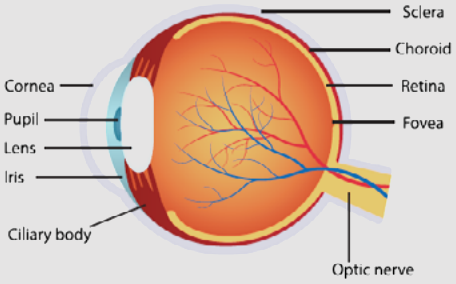

Figure 9. Anatomy of the eye

3.3.1 RETINA

The first biometric eye scanning systems were retinal scanners introduced in 1985. The retina is a thin tissue at the back of the eye that has a pattern of capillaries that is unique, not even identical twins share a similar pattern, furthermore, the retina remains unchanged from birth until death – that is, if there are no diseases, such as diabetic retinopathy, that alters the pattern of capillaries through neovascularization and hemorrhages.

As the retina sits at the back of the eye and is not directly visible, the image capturing cannot be done by a conventional smartphone camera or similar device. The retinal scan is instead performed by shooting a beam of infrared light into the eye which traces a standardized path on the retina detecting the pattern of capillaries used for the authentication.

Although retinal scans provide a high degree of security, the technology have many disadvantages that has resulted in limited commercial use:

- Difficult to acquire useful image
- Lengthy enrolment
- Requires specialized equipment
- Expensive

Retinal scanning has been used for identification (1:n) in high security settings by organizations like FBI, NASA and CIA. Retinal scanning is also used in medical diagnostic applications. There are new laserbased retinal cameras/scanners that are better at capturing images from people who have certain diseases that otherwise makes retinal scans impossible, however, the devices are expensive, about hundred thousand USD, and are mainly used in hospitals.

3.3.2 IRIS

Our colored part of the eye, the iris, is actually a muscle that controls the inflow of light to the eye. Specific features of the iris, called corona, crypts, filaments, freckles, pits, furrows, striations and rings, form patterns that are unique to a person. Over 200 of these features are typically captured using one of several scanning techniques, including CCD/CMOS image sensors and infrared cameras. Typically, there is a need to illuminate the eye with an infrared lamp so a basic smartphone camera is not enough to scan the iris. Iris recognition is a relatively young technology that was first patented in 1994 and incorporated in commercial applications in 1995. Since then iris recognition technology has progressed with better algorithms and hardware. Iris recognition was first used for identification systems in law enforcement and government settings, but has now started to make its way into mobile devices, automotive and other consumer focused devices and applications.

Iris recognition, just like any biometric technology, has its advantages and disadvantages:

+ **Very high accuracy** – Little risk for false authentication
+ **Contactless** – Makes it suitable for identification
- **Processing requirements/power consumption** – The processing power needed for running the algorithms is higher than for fingerprint recognition. Iris recognition also typically requires more data to be stored than fingerprint recognition.

With new advancements and simpler processes there are now solutions on the market suitable for consumer devices.

3.3.3 SCLERAL VEIN (EYEPRINT)

Scleral vein recognition is an emerging biometric technology that has been integrated in some smartphones. The technology behind the most commonly used solution uses the regular CMOS (or CCD) image sensor in the device to capture an image of the user's eyes. From the image a template based on the unique pattern of the scleral vasculature as well as other micro features in and around the eyes is created and the template is then used for authentication. The primary advantage of scleral vein recognition is that it requires no specialized hardware; a camera with at least one-megapixel resolution is enough. However, speed, accuracy and possibly requirements on processing capabilities are still unclear for this very young technology.

3.4 Face Recognition

Figure 10. Face recognition

Face recognition makes use of multiple features of the face that together can be used to uniquely identify a person. Examples of features that can be used are the shape of the nose and the distance between the eyes. In total, about 80 different features similar the ones described are present in our faces and together those are referred to as ***nodal points***. The biometric templates used for authentication are based on these nodal points. Sometimes personal features like moles are also added for enhanced security. Pros and cons of facial recognition include the following:

+ **Low cost** – No additional hardware needed in mobile devices and for other applications a camera is enough.
+ **Range** – Depending on what you want to achieve, facial recognition has an advantage in that it can be used at rather long distances and without a person knowing that he or she is being identified.
- **Requires good lighting.**
- **Low stability over time** – Face changes with age as well as disease and weight loss/gain.
- **Low security** – It is rather easy to spoof a facial recognition system by altering the face with prosthetics, often a photo will do the job.
- **High failure rate** – glasses, hats, haircuts and a myriad of other factors can make facial recognition system unable to capture the required nodal points needed for authentication.

The latest 3D technology has improved security but it comes with a high cost.

3.5 Voice Recognition

Voice prints, not to be confused with the behavioral biometric speech recognition, has been used for a long time and is widely employed in for example customer care centers. Whilst voice recognition is easily implemented at a low cost, requiring no other hardware than a microphone, there are major shortcomings.

- Voice prints can change over time thus requiring regular updates of the voice samples.
- Voice prints can change due to external factors like environment and health – just think about how you sound when you have caught a cold.
- Voice prints can easily be recorded and used to spoof an authentication system.

There have been advancements in voice recognition technology and some systems are much better at handling e.g. noisy environments. A major factor still persists, namely that voice recognition requires the user to speak which is both time consuming and in many situations inconvenient. Voice is perfect as a UI though, as it is a convenient and natural way of interacting with various devices.

3.6 Vein Recognition

The palm has a complex vascular* pattern that is unique to every person. Since the vein patterns lie under the skin they are almost impossible to replicate/spoof and allows for highly secure authentication with false authorization rates as low as 0.00008 percent according to vein scanner provider Fujitsu. Vein recognition, or vascular recognition, can also be done on the user's finger.

The high security levels and the contactless recognition make vein recognition well suited for many appli-

* From the Latin word for "small vessel".

cations requiring very high security. What limits the application areas are the size and cost of the scanners – the scanners are for example simply too bulky to be incorporated in most mobile devices. Also identification involving 1:n matching takes considerable time if the database holds a high number of biometric templates. This is due to the high processing requirements of vein systems as the vein patterns are very complex. As an alternative to vein recognition, the geometric characteristics of the human hand may be scanned and used to create a hand geometry identifier of the individual. However, the same sensor cost and size drawbacks as for vein recognition also applies to hand geometry recognition.

Figure 11. Vein recognition

Figure 12. Gesture recognition

3.7 Behavioral Biometrics: Gait and Gesture Recognition

Minor variations in gait style can be used as a biometric identifier for authentication and identification purposes. The gait parameters measured are typically both spatial-temporal (step length, step width, walking speed, cycle time) and kinematic (joint rotation of the hip, knee and ankle,mean joint angles of the hip/knee/ ankle, and thigh/trunk/foot angles). There is also a high correlation between step length and height of a person. Another appearance-based approach recognizes individuals through binary gait silhouette sequences.

Accurate measurement of gait parameters requires sophisticated equipment such as several video cameras, floor-mounted load transducers etc. which currently makes secure gait recognition a complicated and costly technology to implement.

An alternative to gait recognition is gesture recognition where handmade gestures
are interpreted by a computer system via mathematical algorithms. Gesture recognition evolved as a means for simplified human to computer interactions and has become quite popular, for example in controlling computer games. Using gesture recognition for authentication purposes is still in its infancy, drawing on the advantage of not needing any additional hardware than a camera. However, security and spoofing concerns has so far made this a less attractive authentication method. Interestingly, behavioral biometrics can also be used in the background as a second or third factor to increase security for use cases like online transactions, or in the future of shop & go stores.

3.8 Comparing Biometric Technologies

With the plethora of biometric technologies available, making the correct design choice for a given application is not the easiest thing to do. The general characteristics of some of the major biometric technologies have been described above, but there are also many more performance oriented features to take into consideration, as well as the social acceptability of the chosen technology.

Comparing biometric modules

		FINGERPRINT	IRIS	FACE (2D)	FACE (3D)	VEIN	VOICE
SECURITY	Uniqueness	High	High	Low	High	High	Low
	Hard to copy/spoof	Medium	High	Low	Medium	High	Low
CONVENIENCE	Speed	High	Medium	Medium	Medium	Medium	Low
	Accuracy	Medium	High	Low	Medium	High	Medium
SCALABILITY	Cost efficient	Medium	Medium	High	Low	Medium	High
	Easy to integrate	High	High	High	Low	Low	High

High Medium Low

Figure 13. Comparison of common biometric technologies

4. FINGERPRINT RECOGNITION

The fingerprint is the oldest known biometric identifier that has been used for authentication and identification purposes. Fingerprints have been found on the walls of Egyptian tombs and on Minoan, Greek, and Chinese pottery. Fingerprints were used as signatures in ancient Babylon in the second millennium BC; In order to protect against forgery, parties to a legal contract would impress their fingerprints into a clay tablet on which the contract had been written. More recently, in the 18th century the anatomical features of the fingerprint were described in detail, in the 19th century methods for fingerprint classification were proposed, and in 1975 FBI funded the development of the first computerized fingerprint scanners.

Human fingerprints are detailed, nearly unique, difficult to alter, and durable over the life of an individual, making them very suitable as long-term markers of personal identity. It is therefore natural that a wide range of fingerprint recognition systems exist for use in high security applications and for the automated identification of individuals. The convenience, security and performance characteristics have made fingerprint recognition the most widely used biometric authentication technology today.

As tioned already in section 2.3 an automated authentication system typically performs the following operations:

- **Data capture** – A sensor of some kind captures data from the biometric identifier used.
- **Enrollment** – The captured data is analyzed and its unique features are stored as a digital template.
- **Authentication** – When the enrolled user wants to authenticate himself/herself, his/her biometric data is captured once again and compared against the template generated by the enrollment.
- **Matching** – An algorithm is used to compare if there is a match between the stored template or not. If there is a match the user has been authenticated, otherwise access is denied.

The main elements of such a system and how they interact are shown in Figure 17 below. This chapter takes a closer look at each system element in the context of fingerprint recognition and identifies the characteristic features essential for a secure and convenient authentication system based on the scanned fingerprint. But first we need to familiarize ourselves a bit more with the details of the fingerprint as such.

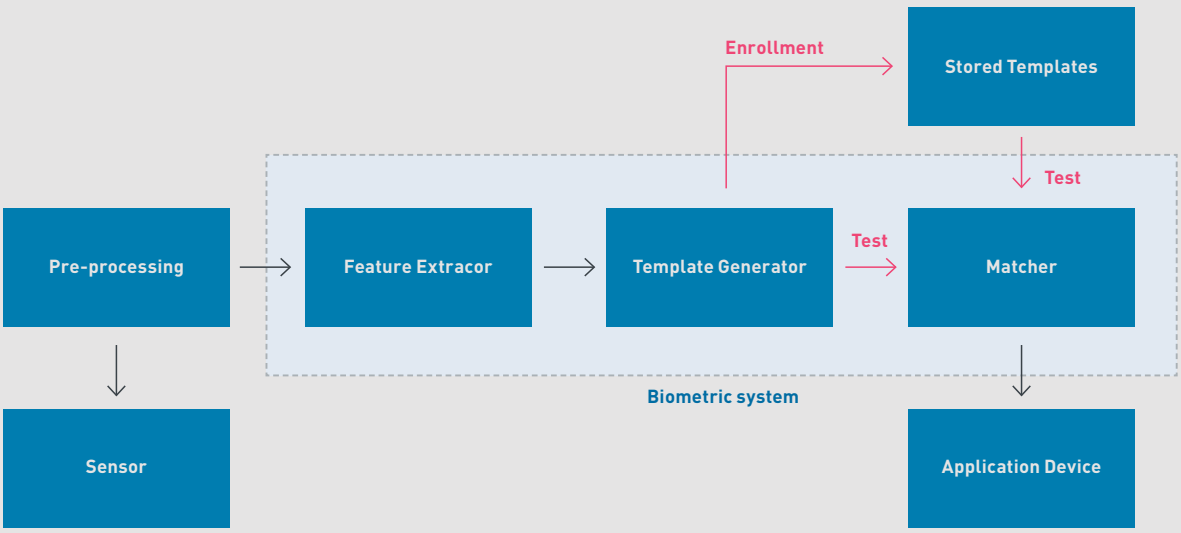

Figure 14. Block diagram showing the main elements of a biometric authentication system

4.1 The Fingerprint

A fingerprint is an impression left by the friction ridges of a human finger. A friction ridge ***(epidermal ridge)*** is a raised portion of the epidermis* on the fingers and toes, the palm of the hand or the sole of the foot. The ridges serve to amplify vibrations triggered, for example, when fingertips brush across an uneven surface, better transmitting the signals to sensory nerves involved in fine texture perception. The ridges may also assist in gripping rough surfaces and may improve surface contact in wet conditions. The epidermal ridges form distinctive patterns, each with their own individual characteristics often referred to as ***minutiae***** in biometrics and in fingerprint recognition systems. The minutiae are highly unique for every human being and can therefore be used for authentication and identification purposes. The patterns of the epidermal ridges are of .three basic types: An arch, a loop, or a whorl (see Figure 18). Loops are most common (~ 65%), followed by whorls (~30%) and arches (~5%) in the human population.

- **Arch:** The ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger.
- **Loop:** The ridges enter from one side of a finger, form a curve, and then exit on that same side.
- **Whorl:** Ridges form circularly around a central point on the finger.

Figure 14. The three main types of epidermal ridge patterns. The pictures represent "full size" or "rolled" fingerprints, such as those captured by ink and paper.

In addition to the basic patterns of the epidermal ridges, a fingerprint is characterized by several other features, some of which are shown in *Figure 15*. The ridges start and end ***(end points)***, cross each other ***(cross-over)*** and separate ***(bifurcation)***. There are small isolated ridges between others (islands), spaces between ridges ***(deltas)*** while individual ***pores*** in the epidermiscan also be identified. The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include the patterns as such plus the various minutia points described above. For successful use of some sensor technologies it is also necessary to know the structure and properties of the human skin. The fingerprint matching techniques in use by automatic fingerprint recognition systems can broadly be divided into two main categories:

Figure 15. Additional characteristic features of a fingerprint. The picture represents a partial or "slapped" fingerprint, such as those captured by a touch sensor on a mobile phone.

* The epidermis is the outer (epi in Greek meaning "over" or "upon") of the two layers that make up the skin (or cutis), the inner layer being the dermis.
** Minutiae is a Latin word for trifles and minor details.

- **Minutiae based** – The minutiae based category has its roots in the manual fingerprint identification methods developed in the late 19th century. A set of minutiae were described by Sir Francis Galton and together with the global ridge pattern classes these are the fingerprint features used traditionally. Standardized matchers (ISO/ANSI) work on a subset of the features (ridge endings and bifurcations). The density of these minutiae is such that systems using minutiae based matching require a large area of skin to work with, thus large area sensors or swipe sensors are normally used.

- **Non-minutiae based** – Non minutiae based methods are everything else and encompass a broad range of matching principles ranging from direct correlation of sub images to vectorizations of the ridge flow and frequency based techniques. Sensor size, type and security operating point (FAR level) will dictate what is viable. Other system resources like available memory and processing power are of course also important for selecting th best approach.

Matching algorithms combining traditional minutia + non-minutia based approaches are often called hybrid methods. Governmental fingerprint identification/authentication systems with large sensors are typically ISO/ANSI minutiae matchers due to the strong requirement for vendor interoperability. As sensor sizes decrease hybrid solutions become more popular and for even smaller sensors, such as those in mobile devices, it is not uncommon that the minutiae part is skipped entirely.

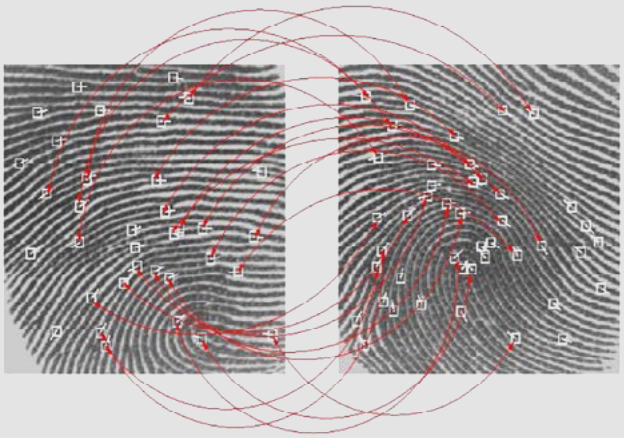

Figure 16. Minutia based fingerprint matching

4.2 Fingerprint Sensors

A fingerprint sensor is an electronic device used to register a digital image of the fingerprint pattern. The image is now and then referred to as a ***live scan**** of the fingerprint and the sensor is sometimes the input element of a dedicated hardware entity, a ***fingerprint scanner***, but often just part of another device, such as a mobile phone. The fingerprint sensor captures the relevant fingerprint features for further processing and is therefore one of the most central elements of the fingerprint recognition system, the others being the image processing/feature extraction and the matching algorithms used.

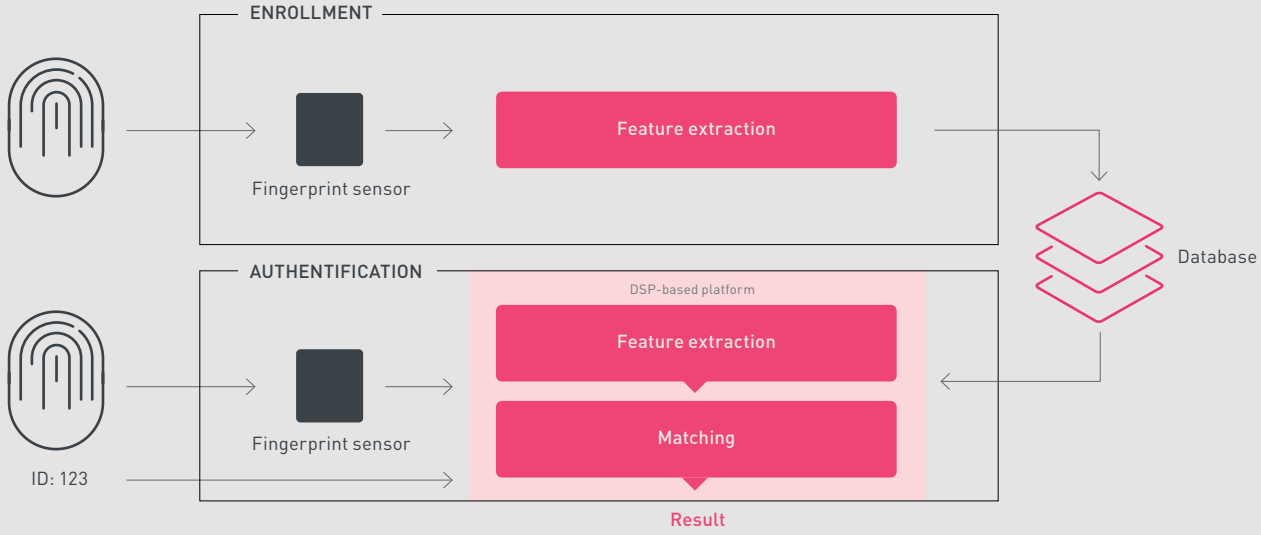

Figure 17. Minutia based fingerprint matching

* As opposed to an off line image retrieved from e.g. a database for identification purposes.

Figure 18. Touch sensors

4.2.1 OPTICAL SENSORS

Optical sensors register fingerprint patterns by capturing visible light and turning it into electrical signals used to create the fingerprint image. The sensors have arrays of photodiodes or phototransistor detectors that convert the energy in the light that hits the detector into electric charge. Most optic sensor packages also include a LED (Light Emitting Diode), or array of LEDs, to illuminate the fingertip so that the detector can capture the fingerprint image from the light reflected on the finger. A prism with a protective coating is then used to reflect the light towards the detector.

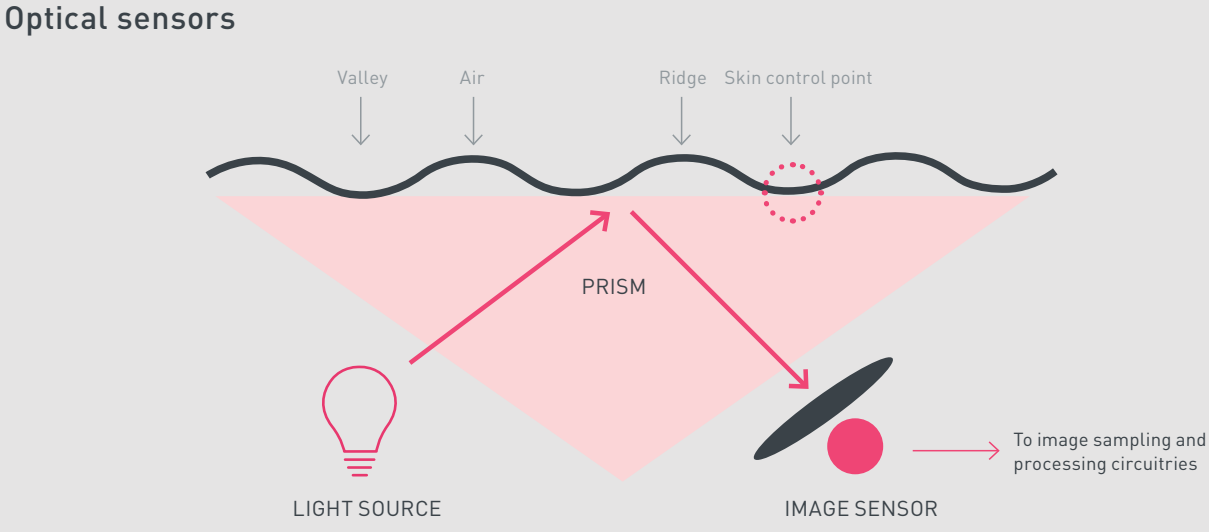

Figure 18. Working principle of an optical fingerprint sensor

The detectors used in optical fingerprint sensors today are either CCD (Charge-Coupled-Devices) or CMOS optical imagers. The CCD and CMOS detectors are of the same type as can be found in digital cameras. CCD detectors are particularly sensitive to low levels of light and are therefore good for capturing grayscales. Historically CCD detectors were much better than CMOS detectors, but as CMOS technology has undergone much development during the past ten years or so, CMOS technology capabilities have caught up with CCD.

CCD fabrication is rather expensive compared to CMOS fabrication. Apart from the cost, CMOS optical imagers also have a clear advantage as they can be built to hold some of the logic for the image processing on the same silicon chip as the detector. This has led to that most optical sensors for consumer electronics, where cost as well as power consumption are important features, use CMOS detectors.

Optical capture was the first electronic fingerprint sensor technology employed and is probably the technology used in the widest number of applications. They are now developed and being used to be integrated into the screen, opening up new use cases like in-display sensors on smartphones. Its main advantage is the relatively technology also has several shortcomings such as being prone to spoofing, do not work well in sunlight, are sensitive to contamination by their environment and often wear with age.

4.2.2 CAPACITIVE SENSORS

Capacitance is the ability of a physical entity to hold electrical charge. ***A capacitive fingerprint sensor*** generates the fingerprint image by using an array containing many thousands of small capacitor plates. The array plates make up the "pixels" of the image: Each of them acts as one plate of a parallel-plate capacitor, while the dermal layer of the finger, which is electrically conductive, acts as the other plate and the non-conductive epidermal layer as the dielectric in between. When the finger is placed on the sensor, faint electrical charges are created, building a pattern between the finger's ridges or valleys and the sensor's plates. Using these charges, the sensor measures the capacitance pattern across the sensed surface. The measured values are digitized by the sensor logic and then sent to a neighboring microprocessor for analysis.

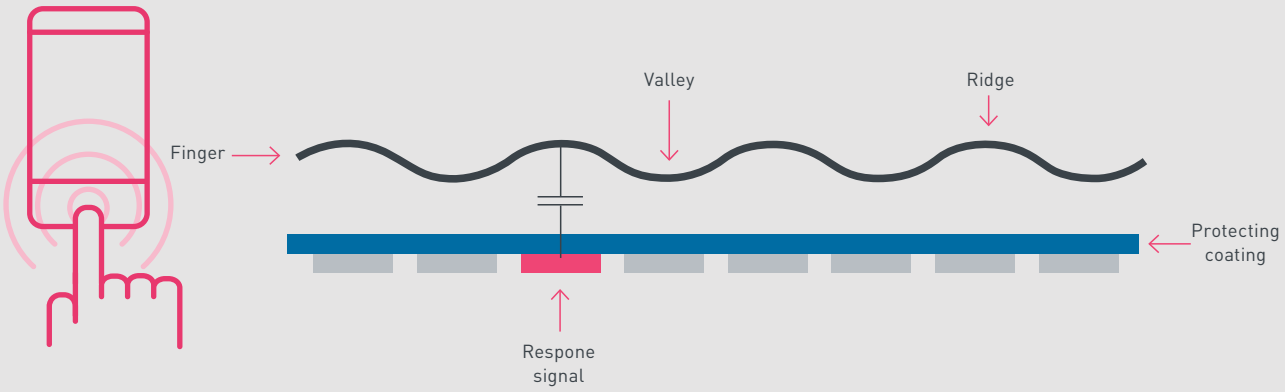

Figure 19. Capacitive sensing principle: The measured capacitances varies with the ridges and valleys of the fingerprint.

You cannot fool a capacitive sensor by using a high-quality photograph rather than an actual finger. Instead of photographing an image of the ridges and valleys in a fingerprint as an optical scanner does, the capacitive scanner's sensor generates a complex pattern of electrical signals, which is processed to form a digital image of the fingerprint. Because the capacitive scanner requires the physical presence of a human finger to generate the image, it is therefore much more difficult to fool than an optical device. Another benefit of capacitive sensing fingerprint readers is that they are more compact and thus easy to integrate into portable devices.

Direct (Passive) Capacitive Measurement

The surface of a capacitive sensor is a neat array of plates, able to measure the capacitance between these plates and the fingerprint pattern. The measurement can be done "directly" based on electrical charges, or by applying a weak electrical signal to the finger.

Direct capacitive measurement utilizes the conductive property of the skin to make a capacitive coupling with the plates of the array. Since the ridges of the outermost skin layer are closer to the plates of the sensor than the valleys, more charge can be hold between plate and finger where there is a ridge, corresponding to a higher capacitance at that point. The pattern of valleys and ridges on the finger is therefore reproduced by the plate capacitances and a corresponding image of the fingerprint is created.

Direct capacitive fingerprint sensors are sensitive to static discharges (ESD) as well as to dry and damaged fingers, but handle different light conditions rather well. A major obstacle with direct capacitive fingerprint sensors is that they require a very thin coating to capture the fingerprint compared to active capacitive fingerprint sensors, since they rely upon the static charges between finger and sensor.

Active Capacitive Measurement

Active capacitive measurement, sometime referred to as RF, reflective or inductive capacitive measurement, uses a weak electrical signal which applies a voltage to the skin before measurement takes place. The voltage that charges the finger may for example be applied via a conductive bezel placed around the sensor array, as shown in *Figure 20*. The charging of the finger takes place during the charging cycle of the sensor. At the discharge cycle the charge across the individual capacitive pixel plates is compared against a reference charge and from this the capacitance can be calculated. As the capacitance is dependent on the distance between the capacitive pixel plates and the epidermal ridges, the distances can be calculated and used to form an image of the fingerprint.

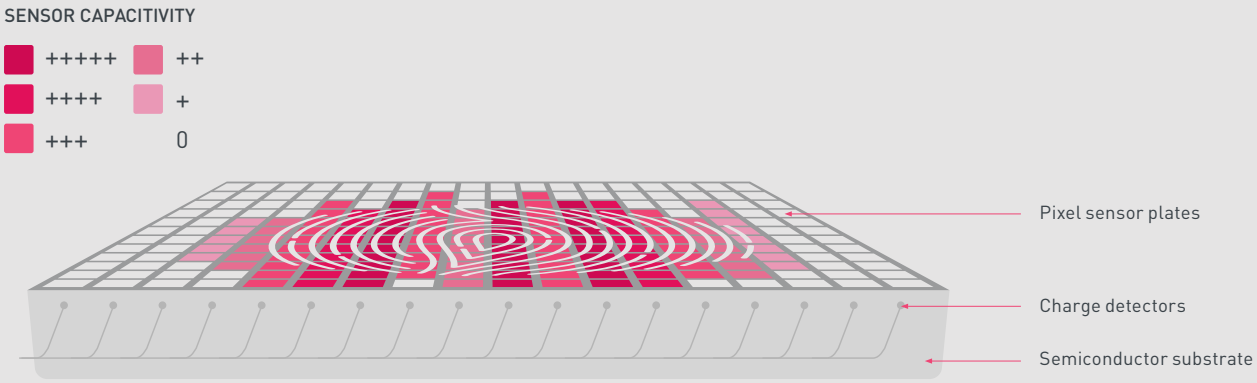

Figure 20. Active capacitive measurement with an active bezel charging the finger

By using additional circuitry, which can be located on the same semiconductor chip as the sensor plates, it is possible to dynamically adjust the sensor reception to different skin types and conditions. This eliminates the need for clean, undamaged epidermal skin and a clean sensing surface, hence making active capacitive measurement the most commonly used type of capacitive technology today. Another very important benefit with active measurement is that the strengthened signal communications between the fingerprint surface and the sensor plates allows for the introduction of a durable, protective coating layer.

Capacitive Fingerprint Sensor ASICs

Sensors for capacitive measurements can be produced as ***Application Specific Integrated Circuits (ASICs)****. An ***integrated circuit*** (IC, "chip") is a piece of semiconductor material (silicon) on which thousands or millions of electronic components, such as sensor plates and transistors, have been created and interconnected. Despite being highly complex products, ICs cost relatively little to produce as all the components are etched onto a silicon wafer in an automated photolithographic process.

The most common technology used when manufacturing ASICS for active capacitive measurements is ***CMOS (Complementary Metal Oxide Semiconductor)***. An inherent advantage of this technology is that it can be used for both digital logic circuits and analogue circuits on the same chip. With CMOS technology, it is therefore possible to mix analogue functions for the pixel plates and digital circuits in the same IC.

* An ASIC is a silicon based semiconductor circuit of high complexity. Other technologies, such as Thin Film Transistor (TFT) and metal grid may also be used to create capacitive fingerprint sensors.

CMOS technology also possesses two other characteristics that are very important for fingerprint sensors, it has high noise immunity (little random variation in the electric signal) and digital circuits produced in CMOS have low static power consumption. Other ASICs designed and manufactured with CMOS technology include image sensors for digital cameras and the microprocessors used in mobile phones.

The signals that are measured by the fingerprint sensor are ***analogue****. The output from the sensor to the biometric microprocessor must however be ***digital data***. On, or close to the sensor plate matrix, there must therefore be circuits that convert the analogue signals to digital format. The digital data then sent to the microprocessor is the fingerprint image. The distances measured at each of the thousands, or even tens of thousands, capacitive pixel plates are represented by gray scale values for each pixel of the fingerprint image. Further processing of the digital image can then be used to create a detailed fingerprint image, even having 3D characteristics such as depicted in Figure 27 below, and to capture the minutiae necessary for a positive identification and authorization.

Packaging Alternatives for Active Capacitive Fingerprint Sensors

Active capacitive fingerprint sensors come in many shapes and formats to suit a large number of applications. The technology can be used both for ***swipe sensors*** and for ***touch sensors*** of various sizes, where the larger sensors capable of readin an entire fingerprint rather than just a portion of it sometimes are referred to as area sensors. To allow application designers more degrees of freedom in designing their products, sensors are available in several different shapes - rectangular, oval and squared - allowing the sensor to be mounted on the side, on the front or at the back of e.g. a mobile device. Sensors can also be integrated with other buttons of the device and be mounted under a protective ceramic or glass layer, if so required.

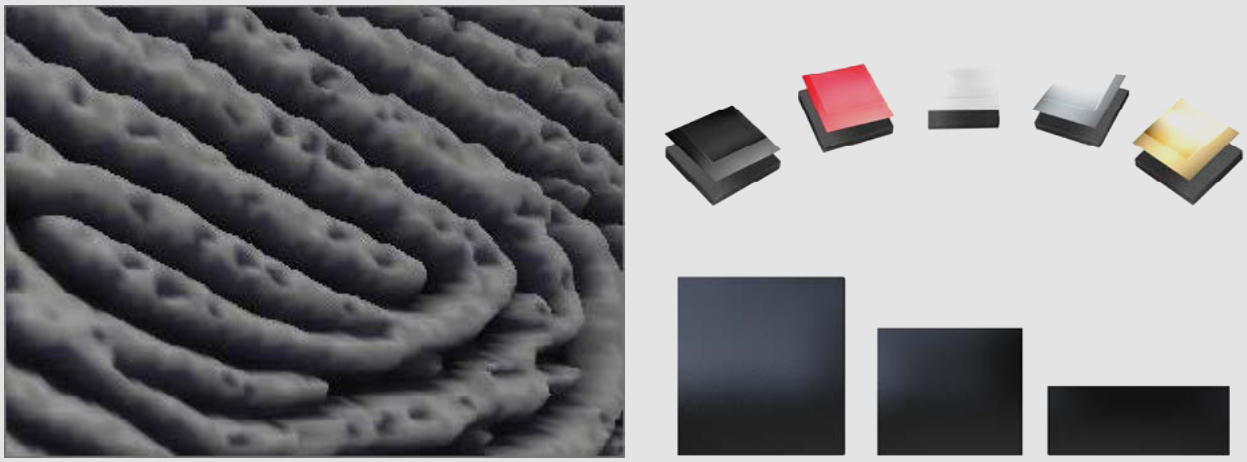

Figure 21. Active capacitive sensors in different packaging.

* An analogue signal is a continuous, varying, electrical signal which represents some other time varying quantity.

Sensors are typically part of other even more complex products, such as mobile phones, security systems etc. To allow for smooth and efficient integration of the sensors in the manufacturing processes, active capacitive sensors can be delivered in various degrees of refinement to the ***module suppliers**** and ***OEMs**** responsible for the final product.

- **Fabricated wafers** where the dies/chips/sensors have not yet been separated. Sensors are sold in the form of wafers in case the module house has its own packaging in-house.
- **Packaged sensors** – sensors in different types of protective encapsulations such as a ***Land Grid Array (LGA)***, a packaging technology with a matrix of solder pads on the underside of the package and optional customized coating. The pads underneath connects the sensor to the processor of the device. Packaged sensors are ready for integration in modules as they come with connections and are normally sold to module houses that do not have their own packaging facwilities.
- **Modules** – sensors having a complete physical enclosure such as a bezel, frame etc., being ready for direct integration into an end-product, for example a mobile phone.
- **Standalone** embedded systems, where the sensor, packaging, software and a biometric microprocessor are all included in a complete biometric solution that can be emedded in various vertical applications such as automotive and IoT.

Figure 22. Wafer, LGA, module and stand-alone embedded system.

Benefits of the Active Capacitive Fingerprint Sensor

The capacitive sensor, and especially the capacitive sensor using the active measurement method described above, possesses several benefits of high value in many applications.

+ Excellent image quality – Designed to deliver a very high image quality, even enabling 3D rendering of the fingerprint, which gives superior security and spoof resilience.
+ Small and compact – Can easily be integrated in portable products such as mobile phones and tablets.
+ Minimal power consumption – The CMOS process used for the sensor ASICs ensures ultra-low power requirements, a further plus in mobile applications.
+ Fast – With an active capacitive touch sensor, fingerprint capture can be done in one go, reducing the need for swiping the finger over a reader.
+ Durable and easy to integrate – The sensor plates do not need to be in direct contact with the finger. An active capacitive sensor can be placed behind a protective layer or behind the glass of a mobile phone with minimal performance degradation.
+ Low cost – The cost of any silicon based sensor is closely correlated to the size of the chip. Since active capacitive sensors can be made small, they can also be produced in high volumes at a low price.

* A module supplier is a company that integrates multiple electronic components into subassemblies to be used by companies manufacturing the end products.
** An Original Equipment Manufacturer is a company that manufactures an end product or a subsystem in another company's end-product..

There are not so many disadvantages to list for the active capacitive sensor. Sensitivity to electrostatic discharges (ESD), a general problem for all types of semiconductor integrated circuits, has been mentioned earlier. Also with the reduction of sensor size, it becomes even more important that enrollment and verification are done carefully and using the best possible matching algorithms. Such advanced algorithms may mean additional cycles of processing, hence increasing the power and performance requirements of the processor involved.

4.2.3 ULTRASONIC SENSORS

Ultrasonic fingerprint sensors make use of the principles of medical ultrasonography to create visual images of the fingerprint. Unlike optical imaging, ultrasonic sensors use very high frequency sound waves to penetrate the epidermal layer of skin. The sound waves are generated using piezoelectric* transducers and reflected energy is also measured using piezoelectric materials. Since the dermal skin layer exhibits the same characteristic pattern of the fingerprint, the reflected wave measurements can be used to form an image of the fingerprint. Using the dermal skin layer eliminates the need for clean, undamaged epidermal skin and a clean sensing surface. This makes the ultrasonic sensors good at reading wet and damaged fingers whilst also verifying the liveness of the finger. Dry fingers can often be a problem though, think about the gel that doctors put on bellies before taking an ultra sound scan to look at babies. The ultrasonic fingerprint sensors have an advantage in that they provide more biometric information than most other fingerprint sensors. The problems with the technology have been that it is slow, expensive, power hungry, bulky (large sensors) and that it requires a lot of processing power as the algorithms are data intense. But technological advancements are looking at improving this for the future.

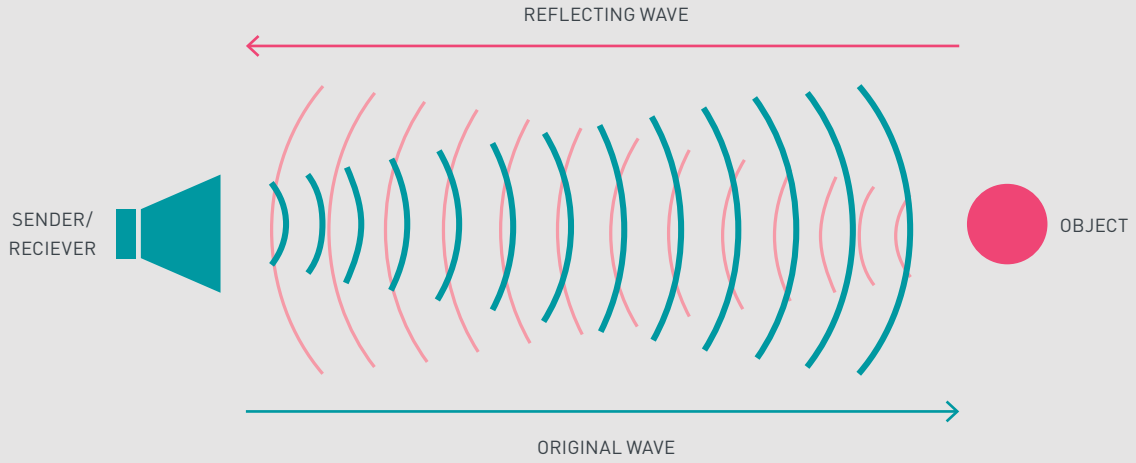

Figure 23. Principle of ultrasonic fingerprint detection

4.2.4 THERMAL AND ACTIVE THERMAL SENSORS

Thermal fingerprint sensors create fingerprint images using temperature measurements. The sensors have arrays of plates in a pyro-electric material of the same kind that is used in infrared cameras. When the finger touches the sensor, the ridges of the finger come in contact with the sensor surface and the temperature is measured. The fingerprint image is then created based on the measurement of the skin-temperature from the ridges and the ambient temperature at the valleys.

* Piezoelectricity is the electric charge that accumulates in certain solid materials in response to applied mechanical stress. It also refers to materials that react mechanically to electric charges.

There are some major problems with thermal fingerprint sensors:

- The temperature change is dynamic, hence, the fingerprint image is transient and is erased after about a tenth of a second when the sensor surface has reached the same temperature as the finger.
- Sensitivity to wear and tear as well as contamination
- When the ambient temperature is close to the temperature of the finger surface, the sensor requires heating so that there is a temperature difference of at least one degree Celsius – otherwise the temperature difference cannot be measured properly and no fingerprint image can be created.

Some of the above problems can be addressed by an ***active thermal sensor.*** An active thermal sensor sends a low-power heat pulse to each sensor pixel when the finger is steadily placed on the sensor surface. The heat pulse breaks the thermal equilibrium and thus enables static acquisition of the fingerprint image.

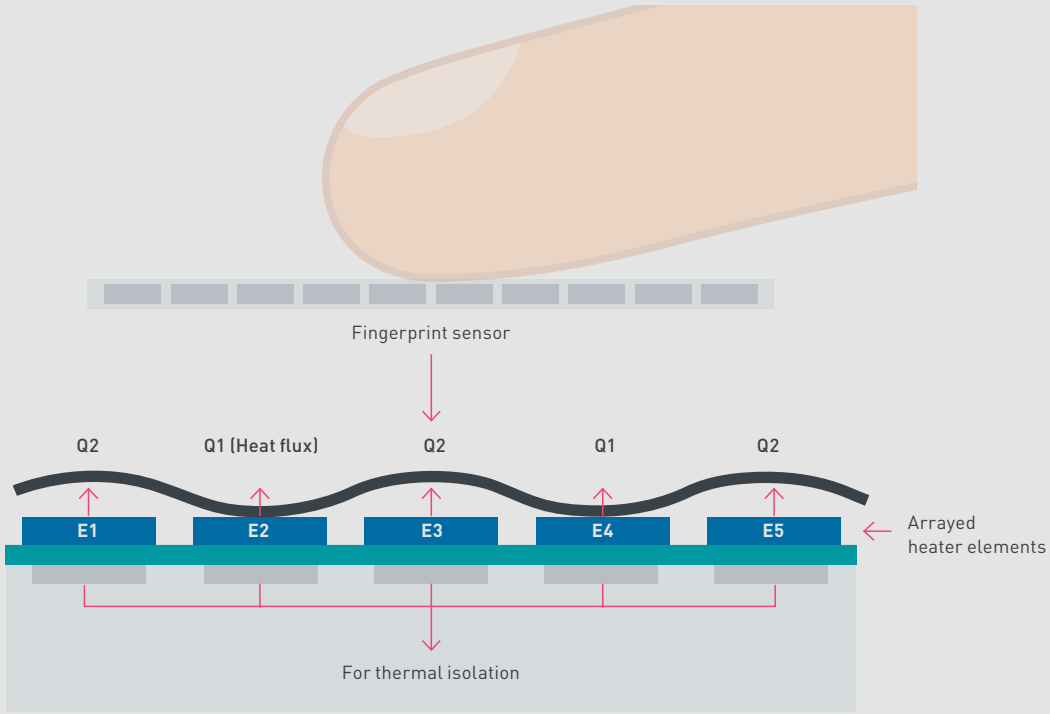

Figure 24. Principle of active thermal fingerprint detection

However, the active thermal technology also has its drawbacks:

- High power requirement
- No ability to capture fine details like sweat pores, thus requires larger sensor area
- Not capable of creating 3D images

4.2.5 PRESSURE SENSITIVE SENSORS

An emerging category of fingerprint sensors are based on thin film materials capable of producing an electrical signal when mechanical stress is applied to them. The sensor surface is implemented as a very thin and flexible, non-conducting dielectric material. When a finger is placed on the sensor, ridges and valleys applies different levels of pressure to the surface, resulting in varying amount of current which can be measured and used to generate a fingerprint image.

Pressure sensitive sensors can be made small, and are one of the few sensor categories beside capacitive sensors that can be integrated in mobile devices such as phones and tablets. However, existing sensors are temperature sensitive and less suitable for use where the environmental conditions are harsh or rapidly changing. Few, if any, pressure sensitive sensors for authentication purposes have been commercially launched.

4.3 Comparing Fingerprint Sensor Technologies

There is a wide range of factors important to consider when choosing the appropriate fingerprint sensor technology and physical sensor to use in a certain product, application or process. The choice of technology will depend on performance parameters such as image quality, speed and power consumption. When designing the "real" product further parameters such as sensor size, cost and packaging options also have to be included in the equation. In this section we discuss some of the most important factors for selecting the best fingerprint sensor technology and sensor.

4.3.1 IMAGE QUALITY AND RESOLUTION

The quality of the image generated by the fingerprint sensor is a fundamental and important parameter. High image quality allows for smaller sensors and a lower cost since more details are captured per area unit. The image quality depends on the sensor's ability to detect weak signals and filter out undesired noise, preferably without requiring a too long and cumbersome "exposure" of the fingerprint. Image quality can be measured in various ways, but a common metric in fingerprint recognition systems is the ***Failure to Enroll (FTE)*** parameter. The FTE ratio simply gives the percentage of times the sensor fails to read the biometric identifier sufficiently well for the continued processing and enrollment of the user. Failures can e.g. be caused by wet or damaged skin when scanning fingerprints or by external no in a voice recognition system. Another metric often used is ***Dot Per Inch (dpi)*** specifying the resolution of the sensor. With a low resolution (low dpi value) fine details cannot be captured, thus reducing the image quality.

Currently very high image quality can be acquired by ultrasonic and active capacitive sensors reading the dermal skin layer which is much more distinct and less prone to distortion than the outer epidermal layer. In an active capacitive sensor each pixel element can also be given its own electronic circuitry within the same ASIC, increasing the sensitivity and reducing the risk that undesired noise enters significantly.

Currently 508 dpi is the normal resolution for active capacitive sensors, which is also consistent with the US ANSI/NIST specification.

4.3.2 SPEED

The speed with which a fingerprint system operates has a major impact on how convenient it is to use. The analogue to digital conversion carried out by the electronic circuitry on the ASIC, as well as the calculations involved in the authentication of the fingerprint needs to be effective to enable a high speed sensor. Writing algorithms in a minimalistic way is important to achieve the desired properties.

In applications using a dedicated biometric processor the calculation intensive parts of the algorithms are executed in hardware which can make the authentication process very fast and accurate. For applications where the algorithms are run in a host processor, such as in a mobile phone, efficient algorithms are key to making the authentication fast.

The speed of the sensor system also varies depending on whether the system performs authentication (1:1) or identification (1:n). Since authentication only requires comparison between the captured image and a stored template the results are generated more quickly than in identification systems. Yet another aspect that determines the speed of the system is the time it takes to get the sensor ready to read.

Capacitive, thermal and pressure based sensors can all be made to operate with very high speed. Currently the time to wake up and verify with such sensors can be below 500 ms.

4.3.3 POWER CONSUMPTION

Power consumption of a sensor system is a very important factor and critical for applications such as mobile phones, smart cards and other portable objects. Not only does a high power consumption drain the battery of the device, it also creates heat which may damage or disturb other elements in the device.

It is essential to consider the sensor's power requirements over time, i.e. the actual amount of energy that is dissipated by the sensor in a given application. In a mobile phone, for example, the sensor may be active a second or so some 20 times per day, while staying idle the remaining 24 hours. It is obvious that it is the stand by (quiescent) power consumption, rather than the power consumption of the active sensor that has the most impact on battery life.

The power consumption is determined by both the hardware and the software of the sensor system. CMOS sensors generally have low power consumption as they consume significant power only when their transistors switches state, that is, when they are used to scan a finger. Furthermore, the size of the sensor also affects the power consumption; a smaller sensor consumes less power. Also, the detailed electrical design of the sensor can heavily influence the power consumption.

Even though a smaller sensor has a lower energy consumption from a hardware perspective, a smaller sensor normally has fewer capacitive pixel plates and thus captures a smaller area of the finger in the image. For a smaller image to provide enough detail for enrollment and authentication a higher picture quality and a more advanced algorithm is needed. Higher quality images and more advanced algorithms both may lead to higher power consumption as it takes more processing power. This effect could overshadow the lowering of the power consumption of the smaller sensor and it is therefore important to have very effective algorithms for producing the fingerprint image as well as the authentication.

Capacitive sensors currently have the lowest power consumption of the sensor technologies commercially available on the market. Optical, ultrasonic and thermal sensors all require significantly more power and are thus less suited for mobile applications.

Typical power consumption for an active capacitive sensor is 5 µA at rest and 20 mA in use.

4.3.4 SIZE

Size, or rather small size, is often a decisive parameter when choosing a fingerprint sensor, especially for mobile applications. The space that can hold all the components needed in a mobile phone, tablet or camera is limited and the exterior of the device may already be filled by a screen, other buttons and dials. Using a small size sensor allows for additional design options when shaping the desired product. Smaller sensors also have a cost benefit over larger sensors, simply because the smaller ASICs use less silicon and can be made cheaper.

However, there is a tradeoff between size and image quality in fingerprint recognition applications. Using a too small sensor with too low resolution will result in a poor image quality, which in turn will require more advanced and power consuming matching algorithms, alternatively make secure enrollment and authentication cumbersome or even impossible.

Active capacitive sensors typically come in sizes 84 x 84 mm up to 160 x 160 mm and can be circular, rectangular or shaped in any other two-dimensional format required by the product designer.

4.3.5 COST

Needless to say, cost is an important factor when choosing sensor systems. The cost becomes increasingly important to drive adoption of fingerprint recognition in cheaper phones, smart cards and other large volume segments that demand low cost components.

The cost of an active capacitive fingerprint sensor which is silicon-based, is highly correlated with the size of the sensor as the material is the major cost driver. Cost is also influenced by the production process, system integration and technology used.

4.3.6 PACKAGING AND OTHER DESIGN OPTIONS

Fingerprint sensors need to be incorporated into end products in a way that does not restrict the design of the original product, but rather compliments and enhances its features. Smart phone manufacturers compete on functionality but also on design. Vehicle manufacturers do not want to compromise on interior design and want a sensor that blends smoothly with the interior of the vehicle. Sensors incorporated in entrance control systems need to endure countless cycles of use and often also harsh weather conditions.

To comply with the above design requirements packaging and protective coating of the sensor becomes very important to consider. One of the great advantages of the active capacitive technology is that it can capture fingerprints through glass and other materials used for encapsulation of an end product. However, for a sensor to be able to capture a fingerprint through 400 micrometer glass or a colorful ceramic it must be able to detect very weak signals. This requires in-sensor signal amplification, advanced signal processing as well as efficient algorithms for the subsequent matching process.

A number of other characteristics also become important when integrating the fingerprint sensor into an end-product. The sensor must have a physical, electrical and logical interface that can be accommodated by the product. A choice must be made if the matching algorithms shall be run in a dedicated biometric processor or within the host processor of the product. And if a host processor is used, does the sensor vendor offer algorithms for the relevant operating system, can they be run in a protected environment and can crucial data be encrypted, just to mention a few parameters of importance for the design.

4.3.7 SECURITY AND CONVENIENCE

We touched upon the security and convenience factors of an automated authentication system and how they can be measured in section 2.3, where we also defined the ***False Acceptance Rate (FAR)*** and the ***False Rejection Rate (FRR)*** metrics. It is intuitively clear that there is a relation between security and convenience: The more secure (reliable) an authentication is to be done, the more data needs to be captured and analyzed, which in turn requires more time and cooperation from the authenticated person, hence is felt more inconvenient.

Different fingerprint recognition technologies show different FRR versus FAR curves, depending on the capabilities of the sensor as such, the image processing done and the matching algorithms used. As usual there is a tradeoff between cost – in this case sensor size and capability – and the shape of the FRR versus FAR curve. However, when an advanced active capacitive sensor is combined with the appropriate algorithms it is possible to achieve FARs as low as 1/100 000 while still maintaining an FRR of only 1%, also for small sensors in mobile devices. This makes active capacitive sensors one of the most convenient sensor technologies, if not the most convenient technology, to use today.

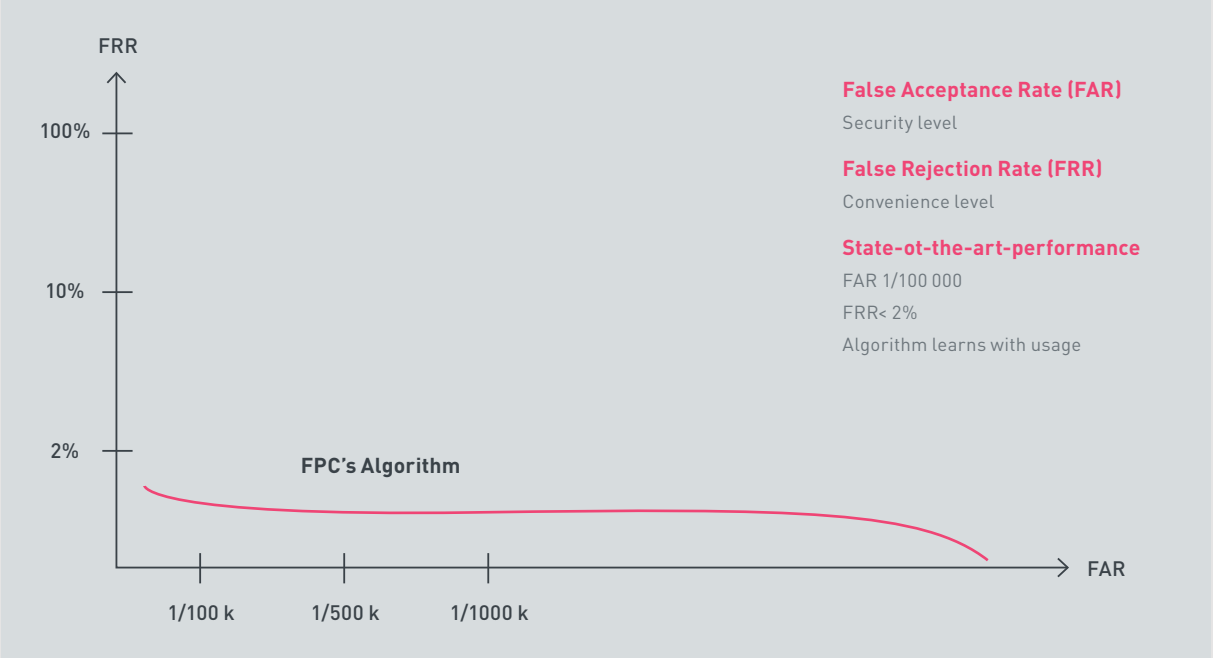

Figure 25. Typical FAR versus FRR curve for an advanced active capacitive fingerprint sensor

4.3.8 CONCLUSIONS

The availability of multiple fingerprint technologies on the market shows that there is no one technology which is ideal for each and every application. Depending on requirements on cost, power efficiency, size, convenience and other characteristics a particular sensor type may be a given winner for a specific application. However, looking on the market as a whole, it turns out that the active capacitive technology has a range of attractive features that makes it a first choice in most applications.

Fingerprints technology comparison

	ACTIVE CAPACITIVE	ULTRASONIC	OPTICAL	ACTIVE THERMAL
Cost efficiency				
Design flexibility				
Technology maturity				
Security				
Convenience				
Power efficiency				
Mobile device adoption				

High Medium Low

Figure 26. Comparison of common fingerprint technologies

4.4 Fingerprint Extraction and Matching

As described earlier enrollment and authentication are two key operations in any biometric authentication system. With fingerprint recognition both operations can be made more convenient by adequate support measures, such as mechanical guides helping the user to place the finger correctly on the sensor and an intelligent user interface, leading the user through the enrollment process. If the fingerprint sensor is in an entity without own I/O capabilities, such as a credit card, additional features such as ***Near Field Communication (NFC)*** with a smartphone must be supported. The fingerprint image captured by the sensor is a monochrom digital image, i.e. an image of the same type that is generated by a digital camera but only containing a grey scale picture of the fingerprint. To enable enrollment and subsequent matching the captured image must first be enhanced in a preprocessing step before the features of the fingerprint can be extracted and used in the matching process. Image processing, feature extraction and matching are commonly referred to as the ***algorithms*** for fingerprint recognition.

Figure 27. Algorithms for fingerprint recognition

4.4.1 PREPROCESSING, FEATURE EXTRACTION AND TEMPLATE

Typically, the original grey scale fingerprint image has a bit depth of 8 bits, and depending on sensor size each such an image will require a few Mbyte of storage. Lossless or irreversible compression methods such as JPEG can be used to compress the image by a factor of 10 or more, but each image will still occupy some memory space. This is one of the reasons why the features of the fingerprint rather than the complete picture is used for matching; digitized features simply require less storage space and even more important, less complicated matching algorithms than should have been needed when using the full image.

The first step in the analysis is to use image processing techniques to obtain as distinct an image as possible of the fingerprint pattern. For grayscale images this can be done by discarding areas lighter than a threshold value, while those darker than the threshold are made black. Additional enhancement algorithms based on fingerprint ridge orientation and frequency may also be applied, resulting in a very high contrast picture of the fingerprint.

When minutiae based matching is used, the next step is the identification and location of these minutiae. For example, the point at which a ridge ends and the point where a bifurcation begins form minutiae. Once a minutia point has been identified, its location is registered as the distance from a central spot (the core) of the print. In addition to the placement of the minutia, the angle of the minutia is also normally registered. For example, when a ridge ends, its direction at the point of termination establishes the angle.

In addition to using the location and angle of minutiae, a minutia can be classified by its type and quality. The advantage of such a classification is that searches can be made quicker, as a particularly notable minutia may be distinctive enough to lead to a match.

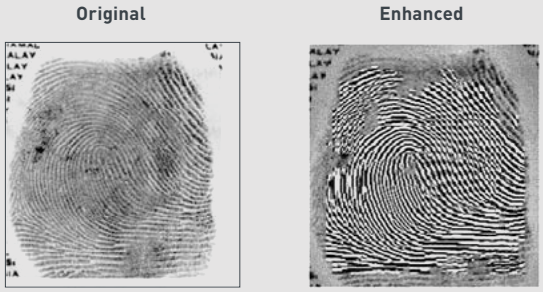

Figure 28. Original and enhanced fingerprint image

Anomalies caused by scars, sweat, or dirt appear as false minutiae, and algorithms locate any points or patterns that do not make sense, such as a spur on an island or a ridge crossing perpendicular to several others (probably a scar or dirt). A large percentage of would-be minutiae are therefore discarded in this process.

The matching accuracy of the authentication system relies on the stability of the biometric data associated with an individual over time. If my fingerprint looks different today than when I registered it in the enrollment process, I will not be authenticated.

The biometric data acquired from an individual is susceptible to changes introduced due to improper interaction with the sensor (e.g., partial fingerprints), modifications in sensor characteristics (e.g., optical vs. solid-state fingerprint sensor), variations in environmental factors (e.g., dry weather resulting in faint fingerprints) and temporary alterations in the biometric trait itself (e.g., cuts/scars on fingerprints). Thus, it is possible for the stored template data to be significantly different from those obtained during authentication, resulting in an inferior performance (higher number of false rejects) of the biometric system.

One way of overcoming the problems with varying fingerprints from the same individual is to store multiple templates of the same fingerprint in the template database. One could for example store multiple impressions pertaining to different portions of a user's fingerprint to deal with the fact that the user will place his finger in various ways on the sensor. There is however a tradeoff between the number of templates used and the storage and computational requirements of multiple templates.

4.4.2 MATCHING

Minutiae based algorithms

Automatic minutiae detection is a complex process, especially with low-quality fingerprints where noise and contrast deficiencies can originate pixel aggregations similar to minutiae and hide the real minutiae. Successful matching requires that the fingerprint features have been extracted with care, that a template with matching characteristics can be found and that the matching algorithm as such can perform an efficient comparison of the minutiae of the image with those on the template.

Non-minutiae based algorithms

Non-minutiae based algorithms – i.e. various alternative algorithm approaches – compare the basic fingerprint patterns (arch, whorl, and loop) between a previously stored template and a candidate fingerprint. This often requires that the images can be aligned in the same orientation. To do this, the algorithm finds a central point in the fingerprint image and centers on that. In a non-minutiae based algorithm, the template contains the type, size, and orientation of patterns within the aligned fingerprint image. The candidate fingerprint image is compared with the template to determine the degree to which they match.

4.4.3 BIOMETRIC PROCESSORS

The execution of fingerprint recognition algorithms requires digital processing capabilities and memory space. In some applications having their own powerful processors, such as mobile phones, these algorithms can be executed by the main processor acting as a host processor. Other applications, such as door locks and card readers which do not have a host processor in the product capable of interacting directly with a fingerprint sensor, will require a dedicated ***biometric processor*** as part of the solution.

Biometric processors are digital ASICs specifically designed for the purpose of biometric authentication. The processor runs the relevant extraction and matching algorithms and performs enrollment, identification and verification. As power consumption and size are important in many applications, the biometric processors must be small and power efficient. The biometric processor is then interfaced to the main processor of the product over a standard interface, for example a serial port, from which it takes commands and delivers results.

5. SUMMARY

Biometrics is in many ways the ideal way to identify and authenticate a human being. Biometric sensors can be made very secure while still fast and easy to use – and the biometrics always stays with the user and is never forgotten or left at home. Among the various biometric identifiers (modalities) fingerprintrecognition has several advantages and it has therefore taken the lead when it comes to driving consumers´ use and acceptance of biometrics in e.g. mobile devices such as smartphones.

Fingerprint recognition relies upon the unique pattern of ridges and valleys on the outer skin of the fingers, a pattern which normally stays invariant over the whole life of a person. The fingerprint pattern can be read by various methods such as optical, capacitive and ultrasonic, where the active capacitive technology has proven to be the most reliable and cost efficient for use in mass market devices. Thanks to small size, low power consumption and a high degree of flexibility in packaging, active capacitive sensors can also easily be integrated with other products, may it be PCs, smartcards or IoT.

An equally important element of efficient fingerprint recognition are the algorithms used for extraction and matching of the fingerprint pattern. Choosing the best algorithms impacts both how convenient it will be to use the sensor as well as the power consumed by the processor performing the matching.

Fingerprints™ is a publicly traded company that offers a complete range of user friendly fingerprint biometrics solutions. The solutions meet the highest demands in both industrial design process as in end user experience. The hardware covers sensors and complete modules and is combined with software that enhances the end user experience and offers multiple possibilities of differentiation for the Fingerprints™ customer.

For more information about Fingerprints™ portfolio visit: www.fingerprints.com

FINGERPRINTS