Chapter 5

State of the art in fingerprint recognition

Ondřej Kanich[1] and Martin Drahanský[1]

5.1 Introduction

This chapter deals with fingerprint recognition technology. Each of us has *papillary lines* (elevated skin reliefs, called often *ridges* and the gaps between ridges are called *valleys*) that are uniquely shaped for each person so that they can be distinguished on the basis of their passing through each other on the surface of their fingers (hands and feet). Today, it is the most widespread technology that can be met in almost everyday life.

5.1.1 User acceptance

Due to the relatively massive expansion of fingerprint technology to everyday life, there is a problem with the user's acceptance of this technology. Nowadays almost everyone saw or used fingerprint readers—they are integrated into laptops, mobile phones and other mobile devices, various attendance or access systems are based on fingerprints, etc. However, some users are negatively linking fingerprints with criminal police and investigations. Another part of the people has (legitimate) fear of fingerprint abuse—the fingerprint itself is easily obtainable because everything someone touches contains his/her fingerprint. This is a relatively easy way to get it, to make an artificial fingerprint fake and use it for spoofing the biometric system.

Another danger that exists here is the abuse of a template with stored minutiae, that is, a template that does not contain a fingerprint image but only extracted features. Even from this data, it is possible to generate a synthetic fingerprint and create a fake fingerprint, which is most likely to be used with most fingerprint systems. On the other hand, the user needs to be reassured—the templates are cryptographically protected, i.e., the data cannot usually be read directly, and many existing sensors already have built-in liveness detection (antispoofing methods) that reveals fake or dead fingers, i.e., the security of this technology is really high.

[1]Faculty of Information Technology, Centre of Excellence IT4Innovations, Brno University of Technology, Czech Republic

5.1.2 Reliability

First, let's look at fingerprint technology representation on the biometric market (see Figure 5.1—the trend did not change significantly since 2011, and the prognosis till 2021 is still the same, i.e., people will still trust to the same technologies [1]). The fingerprint technology itself, which includes access and attendance systems in particular, occupies 17% of the total market, excluding automated fingerprint identification systems (AFISs) (fingerprint recognition systems for identification and verification purposes in forensic practice). The main market share belongs to iris (20%), followed by fingerprints (17%), face (17%), hand/palm (16%) and voice (15%). The vein structure has 10% and other biometric technologies reach together 5% of the market share. However, AFISs would change the role, because they are used in nearly each country for forensic purposes (crime investigation), i.e., fingerprints have probably still the majority on the market.

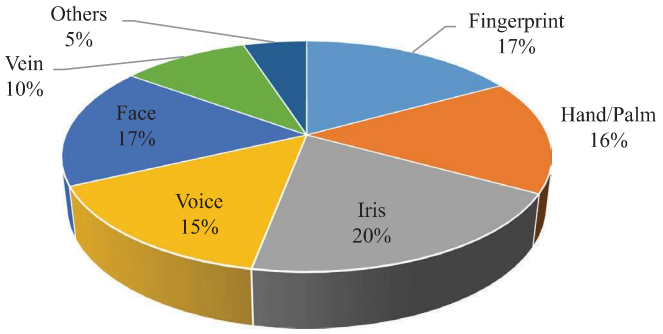

Figure 5.1 Distribution of biometric technologies on the market [1]

One reason for the massive spread of fingerprints is the use for criminal investigation, where fingerprints are taken as the main evidence, which associates a sense of confidence in this technology, when it clearly demonstrates the identity of a person in such a sensitive area as criminal investigation and subsequent law case.

One important factor is the amount of information that is hidden in the fingerprint, so how many people can be theoretically recognized from each other just using their fingerprints. This quantity, even if it is not fully correct from the viewpoint of information theory, is usually called biometric entropy. The creation of the fingerprint model and the subsequent calculation of the amount of information contained therein could be found, e.g., in these works [2,3]. Table 5.1 shows that, according to the set parameters (N, R and M), the probability of matching two fingerprints is in the order of 10^{-7} to 10^{-80}. On the contrary, the model proposed in [3] posed a different question—how large is the maximum amount of information contained in the fingerprint, i.e., how many people can be recognized on the basis of this information. The result is in the order of 2^{122}, i.e., 10^{36}. The range is of course larger—depending on the parameters used in the computational model, but in real conditions, the idealized results cannot be taken seriously.

Table 5.1 Comparison of probability of fingerprint matching for different models [2]

Author	p (fingerprint configuration)	$N = 36$, $R = 24$, $M = 72$	$N = 12$, $R = 8$, $M = 24$
Galton (1892)	$(1/16) \times (1/256) \times (1/2)^R$	$1.45 \cdot 10^{-11}$	$9.54 \cdot 10^{-7}$
Pearson (1930)	$(1/16) \times (1/256) \times (1/36)^R$	$1.09 \cdot 10^{-41}$	$8.65 \cdot 10^{-17}$
Henry (1900)	$(1/4)^{N+2}$	$1.32 \cdot 10^{-23}$	$3.72 \cdot 10^{-9}$
Wentworth and Wilder (1918)	$(1/50)^N$	$6.87 \cdot 10^{-62}$	$4.10 \cdot 10^{-21}$
Cummins and Midlo (1943)	$(1/31) \times (1/50)^N$	$2.22 \cdot 10^{-63}$	$1.32 \cdot 10^{-22}$
Gupta (1968)	$(1/10) \times (1/10) \times (1/10)^N$	$1.00 \cdot 10^{-38}$	$1.00 \cdot 10^{-14}$
Roxburgh (1933)	$(1/1{,}000) \times (15/(10 \times 2.412))^N$	$3.75 \cdot 10^{-47}$	$3.35 \cdot 10^{-18}$
Trauring (1963)	$(0.1944)^N$	$2.47 \cdot 10^{-26}$	$2.91 \cdot 10^{-9}$
Osterburg (1980)	$(0.766)^{M-N} \times (0.234)^N$	$1.33 \cdot 10^{-27}$	$1.10 \cdot 10^{-9}$
Stoney (1985)	$(N/5) \times 0.6 \times (0.5 \cdot 10^{-3})^{N-1}$	$1.20 \cdot 10^{-80}$	$3.50 \cdot 10^{-26}$

As with other technologies, error rates for the fingerprint technology are expressed using false acceptance rate (FAR)/false rejection rate (FRR), false match rate (FMR)/false non-match rate (FNMR) and receiver operating characteristics (ROC)/detection error tradeoff (DET) values. Normally, industrial fingerprint algorithms move at FAR or FRR (calculated according to equal error rate (EER)) around 10^{-1} [4]. The individual values vary depending on the sensor manufacturer and the algorithm, not least the population that uses the technology. According to [5], the FAR was around 0.01%, while the FRR was around 0.6%. An inappropriate example of a population can be, e.g., a company where employees have a damaged papillary lines due to hard work. They may be, e.g., elderly people, who develop creases (wrinkles) on the fingertips—the papillary lines recede into the background. Generally speaking, fingerprint technology has an almost excellent recognition capability that is close to 100% thanks to very advanced algorithms. Some works are devoted to fingerprint image enhancement, including fingerprints with skin diseases.

5.2 History

The use of biometric characteristics is known since ancient times. Basically, people use biometric recognition on a daily basis—they are able to recognize a concrete person by voice, face, walk, etc. All this information is human biometric—it can be recorded and then process it using a machine.

The oldest documented information regarded to the use of fingerprinting comes from China from the fourteenth century. However, these are indirect proofs of biometrics—the surviving drawings on the rock walls were similar to fingerprints, or the fingerprints of the author on surface (perhaps as evidence of authorship) were found on ceramics.

The first evidence of the use of fingerprints comes from the nineteenth century A.D. At this time fingerprints began to be used in crime investigation. The preserved written materials are specifically the following:

- 1858—*William James Herschel* was the English Governor of India (Hooghly) and began to use fingerprints for track-recorders to confirm people's identity. Most of the local workers could not read and write, and it was impossible for them to expect a signature when they received the paycheck. Mr. Herschel let every laborer print the fingerprint original to his payroll tape, confirming the identity of the worker and at the same time the lawful remittance of money. At the same time, he began to collect fingerprints for his own research, which helped to write a work on the origin of fingerprints [6].
- 1865—*Francis Galton* came up with a study of the inheritance of physical properties [7], in which he discussed the fact that children inherit from their parents some of their properties, including physical characteristics and behavioral characteristics.
- 1869—*Francis Galton* becomes cofounder of science called *eugenics*, which is a doctrine of hereditary diseases and defects in the fetus. This field is based on his previous work. Later, in 1875, Francis Galton became the founder of twin research.
- 1880—*Francis Galton* comes with the science of *anthropometry* [8], which is a method of measurement of human body dimensions.
- 1882—*Alphonse Bertillon* introduced and used the *Bertillionage* [9] since 1879. It is essentially anthropometry, which has led to a collision with Francis Galton's anthropometric approach.
- 1892—*Francis Galton* published a complete work of "Fingerprints" [10], which brought dactyloscopy [11] into practice in 1900. In the following year (1893), Francis Galton compares dactyloscopy with anthropometry, and in 1894 concludes that both methods are good and reliable, so they both provide practical use. In 1896, the dactyloscopy was used as an identification system in Argentina.
- 1900—Francis Galton enforces dactyloscopy for identification and verification purposes. He proved the permanence and uniqueness of the skin reliefs (papillary lines) on his fingers. Dactyloscopy was introduced into police practice.
- 1924—in this year, the Federal Bureau of Investigation (FBI) was established.
- 1965—for the first time, an AFIS [12] with 810,000 fingerprints was used.
- 2000—the AFIS at the FBI contains a total of 47 million ten prints of fingerprints (fingerprints from each hand). On average, there will be 50,000 searches per day. The response to remote search in the database is approximately 2 h.
- 2010—the AFIS at the FBI contains a total of 66 million ten prints of fingerprints (fingerprints from each hand). On average, there will be 162,000 searches per day. The response to remote search in the database is approximately 1 h and 10 min (processing an electronic request in an urgent case takes 10 min).
- 2011—the Advanced Fingerprint Identification Technology was deployed as part of NGI (Next-Generation Identification) project of FBI. It improves matching accuracy from 92% to over 99.6% [13].

- 2017 (September)—the NGI at the FBI contains a total of almost 120 million ten prints of fingerprints. On average, there is 210,358 ten-print fingerprint processed. Criminal response time (urgent) on average is 9 min and 58 s. Civil response time on average is 36 min and 11 s [14].

As mentioned above, each of us has papillary lines on the surface of our hand palms and feet soles, whose structure clearly determines the physical identity of a person. An exception is for people with various types of illnesses and skin disorders. Papillary lines have their own graphic representation—a *fingerprint*. Papillary lines are formed during embryonic development. The structure of the papillary lines is unchanged over time, of course, unless they are damaged by, e.g., cuts in dermis. Each finger is a unique pattern, i.e., there are no two identical fingers in the world [11].

At the beginning of the introduction to the theory of fingerprint recognition, history will be described. The first preserved remains are archeological artifacts and cave paintings. Names associated with the history of fingerprints:

- *Nehemiah Grew*—a pioneer of dactyloscopy, devoted his activity to the study of papillary lines and the location of sweat pores on his hands; in 1684, he published a work on the structure of papillary lines on his fingers and hands.
- *Johann Christoph Andreas Mayer*—published in 1788, a work on the uniqueness of fingerprints for each individual.
- *Thomas Bewick*—was a woodcutter and ornithologist, but since 1809, he used his fingerprint along with the written form of his name as a trademark, confirming the theory of the uniqueness of his fingerprint.
- *Jan Evangelista Purkyně*—in 1823, he published a work on nine classes of fingerprints but did not mention the use of fingerprints for identifying people.
- *Henry Faulds*—in 1880, he published a work on the usability of fingerprints for the purpose of identifying people and suggested a method for fingerprinting using ink.
- *Juan Vucetich*—in 1891, he introduced the use of fingerprints for criminalistics purposes, i.e., their categorization and use of the filing cabinet.
- *Francis Galton*—published a book on fingerprints [10] and calculated the probability of matching two fingerprints as 1–64 billion.

In the field of *dactyloscopy* [11], i.e., fingerprint recognition in forensic applications (for forensic purposes), so-called dactyloscopic laws [15] apply:

- There are no two people in the world whose papillary lines would have the same structure.
- A pattern formed by papillary lines remains relatively unchanged throughout the life of an individual.
- Papillary lines are restored by growing the skin at the finger surface. These cannot be altered or removed unless the dermal layer of the skin is damaged. Then there will be no renewal of papillary lines at this point.
- Configuration types vary individually, but the changes are small enough to lie within tolerance limits and thus allow for systematic classification.

5.3 Fingerprint types and acquisition methods

In dactyloscopic practice, three kinds of fingerprint that differ not only in appearance and location but also in the way of scanning can be seen (Figure 5.2):

- rolled (also colored)
- plain (alive)
- latent (also hidden)

However, there are fingerprints that are totally inappropriate for automated recognition or minutiae comparisons—these are primarily fingers suffering from various skin diseases or disorders on the surface of the fingertips.

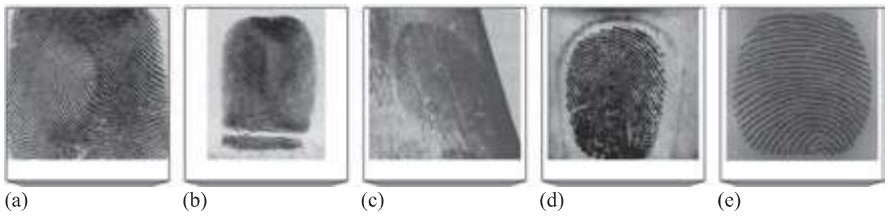

Figure 5.2 Fingerprints: (a) and (b) rolled, (c) latent, (d) and (e) plain

The term fingerprints is related to the basic term—the *papillary line = ridges* (Figure 5.3). A fingerprint is a pattern formed by a structure of papillary lines. The height of the papillary lines lies between 0.1 and 0.4 mm, and the width of the papillary lines is ranging from 0.2 to 0.5 mm.

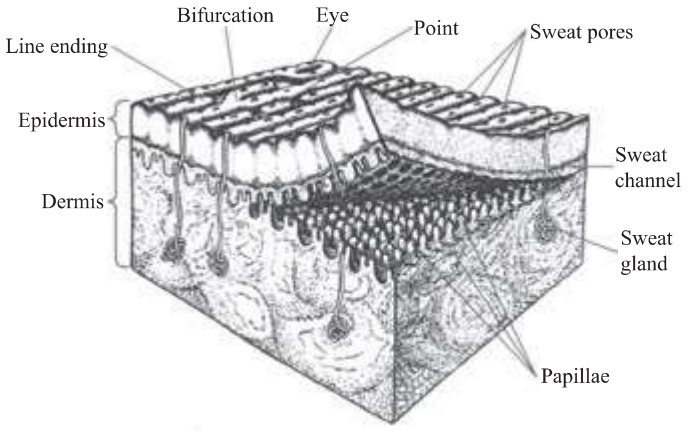

Figure 5.3 Cut of the skin with papillary lines [16]

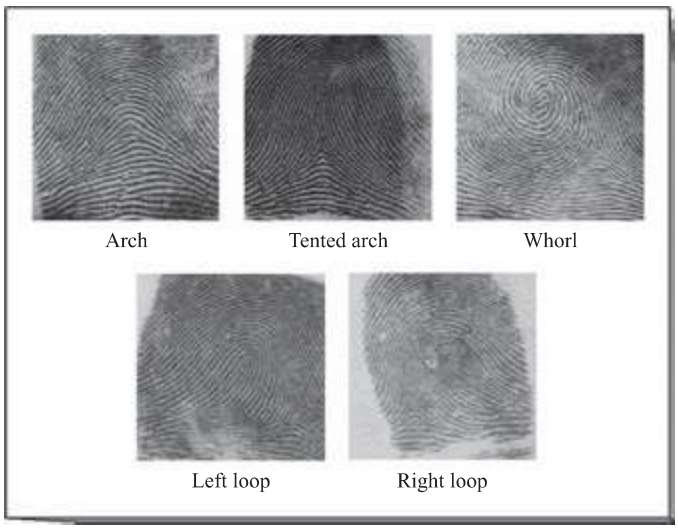

Figure 5.4 Fingerprint classes

From a global perspective, the papillary lines in the fingerprint create a pattern called the *fingerprint class* [17] (see Figure 5.4). The following fingerprint classes are known:

- arch
- tented arch
- whorl (spiral)
- left loop
- right loop

For classification of fingerprints in AFISs [12], *Henry's classification scheme* is used, which is based on the categorization of fingerprints into three basic classes—arch, loop and whorl. Individual derivations, such as tented arches, right or left loops and possibly double loops, divide fingerprints into other classes. In order to create a classification system, it was necessary to classify fingerprints into smaller subclasses so that it would not be necessary to search the whole database to find the identity of the criminal. Henry's classification system is named after Edward Henry, who has been linked to works by well-known researchers—W. Herschel, H. Faulds and F. Galton.

In dactyloscopic systems (for criminal police forensic purposes), all classes for classification are used. The fingerprint classification algorithm is based on the information contained in the fingerprint. Basic terms related to the classification [see Figure 5.5(a)] [18] are as follows:

- *Delta*—a fingerprint location where the papillary line runs in three directions (most of which are on the edge, there may be two deltas).

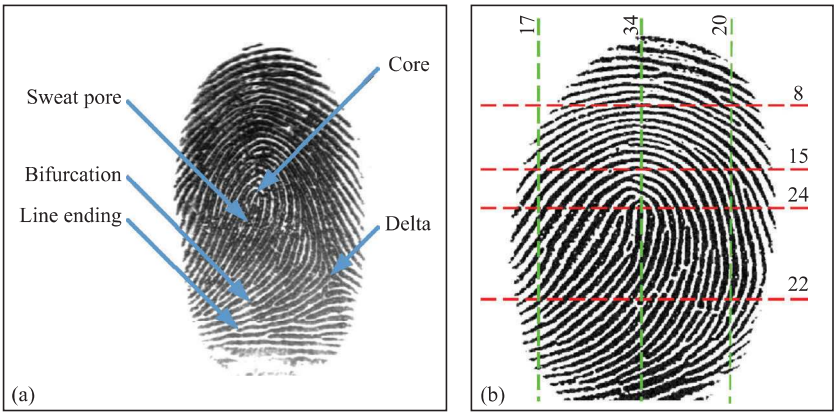

Figure 5.5 (a) Significant features of a fingerprint and (b) numbers of papillary lines

- *Core*—the center of the fingerprint, located at the lowest arch of the run of papillary lines in the fingerprint; the position does not match the actual center of the image.
- *Type lines*—they define the space between the topmost papillary line belonging to the center and the lowest one belonging to the delta.

The amount of papillary lines between two defined fingerprint points (most commonly between core and delta) is used as another metric for fingerprint classification. An example of the number of papillary lines in the vertical and horizontal directions is shown in Figure 5.5(b) (the number of papillary lines increases in the direction to the fingerprint core, similar to the concentric circles).

Fingerprints are distinguished, however, on the basis of special shapes that form papillary lines. These formations are called *minutiae* points. The basic minutiae include (see Figure 5.6, respectively) line ending, single fork, double fork (bifurcation), triple fork, hook, cross and side contact; bottom line of Figure 5.6: point, interval, single loop, double loop, single bridge, double bridge and intersection. In dactyloscopic systems for criminological purposes, much more minutiae are used than those listed here—but these are derived from the basic types of minutiae. Conversely, only two types are used for access systems: line ending and bifurcation.

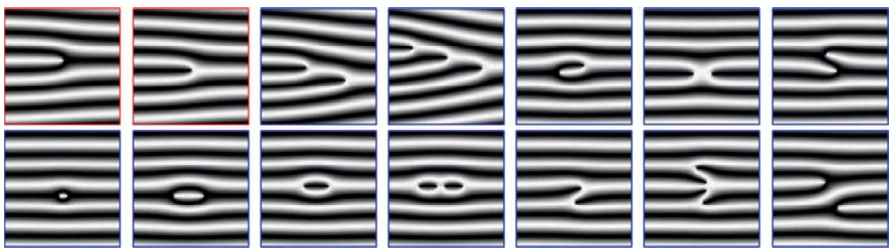

Figure 5.6 Basic types of minutiae

The *gradient* (*orientation*) of the minutia is the direction in which the papillary line would continue at the minutia point. Two notations can be distinguished (Figure 5.7: left image = line ending and right image = bifurcation):

- Mark A: standard notation
- Mark B: FBI/AFIS notation (opposite to standard notation)

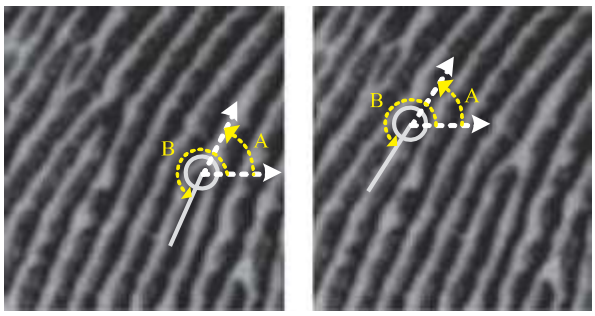

Figure 5.7 Standard (left) and FBI (right) notation of the minutia orientation

Electronic fingerprint readers are used in biometric fingerprint systems to acquire fingerprint images. The only exception being dactyloscopic cards, where the classic fingerprinting still prevails on a paper dactyloscopic card that is later loaded into the computer using a scanner. Some of the important parameters for fingerprint readers are resolution (ranging from 250 up to 1,000 dpi, the most common being around 500 dpi), scanning area (FBI recommends the area of 1×1 in., however, typically is around 0.7×0.7 cm for access systems and 10×6 cm for dactyloscopic fingerprint systems), amount of bits (number of bits for color coding—the standard is 8 bits for gray-scales, but sensors that only use 3 bits can be found), geometric accuracy (the amount of geometric fingerprint distortion versus reality) and image quality (various metrics such as [19] have been proposed for this parameter).

Following sensor technologies are distinguished [19]: *optical*, *capacitive*, *ultrasonic*, *e-field*, *electro-optical*, *pressure*, *thermal* and *microelectromechanical system (MEMS)*, including other less known methods (e.g., optical tomography).

However, exception will be discussed as first—ink fingerprint on a *dactyloscopic card* (see Figure 5.8). The dactyloscopic card consists of the description margins and the fingerprints themselves—the upper part prints all ten fingers in the form of plain fingerprints, and the control fingerprints of the fingertips are printed at the bottom. On the other side of the dactyloscopic card, there are palmprints.

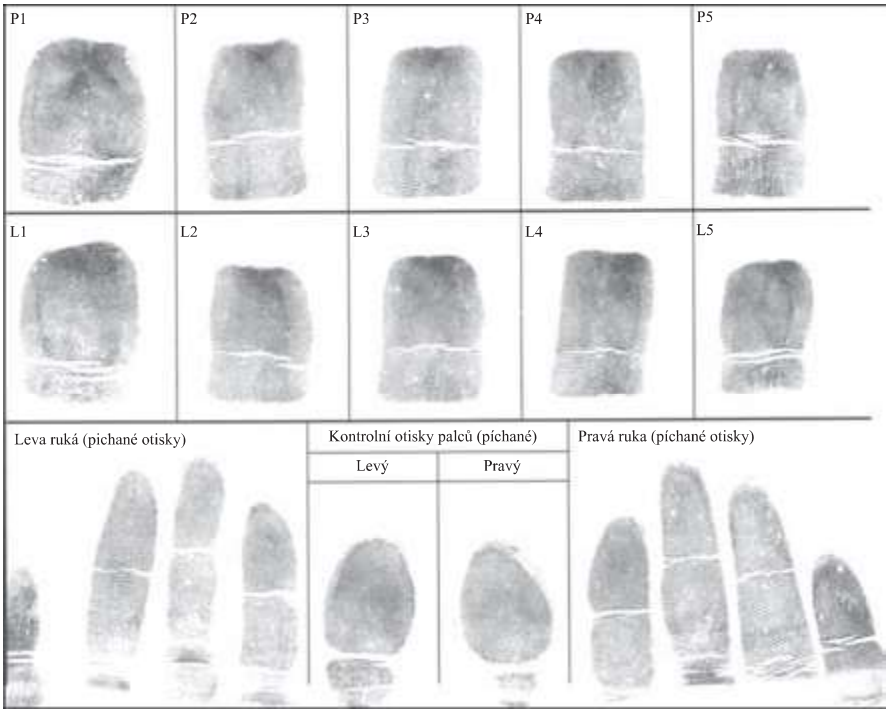

Figure 5.8 Example of a Czech dactyloscopic card (without description margins)

5.3.1 Optical technology

This is a relatively simple optical principle (see Figure 5.9), i.e., the light source (LED) illuminates the finger surface that is attached to the sensor's glass surface (there are also contactless 3D optical sensors, i.e., the finger has to not touch the surface in all cases—one example is the contactless fingerprint reader from the Swiss Company Touchless Biometric Systems) and the camera (CCD/CMOS) scans the image. When protective glass is replaced by a transparent roller tube and optics, the camera and light source are in it, and then the result is simple swipe optical sensor. It is also possible that such a roller functions like an optics and camera with a light source that is beneath it.

Another type of optical sensor uses optical coherence tomography (OCT) [20]. It is very expensive, but it gets the image from a deeper layer of the skin, which is harder to spoof. It can also obtain a view where sweat pores are clearly visible.

5.3.2 Capacitive technology

For capacitive technology (see Figure 5.10), the sensor is composed of a matrix of small conductive areas on which a layer of nonconductive silicon dioxide is put. The fineness of these conductive surfaces is higher than that of the papillary lines.

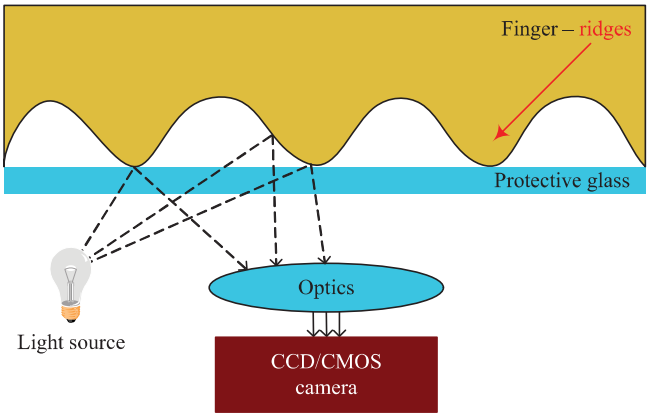

Figure 5.9 Principle of optical technology

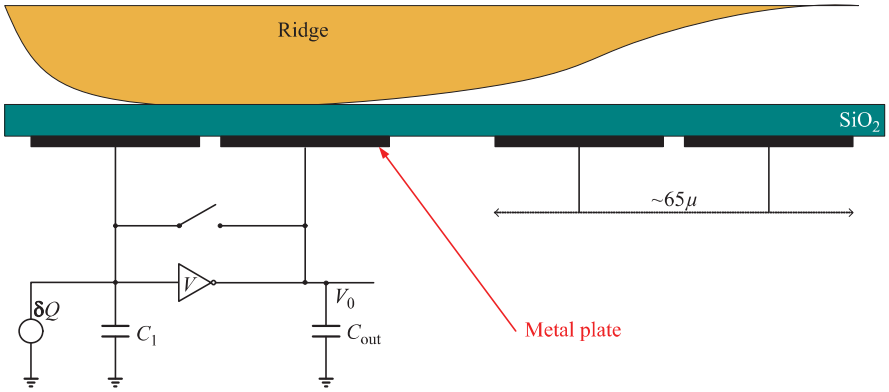

Figure 5.10 Principle of capacitive technology

By attaching a finger, capacitors (one electrode is the papillary line at the point of contact with the face of the sensor matrix and the other is just matrix plane) make the output of which is the value corresponding to the overlap of the surface area (see the capacitor principle). To create swipe sensor, one of the dimension is shortened. A related technology is so-called e-field technology [21].

There is one modification of the capacitive sensor that is worth mentioning. It is a combination of e-field and capacitive technology. It uses a low-radio frequency (RF) signal and because of that it is often known as RF technology. This signal is sent to the skin, and because of that, between the signal references plane and the live (conductive) layer of the skin, an RF electric field is created. Its equipotential contours mimic the shape of the live layer of the skin, so when it is measured by an antennae array, fingerprint image is produced. This principle can be seen in

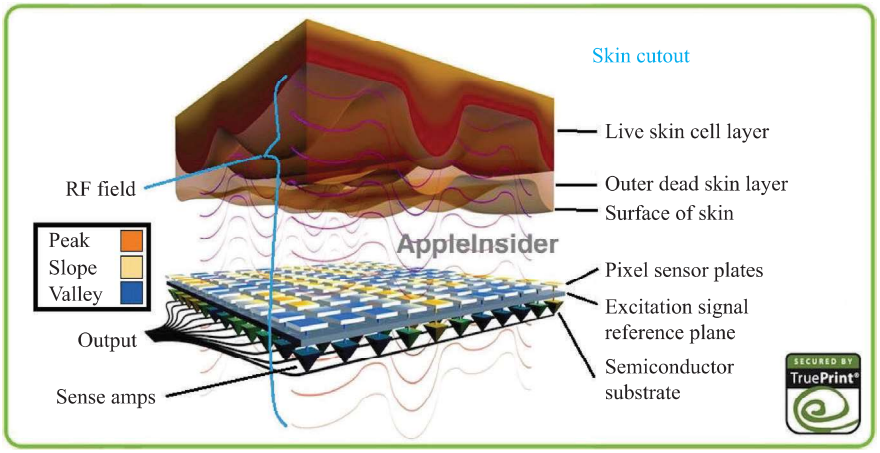

Figure 5.11 Principle of RF technology

Figure 5.11. Another interesting principle is using thin-film transistors on a capacitive touch panel. That way it is possible to have a touch-sensitive area (i.e., a smartphone can be controlled this way) and fingerprint sensing at the same time [22–24].

5.3.3 Ultrasonic technology

The ultrasonic technology is based on a rotating ultrasonic transducer (see Figure 5.12), which incorporates a receiver. This rotates along the circular path and scans the fingerprint. Ultrasonic waves penetrate even under the surface of the skin. This technology can easily detect fake fingers.

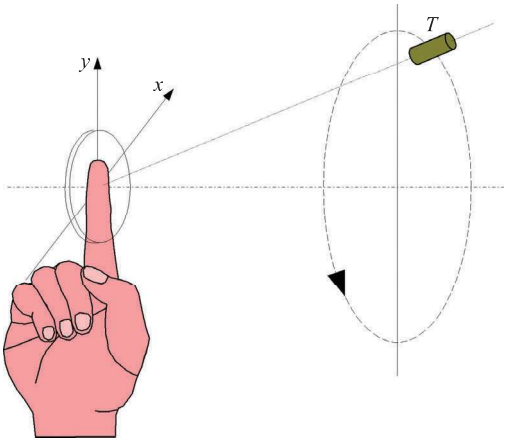

Figure 5.12 Principle of ultrasonic technology

5.3.4 Electro-optical technology

The sensor based on electro-optical technology consists of four layers, with the finger pressure eliciting contact of the black coaxial layer of emitting light in the phosphor layer. This radiation passes through the base layer into the sensor (see Figure 5.13).

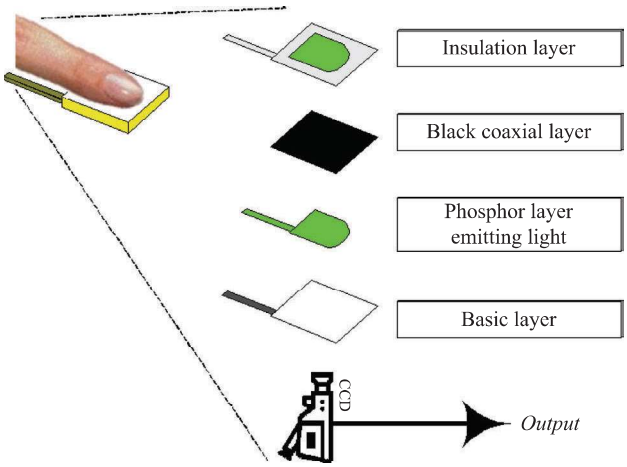

Figure 5.13 Principle of electrophoretic technology

5.3.5 Pressure technology

The pressure technology sensor consists of three layers, with a nonconductive gel inserted between the electroconductive layers (see Figure 5.14). By attaching a finger to the sensor surface, the nonconductive gel is pressed at the point of contact with the papillary lines and brings both electroconductive layers in touch.

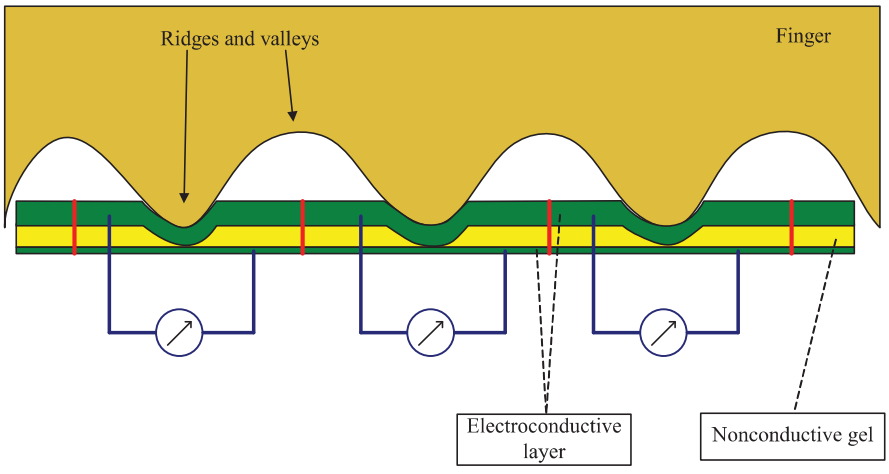

Figure 5.14 Principle of pressure technology

5.3.6 Thermal technology

The thermal technology principle is based on thermal radiation (see Figure 5.15). The papillary lines have a higher heat radiance than the valleys between them. The finger is swept over a pyroelectric cell that senses this thermal radiation.

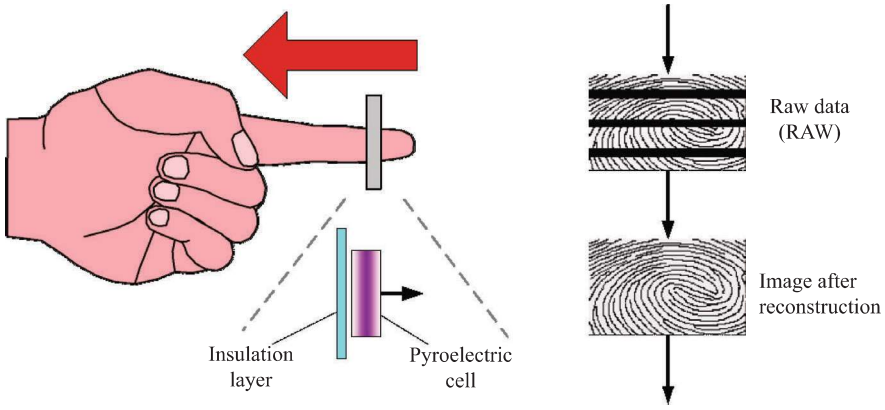

Figure 5.15 Principle of thermal technology

5.3.7 E-field technology

In this technology, the sensor consists of a drive ring and a matrix of antennas. The drive ring generates a sinusoidal radio frequency signal, and the matrix of active antennas receives that signal modulated by the skin structure, or, more precisely, modulated by the dermis structure, because the electric field passes the upper parts of the skin (the epidermis). Similarly to the ultrasonic technology, this technology is also resistant to fake fingers and ignores the dirt and light injuries on the finger. The image quality here is better than the one from capacitive or electro-optical sensors [17,25].

5.3.8 MEMS technology

The MEMS [25] uses micro parts to scan a fingerprint. One of the methods uses piezo-resistive micro beams. The user sweeps his finger along the sensor which consists of three rows of piezo-resistive gauges. Their parallel deflection will create a voltage variation which is measured and transformed into the fingerprint. The resulting image is only binary-colored, which is a big disadvantage of this type of sensor technology. This pressure-based MEMS swipe sensor principle can be seen in Figure 5.16. Another method is using microheaters. This method heats the finger a little bit and measures the change of temperature of the heat element. A ridge works as a heat sink, so the heat element which is connected to the ridge shows less of a rise in temperature [17,23,25].

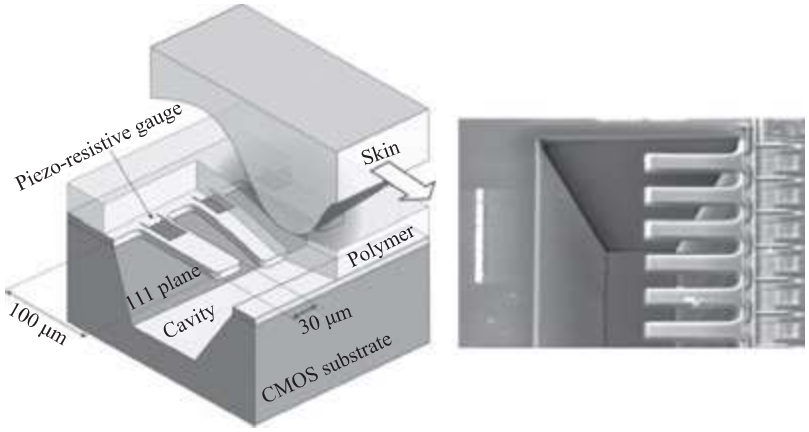

Figure 5.16 Principle of tactile MEMS technology

5.4 Fingerprint recognition

In general, there are two modes of use of the biometric system—registration and verification/identification. Registration usually takes place by the user having to place his or her registered finger three or five times on the sensor surface, and the system calculates the average of these fingerprints to produce the template with a high quality. Comparison (verification/identification) works similarly, but fingerprints can be mistaken either same fingerprints can be compared as different (due to intraclass variability) or similar fingerprints that come from totally different individuals (due to interclass variability). Therefore, the comparison process is not very simple. The fingerprint process is illustrated in Figure 5.17. This process consists of the steps described in the following subsections.

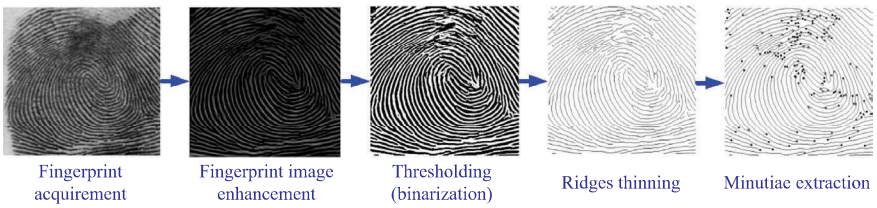

Figure 5.17 Scheme of the fingerprint processing

5.4.1 Fingerprint image and its processing

The first step of fingerprint processing is to capture (acquire) an input image, preprocess and extract papillary lines. Through this process, a proper description of the course of the papillary lines is obtained from the fingerprint image and can be further processed.

5.4.1.1 Image capture

Sensing a fingerprint image, such as getting a fingerprint image from a sensor (optical, capacitive, ...), or another template, gives us a basic, digital form of fingerprint. There is a large amount of noise in the input image, which requires subsequent enhancement. When scanning, it is necessary to distinguish between rolled/plain and possibly latent fingerprints. In addition, it is necessary to take care of the effects of damaged fingerprints, injuries, etc. It is necessary to check the liveness of the finger (antispoofing), whether there is not any spoof used instead of a real finger from a genuine user.

5.4.1.2 Orientation field

For the computation of the orientation field, it is necessary to calculate the direction of the papillary line from the surroundings (according to the gray color tone) at each point of the image. If the point is directly on the papillary line, it will most likely determine its direction. First, the orientation field for each pixel is calculated. In the second step, the transformation to the block orientation field is done. The block orientation field is then mapped on the original fingerprint image. A sample of the (block) orientation field is shown in Figure 5.18. Methods used are usually focusing on local analysis, global analysis or adaptive methods which are trying to combine both approaches [26].

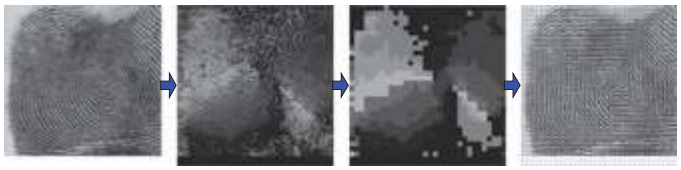

Figure 5.18 Calculation of the orientation field

5.4.1.3 Extraction of papillary lines

Further enhancement of the image and thresholding will provide black papillary lines and white background. This image enhancement includes, e.g., histogram scaling. This is related to the quality control of the input image [19]. The 2D Gabor function is used for filtering (often in the previous step—computation of orientation field). For filtering in the frequency domain (FFT → Filter Application → IFFT), the following filters are used:

Low Pass:

$$H(u,v) = \begin{cases} 1 & D(u,v) \le D_0 \\ 0 & D(u,v) > D_0 \end{cases} \tag{5.1}$$

where D_0 is the border frequency and $D(u,v) = \sqrt{u^2 + v^2}$.

Filter Butterworth [27]:

$$H(u,v) = \frac{1}{1 + [D(u,v)/D_0]^{2n}} \tag{5.2}$$

Filter Ikonomopoulos [28]:

$$H_i = \begin{cases} 1 & \theta_i < \tan^{-1}(v/u) < \theta_{i+1} \wedge u^2 + v^2 > r_c^2 \\ 0 & \text{otherwise} \end{cases} \tag{5.3}$$

where u and v are frequency coordinates, n is number of directions and $\theta_i = (i-1)\pi/2n$.

For example, the *regional average thresholding* scheme [18], which first divides the image into 8×8 blocks, is used for image thresholding (except for other methods), then calculates the average level of gray in that area, then sets the value of the left 8×4 to this value and moves the operation window 4 points to the right. When the right edge is reached, the window moves 8 points down and starts again from the left.

5.4.1.4 Thinning of papillary lines

From the previous step, image of papillary lines is obtained, each of which could have various widths. The next step is to thin the papillary lines to a 1 point thickness. For thinning, a relatively simple algorithm is used to reduce the number of dots on the image of the papillary line so that its thickness will be only 1 point. The most commonly used method is based on Emyroglu [28], which uses two types of points (*ridge meeting point* and *ridge continuity point*). It must be true that the papillary line must not dwindle in any direction in order to avoid a problem with the position of the minutiae.

5.4.2 Detection and extraction of minutiae

For the detection and extraction of minutiae, the method of detecting papillary lines according to Hong, the so-called Hong method [29], is used (among other possible methods). This method is based on the fact that the papillary lines run parallel to each other and reach the maximum level of gray in the middle of the line (black/dark points). The fingerprint is multiplied by two h_t and h_b masks that have a 180° offset phase [29]:

$$h_t(i,j;u,v) = \begin{cases} -\dfrac{1}{\sqrt{2\pi}\delta} e^{-\left(u^2/\delta^2\right)} & \text{for } u = (v \cdot \cot(\mathrm{O}(i,j))) - \dfrac{H}{2\cos(\mathrm{O}(i,j))} \wedge v \in \Omega \\ \dfrac{1}{\sqrt{2\pi}\delta} e^{-\left(u^2/\delta^2\right)} & \text{for } u = (v \cdot \cot(\mathrm{O}(i,j))) \wedge v \in \Omega \\ 0 & \text{otherwise} \end{cases} \tag{5.4}$$

$$h_b(i,j;u,v) = \begin{cases} -\dfrac{1}{\sqrt{2\pi}\delta} e^{-\left(u^2/\delta^2\right)} & \text{for } u = (v \cdot \cot(\mathrm{O}(i,j)) + \dfrac{H}{2\cos(\mathrm{O}(i,j))} \wedge v \in \Omega \\ \dfrac{1}{\sqrt{2\pi}\delta} e^{-\left(u^2/\delta^2\right)} & \text{for } u = (v \cdot \cot(\mathrm{O}(i,j))) \wedge v \in \Omega \\ 0 & \text{otherwise} \end{cases} \tag{5.5}$$

$$\Omega = \left[-\left| \frac{L \sin(\mathrm{O}(i,j))}{2} \right|, \left| \frac{L \sin(\mathrm{O}(i,j))}{2} \right| \right] \tag{5.6}$$

On average, $L \times H$ is 11×7 [29]. Ideally, the mask width should be equal to the width of the local line. Point (i, j) is marked as a point of the papillary line if both values after convolutions (h_t and h_b filters) are larger than the threshold T_R. With respect to the parameter δ, both masks and smoothing are performed. In the resulting image, it is necessary to check and correct the damages of papillary lines and filling breaks in the papillary lines run.

Generally, two basic types of minutiae are detected: papillary *line ending* and *bifurcation*, while other types of minutiae are a combination of these two basic types. Detection decisions are made on the basis of the following conditions:

- If $\sum_{u=-1}^{1} \sum_{v=-1}^{1} T_R(i+u, j+v) = 2$, then it is a *line ending*.
- If $\sum_{u=-1}^{1} \sum_{v=-1}^{1} T_R(i+u, j+v) > 3$, then it is a *bifurcation*.

This situation is schematically illustrated in Figure 5.19. Both conditions mean, in essence, that the sum of points in the neighborhood is made, and if it is equal to 2, it is a line ending, and if it is greater than 3, it is a bifurcation.

The following data is stored for each minutia: the *position* of the minutia (coordinates x and y), the *type* of the minutia (line ending/bifurcation) and the *gradient* (the orientation of the papillary line).

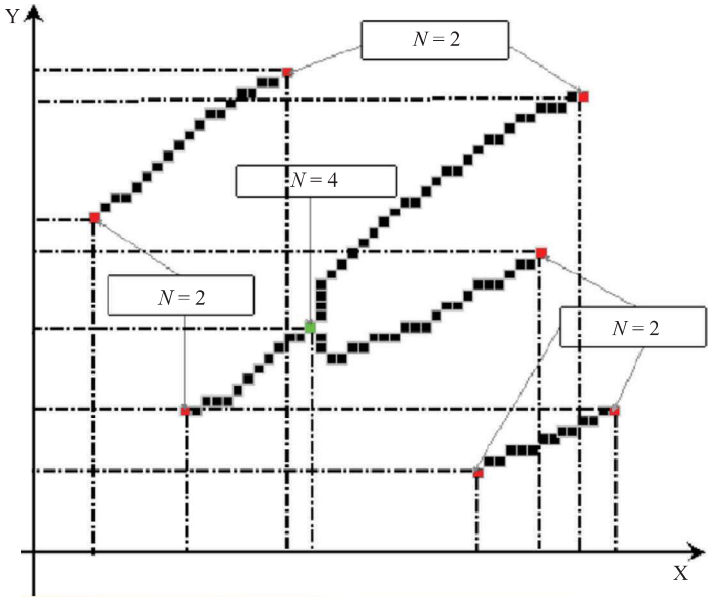

Figure 5.19 Representation of the detection of minutiae on thinned papillary lines

5.4.2.1 Methods of fingerprint recognition

The result of the extraction of minutiae is compared with the stored template from the database, smart cards, etc. The methods for comparing fingerprints are as follows:

- Methods based on minutiae [3,17,30]
  - They use position, type and gradient (direction)
  - Generally, issues of pattern comparison.
- Methods based on correlation [31,32]
  - 2D correlation between input and template
  - Computationally demanding but implementable in hardware.
- Methods based on the properties of papillary lines [33]
  - Orientation and frequency of papillary lines, line shape, texture information, etc.
  - Low resolution, but often used as support information for the minutiae-based method.
- Methods based on high resolution or 3D properties of the finger or papillary lines [34]
  - Usage level of 3D features e.g., sweat pores placement and distribution, ridge edge features, etc.
  - Usage of 3D features such as curvature of the finger, depth values, etc.
  - Can be combined with traditional 2D methods mentioned above.

5.4.2.2 Recognition based on minutiae

The method based on minutiae is the most commonly used method. This is practically a problem of comparing patterns—two sets of minutiae. Two basic methods for comparison using the minutiae are *Hong method* [35] and *Ratha method* [36]. Both methods are based on two main steps: generating a global overlap (alignment) and locating a local overlap (compare)—see Figure 5.20. A schematic representation of the course of the methods is shown in Figure 5.21.

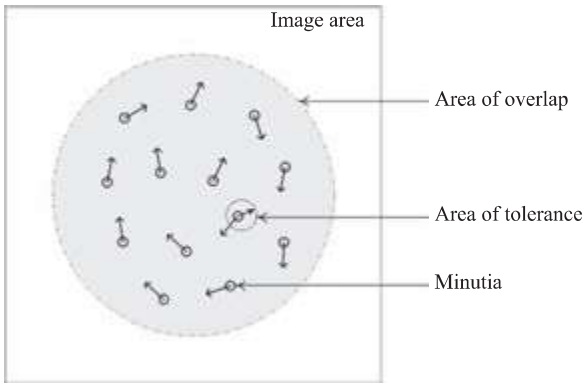

Figure 5.20 Areas of overlap and tolerance

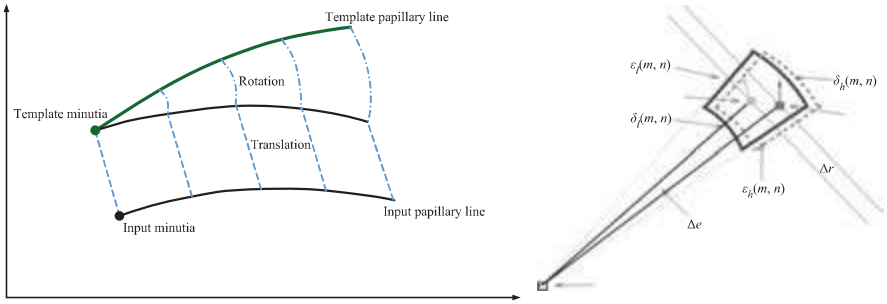

Figure 5.21 A schematic representation of the comparison based on minutiae

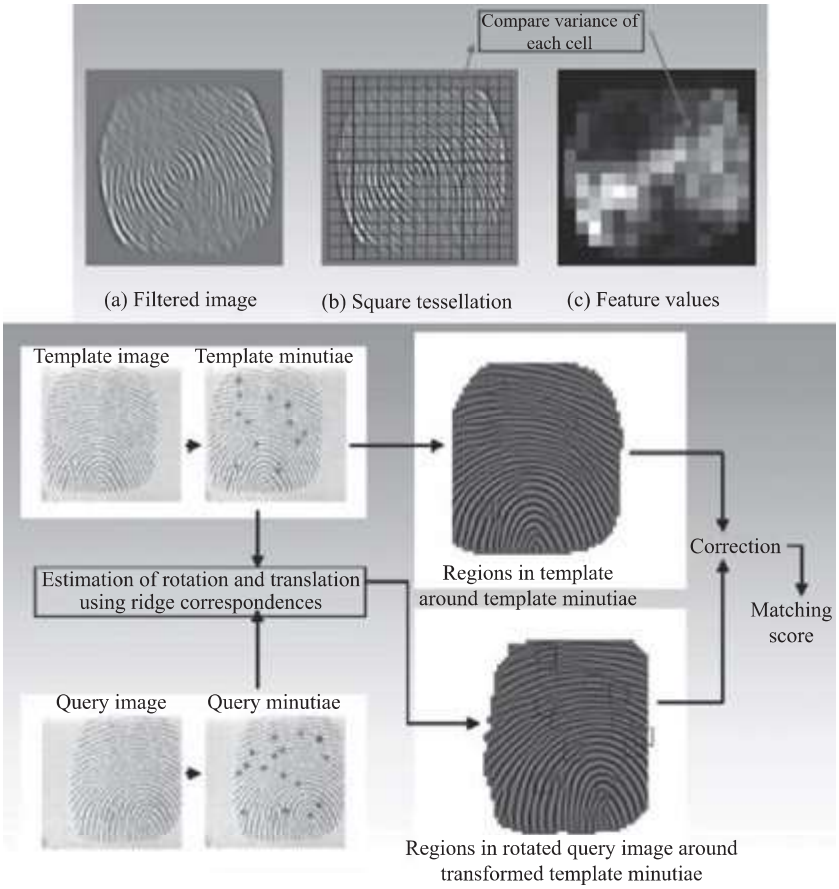

Figure 5.22 Recognition based on the properties of papillary lines (top) and recognition based on correlation (down) [39]

The more recent methods are focused on their portability on light architectures (like smart card or system-on-a-chip) or to suitability for template-protection techniques (necessity of fixed-length, alignment free, noise-tolerant feature coding). Example can be minutia cylinder-code which encodes spatial and directional relationships between minutia and its neighborhood [30].

5.4.2.3 Recognition based on the properties of papillary lines

The procedure for the method based on the properties of the papillary lines is shown in Figure 5.22. This is a description of peculiarities (curvature) of the papillary lines, which are then used for comparison.

5.5 Difficult fingerprints

From the beginning of use of fingerprints, it is fully obvious that sometimes the fingerprint has a very low quality. First of all, phenomena that are connected to the finger itself will be discussed—the *dirt on the finger* which can be caused by a few grains of dust, small particle or a greasy finger from some meal. Liquids or generally conductive materials are one of the most problematic types of dirt. For every sensor technology, the most problematic type of dirt is different. These phenomena can be in conjunction with the *dry or moist finger*. Sweaty fingers for example could be assigned to both groups. The effect of moisture or dryness of the finger is very significant. It is also a very frequent way of damaging the fingerprint. Investigated user can be very nervous which leads to sweaty or extremely dry fingers. On the other hand, in the everyday usage, fingers can be moist after using some lotion or they can be simply recently washed. The skin resistance which is important for some sensors can be up to ten times higher or lower than the average value. The *physically damaged finger* is common in some groups of users, namely, among people who are employed in manual work. In their jobs, some abrasions or cuts are inevitable. If it is only a small injury or everyday wear damage, the papillary lines will regenerate. On the contrary, a deep wound will affect the papillary lines forever. Fingers can be also damaged by *skin diseases*—this will be described in Chapter 7 [37,38].

The second part of this category is the phenomena caused by users when acquiring the image. One of them, usually caused by inexperienced users, is small or insufficient *contact region*. That simply means that the finger was presented to the sensor in a way which allows only a partial acquisition of the fingerprint. The small contact region can also be caused by extremely low *pressure*. The other way around, very high pressure can create a black oval instead of the fingerprint image. When the pressure is somewhere between these extremes, it can cause either very thick or very thin papillary lines. It is very sensor dependent what the "right" pressure is. There is an endless number of movements that users can do when showing the *noncooperative behavior*. It can be dynamic or static behavior which is done on purpose, i.e., it is not an accident. The line between an unintentional wrong usage and a noncooperative behavior is very thin. Nevertheless, there are users who resent biometric systems or just try to push to its limits. They can move the finger

or change the pressure while the sensor is acquiring image. The other possibility is the static behavior like a rotation of the finger, a small contact region with just a side of the finger, etc. The details about damaged fingerprints will be discussed in Chapter 7.

5.6 Fingerprint related standards

The most standards generally affect all biometrics, including fingerprints. Still, there are some specific standards or parts of them that are tightly bound only to fingerprints. Specific fingerprint standards are as follows (these are the most important):

- ISO/IEC 19794-2: Information technology—biometric data interchange formats—finger minutiae data, September 2005 and December 2011.
- ISO/IEC 19794-3: Information technology—biometric data interchange formats—finger pattern spectral data, August 2006.
- ISO/IEC 19794-4: Information technology—biometric data interchange formats—finger pattern skeletal data, October 2006.
- ISO/IEC 19794-8: Information technology—biometric data interchange formats—finger pattern skeletal data, December 2011.
- ISO/IEC 20027: Biometrics interoperability profiles—best practices for slap ten-print captures, September 2015.
- ISO/IEC 24779-4: Information technology—cross-jurisdictional and societal aspects of implementation of biometric technologies—pictograms, icons and symbols for use with biometric systems—fingerprint applications, January 2017.
- ISO/IEC 29198: Information technology—biometrics—characterization and measurement of difficulty for fingerprint databases for technology evaluation, December 2013.
- ANSI/INCITS 381-2009: ANSI—finger-image-based interchange format, NIST, 2009 (revision of ANSI/INCITS 381-2004, May 2004).
- ANSI/INCITS 377-2009: ANSI—finger-pattern-based interchange format, NIST, 2009 (revision of ANSI/INCITS 377-2004 from February 2004).
- ANSI/INCITS 378-2009: ANSI—finger minutiae format for data interchange, NIST, 2009 (revision of ANSI/INCITS 378-2004 from February 2004).
- ANSI/INCITS 398/2008: ANSI—common biometric exchange formats framework (CBEFF), NIST, 2008 (revision of ANSI/INCITS 398-2005 from 2005).
- ANSI/NIST CSL 1-1993: Data format for the exchange of fingerprint information, ANSI, November 1993.
- ANSI/NIST ITL 1-2007: Data format for interchange of fingerprint, facial and other biometric information, NIST, May 2007 (revision of ANSI/NIST ITL 1-2000 from September 2000).
- IAFIS-IC-0010: Electronic fingerprint specification, FBI, December 1995.
- IAFIS-IC-0110V2: WSQ—fingerprint script compression specifications, FBI, February 1993.

- CJIS-IC-0020: WAN interface specification (fingerprint transfer), FBI, November 1995.
- Further parts of the ISO/IEC 19795 standards, which deal with biometric systems in general, but also specify some specific requirements for fingerprints.

5.7 Commercial devices and applications

The focus will be on commercial devices that are available on the market. Their distribution will be based on the scanning technologies of the individual devices. Firstly, *optical* technology—examples are shown in Figure 5.23 (left to right: Identix BioTouch® 500; Sagem MorphoSmart Optic 300; BioLink MatchBook 3.5). Other technologies are *capacitive* sensors, as shown in Figure 5.24 (from left to right: Veridicom 5th Sense; Fujitsu MBF200; UPEK TouchStrip™ TCS3-TCD4). Follow the *ultrasound* and *e-field* technology—see Figure 5.25 (left to right: UltraScan; Optel, the right-hand side is Bio-i CYTE). *Pressure* and *temperature* sensitive technologies are also shown—see Figure 5.26 (left to right: BMF BLP-100; Fidelica FIS-3002; Atmel® AT77C104B is thermal (right)). Lastly *RF* sensors and prototype of *OCT technology* can be seen in Figure 5.27 (from left to right: Swipe Sensor Development Kit FPC-SSD with Fingerprints FPC1080A Swipe Sensor, Zvetco Verifi P5100 with AuthenTec TCS1 sensor and lastly OCT prototype from Langevin Institute in Paris [40]).

Fingerprint information can also be used to generate a key that can be used for cryptographic purposes. This is called a biometric security system. Figure 5.28

Figure 5.23 Commercial devices—optical technology

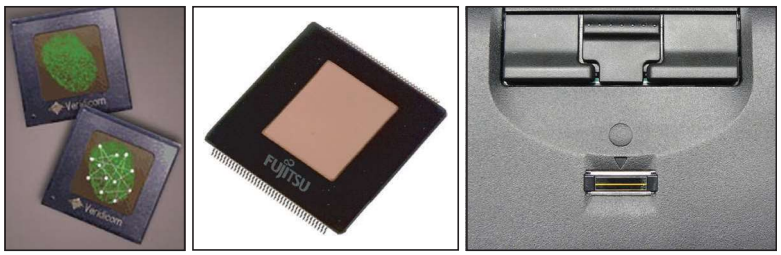

Figure 5.24 Commercial devices—capacitive technology

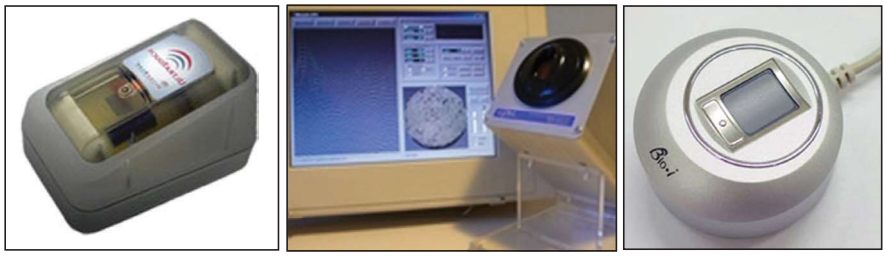

Figure 5.25 Commercial devices—ultrasound and e-field technology

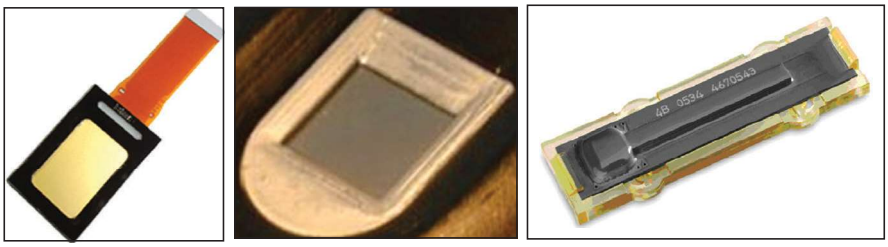

Figure 5.26 Commercial devices—pressure and temperature sensitive technology

Figure 5.27 Commercial devices—RF and OCT technology

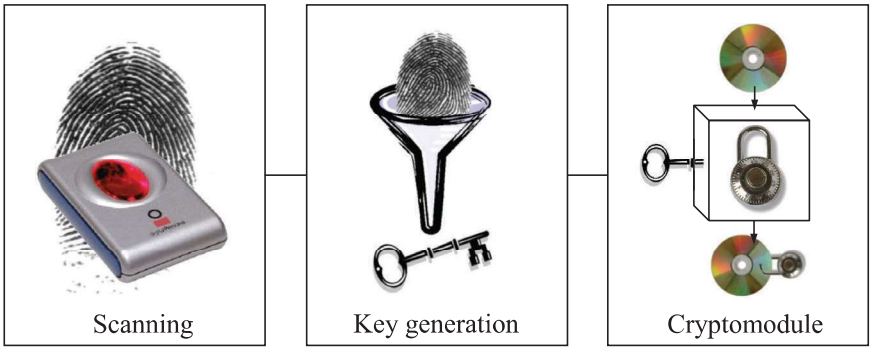

Figure 5.28 Biometric security system

Figure 5.29 TBS 3D terminal

shows the process of generating the key from the fingerprint. First fingerprint is loaded. Then, the key generation process takes place using the above methods, and then the information is transformed into a key that is passed to the last module that uses the key to encrypt. More information can be found in [3].

An interesting application is the 3D fingerprint reader from the company Touchless Biometric Systems AG—see Figure 5.29. This sensor contains three cameras that acquire your finger at different angles, including structured multispectral light. From these three images supported by projected patterns, it is possible to reconstruct a 3D fingerprint image with a 3D profile of the papillary lines visible on the images. It is also a contactless sensor—the finger is only placed on the edge, the fingertip is in the air without touching the sensor. A great advantage is the nondistortion of the course of the papillary lines by pressure, which often causes a distortion to them by a variety of pressures or sweeping of the finger across the surface of the sensor.

Of course, there is another line of exciting industry solutions, such as fingerprint flash drives. However, these specific solutions go beyond the original intention of this book. Some interesting examples can be found, for example, in [3] or [41].

5.8 Conclusion

Fingerprints are currently the most widely used biometric technology. Their enforcement is supported by many factors—they are well accepted by users, they have high biometric entropy (they are suitable for distinguishing large numbers of people), technology is advanced (reliability is high), fingerprints are accepted from legal point of view (fingerprints serve as evidence in court) and, moreover, the sensors are already too small and have little consumption that can be integrated into mobile devices. It is, of course, a question of whether the development of other biometric technologies will cause users to lose interest in this technology or not.

If we neglect forensic (criminal) purposes of use of fingerprints, our fingerprints are often used in special scenarios not belonging to the classical area of identity verification. These exceptions include a variety of fingerprint or fingerprint access for cryptographic purposes for accessing notebooks or external storage media. In this case, fingerprint is used as a key, but it is disadvantageous when fingerprint is revealed—then the key is revealed directly as well. A new trend is to combine fingerprint with cryptographic key so that a mathematical combination is used for encryption, with only the knowledge of the key or knowledge of the fingerprint being insufficient to perform the required cryptographic transaction. Of course, this principle can be also used with other biometric features, but fingerprint was the first use.

A complete conclusion is that the area of fingerprints is one of the most explored and experienced biometrics. When selecting this biometric property for verifying or identifying people, you cannot make a practical mistake—it is of course desirable to choose the right technology vendor who has experience in the field and has undergone independent testing. Integrated liveness detection should be integrated in the sensor, of course. Most manufacturers are already doing this, and liveness detection really becomes an obvious part of fingerprint reader hardware.

Acknowledgment

This work was supported by The Ministry of Education, Youth and Sports of the Czech Republic from the National Programme of Sustainability (NPU II); project IT4Innovations excellence in science—LQ1602.

References

[1] *Global Biometrics Market by Type, by End Use Sector, by Region, Competition Forecast and Opportunities 2011–2021*, TechSci Research, p. 13, 2016. Available online: https://www.slideshare.net/TechSci_Research/biometrics-market-size-share-2021-brochure?from_action=save.

[2] Pankanti S., Prabhakar S., Jain A.K. *On the individuality of fingerprints*. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2002, 24.8: 1010–1025.

[3] Drahanský M. *Biometric security systems fingerprint recognition technology*. Brno: VUTIUM, 2005.

[4] Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security of Germany). *Evaluation of fingerprint recognition technologies—BioFinger*. Darmstadt: Fraunhofer IGD, 2004.

[5] Wilson C.L., Grother P.J., Micheals R.J., *et al. Fingerprint vendor technology evaluation 2003: Summary of results and analysis report*. NIST Technical Report NISTIR, 2004, 7123.

[6] Herschel W.J. *The origin of finger-printing*. London: H. Milford, Oxford University Press, 1916.

[7] Galton F. *Hereditary talent and character*. Macmillan's Magazine, 1865, 12.157–166: 318–327.

[8] Krishan K. *Anthropometry in forensic medicine and forensic science—'Forensic Anthropometry'*. The Internet Journal of Forensic Science, 2007, 2.1: 95–97.
[9] Hauptvogel K.H., Ritzschke M. *Biometrie um die Jahrhundertwende*. Berlin: Humboldt University of Berlin, 2004. Available online: http://www2.informatik.hu-berlin.de/~ritzschk/paper/bertillon_1.pdf.
[10] Galton F. *Fingerprints*. London: Macmillan and Co., 1892.
[11] Straus J., Porada, V., *et al*. *Kriminalistikcá daktyloskopie (Criminalistic dactyloscopy)*. Prague: Police Academy of the Czech Republic, 2005.
[12] Komarinski P. *Automated fingerprint identification systems (AFIS)*. Burlington, MA: Academic Press, 2005.
[13] U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division. *Next Generation Identification Flyer*, [cit. 2017-08-11]. Available online: https://www.fbi.gov/file-repository/about-us-cjis-fingerprints_biometrics-biometric-center-of-excellences-ngi-one-pager-final.pdf.
[14] U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division. *Next Generation Identification (NGI) Monthly Fact Sheet*, [cit. 2017-08-11]. Available online: https://www.fbi.gov/file-repository/ngi-monthly-fact-sheet.
[15] Jozefek A. *Principy některých daktyloskopických klasifikačních systémů* (*Principles of some dactyloscopic classification systems*). Prague: Ústav kriminalistiky Právnické fakulty University Karlovy (Department of Criminology, Faculty of Law, Charles University), 1972.
[16] Collins C.G. *Fingerprint science*. USA: Custom Publishing Company, 1985. Available online: http://www.handanalysis.co.uk/EdCampbell-PalmD-History.htm.
[17] Maltoni D., Maio D., Jain A.K., Prabhakar S. *Handbook of fingerprint recognition*. London: Springer Science & Business Media, 2009.
[18] Drahanský M. *Fingerabdruckerkennung mittels neuronaler Netze*. MSc. thesis, FernUniversität in Hagen, 2001.
[19] Drahanský M., Březinová E., Orság F., Lodrová D. *Classification of skin diseases and their impact on fingerprint recognition*. In: BIOSIG, 2009. p. 173–176.
[20] Auksorius E., Boccara A.C. *Fingerprint imaging from the inside of a finger with full-field optical coherence tomography*. Biomedical Optics Express, 2015, 4465–4471. DOI 10.1364/BOE.6.004465.
[21] Setlak D. *Electric field fingerprint sensor apparatus and related methods*. International patent US 5963679, May 10, 1999.
[22] Koundinya P., Theril S., Feng T., Prakash V., Bao J., Shi W. *Multi-resolution touch panel with built-in fingerprint sensing support*. In: Design, Automation and Test in Europe Conference and Exhibition (DATE), 2014. DOI 10.7873/DATE.2014.258.
[23] Mainguet J.F. *Personal Website—Fingerprint*, [cit. 2015-26-02]. Available online: http://fingerchip.pagesperso-orange.fr/biometrics/types/fingerprint.htm.
[24] Apple Insider. *Apple Preparing Software Update to Enhance Functionality of iPhone 5s Touch ID*, [cit. 2016-13-12]. Available online:

http://appleinsider.com/articles/14/02/28/apple-preparing-software-update-to-enhance-functionality-of-iphone-5s-touch-id.

[25] Drahanský M. *Fingerprint recognition technology—related topics*. LAP LAMBERT Academic Publishing GmbH & Co. KG, 2011, p. 172.

[26] Turroni F., Maltoni D., Cappelli R., Maio D. *Improving fingerprint orientation extraction*. IEEE Transactions on Information Forensics and Security, 2011, 6.3. DOI 10.1109/TIFS.2011.2150216.

[27] *Butterworth filter*. Available online: https://en.wikipedia.org/wiki/Butterworth_filter.

[28] Emyroglu Y. *Fingerprint image enhancement & recognition*. Turkey: Yldyz Technical University, 1997.

[29] Hong L., Wan Y., Jain A. *Fingerprint image enhancement: Algorithm and performance evaluation*. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1998, 20.8: 777–789.

[30] Cappelli R., Ferrara M., Maltoni D. *Minutia cylinder-code: A new representation and matching technique for fingerprint recognition*. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2010, 32.12. DOI 10.1109/TPAMI.2010.52.

[31] Bazen A.M., Verwaaijen G.T.B., Gerez S.H., Veelenturf L.P.J., Zwaag van der B.J. *A correlation-based fingerprint verification system*. In: ProRISC 2000 Workshop on Circuits, Systems and Signal Processing, Veldhoven (NL), 2000.

[32] Koichi I., Hiroshi N., Koji K., Takafumi A., Tatsuo H. *A fingerprint matching algorithm using phase-only correlation*. IEICE Transactions on Fundamentals, 2004, E-87A.3: 682–691.

[33] Krivec V., Birchbauer J., Marius W., Bischof H. *A hybrid fingerprint matcher on card*. In: Proceedings of the 1st Conference on Biometrics and Electronic Signatures of the GI Working Group BIOSIG, 2003.

[34] Liu F., Zhang D., Shen L. *Study on novel curvature features for 3D fingerprint recognition*. Neurocomputing, 2015, 168: 599–608. DOI https://doi.org/10.1016/j.neucom.2015.05.065.

[35] Hong C., Jie T., Xin Y. *Fingerprint matching with registration pattern inspection*. In: Proceedings of the 4th International Conference on Audio- and Video-based Biometric Person Authentication, Guildford (UK), 2003.

[36] Ratha N., Bolle R. *Automatic fingerprint recognition systems*. New York: Springer-Verlag, 2004.

[37] Kanich O. *Fingerprint damage simulation*. Saarbrücken: Lambert Academic Publishing, 2014.

[38] Kanich O., Drahanský M. *Simulation of synthetic fingerprint generation using Petri nets*. IET Biometrics, 2017, 6.6: 402–408. DOI 10.1049/iet-bmt.2016.0041.

[39] Jain A.K. *CSE 891—Selected Topics: Biometrics*. 2004. Available online: https://is.muni.cz/el/1433/jaro2013/PV204/um/03bio/NonminutiaeRepresentations.pdf.

[40] Photonics. *OCT System Captures "Internal" Fingerprint*. [cit. 2017-08-11]. Available online: https://www.photonics.com/Article.aspx?AID=58100.

[41] Drahanský M. *Nutzung biometrischer Daten zur Gewinnung personenbezogener krypto-graphischer Schlüssel*. Darmstadt (DE), 2004.