Chapter 4
Challenges for Fingerprint Recognition—Spoofing, Skin Diseases, and Environmental Effects

Is Fingerprint Recognition Really so Reliable and Secure?

Martin Drahanský, Ondřej Kanich and Eva Březinová

Abstract This chapter tries to find answers to the questions whether the fingerprint recognition is really so reliable and secure. The most biometric systems based on fingerprint recognition have very low error rates, but are these error rates really telling us everything about the quality of such a biometric system? What happens when we use spoofs to deceive the biometric system? What happens when the genuine user has any kind of skin disease on his fingertips? And could we acquire a fingerprint with acceptable quality if there are some distortions on a finger or there are some environmental effects influencing the scanning technology? Reading this chapter brings you an introduction of preparation of finger fakes (spoofs), spoof detection methods, summarization of skin diseases and their influence on papillary lines, and finally the environmental effects are discussed at the end.

4.1 Spoofing and Anti-spoofing

The first subchapter starts with spoofing and anti-spoofing techniques for fingerprint recognition systems. It means that we try to use any kind of finger fake or dead real finger to get an unauthorized access to a biometric system. When a genuine user has already registered his finger in a fingerprint recognition system, there are still several ways how to deceive the biometric system. In order to deceive the

M. Drahanský (✉) · O. Kanich
Brno University of Technology, Faculty of Information Technology,
Brno, Czech Republic
e-mail: drahan@fit.vutbr.cz

E. Březinová
1st Department of Dermatovenereology, St. Anne's University Hospital,
Faculty of Medicine & Masaryk University, Brno, Czech Republic

M. Tistarelli and C. Champod (eds.), *Handbook of Biometrics for Forensic Science*, Advances in Computer Vision and Pattern Recognition,
DOI 10.1007/978-3-319-50673-9_4

fingerprint system, an attacker may put the following objects on the fingerprint scanner [1, 3]:

- *Registered* (enrolled) *finger*. The highest risk is that a legitimate user is forced, e.g., by an armed criminal, to put his live finger on the scanner under duress. Another risk is that a genuine user is compelled to fall asleep with a sleeping drug in order to make free use of his live finger.
- *Unregistered finger* (an impostor's attempt). An attack against a biometric system by an impostor (not necessary an attacker—this could be only an inquisitive person) with his own biometric characteristic is referred as a non-effort forgery.
- *Severed fingerprint of enrolled finger*. A reprehensible attack may be performed using the finger severed from the hand of a genuine user, registered in the biometric system. This kind of attack could be done on a living user or dead user. In both cases, the finger could be used for a limited time only. After several hours, the fingerprint is very often in so bad condition that no papillary lines could be acquired.
- *Genetic clone of enrolled finger*. It should be stated that monozygotic twins do not have the same fingerprint, and the same will be very probably true for clones [10]. The reason is that fingerprints are not entirely determined only genetically but rather by the pattern of nerve growth in the skin. Furthermore, different intrauterine pressures in mother's uterus play an important role in creation of the fingerprint global structure (class) of the fingerprint. It means that such pattern is not exactly the same even for identical twins.
- *Artificial clone of enrolled finger*. More probable attacks against fingerprint systems may use an artificial finger. An artificial finger can be produced from a printed fingerprint made by a copy machine or a graphical processing technique in the same way as forged documents. If an attacker can make then a mold of the enrolled finger by directly modeling it, he can finally also make an artificial finger from a suitable material (see examples in this subchapter). He may also make a mold of the enrolled finger by making a 3D model based on its residual fingerprint.
- *Others*. In some fingerprint systems, an error in authentication may be caused by making noise or flashing a light against the fingerprint scanner, or by heating up, cooling down, humidifying, impacting on, or vibrating the scanner outside its environmental tolerances. We will discuss some of these factors in the third subchapter.

There are possible attacks on algorithms, data transport, and hardware, but these kinds of attacks are out of scope of this subchapter. We will discuss attack possibilities on the input device—fingerprint scanner. One of the simplest possibilities is to produce an artificial finger(print) using soft silicon, gummy and plastic material, or similar substances [10, 18]—see the later part of this subchapter. The fingerprint of a person enrolled in a database is easy to acquire, even without the user's cooperation. Latent fingerprints on daily-use products or on sensors of the access control system itself may be used as templates. To discourage potential attackers from presenting a fake finger (i.e., an imitation of the fingertip and the papillary lines) or, even worse, to hurt a person to gain access, the system must be augmented by an anti-spoofing component [3]. To prevent false acceptance we have to recognize whether the finger on the plate of the fingerprint sensor (also referred to as fingerprint scanner) is alive or not. First of all, we will introduce anti-spoofing techniques (often called liveness detection methods), which are based on various principles. Their purpose is to detect whether the presented finger is alive (and simultaneously the fingerprint is acquired) or any kind of finger(print) spoof is used.

4.1.1 Perspiration

This software-based method processes the information already acquired by a fingerprint scanner—the principle of this technique is the detection of perspiration as an indication of liveness (see Fig. 4.1) [17]. It is worth noting that the outmost layer of the human skin contains around 600 till 1,000 sweat glands per square inch [17] —this amount changes according to the position of skin on the body. These sweat glands diffuse sweat (a dilute sodium chloride solution) on to the surface of skin through pores. The position of skin pores does not change over time and their pore-to-pore distance is approximately 0.5 mm over fingertips [17].

The perspiration method is based on a high difference in the dielectric constant and electrical conductivity between the drier lipids that constitute the outer layer of the skin and the moister sweaty areas near the perspiring pores. The dielectric constant of sweat is around 30 times higher than the lipid.

4.1.2 Spectroscopic Characteristics

This hardware-based method may be regarded not only as an anti-spoofing mechanism but also as an individual biometric system with an inherent anti-spoofing capability.

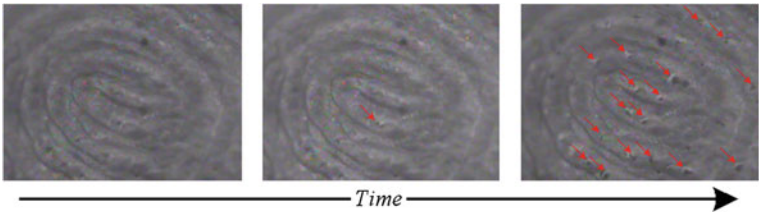


Fig. 4.1 Ascent of sweat from sweat pores on a fingertip (4 × zoomed)

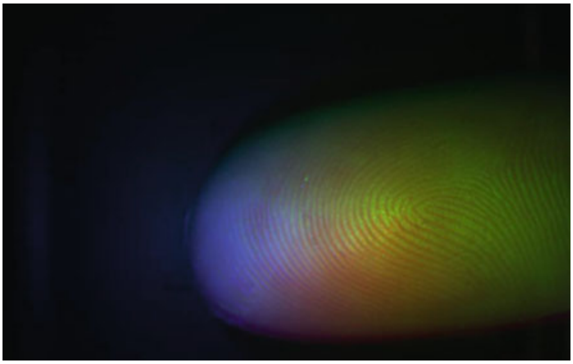


Fig. 4.2 Merge of original fingerprint images illuminated by various wavelengths in RGB [13]

Living human skin has certain unique optical characteristics due to its chemical composition, which predominately affects optical absorbance properties, as well as its multilayered structure, which has a significant effect on the resulting scattering properties [16]. When collecting images generated from different illumination wavelengths sent into the skin, different subsurface skin features may be measured and used to ensure that the material is a living human skin. When such a multispectral sensor is combined with a conventional fingerprint reader, the resulting sensing system can provide a high level of certainty that the fingerprint originates from a living finger. The principle of this technique lies in passing light of different wavelengths through a sample and measuring the light returned, which is affected by the structural and chemical properties of the sample. Figure 4.2 shows the color image obtained from a finger illuminated by light with various wavelengths and by merging the original images in RGB color model to one final image.

4.1.3 Ultrasonic Technology

General ultrasonic method [10] uses a transmitter, which emits acoustic signals toward the fingerprint, and a receiver, which detects the echo signals affected by the interaction with the fingerprint—very often transmitter and receiver are combined into one unit called transceiver. A receiver utilizes the fact that ridges (skin) and valleys (air) have difference in acoustic impedance, therefore the echo signals are reflected and diffracted differently in the contact area. This approach with inherent anti-spoof testing capability among its foremost principles uses the fact that sound waves are not only reflected and diffracted, but are also subject to some additional scattering and transformation. This phenomenon is called contact scattering [10] and it was discovered that this scattering is, to a significant extent, affected by the subsurface structure of the acquired object. Hence, the class corresponding to the live tissue could be modeled and whenever the received acoustic waves are inconsistent with this class, they are rejected. The main problem here is not to obtain clear signals, but to analyze and to make a reconstruction of internal structures from signals, which are very difficult to interpret.

4.1.4 Physical Characteristics: Temperature

This simple method measures the temperature of epidermis during a fingerprint acquisition. The temperature of human epidermis of a finger lies in the range of approximately 25–37°C (see examples in Fig. 4.3). However, this range usually has to be wider to make the system usable under different conditions. In addition, there are many people who have distortions in blood circulation, i.e., a fact which leads to deviations in the body temperature and hence to wrong anti-spoof module decision.

4.1.5 Physical Characteristics: Hot and Cold Stimulus

This technique is based on the fact that the human finger reacts differently to thermal stimuli compared with other artificial (nonliving) material.

The designed anti-spoofing testing module [19] works as follows. A stimulus-giving section gives a stimulus (it may cover cool and hot stimulus) to the finger by a contact plate with which the finger makes contact. Next, typical information could be measured by an organism information-measuring section, which is produced by the live finger in response to the stimulus. Concretely, the amount of the fluctuation for the flow rate of the blood flowing in the peripheral vascular tracts varies according to the stimuli. Hence, as peripheral vascular tracts of the fingertip are extended or contracted, the amplitude value of the blood flow is measured and processed by an organism information-measuring section. Under hot stimulus the amplitude of the blood flow increases, while it decreases under cold stimulus. Moreover, according to the autonomic nervous system, the amplitude is delayed a

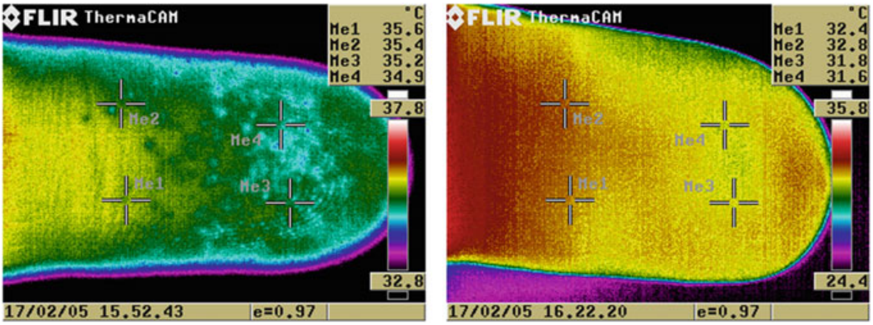


Fig. 4.3 Thermo-scans of fingertips acquired using a thermo-camera FLIR

little with respect to the application of the stimulus. Since these facts are typically observed when the live fingers are measured, they could be employed to distinguish live among artificial and dead samples.

4.1.6 Physical Characteristics: Pressure Stimulus

The principle of this method lies in concrete changes in characteristics of the live skin, which are realized due to pressure applied to the finger [11]. Since the structure and the characteristics of artificial and dead samples are different, when compared with a live finger, this phenomenon could not be seen if such samples were used.

The color of the live skin of the finger without pressure is usually reddish, but becomes whitish when pressure is applied to the skin of the finger. Hence, for the purposes of the device it is suitable to measure the spectral reflectance in the blue and green spectral range (see Fig. 4.4). The difference (in RGB model) between average R values is approximately 11, in G approximately 42, and in B approximately 20 [11].

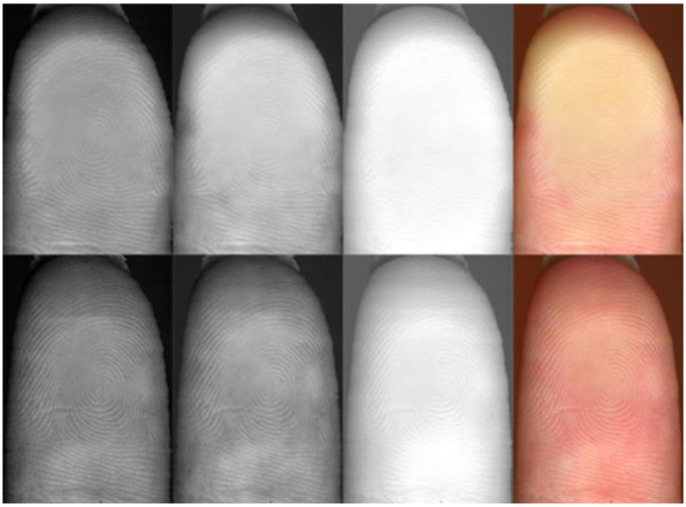


Fig. 4.4 Comparison of pressed finger (*1st row*) and non-pressed finger (*2nd row*). In the *1st column* (from the *left*), there is only the R-channel, the G-channel is in the *2nd column*, the B-channel is in the *3rd column* and in the *4th channel* there is the finger in all RGB colors [11]

4.1.7 Physical Characteristics: Electrical Properties

Some anti-spoofing methods are based on the fact that the live human skin has different electrical properties compared with other materials [10, 14]. The suitable fingerprint recognition system could be extended by an electrode system and an electrical evaluation unit.

The *conductivity* [10] of the human skin is based on humidity, which is dependent on people's biological characteristics and environmental conditions: some people have dry fingers and others have sweaty (wet) ones; also during different seasons, climatic, and environmental conditions, humidity differs significantly. As a result, the span of permissible resistance levels has to be big enough to make the system usable. In such a situation it is quite easy for an impostor to fool the system.

The *relative dielectric constant* (RDC) [10] of a specific material reflects the extent to which it concentrates the electrostatic lines of flux. Many advocates claim that the RDC has the ability to distinguish between real and artificial samples. However, the RDC is highly dependent on the humidity of the sample, so the same situation as in the case of conductivity arises. To fool this method, an attacker can simply use an artificial sample and dip it into a compound of 90% alcohol and 10% water.

Bio-impedance [14] describes the passive electrical properties of biological materials and serves as an indirect transducing mechanism for physiological events, often in cases where no specific transducer for that event does exist. It is an elegantly simple technique that requires only the application of two or more electrodes (this is a big disadvantage of this method). The impedance between the electrodes may reflect "seasonal variations in blood flow, cardiac activity, respired volume, bladder, blood and kidney volumes, uterine contractions, nervous activity, the galvanic skin reflex, the volume of blood cells, clotting, blood pressure and salivation" [14].

4.1.8 Physical Characteristics: Pulse

Scanners based on this technique try to detect whether the scanned object exhibits characteristics of the pulse and blood flow consistent with a live human being [4, 10]. It is not very difficult to determine whether the object indicates some kind of pulse and blood flow, but it is very difficult to decide whether the acquired characteristics are coincident with a live sample. It is difficult to create an acceptance range of the sensor, which would lead to small error rates. The main problem is that the pulse of a human user varies from person to person—it depends on the emotional state of the person and also on the physical activities performed before the scanning procedure. In addition, the pulse and blood flow of the attacker's finger may be detected and accepted when a wafer-thin artificial sample is used.

The sensor usually detects variation in the levels of the reflected light energy from the scanned object as evidence of the pulse and blood flow [3, 4]. First, the light source illuminates in infrared the object and then a photodetector measures the light energy reflected from the object. Finally, there is the processing instrument (this also controls the light source) which processes the output from the photodetector. Since there are some ways how to simulate pulse and blood flow characteristics (e.g., by flashing the light or by motion of the scanned object), scanners should have a deception detection unit [10].

4.1.9 Physiological Basics of Heart Activity

Heart activity measurements are well known as electrocardiogram (ECG) in medicine. In [4], two approaches for measuring of fine movements of papillary lines, based on optical principles, are suggested. The first solution is based on a close-up view of the fingertip acquired with a camera; the second one is distance measurement with a laser sensor. It should be noted that adding the proposed anti-spoof detection solution (either camera or laser based) to a fingerprint recognition system may significantly influence the hardware requirements imposed on the complete system. Both solutions measure the fine movements of skin on a fingertip caused by heart activity (blood circulation in a cardiovascular system), i.e., volume changes in arteries and veins.

4.1.10 Physical Characteristics: Blood Oxygenation

Sensors which measure blood oxygenation [10] are mainly used in medicine (oximeters) and have also been proposed for use in anti-spoof testing modules. The technology involves two physical principles. First, the absorption of light having two different wavelengths by hemoglobin differs depending on the degree of hemoglobin oxygenation. The sensor for the measurement of this physical characteristic contains two LEDs: one emits visible red light (660 nm) and the other infrared light (940 nm). When passing through the tissue, the emitted light is partially absorbed by blood depending on the concentration of oxygen bound on hemoglobin. Second, as the volume of arterial blood changes with each pulse, the light signal obtained by a photodetector has a pulsatile component which can be exploited for the measurement of pulse rate.

4.1.11 Fingerprint Spoof Preparation

Nowadays, it is well known that there do exist many various materials, which could be used for production of fingerprint fakes [3].

The whole process of creation of the fingerprint fakes can be divided into several categories according to input data that are available. Usually, we do not have the possibility of cooperation with the user and simultaneously we have to create a mold indirectly using another information. This method is very popularized by films but we need a little bit of “cooperation” from a genuine user.

Other methods suppose that we have an access to a sensor that we want to deceive. It is possible to either use fingerprint reactivation or fingerprint synthesis [8]. The first method is based on reactivation of a fingerprint, which remains on the sensor, using for example our breath. The second method gets fingerprint image by reconstruction from enrolled template in the biometric database.

The planned procedure of making fakes using manufactured mold and chosen material is described below. First of all the mold (we used a printed circuit board) has to be cleaned—the best way appeared to be a common toothbrush and tooth paste. After cleaning the CH14 separator is applied. When the applied separator becomes dry (approx. after 10 min, i.e., the white film can be observed), it is possible to continue. A sufficient amount of silicon is placed into a measuring glass. Optionally, a small amount of body tone paint or grated graphite powder is added. In that case the silicon mixture has to be stirred thoroughly. This mixture is then spread on the mold and pushed with spatula in order to get rid of as many air bubbles as possible. When the silicon mixture gets dry, we can remove it from the mold. The removing is performed from one chosen mold side by slowly pulling. Due to the usage of CH14 separator, the dried silicon mixture does not tear apart and it is not glued to the mold (see Fig. 4.5).

Generally, we are using over 30 various materials for preparation of a fingerprint spoof, i.e., gelatin, aspic, gummy bears, aquarium silicone (black, white, skin color), epoxy resin (CHS 1200, L285, Hobbyking), latex, etc. Some of these

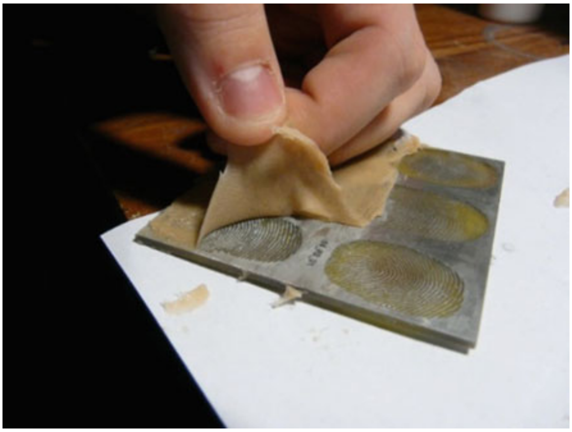


Fig. 4.5 Removing dried mixture from the mold

materials are mixed with skin color or graphite, as mentioned before, because we need skin color for optical sensor or conductivity for capacitive sensors. Using these materials in combination with other advanced methods, we are able to deceive many of fingerprint sensors, incl. those ones with built-in anti-spoof mechanism.

4.2 Skin Diseases

The skin is one of the largest organs in the body, having a surface area of 1.8 m^2 and making up to 12–15% of an adult's body weight. It consists of three layers (see Fig. 4.6) [7]: *epidermis* (the outer layer), *dermis* ("true skin") and *subcutaneous* (fatty) *layer*. Structure and thickness of the skin vary with site (e.g., thick epidermis on palms and soles due to mechanical protection—up to 1.4 mm).

Skin diseases represent very important, but often neglected factor of the fingerprint acquirement. It is not possible to say in general how many people suffer from skin diseases, because there are so many various skin diseases [8, 20]. In a general, medical practice about 20–25% of patients with skin complaints are referred. When discussing whether the fingerprint recognition technology is a perfect solution capable to resolve all our security problems, we should always keep in mind those potential users who suffer from some skin disease.

The situation after successful recovery of a potential user from such skin diseases is, however, very important for the possible further use of fingerprint recognition devices. If the disease has attacked and destroyed the structure of papillary lines in the epidermis and underlying dermis (so-called dermoepidermal junction—connection of the top two layers of the skin), the papillary lines will not grow in the same form as before (if at all) and therefore this user could be restricted in his future life by being excluded from the use of fingerprint recognition systems, though his fingers do not have any symptoms of the skin disease anymore.

Skin is constantly being regenerated. A keratinocyte ("skin cell") starts its life at the lower layer of epidermis (the basal layer), which is nourished by blood vessels and is supplied with nerve endings from dermis. The cell migrates upward from basal layer to stratum corneum (the outermost skin layer). During 4 weeks the cell undergoes a series of changes, gradually flattening out and moving toward the surface. Then it dies and is shed. This physiological process can be negatively affected in many diseases of the skin. The epidermis is not supplied with blood vessels, but has nerve endings. The shape of dermoepidermal junction basically forms the structure of papillary lines.

In the most cases of dermatological disorders we find a lot of changes in the ultrastructure of the skin, including epidermis and dermis. There is often inflammation (inflammatory cells), atrophy or hypertrophy, fibrotisation and many other changes visible in the microscope. These differences result in changes of color (optical characteristics), changes of dermal vessels and capillaries (blood perfusion), changes of elasticity, and thickness of the skin (optical characteristics after pressure change).

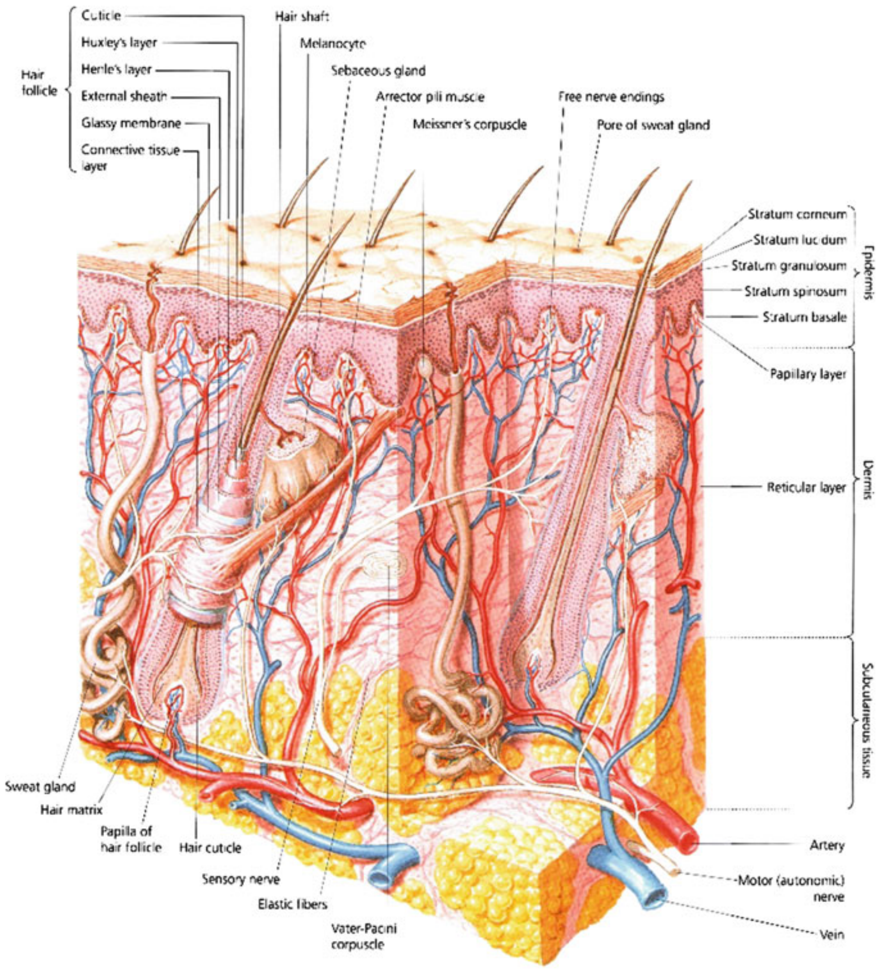


Fig. 4.6 Skin structure [7]

Diseases Causing Histopathological Changes of Epidermis and Dermis

These diseases usually cause problems for all kinds of fingerprint scanners, because they can influence either color or internal structure of the skin.

The most common representatives of this group are [7, 20]: *Hand and fingertip eczema*, *Dyshidrosis*, *Tinea*, *Pyoderma*, *Pitted keratolysis*, *Pyogenic granuloma*, *Systemic sclerosis,* or *Raynaud's phenomenon*.

Diseases Causing Skin Discoloration

These diseases may cause problems for optical fingerprint scanners and also for scanners which use a fingerprint anti-spoof detection check based on the color or spectral analysis of the human skin.

Typical representatives are [7, 20]: *Macular drug eruptions and rashes in infectious diseases (Hand, foot and mouth disease*, *Scarlet fever*, *Secondary syphilis, Kawasaki's disease*), *Pitted keratolysis, Raynaud's phenomenon, Xanthomas*, *Carotenosis,* or *Hereditary hemorrhagic teleangiectasia.*

Diseases Causing Histopathological Changes in Junction of Epidermis and Dermis

These diseases could cause structure changes underneath the skin in the junction between dermis and epidermis, i.e., in the area from that ultrasonic fingerprint

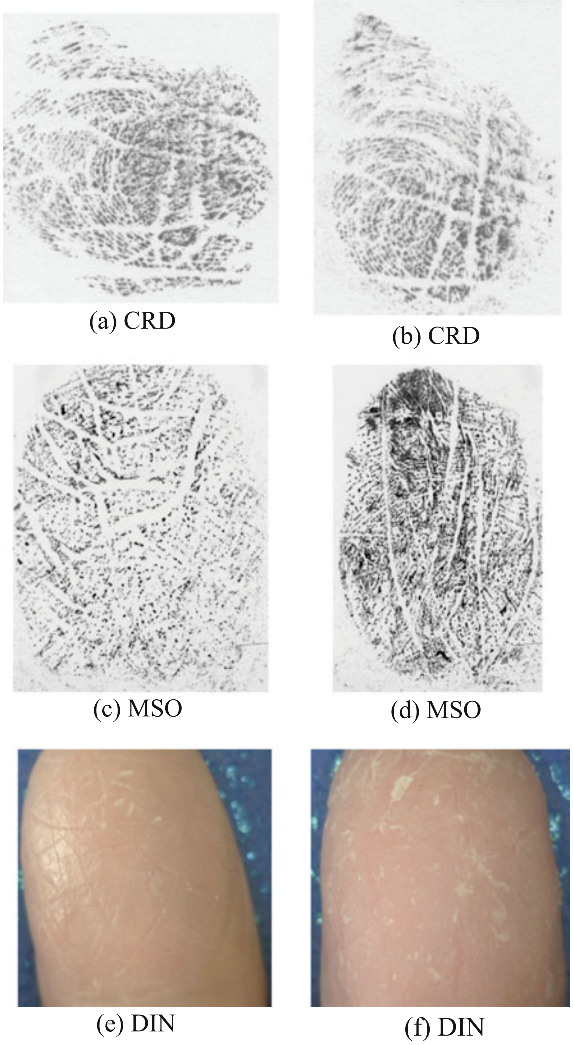
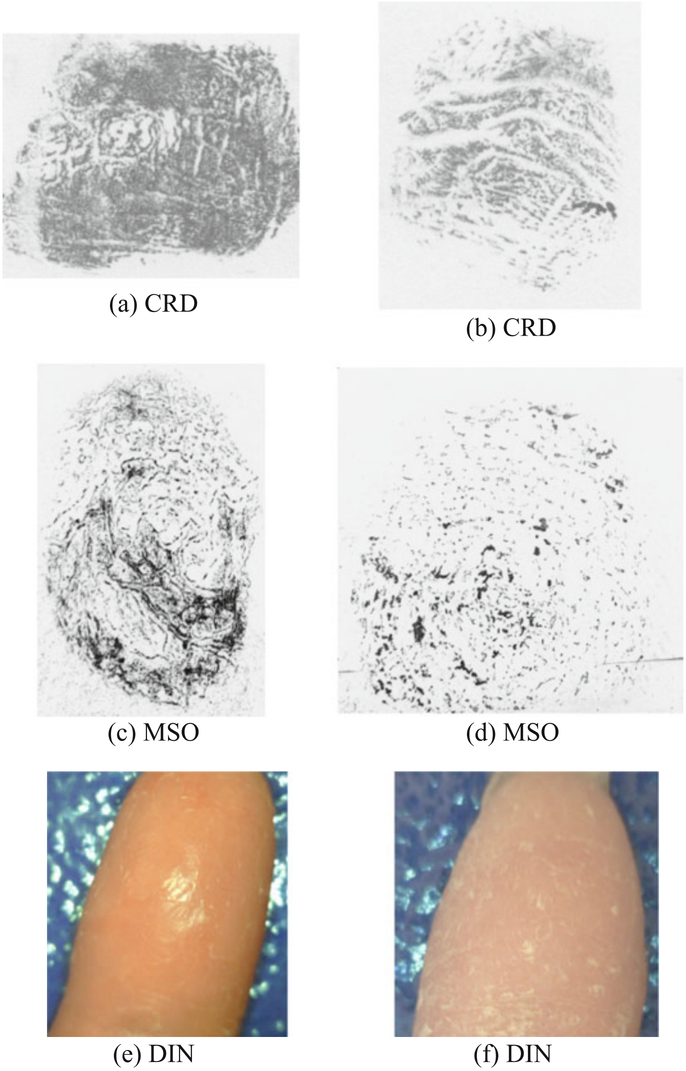

(a) CRD
(b) CRD
(c) MSO
(d) MSO
(e) DIN
(f) DIN

Fig. 4.7 Fingertip eczema—a severe form


(a) CRD

(b) CRD

(c) MSO

(d) MSO

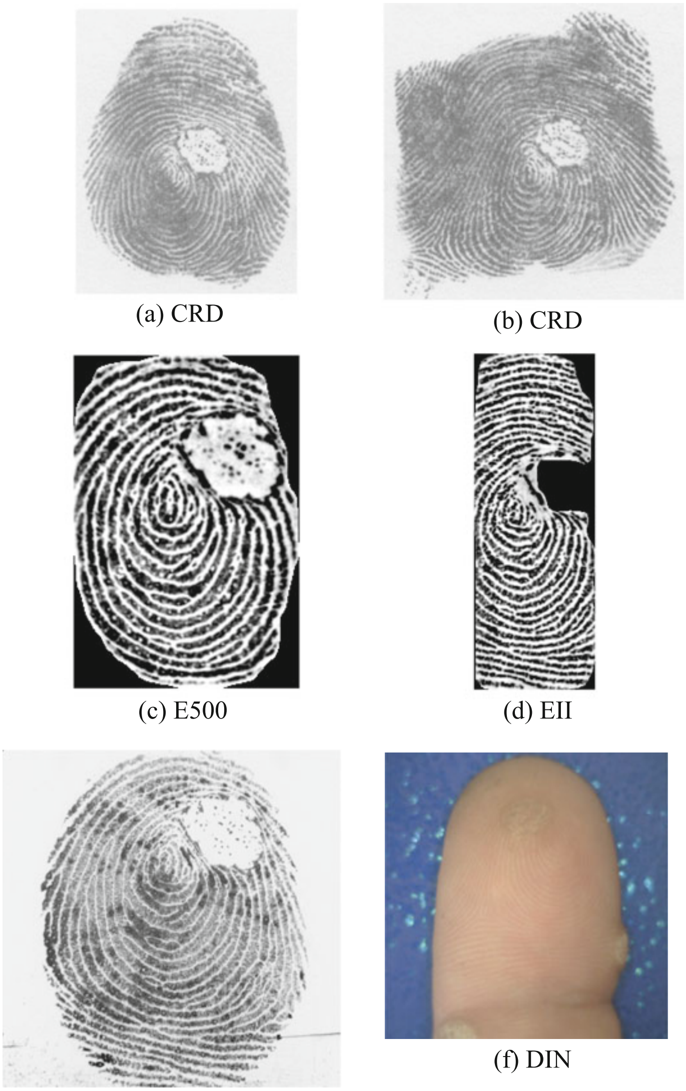
(e) DIN

(f) DIN

Fig. 4.8 Psoriasis—a full seizure

scanners acquire fingerprint pattern images. Typical representatives are [7, 20]: *Hand eczema*, *Verruca vulgaris* (*warts*), *Psoriasis,* or *Epidermolysis bullosa*.

In the following section, examples (Figs. 4.7, 4.8, 4.9 and 4.10) of results of disease-affected fingerprint data collection are shown. The name of the disease and description are given in each figure heading. The codename of applied capturing



(a) CRD

(b) CRD

(c) E500

(d) EII

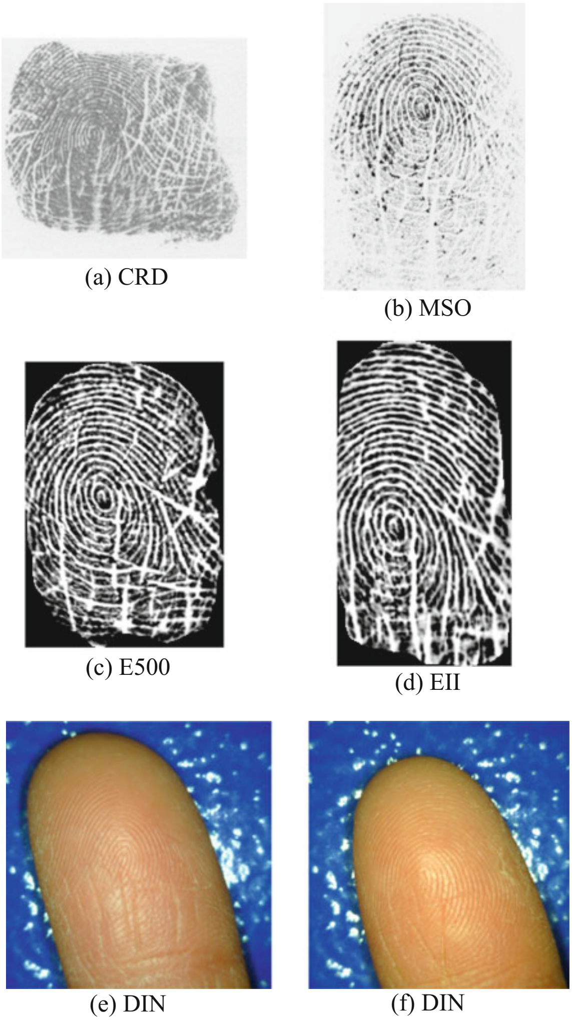
(e) MSO

(f) DIN

Fig. 4.9 Verruca vulgaris (wart)

principle is stated under each subfigure. We use the following codenames: CRD (dactyloscopic card), MSO (Sagem MSO 300), E500 (UPEK EikonTouch500), EII (UPEK Eikon II), TBS (TBS 3D Enroll 2011), and DIN (Dinolite).

Fig. 4.10 Colagenosis



(a) CRD

(b) MSO

(c) E500

(d) EII

(e) DIN

(f) DIN

4.3 Environmental Distortions

When we finally place finger in the acquisition area there are still some difficulties. Environment around us is not ideal like in laboratory—so there are some influencing factors. We can divide them into three categories: *finger condition*, *sensor condition,* and *environment itself*. Some of these factors can be prevented but only with full support of users and thorough care of the sensor and specialized room. As you can see it is not possible to fully prevent all these factors. Consequently, sensors and recognition algorithms have to be prepared for this situation. The only way how to prepare them is by using large test dataset of damaged fingerprints. Unfortunately such data is not usually available. But we can create this data artificially. These topics are covered in the following subsections, first factors that influence resulting fingerprint are discussed, followed by creation of artificial fingerprints.

4.3.1 Phenomena Influencing Fingerprint Acquisition

As was mentioned before we can divide these factors into three groups: *user condition*, *sensor condition,* and *environment*—these factors will be discussed next. Each of these factors is described with example and sensor technologies that are influenced more or technologies that are not influenced at all.

First user condition is a *dirt on the finger*—it could be a small particle, a few grains of dust, or just a greasy finger. Conductive materials and liquids are usually the most problematic types of dirt. Only ultrasonic, contactless, and e-field technologies are resistant against this type of damage. *Dry or moist finger* is one of the most typical cases of damage done to a fingerprint. This is caused because we wash our hands or we are nervous and our fingers are getting sweat or on the other hand we have very dry hands because of some lotion, our skin resistance can increase or decrease ten times to the normal value. This plays usually a huge role in the recognition by optical, capacitive, and e-field sensors. *Physical damage* of a finger like cuts or abrasions is obviously damaging the fingerprint. If it is not a deep injury that influences papillary lines forever, the ultrasonic and e-field technologies scan the finger in the deeper dermis layer where the fingerprint keeps undamaged. Another factor is *skin diseases* which were thoroughly described in the previous subchapter. *Pressure and skin plasticity* can turn the fingerprint into a big black oval. Only contactless sensors are fully immune to the damage that the pressure can make. The change of pressure, very big or very low pressure or moving of the finger is also considered being part of the next category that is *non-cooperative behavior*. The user usually uses an unexpected pressure, moves when the device is scanning and/or places the finger in a wrong place or with a wrong rotation. None of the technologies is fully resistant to these types of behavior [3, 9].

The second group of factors is connected to the sensor. *Dirt on the surface* has the same effects like the dirt on the finger. The problem is that it is affecting everyone who is using this device. It means that in the registration phase this factor can create a common error for every user and there is a danger that these users will not be able to be identified after cleaning up the device. In addition to fingers there are more types of dirt than can pollute the sensor area: for example metallic dust, wooden dust, earth dust, fine sand, excrements (in outdoor use). In addition to ultrasonic and e-field technologies, every sweep sensor is also more resistant to this type of damage. *Latent fingerprint* is closely related to the previous topic. It is in some way a type of dirt on the surface of the sensor. More than damaging a new fingerprint there is a security hazard. The technologies, which are resistant to latent fingerprint, are the same like those in the previous topic. *Sensor technology* itself determines how the fingerprint will look like. Some technologies support only binary images or use specific pallet of colors to represent ridges and valleys, some can create 3D maps. *Physical damage* is an extreme but a possible influencing factor of the resulting fingerprint. There is no easy way to prevent the sensor from damaging. The damage of the sensor will have various effects on every technology [3, 9].

Finally, the surrounding environment itself will be discussed. *Vibration* can break down the sensor and slightly change the position of a finger. Only sensors using the sweep technology are, to a certain degree, resistant to this type of damage. *Temperature* can be different for the sensor, the finger or the environment. Typically, there are no problems with the exception of the thermal technology. But when we think about extreme temperatures, we have to deal with very dry or very moist fingers which can affect the resulting image. Also it is known that the ultrasonic technology does not operate properly in extremely low temperatures. *Surrounding light* is only affecting optical and electrooptical technologies because they have a light sensing unit. When the sensor area is larger or the finger of the user is smaller or the contactless technology is used, the influence of the surrounding light can be huge. *Electromagnetic radiation* is an influencing factor which affects every technology. The device as a whole can be influenced by electromagnetic radiation. Wires inside or outside connecting it to other parts of a biometric system and all electronic components can be influenced [3, 9].

4.3.2 Methods for Generation of Synthetic Fingerprints

The synthetic fingerprint generation is an inverse biometrics problem. According to input variables we basically do the fingerprint recognition process from the end to the start. There are several methods how to generate a synthetic fingerprint. When we thoroughly study them, we can find that they are all based on the same principle. The method used by the SFinGe seems to be the oldest one and also the most commonly known so it will be described as a pattern for others.

For better understanding we can look at the upper part of Fig. 4.11 to see the process of the generation. Firstly, the fingerprint shape is determined. The basic shape is oval and each elliptical segment can be changed to create the required shape. The second step is the directional field model. In this step, the fingerprint class is chosen and together with that the position of cores and deltas. This step is using the Sherlock and Monroe ridge [12] flow model to generate a consistent directional field. The third step creates the density map. When we look at a fingerprint, we can find that the density of papillary lines is not the same throughout the whole area. After examining several real fingerprints some heuristic criteria could be made. These criteria are based on the position of singularities (cores and deltas) and according to them the density map is generated. The last step is ridge pattern generating. This phase uses all previous steps and some initial seeds. Iteratively, the image with initial seeds is refined with the Gabor filter. The filter

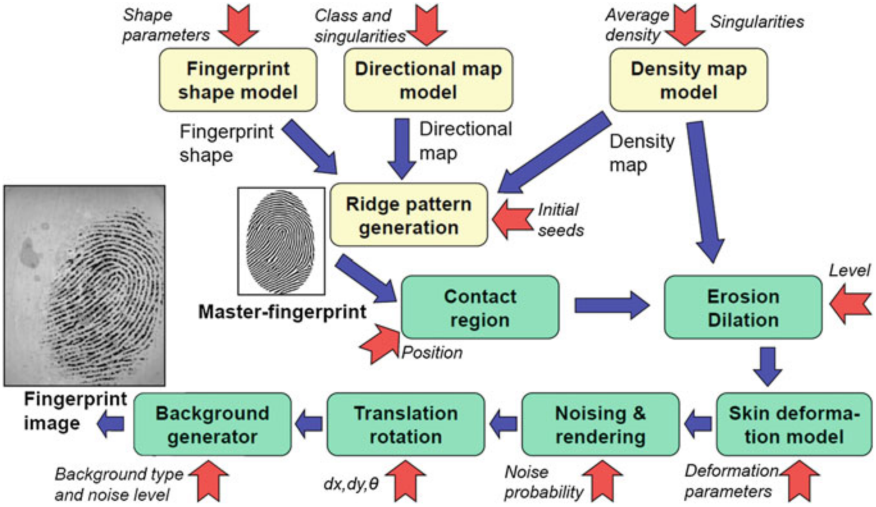


Fig. 4.11 SFinGe process of artificial fingerprint generation

orientation and frequency is adjusted according to the directional field and density map. Minutiae are automatically generated at random places with random types that are not only ridge ending and bifurcation, but also more complex ones. After that phase, the fingerprint is done [9, 12, 21].

As we can see, the SFinGe[1] generating process is not exactly an inverted recognition process. When we strictly follow this process, we do the so-called fingerprint reconstruction. These are the methods that focus on the creation of the whole fingerprint only from minutiae saved as a template in fingerprint recognition. Another method is somewhere between these two. It says that fingerprint features are dependent on each other. It is following the same scheme but with dependencies on other steps. The orientation field is influenced by singular points. The minutiae density is higher around singularities and also their appearance is not random but it is statistically driven. The minutiae direction is also dependent on their types and on the orientation of ridges around. This method firstly determines singular points, after that the orientation field and lastly the minutiae. Each step is dependent on the previous one. After all the steps the fingerprint is made with the use of the AM-FM method [21].

The last method uses minutiae as an input. The creation of the whole fingerprint is based only on these minutiae. The biggest difference is that the orientation field is generated from minutiae and not from classes or singular points as it was in the previous methods. It is generated from the minutiae direction and each minutia has a weight based on the distance of it from the point where we are determining the orientation field. The disadvantage of this method is that the final fingerprint could

[1] http://biolab.csr.unibo.it/sfinge.html.

have a class that does not exist in the real world. The density map can be manually changed in this method. After that, using a similar method of Gabor filter like in SFinGe, master fingerprint is generated. Note that instead of initial seeds, this method uses minutiae as these seeds and the generation start with them so the precisely defined minutiae don't change in the process of generation [9].

To sum it up, we can create these artificial fingerprints from ISO template, based on statistical values, using random seeds and random minutiae points or using fixed minutiae points. For testing random fingerprints is this usually fully sufficient. All these methods end with creation of the artificial fingerprint which is called master fingerprint. This master fingerprint is what was mentioned at the start of this chapter that is perfect finger perfectly scanned with no influence of the environment.

To create more realistic fingerprint we have to add these influential factors. It is time to look at the lower part of the Fig. 4.11. There are certain damage simulation methods. The first step is the selection of the contact region. To simulate the different placements of the finger on the sensor area a random translation of the ridge pattern is made. The next step is the variation in ridge thickness. The ridge thickness is modified to simulate various skin dampness and finger pressure. The next phase is the fingerprint distortion. In this phase, the skin deformation according to different finger placements over the sensor is simulated. The skin plasticity (compression or stretching) and a different force applied on each part of the finger creates a nonlinear distortion. The next step is noising and rendering. Another phase is the global translation or rotation. This phase simulates the not perfectly placed finger on the sensor. So it slightly translates and/or rotates the whole image. The last step is the generation of a realistic background. The background is generated randomly from a set of background images. At the end of that step, the fingerprint impression is made [9, 12, 21].

Please note that SFinGe system, which was used here as an example of generation and damaging of the artificial fingerprint, lies the focus in realistic looking fingerprints without exact simulation of the damage done to the fingerprint. Some steps clearly simulate specific damage, others are used as an appropriation of several factors, which is to some extent sufficient but when we want to create fingerprints acquired in some extreme environment or one which is often and more severely influenced by some phenomena we have to use precise damage simulations. We work on these damage simulations (incl. skin diseases) at the moment.

4.4 Conclusion

At the beginning of this chapter, there are described anti-spoofing methods, which are used for liveness detection on fingers in general. Some relevant advantages and disadvantages of these methods are discussed as well. Furthermore, the second part includes description of skin diseases on fingers influencing the fingerprint recognition process. It has to be noted that the anti-spoofing methods have big troubles with diseased fingers, because these fingers are very often falsely evaluated as nonliving (fake fingers). Therefore, it is very important to implement appropriate methods for anti-spoofing, which can handle diseased fingers. The last part of this chapter is devoted to other environmental influencing factors, which can cause troubles in the process of fingerprint recognition. These factors have similar impact as diseased fingers, i.e. there could be seen comparable impact to the fingerprint recognition process. As mentioned before, it is very important to find a good and reliable method for anti-spoofing, which can correctly treat diseased fingers or acquired fingerprints by various influencing factors coming from the environment.

Acknowledgments 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; "New solutions for multimodal biometrics—enhancement of security and reliability of biometric technologies"—COST LD14013 (CZ); "Reliability and Security in IT"—internal Brno University of Technology project FIT-S-14-2486 (CZ).

References

1. Ambalakat P (2005) Security of biometric authentication systems. In: 21st Computer Science Seminar, SA1-T1–1 (2005), p 7
2. Daugman J (2001) Biometric Decision Landscapes, University of Cambridge, p 13
3. Drahanský M (2011) Fingerprint Recognition Technology—Related Topics. Saarbrücken, DE, LAP, 2011, p 172. ISBN 978-3-8443-3007-6
4. Drahanský M, Funk W, Nötzel R (2006) Liveness detection based on fine movements of the fingertip surface. In: IEEE—The West point workshop, West Point, New York, USA, pp 42–47. ISBN 1-4244-0130-5
5. Drahanský M, Hejtmánková D (2010) New experiments with optical liveness testing methods. J Inf Hiding Multimedia Signal Process 1(4):301–309. ISSN 2073-4212
6. Habif TP (2004) Clinical dermatology, 4th edn. Mosby, China, p 1004. ISBN 978-0-323-01319-2
7. Habif TP (2004) Clinical dermatology, 4th edn. Mosby, China, p 1004. ISBN 978-0-323-01319-2
8. Jain AK, Flynn P, Ross AA (2008) Handbook of biometrics. Springer, p 556. ISBN 978-0-387-71040-2
9. Kanich O (2014) Fingerprint damage simulation—A simulation of fingerprint distortion, damaged sensor, pressure and moisture, LAP LAMBERT Academic Publishing GmbH & Co. KG, p 57. ISBN 978-3-659-63942-5
10. Kluz M (2005) Liveness testing in biometric systems. Master Thesis, Faculty of Informatics, Masaryk University Brno, CZ, p 57
11. Lodrová D (2013) Security of biometric systems. Dissertation thesis, FIT BUT, Brno (CZ), p 152
12. Maltoni D, Maio D, Jain AK, Prabhakar S (2009) Handbook of fingerprint recognition, 2nd edn. Springer, p 494. ISBN 978-1-84882-253-5
13. Malý T (2013) Detekce živosti prstu pomocí osvětlení různé vlnové délky (Detection of Finger Liveness using Illumination with Different Wavelengths), Diploma thesis, FIT BUT, Brno (CZ), p 59
14. Martinsen ØG, Grimnes S, Haug E (1999) Measuring depth depends on frequency in electrical skin impedance measurements. In: Skin research and technology, No. 5, pp 179 –181. ISSN 0909-752X

15. Matsumoto T, Matsumoto H, Yamada K, Hoshino S (2005) Impact of artificial “Gummy” fingers on fingerprint systems. In: Proceedings of SPIE, Optical Security and Counterfeit Deterrence Techniques IV, vol 4677, p 11
16. Rowe RK (2008) Spoof Detection. Summer school for advanced studies on biometrics for secure authentication. Italy, Alghero, p 43
17. Schuckers S, Hornak L, Norman T, Derakhshani R, Parthasaradhi S (2003) Issues for liveness detection in biometrics. West Virginia University, Presentation, CITeR, p 25
18. Tan B, Lewicke A, Schuckers S (2008) Novel methods for fingerprint image analysis detect fake fingers. In: SPIE, p 3. doi:10.1117/2.1200805.1171
19. Organism Identifying Method and Device. US Patent 6,314,195, Nov 2001
20. Wolff K, Johnson RA, Suurmond D (2005) Fitzpatrick’s Color Atlas and Synopsis of Clinical Dermatology, 5th Edition. McGraw-Hill, USA, p 1085. ISBN 0-07-144019-4
21. Zhao Q, Jain AK, Paulter NG, Taylor M (2012) Fingerprint image synthesis based on statistical feature models. In: 2012 IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS). IEEE, pp 23–30