Chapter 15

Spoofing methods in hand-based biometrics

Martin Drahanský[1], Ondřej Kanich[1], and Michal Dvořák[1]

15.1 Introduction

The biometric systems, oriented in this chapter especially on fingerprints, have been introduced in the previous chapters. The functionality of such systems is influenced not only by the used technology but also by the surrounding environment (including skin or other diseases). Biased or damaged biometric samples could be rejected after revealing their poor quality, or may be enhanced, what leads to the situation that samples, which would be normally rejected, are accepted after the enhancement process. But this process could present also a risk, because the poor quality of a sample could be caused not only by the sensor technology or the environment, but also by using an artificial biometric attribute [imitation of a finger(print)]. Such risk is not limited just to the deceptional technique, but if biometric system is not able to recognize whether an acquired biometric sample originates from a genuine living user or an impostor, we would then scan an artificial fake and try to enhance its quality using an enhancement algorithm. After a successful completion of such enhancement, such fake fingerprint would be compared with a template and if a match is found, the user is accepted, notwithstanding the fact that he can be an impostor! Therefore the need of careful liveness detection, i.e., the recognition whether an acquired biometric sample comes from a genuine living user or not, is crucial.

Each component of a biometric system presents a potentially vulnerable part of such system. The typical ways of deceiving a biometric system are as follows (Figure 15.1) [1–4]:

1. *Placing fake biometrics on the sensor.* A real biometric representation is placed on the device with the aim to achieve the authentication, but if such representation has been obtained in an unauthorized manner, such as making a fake gummy finger, an iris printout or a face mask, then it is considered as a deceiving activity.
2. *Resubmitting previously stored digitized biometric signals (replay attack).* A digitized biometric signal, which has been previously enrolled and stored in

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

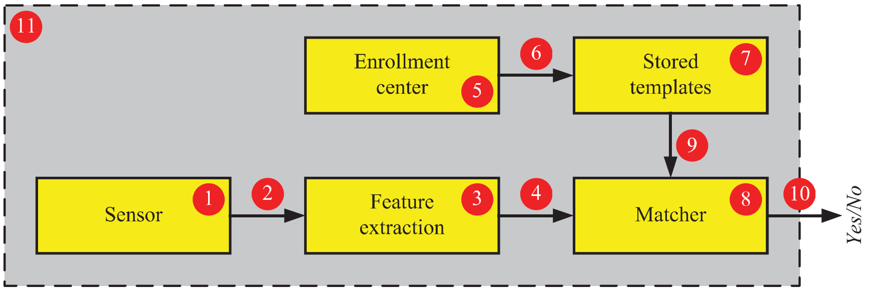

Figure 15.1 Basic components of a biometric system

the database, is replayed to the system, thus circumventing the acquisition device.

3. *Overriding the feature extraction process.* A preselected template is produced in the feature extraction module using a Trojan horse.
4. *Tampering with the biometric feature representation.* During the transmission between the feature extraction and matching modules, a fraudulent feature set replaces the template acquired and processed by the device.
5. *Attacking the enrollment center.* The enrollment module is also vulnerable to spoof attacks such as those described in the previous points 1–4.
6. *Attacking the channel between the enrollment center and the database.* During the transmission, a fraudulent template replaces the template produced during the enrollment.
7. *Tampering with stored templates.* A template, previously stored in the database (distributed or not), can be modified and used afterward as corrupted template.
8. *Corrupting the matcher.* A preselected score is produced in the matching extraction module using a Trojan horse.
9. *Attacking the channel between the stored templates and the matcher.* During the transmission between the database and the matching module, a fraudulent template replaces the template previously stored.
10. *Overriding the final decision.* The result of the decision module can be modified and then used for the replacement of the output obtained previously.
11. *Attacking the application.* The software application can also be a point of attack and all possible security systems should be used to reduce the vulnerability at this level.

From the above list of possible attacks, we can deduce that most security risks or threats are quite common and could be therefore resolved by traditional cryptographic tools (i.e., encryption, digital signatures, public key infrastructure authentication of communicating devices, access control, hash functions, etc.) or by having vulnerable parts at a secure location, in tamper-resistant enclosure or under constant human supervision [1].

When a legitimate user has already registered his finger in a fingerprint system, there are still several ways how to deceive the system. In order to deceive the fingerprint system, an attacker may put the following objects on the fingerprint scanner [3,5,6]:

- *Registered (enrolled) finger.* The highest risk is that a legitimate user is forced, e.g., by an armed criminal, to put his/her live finger on the scanner under duress. Another risk is that a legitimate user is compelled to fall asleep with a sleeping drug in order to make free use of his/her live finger. There are some deterrent techniques against similar crimes, e.g., to combine the standard fingerprint authentication with another method such as a synchronized use of PINs or identification cards; this can be helpful to deter such crimes.
- *Unregistered finger (an impostor's finger).* An attack against authentication systems by an impostor with his/her own biometrics is referred to as a noneffort forgery. Commonly, the accuracy of authentication of fingerprint systems is evaluated by the false rejection rate and false acceptance rate (FAR) as mentioned in the previous chapters. FAR is an important indicator for the security against such method (because a not enrolled finger is used for authentication). Moreover, fingerprints are usually categorized into specific classes [7]. If an attacker knows what class the enrolled finger is, then a not enrolled finger with the same class (i.e., similar pattern) can be used for the authentication at the scanner. In this case, however, the probability of acceptance may be different when compared with the ordinary FAR.
- *Severed fingertip of enrolled finger.* A horrible attack may be performed with the finger severed from the hand of a legitimate user. Even if it is the finger severed from the user's half-decomposed corpse, the attacker may use, for criminal purposes, a scientific crime detection technique to clarify (and/or enhance) its fingerprint.
- *Genetic clone of enrolled finger.* In general, it can be stated that identical twins do not have the same fingerprint, and the same would be true for clones [5]. The reason is that fingerprints are not entirely determined genetically but rather by the pattern of nerve growth in the skin. As a result, such pattern is not exactly the same even for identical twins. However, it can be also stated that fingerprints are different in identical twins, but only slightly different. If the genetic clone's fingerprint is similar to the enrolled finger, an attacker may try to deceive fingerprint systems by using it.
- *Artificial clone of enrolled finger.* More likely 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 DTP 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. He may also make a mold of the enrolled finger by making a 3D model based on its residual fingerprint. However, if an attacker can make an artificial finger which can deceive a fingerprint system, one of the countermeasures against such attack is obviously based on the detection of liveness.

- *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. Some attackers may use such error to deceive the system. This method is well known as a "fault-based attack" (e.g., denial of service) and may be carried out by using one of the above-mentioned techniques. Furthermore, a fingerprint image may be made protruding as an embossment on the scanner surface, if we spray some special material on such surface.

Many similar attacks are documented in the literature, including all the above-mentioned types. In this chapter, however, we will focus only on finger(print) fakes. One example of the attack on fingerprint technology has been presented in [8]. Hackers in the club-magazine "Die Datenschleuder" (4,000 copies in one edition) have printed a fingerprint of the thumb from the right hand of the German minister of the interior—Dr. Wolfgang Schäuble, and invited readers to make a fake finger(print) of the minister and to try to pretend that their identity is those of the minister. This could be considered as a bad joke, as a fingerprint also serves as a conclusive proof of a person's identity. A hacker has acquired this fingerprint from a glass after some podium discussion. Nevertheless, biometric travel documents (issued in Germany starting from 2007, issued in the Czech Republic from 2009), enforced not only by Dr. Schäuble, should be protected just against this situation. The implementation of fingerprints into the travel documents was prescribed by a direction of the European Union in 2004.

It is clear from [5] that the production of a fake finger(print) is very simple [9]. First step is acquiring fingerprint of desired person. Fingerprints are left on everything the person touched. By using dactyloscopic dust (there are many types of them) or special vapor (dusting) techniques [10] fingerprints can be made visible from many, even unexpected materials. And from almost all of them, it can be acquired and used for fake fingerprint production.

Our own experiments have shown that to acquire some images (e.g., from glass, CD, film or even paper) is not very difficult and, in addition, such image could be enhanced and postprocessed, what leads to a high-quality fingerprint. The following production process of a fake finger(print) is simple and can be accomplished in several hours. After that, it is possible to claim the identity as an impostor user and common (nearly all) fingerprint recognition systems confirm this false identity supported by such fake finger.

Therefore, the application of liveness detection methods is a very important task, and should be implemented (not only) in all systems with higher security requirements, such as border passport control systems, bank systems, etc. The biometric systems without the liveness detection could be fooled very easily and the consequences might be fatal.

The security of a biometric system should never be based on the fact that biometric measurements are secret, because biometric data can be easily disclosed. Unlike typical cryptographic measures, where a standard challenge–response protocol can be used, the security of a biometric system relies on the difficulty of replicating biometric samples [11]. This quality known as the liveness ensures that the measured characteristics come from a live human being and are captured at the time of verification. We should realize that any testing of liveness is worthless unless the capture device and communication links are secure. Due to the fact that a biometric system uses physiological or behavioral biometric information, it is impossible to prove formally that a capture device provides only genuine measurements. Consequently, it cannot be proven that a biometric system as a whole is foolproof [11]. Each solution of this problem has its own advantages and disadvantages; it is more suitable for a certain particular type of the biometric system and environment than for other. Some solutions are software-based; others require a hardware support. Methods that combine both approaches can also be used.

15.2 Liveness detection

Securing automated and unsupervised fingerprint recognition systems used for the access control is one of the most critical and most challenging tasks in real world scenarios. Basic threats for a fingerprint recognition system are repudiation, coercion, contamination and circumvention [12,13]. A variety of methods can be used to get an unauthorized access to a system based on the automated fingerprint recognition. If we neglect attacks on the algorithm, data transport and hardware (all these attacks demand good IT knowledge), one of the simplest possibilities is to produce an artificial fingerprint using soft silicon, gummy and plastic material or similar substances [5,14]. A 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 a liveness detection component [12,13]. To prevent false acceptance, we have to recognize if the finger on the plate of the fingerprint sensor (also referred to as fingerprint scanner) is alive or not. There are decent amount of liveness detection methods in fingerprint recognition. That is because producers are trying to push their technology to the top. Hence, recent topics for research are usually aimed at liveness detection. Some methods are simple and cheap, others are more demanding but also more reliable. Each producer chooses liveness detection that suits their products. In the following subsections, various liveness detection in fingerprint recognition principles will be described [9].

15.2.1 Perspiration

A noninvasive biomedical measurement for determination of the liveness for use in fingerprint scanners was developed by the Biomedical Signal Analysis Laboratory at Clarkson University/West Virginia University [15]. This software-based method processes the information already acquired by a capture device and the principle of this technique is the detection of perspiration as an indication of liveness (see Figure 15.2).

It is worth noting that the outmost layer of the human skin houses around 600 sweat glands per square inch [15]. These sweat glands diffuse the sweat (a dilute sodium chloride solution) on to the surface of the skin through pores. The position

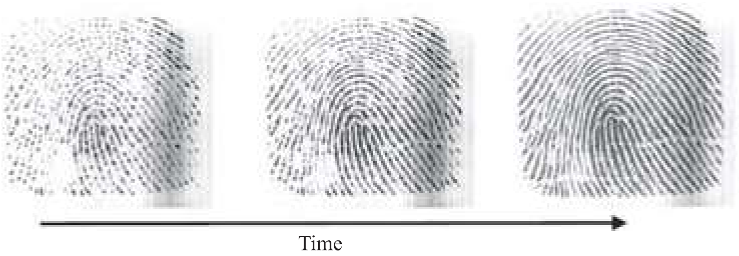

Figure 15.2 Example of live fingerprint images acquired some time apart [15]

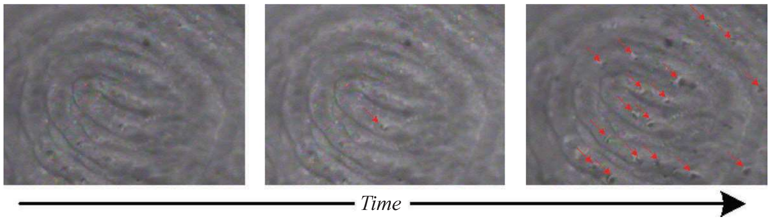

Figure 15.3 Ascent of sweat from sweat pores on a fingertip (4× zoomed)

of skin pores does not change over time and their pore-to-pore distance is approximately 0.5 mm over fingertips.

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, so the electrical model of the skin thanks to perspiration can be created. If we can detect activity of sweat pores then we can also detect if presented finger is alive. First, finger is pushed to sensing part of fingerprint scanner. After that, it is left on the scanner for approximately 5 s. Meanwhile, droplets of sweat start to leak from the sweat pores in ridges. Because of that ridges became darker in the fingerprint image (or final image). Example of this behavior is shown in Figure 15.3 where 4× zoom factor was used and 10 s time delay between each fingerprint scan.

15.2.2 Spectroscopic characteristics

The technology discussed in this section was developed by the Lumidigm company [11,16] from Albuquerque and is based on the optical properties of human skin. This hardware method may be regarded not only as a liveness detection mechanism but also as an individual biometric system with an inherent liveness capability.

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 [16,17]. By collecting images generated from different illumination wavelengths passed into the skin, different subsurface skin features may be measured and used to

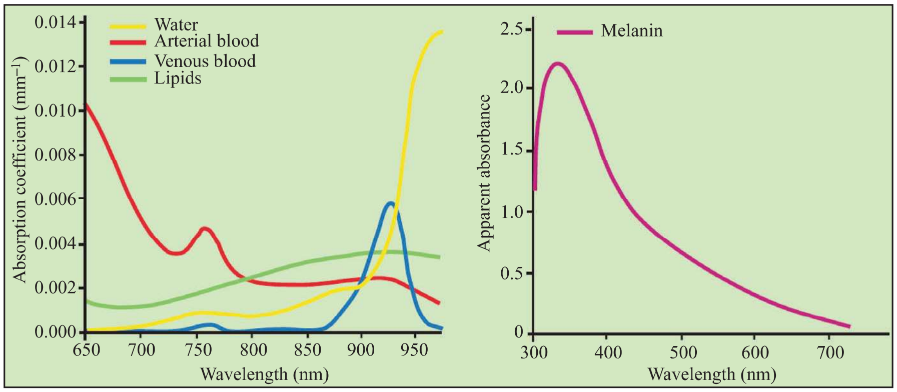

Figure 15.4 Spectrographic properties of different components of living tissue (suitable for detection of spoofing attacks on iris recognition) [18]

ensure that the material is 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 various wavelengths through a sample and measuring the light returned, which is affected by the structural and chemical properties of the sample. Different wavelengths have to be used to measure the sample satisfactorily, because diverse wavelengths penetrate to different depths into the sample and are differently absorbed and scattered [11]. For example, when we put a flashlight against the tip of a finger, only the red wavelengths can be seen on the opposite side of the finger. This is because shorter (mostly blue) wavelengths are absorbed and scattered quickly in the tissue, unlike longer (red and very near infrared) ones, which penetrate deep into the tissue. In addition, there is an interesting fact about this—each user can have its own profile because skin of each person is reacting on different wavelengths a little bit differently. Differences are so subtle that using spectral properties as biometrics itself is not possible; however for liveness detection, it is more than enough.

The measurements can be transformed into a graph (Figure 15.4) that shows the change in all measured wavelengths after interacting with a sample and is known as a spectrum. Next, the proper analysis of tissue spectra, based on multivariate mathematical methods, has to be done to provide correct results.

Figure 15.5 shows the principle of multispectral fingerprint sensor. The light sources are LEDs of various wavelengths spanning the visible and short-wave infrared region. Crossed linear polarizers may be included in the system to reduce the contribution of light that undergoes a simple specular reflection to the image, such as light that is reflected from the surface of the skin. The crossed polarizers ensure that the majority of light seen by the imaging array has passed through a portion of skin and undergone a sufficient number of scattering events to have randomized the polarization. The imaging array is a common silicon complementary metal–oxide–semiconductor (CMOS) or CCD detector.

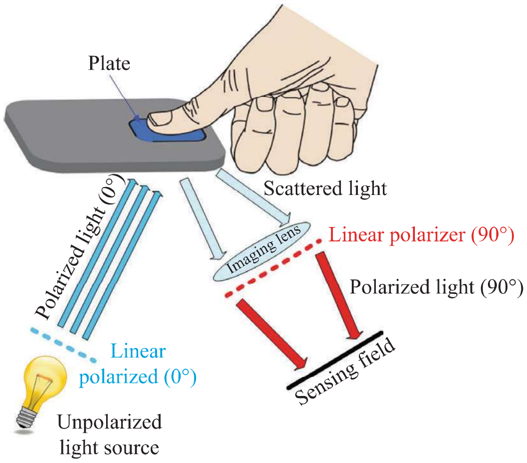

Figure 15.5 Multispectral fingerprint sensor (reworked from [17])

A highly realistic artificial finger made by Alatheia Prosthetics [16] was one of a number of different spoof samples used to test a multispectral imager's ability to discriminate between real fingers and spoofs. Figure 15.6 shows the results of a multivariate spectral discrimination performed to compare the consistency of the spectral content of a multispectral image of a real finger with both a second image of a real finger and a prosthetic replica of the same finger. The imager's ability to distinguish between the two sample types is clear.

Another approach of the liveness detection using the wavelet analysis in images is presented in [19].

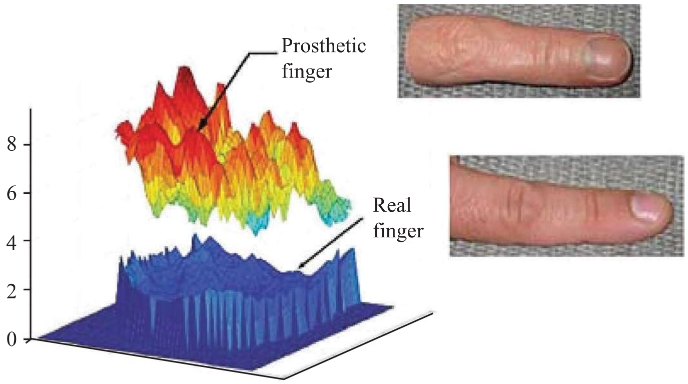

Figure 15.6 Multispectral image data can clearly discriminate between a living finger and an ultrarealistic spoof. The graphs on the left side show how similar the spectral content of each image is to that expected for a genuine finger [16,18]

15.2.3 Ultrasonic technology

In this paragraph, a biometric system using an ultrasonic technology with inherent liveness testing capability will be described. This technique was first developed by the company Optel from Poland and is based on the phenomenon called contact scattering. Another ultrasonic biometric device is offered by the company Qualcomm [20] (former Ultra-Scan) from the United States. Companies Sonavation [21] and InvenSense [22] have also some products in this sector [23].

Standard ultrasonic methods [11] use a transmitter, which emits acoustic signals toward the fingerprint, and a receiver, which detects the echo signals affected by the interaction with the fingerprint (Figure 15.7). A receiver utilizes the fact that the skin (ridges) and the air (valleys) have difference in acoustic impedance; therefore the echo signals are reflected and diffracted differently in the contact area. This approach with inherent liveness 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 [11] 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. This can easily detect fingerprint spoof because reflected signals from one (spoof material) layer have different characteristics than signals reflected from several layers of living tissue.

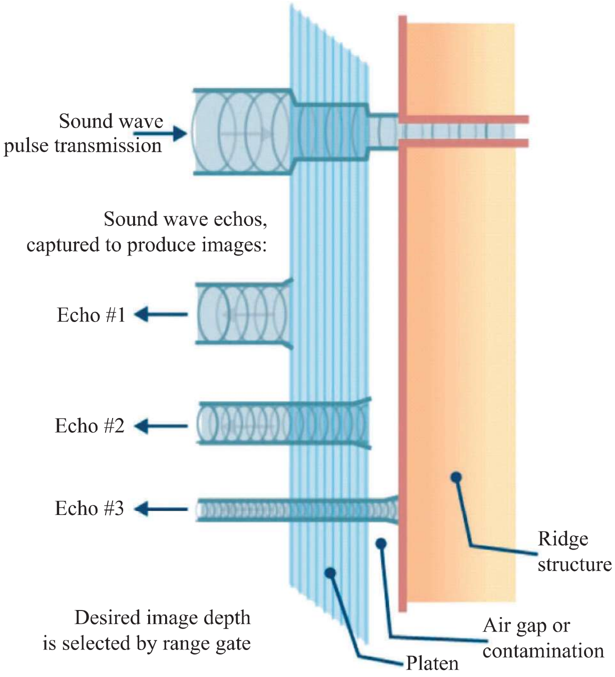

Figure 15.7 Schematic of ultrasonic pulse/echo principle [24]

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.

The ultrasonic device reached the following conclusions [11,25]:

- As the inner structure of the live skin compared with spoof samples differs, the character and the amplitude of acoustic signals also differ significantly. Hence, it is possible to distinguish between live and artificial fingers.
- There is no need to deal with the problem known as latent print reactivation because the signal level from the latent print is at least 30 dB lower than the signal given by the real finger. Even when the soot or metal powder is used in order to enhance the quality of signal, the previous is true.
- This method is much less sensitive to dirt, grease and water compared with other methods. In addition, fingers with damaged surface give a relatively clear image, because their inner structure seems to be visible.
- Since this approach scans the inner structure of the object, it has the ability to check for pulse by measuring volumetric changes in the blood vessels [25].

15.2.4 Physical characteristics

Physical characteristics belong to the easiest methods for liveness detection. They are usually based on various measurable phenomena connected to the skin tissue.

15.2.4.1 Temperature

This simple method measures the temperature of the epidermis during a fingerprint acquisition. According to our measurement, in different environment conditions including different seasons, mental and physical state of the user, it was determined that temperature of human finger is in the range of 25–37°C. Unfortunately, temperature also change while scanning so intraclass variability is huge and interclass variability is small.

In addition, there are many people who have problems with blood circulation, a fact which leads to deviations in the body's temperature and hence to wrong liveness module decision. The only way how to improve such a situation is to make the working range broader again or simply warm the user's finger. The former will increase the likelihood that the system will be deceived while the latter can also be applied to fake samples. In the case where an attacker uses a wafer-thin artificial fingerprint glued on to his finger, this will result in a decrease by a maximum of 2°C [26] compared with an ordinary finger. Since the difference in temperature is small, the wafer-thin sample will comfortably fall within the normal working margin. In consequence, this method is not a serious security measure at all (Figure 15.8).

15.2.4.2 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.

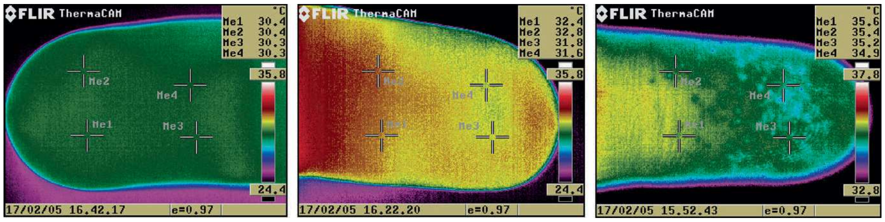

Figure 15.8 Thermo-scans of the fingertips acquired using a thermo-camera FLIR

The designed liveness testing module [11,27] is working as follows. A stimulus-giving section gives a stimulus (it may cover a cool and a 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 tip of the finger 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 cool stimulus. Moreover, according to the autonomic nervous system, the amplitude is delayed a 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. After the processing phase, such information is transferred to a determining section, where together with the other information related to stimulus (i.e., the time intervals, the strength of stimuli, etc.) is evaluated. Finally, a determining section analyses how the amplitude of the blood flow fluctuates in response to the stimulus to make the right decision.

Since the human peripheral nervous system is very sensitive, it is able to react to weak cool and hot stimuli without being noticed by the person whose fingerprint is checked. This fact should also reduce success spoofing ratio. More information about the method discussed here can be found in [27].

15.2.4.3 Pressure stimulus

The principle of this method lies in some changes in characteristics of the live skin, which are realized due to pressure applied to the finger [11,28]. 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 unpressured finger is usually reddish but becomes whitish when pressure is applied to the skin of the finger. This change of coloration is because skin is reacting to increasing pressure by pushing out blood from pressured spot.

It has been shown that the spectral reflectance of the light in the red spectral range (i.e., the light wavelength of approximately 640–770 nm) [28] does not show a substantial difference between the pressed state and the nonpressed state. On the other hand, the spectral reflectance of the light in the blue and green spectral range (i.e., the light wavelength of approximately 400–600 nm) [28] in the not pressed state is much smaller than in the pressed state. Hence, for the purposes of the device discussed in this section, it is suitable to measure the spectral reflectance in the blue and green spectral range (see Figure 15.9).

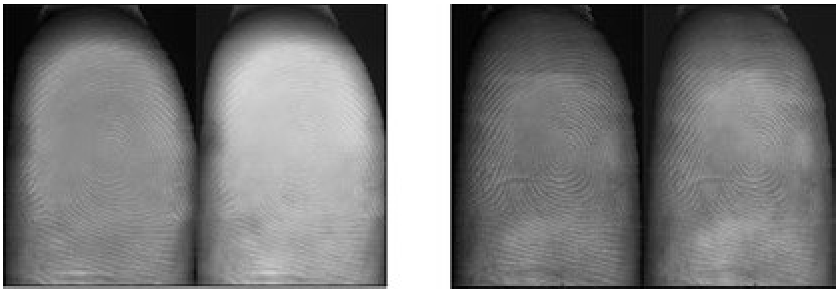

Figure 15.9 Images of the fingertips pressed tightly (left) and slightly (right) to the sensor [29]

A liveness testing module is proposed in [28] and consists of a transparent plate, a light source, a light detection unit and a determining section. Since the light source and the light detection unit are placed under the plate, this plate has to be transparent to enable light to be sent toward the finger and receiving the reflected light. The light source projects a light beam toward the surface of the placed finger. Next, depending on the pressure or nonpressure state, the reflected light is measured by the light detection unit.

Based on such measurements, the determining section returns the right decision, i.e., as the finger changes its state from nonpressure to pressure, the color of the skin changes from reddish to whitish, what leads to a change in the spectral reflectance. As a result, the light detection unit can detect that the spectral wavelength of the spectral ranges is increased.

Another method using pressure-based characteristics is discussed in [30], but unlike the method described in the previous paragraph, this technique employs the change in fingerprint ridges width. That is because ridges are elastic. When applying pressure, they tend to widen themselves.

When the fingerprint changes its state from nonpressure to pressure, the fingerprint ridges change, i.e., as the pressure becomes stronger, the fingerprint ridges flatten out, and therefore their change of width could be measured. Only objects which demonstrate the typical change in fingerprint ridge width due to pressure could be determined as live ones.

A new approach to the fake finger detection based on skin elasticity analysis has been introduced in [31]. When a user puts a finger on the scanner surface, the scanner captures a sequence of fingerprint images at a certain frame rate. The acquired image sequence is used for the fake finger detection. One or more of them (see Figure 15.10) can be used for fingerprint authentication.

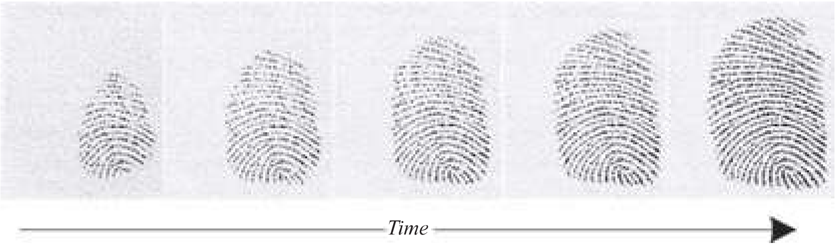

Figure 15.10 A sequence of fingerprint images describing the deformation of a real finger [11]

15.2.4.4 Electrical properties

Some methods of liveness testing are based on the fact that the live human skin has different electrical properties compared with other materials [11]. The suitable fingerprint recognition system could be extended by an electrode system and an electrical evaluation unit. These sections are the main parts of the liveness testing module where the electrical evaluation unit can evaluate the change in the state in the electrode system. The sensing of the electrical change should take place simultaneously with the recognition of the fingerprint. Therefore, these parts of biometric systems should be designed in such a way that two simultaneous measurements cannot disturb each other. Furthermore, such a system may be able to measure more than one of the fingerprint liveness characteristics related to electrical properties (e.g., conductivity, dielectric constant).

The conductivity [11] 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 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 intruder to fool the system. Moreover, the intruder can use a salt solution of a suitable concentration or put some saliva on the fake finger to imitate the electric properties of the real finger.

The relative dielectric constant (RDC) [11] 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. In [32], we can read that the RDC values of alcohol and water are 24 and 80, respectively, while the RDC of the normal finger is somewhere between these two values. Since the alcohol will evaporate faster than the water, the compound will slowly turn into the water. During evaporation, the RDC of spoof samples will soon be within the acceptance range of the sensor.

We have run a small test series with ten people, each finger, horizontal and vertical measurement strips, and five measurements per finger—conductivity (resistance) measurements. The range of values we found was from 20 kΩ to 3 MΩ [26]. A paper copy or an artificial finger made of nonskin-like material has higher electrical resistance, but for example, soft silicon (moisturized) shows resistance values close to the range found in our experiments.

15.2.4.5 Bio-impedance

Bio-impedance [33–35] 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 exists. It is an elegantly simple technique that requires only the application of two or more electrodes. 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."

Impedance Z [34] is a general term related to the ability to oppose AC (alternating current) flow, expressed as the ratio between an AC sinusoidal voltage and an AC sinusoidal current in an electric circuit. Impedance is a complex quantity because a biomaterial, in addition to opposing current flow, phase-shifts the voltage with respect to the current in the time-domain.

The conductivity of the body is ionic (electrolytic) [34], because of the presence of, e.g., Na^+ and Cl^- in the body liquids. The ionic current flow is quite different from the electronic conduction found in metals: the ionic current is accompanied by a substance flow. This transport of substance leads to concentrational changes in the liquid: locally near the electrodes (electrode polarization), and in a closed-tissue volume, during prolonged direct current flow.

The body tissue is composed of cells with poorly conducting, thin-cell membranes. Therefore, the tissue has capacitive properties [34]: the higher the frequency, the lower the impedance. The bio-impedance is frequency-dependent, and impedance spectroscopy, hence, gives important information about tissue and membrane structures as well as intra- and extracellular liquid distributions.

Figure 15.11 shows three most common electrode systems. With two electrodes, the current carrying electrodes and signal pick-up electrodes are the same. If the electrodes are equal, it is called a bipolar lead, in contrast to a monopolar lead. With 3-(tripolar) or 4-(tetrapolar) electrode systems, separate current carrying and signal pick-up electrodes are used. The impedance is then transfer impedance [34]: the signal is not picked up from the sites of current application.

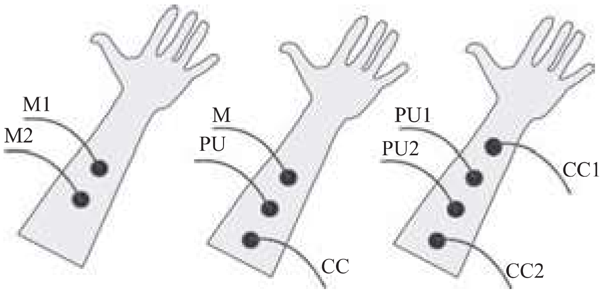

Figure 15.11 Three skin surface electrode systems on an underarm [34]. Functions: M—measuring and current carrying, CC—current carrying, PU—signal pick-up

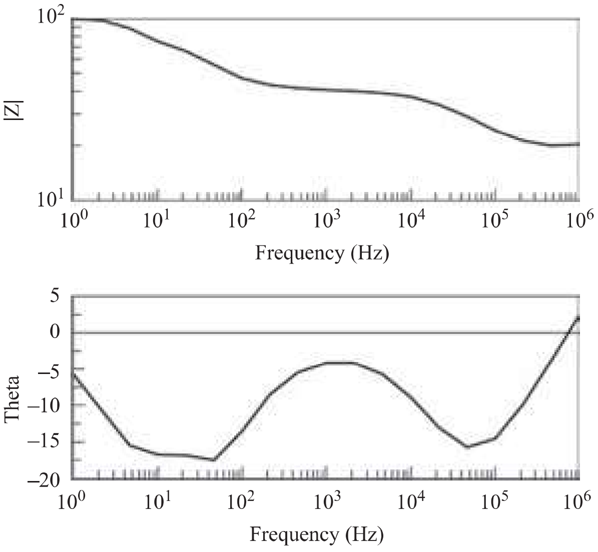

Figure 15.12 Typical impedance spectrum obtained with four equal electrodes attached to the skin of the underarm [34]

Figure 15.12 shows a typical transfer impedance spectrum obtained with the 4-electrode system from Figure 15.11. It shows two dispersions [34]. The transfer impedance is related to, but not solely determined by the arm segment between the polyurethane (PU) electrodes. The spectrum is determined by the sensitivity field of the 4-electrode system as a whole. The larger the spacing between the electrodes, the more the results are determined by deeper tissue volumes. Even if all the electrodes are skin surface electrodes, the spectrum is, in principle, not influenced by skin impedance or electrode polarization impedance.

The necessity of this method is to apply electrodes on user forearm which is something that majority of users would not be willing to do.

15.2.4.6 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 [11]. 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 if the acquired characteristics are coincident with a live sample. As a result, 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.

One of the sensors usually detects variation in the levels of the reflected light energy from the scanned object as evidence of the pulse and blood flow [11]. First, the light source illuminates the object and then a photo-detector measures the light energy reflected from the object. Finally, there is the processing instrument (which also controls the light source) which processes the output from the photo-detector. 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 [11].

Our skin is semipermeable for light, so that movements below the skin (e.g., blood flow) can be visualized. One example of an optical skin property is the skin reflection [12,36]. The light illuminating the finger surface is partly reflected and partly absorbed (Figure 15.13). The light detector acquires the reflected light which has been changed in phase due to dispersion and reflection and thus has a slightly different wavelength compared to the original light source. One can try to link the change in wavelength to the specific characteristics of the skin with respect to light dispersion and reflection to detect whether the light has been scattered and reflected only from the fingerprint skin, or if there is some intermediate layer between the finger skin and the light source or detector.

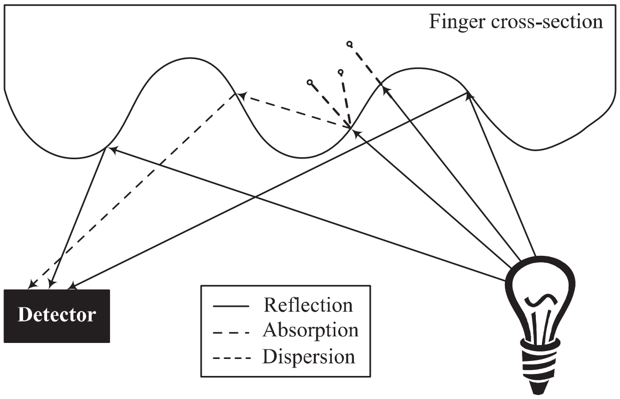

Figure 15.13 Light absorption, dispersion and reflection by a fingerprint [12]

Another example for optical skin feature is the saturation of hemoglobin [12,36], which binds oxygen molecules. When blood comes from the heart, oxygen molecules are bound to the hemoglobin, and vice versa, when blood is flowing back to the heart, it is less saturated by oxygen. The color of oxygenated blood is different from that of nonoxygenated blood. If we use a light source to illuminate the finger skin, we can follow the blood flow based on the detection of oxygenated and nonoxygenated blood, respectively [12,36]. The blood flow exhibits a typical pattern for a live finger, i.e., the analysis of blood flow is well suited for finger liveness detection.

In both above-mentioned examples, it is shown that the human skin has special characteristics which can be used for the liveness testing. It can be argued that it is possible to confuse such system, e.g., by using a substance with similar optical characteristics as a human skin, or, in the second example, to simulate the blood flow. Even though the argument is correct, obviously the effort to be exerted for these attacks is much higher than for the other physical characteristics presented so far.

Another solution is proposed in [12,36] based on the analysis of movements of papillary lines of the fingertips and measurements of the distance of the fingertip surface to a laser sensor, respectively. The system is compact enough to be integrated with optical fingerprint sensors.

One advantage of this implementation is that the finger is not required to be in contact with a specific measuring device, and so it can be integrated with standard fingerprint sensors. Moreover, the implementation could be acceptably low. This is of particular importance, as in most cases, the liveness detection will be an add-on that augments already existing robust and field-tested fingerprint scanners.

The method presented in [12,36] requires the analysis of at least one heart activity cycle, thus both the camera and the laser measurement method sketched in this section would add an extra time of at least 1 or 2 s to the overall authorization process interval.

In [12,36], two approaches for measuring of fine movements of papillary lines, based on optical principles, are suggested (Figure 15.14). The first solution is based on a close-up view of the fingertip acquired with a charge-coupled device (CCD) camera; the second one is distance measurement with a laser sensor. It should be noted that adding the proposed liveness detection solution (either camera or laser-based) to a fingerprint recognition system, as proposed in Figures 15.15 and 15.16, may significantly influence the hardware requirements imposed on the complete system.

Camera solution

The camera solution scheme is outlined in Figure 15.15. The main idea is that a small aperture (approximately 6 mm) is created in the middle of a glass plate with an alternately functioning mirror below the plate.

First, during the fingerprint acquirement phase, the whole fingerprint is stored and the system operates as a classical fingerprint acquisition scanner (mirror permeable) by projecting the fingerprint on the CCD/CMOS camera. Next, in the liveness detection phase, the mirror is made impermeable for light and a part of the fingertip placed on the aperture is mirrored to the right and projected on the CCD/CMOS camera by a macro lens. This macro lens has to magnify minimally 10–12× of original. The latter part of the system is used to acquire a video sequence for the liveness detection analysis.

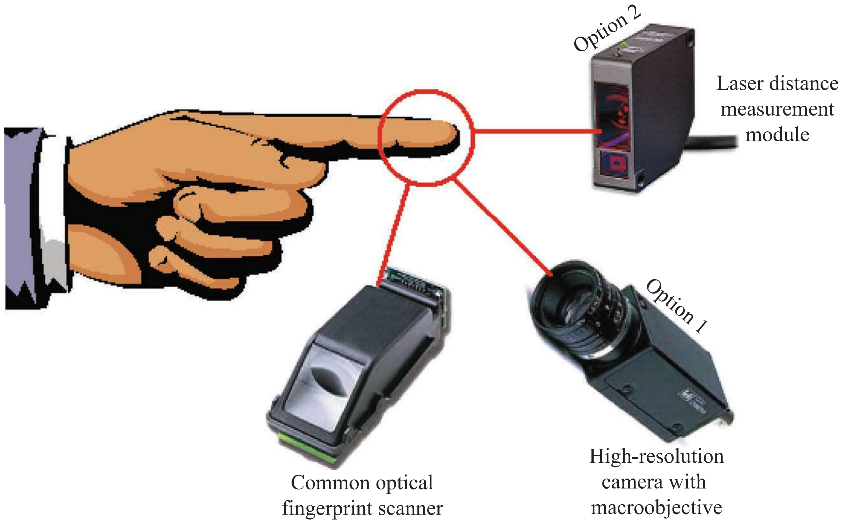
Option 2
Laser distance measurement module
Option 1
High-resolution camera with macroobjective
Common optical fingerprint scanner

Figure 15.14 Integrated liveness detection—scanner + optical and laser solution [37]

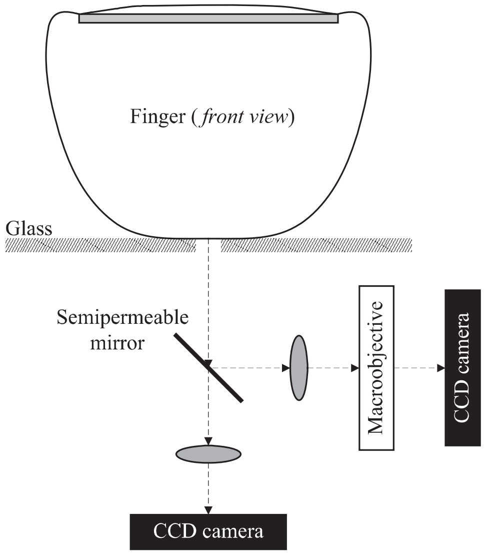

Figure 15.15 Possible integration of a camera-based measurement system for liveness detection with optical fingerprint sensor (CCD/CMOS camera) [12]

Laser solution

The second optical method for the liveness testing is based on laser distance measurements [12,36]. Figure 15.16 outlines the laser distance measurement module, which could be integrated with a standard optical fingerprint sensor. The optical lens system and CCD camera for acquisition of the fingerprint are the same as in Figure 15.15. However, unlike the solution shown in Figure 15.15, the laser distance measurement module is placed to the right side of the glass plate, which is L-shaped here. The user places his finger in such a way that it is in contact with the horizontal and the vertical side of the glass plate.

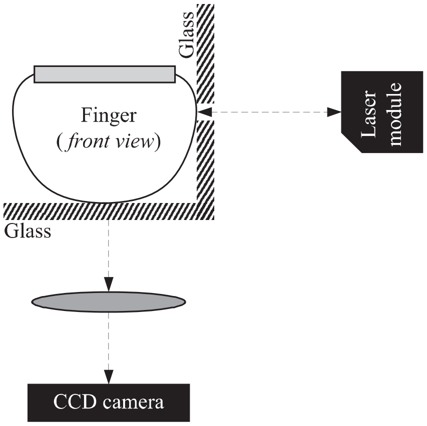

Figure 15.16 Possible integration of laser distance measurement for liveness detection with optical fingerprint sensor (CCD/CMOS camera; aperture approx. 6 mm) [12]

The underlying physical measurement principle is the same as in the video camera solution. We assume volume changes (expansion and contraction) due to the heart activity, which causes fine movements of the skin. The laser sensor is able, based on the triangulation principle, to measure very small changes in distance down to several μm.

The comparison of the computed curve and a normalized standard curve (the template) will reveal whether the measurement corresponds to a standard live fingerprint or indicates a fake finger or another attempt of fraud. For example, the comparison between both curves can be realized by the normalization followed by the cross correlation.

There are other liveness detection methods based on optical principles, see [28,30]. They coincide in principles (both are optical) but differ in monitored physical characteristics.

15.2.4.7 Blood oxygenation

Sensors that measure blood oxygenation [11] are mainly used in medicine and have also been proposed for use in liveness 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. Important thing is that in case of live finger, there has to be reaction for both type of light. This liveness detection can also very easily distinguish between amputated and live finger. Former contain only deoxygenated blood. Second, as the volume of arterial blood changes with each pulse, the light signal obtained by a photo-detector has a pulsatile component which can be exploited for the measurement of pulse rate.

The sensors mentioned above are able to distinguish between artificial (dead) and living samples but, on the other hand, many problems remain. The measured characteristics vary from person to person and the measurement is strongly influenced by dyes and pigments (e.g., nail varnish).

15.2.4.8 Blood pressure

There are some other methods based on the medical science characteristics which have been suggested for liveness testing purposes [11]. Nonetheless, they are mostly inconvenient and bulky. One example can be the measurement of blood pressure [12] but this technology requires to perform measurement at two different places on the body, e.g., on both hands.

We distinguish between the systolic and diastolic blood pressure [12,38]; these two levels characterize upper and lower blood pressure values, respectively, which depend on heart activity. For a healthy person, the diastolic blood pressure should not be lower than 80 mmHg (lower values mean hypotension) and the value of the systolic blood pressure should not be below 120 mmHg (again, lower values mean hypotension). People with hypertension have higher blood pressure values, with critical thresholds 140 mmHg for the diastolic blood pressure and 300 mmHg for the systolic blood pressure. In fact, diastolic and systolic blood pressure values are bound up with the ranges from 80 to 140 mmHg and from 120 to 300 mmHg, respectively [38]. On the one hand, blood pressure values outside these normal ranges can indicate a fake fingerprint [12]. On the other hand, we can think of configurations, where the blood pressure measurement of a fake fingerprint glued to the finger which significantly lowers the measured blood pressure value can still give us a measurement value within the accepted range. An attacker with hypertension would be accepted as a registered person in such configuration [12].

15.2.5 Other methods

There are specific solutions that use or combine previously mentioned methods. Also secret commercial solutions exist where even if the principle was known to authors for obvious reason they cannot be explained. It is literally impossible to list all combinations and variations of liveness detection methods.

15.3 Fingerprint spoofs

Efforts to break into fingerprint access systems are probably as old as these systems. With the boom of personal devices secured by fingerprint technology, there is more attention focused on the ways of bypassing them. The motivation for doing so may be lawful or unlawful. This section is an introduction to production and usage of fingerprint spoofs. First, there is description of what kind of preparation is needed, after that, materials and production of a spoof itself is described. Finally, the last subsection is about usage of fingerprint spoofs, experience with different fingerprint sensors, materials of spoofs and liveness detection [39,40].

15.3.1 Preparation phase for spoof production

Generally, there are several methods of spoofing fingerprint access system. They can be seen in Figure 15.17. There is cooperative branch which presumes that a mold can be done directly with the cooperation of the person which is impersonated. That is usually not the case and there are four other possibilities left. Either the latent fingerprint can be reactivated on the device which is possible for some fingerprint sensor technologies or a cadaver finger or cut finger can be used. All these options presume some cooperation or very specific actions of the impersonated user [39,40].

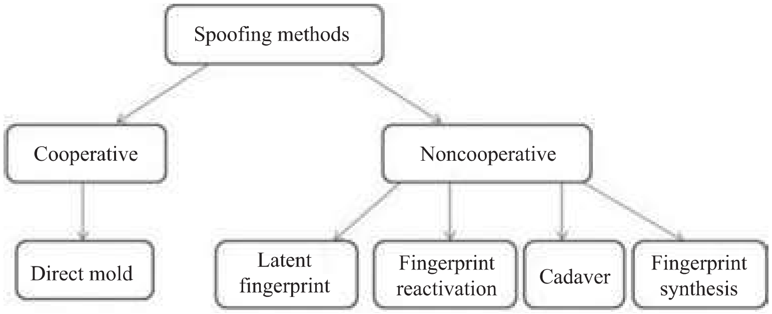

Figure 15.17 Overview of various spoofing methods [39]

15.3.1.1 Desired fingerprint acquirement

Without this cooperation or specific actions from the original user, the only remaining action presumes that the latent fingerprint can be obtained. Last part, the fingerprint synthesis is also somewhat relevant to this part because latent fingerprint often needs quality enhancement. This can be done by automatic or manual tools for fingerprint reconstruction. Fingerprint synthesis can be classified as an automatic method, but rather it should be seen as another type of reconstruction—the aim is from whatever information is present to create a perfect synthetic fingerprint. One method or another, the focus is on getting the best possible quality digitized latent fingerprint [39,40].

As it was stated in section 15.1, process usually starts with securing desired objects with latent fingerprints on them. After that, vapor (dusting) techniques are used to make these fingerprints visible. Next step is scanning the fingerprints to get digitized images. Final step is to get the best quality out of input data.

Process of fingerprint acquirement is the most difficult task in the spoof production. From this fingerprint a mold will be produced. Final spoof will never have better quality than quality of the mold. Acquiring several latent fingerprints and combining them together, patient reconstruction of ridges and minutia all these tasks are important for the final image quality. Note the difference between perfect synthetic fingerprint and real fingerprint in Figure 15.18.

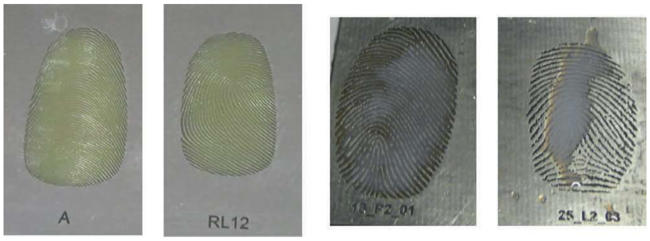

Figure 15.18 Synthetic (left) and real (right) fingerprint molds

15.3.1.2 Production of the mold

Mold can be made from various materials. Basically, it can be anything which will (a) form the spoof material, (b) allow easy removal of spoof without damage and (c) optionally be used multiple times. Ideal mold material also depends on material which is used for spoofs. Soft materials as latex can be used on relatively fragile material. Some play-doh which need steady pressure to form needs more durable one.

One of the most durable and also most commonly used mold is made as printed circuit board (PCB). Digitized fingerprint image is converted to the PCB drawing file. File is transferred to the company dealing with PCBs which create the cuprextit fingerprint mold. Metal is durable—it can withstand physical damage, temperature changes both hot and cold without damaging the fingerprint image. It can be easily cleaned and use of separators or others special materials is usually not a problem. Some spoof materials need special treatment which includes previously stated dangers for mold. Presumably, this type of mold was chosen, next step is production of the spoof itself [39–41].

15.3.2 Materials for spoof production

There are dozens of materials which can be used for fingerprint spoof. Ideal spoof material would be something with same properties (i.e., physical, electrical, etc.) as human skin and it should be easy to work with. From properties perspective, the most important is elasticity, greasiness and durability. That is because these are almost necessary to scan spoof with any sensor. Other properties (like color, conductivity, resistance, pulse, sweat, etc.) are usually important when facing a specific sensor and/or liveness detection technology. From production perspective, the most important factors are (a) how easy it is to copy mold image, (b) how easy it is to remove material from mold, (c) how long does this process take and (d) whether some special treatment is needed and difficulty of using this treatment.

It is almost impossible to list all materials which were ever used. Also, it is very difficult to sort the best material because all of them lack some important parts which were defined in previous paragraph. Often the material is either not durable and can be used only few times before image on the material disappear or is durable and elastic but special treatment is needed when producing. Nevertheless, description and figures of some of the most used or often mentioned materials are given below.

Play-doh can be categorized as modeling clay designed mainly for children. It is soft and malleable and it cannot be hardened (this is not true for some clays). Spoofs are not durable but they are very easy to use. In Figure 15.19, spoof and its image can be seen [40].

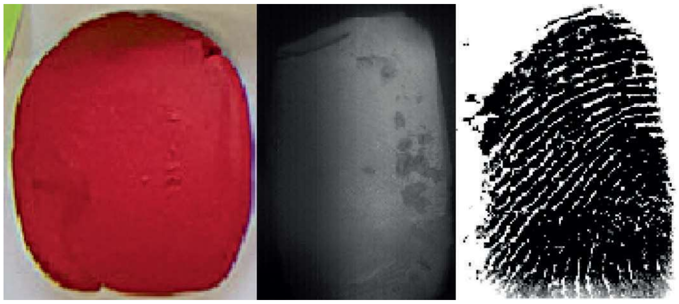

Figure 15.19 Play-doh spoof [40]

Latex is a white fluid which can be found inside of some plants. It is a base for natural rubber, tires, etc. Latex can be seen as category of rubbers or similar materials. When making spoofs, the biggest challenge is to make an equally thick layer. This layer should be at the same time as thin as possible, however thick enough to be easily removed. It is fairly durable, elastic but not so easy to make. Example of latex spoof is shown in Figure 15.20 [40].

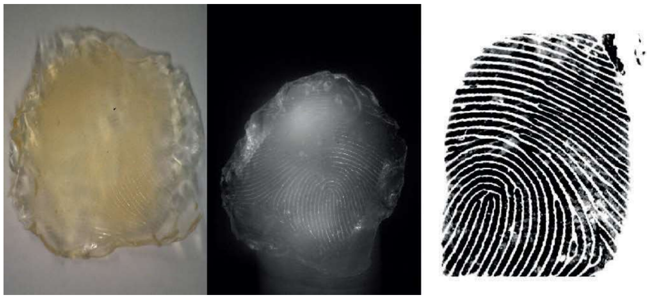

Figure 15.20 Later spoof [40]

Gelatin belongs to food industry spoofs category. Spoofs made from gelatin have to stick to a transparent glue tape during removing them from the mold. Gelatin is too soft and fragile material to be removed directly without the glue tape, otherwise during the removing the fingerprint spoofs could be damaged. They are usually made soft by heating and harden when they cool off. Spoofs are elastic, easy to make, not so easy to remove and also not durable. In Figure 15.21, gelatin spoof can be seen [39].

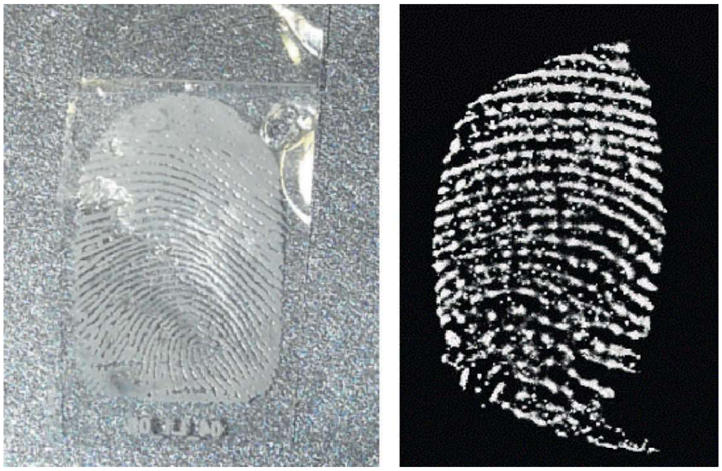

Figure 15.21 Gelatin spoof [39]

Aquarium silicone can be categorized as glues and other industrial materials. Spoofs are nicely soft after drying, flexible and durable with clearly visible ridges, where the minutiae points could be precisely located. On the other hand, it is very hard to remove them from mold, not so easy to be made without air bubbles. Examples can be seen in Figure 15.22 [39].

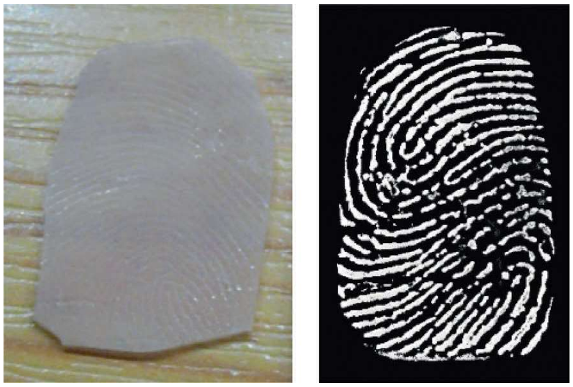

Figure 15.22 Aquarium silicone spoof [39]

Glass colors could form a special "others" category. These are special colors which can be used on glass, windows, mirrors, bathroom tiles, etc. The colors are applied to a plastic foil after that they can be peeled off and stuck to another similar surface. The mold can be filled with a really thin layer by pouring a small drip and spreading the color with a knife. If it is too thin, then it stretches out and can even tear apart while removing it from the mold. Spoofs can be done also by just pouring the color until it fits the mold. Spoofs are relatively durable, relatively elastic, very easy to make and the only problematic part is the removal. Spoofs from this material can be seen in Figure 15.23 [40].

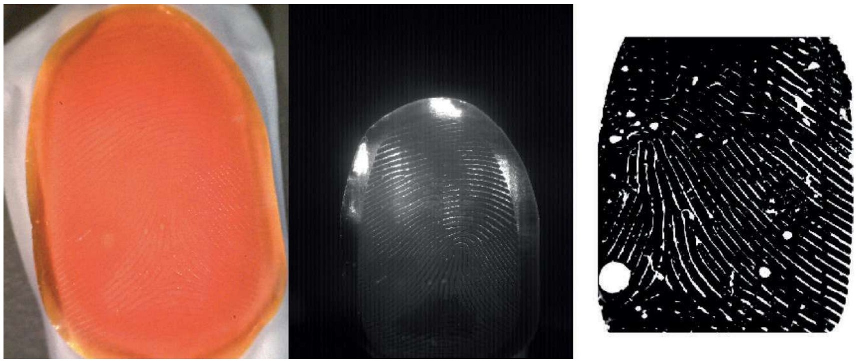

Figure 15.23 Glass colors spoof [40]

15.3.3 Spoof usage

Spoof usage is generally simple—spoof is used instead of a finger on the fingerprint scanner. There are two main choices how to present the spoof, either use it as a new layer on finger or to present it with other material (e.g., fake rubber finger). Now the specific attributes of the spoof material, sensor technology and (if present) liveness detection are determining how successfully spoof will perform.

If the spoof material is not durable, then it will (a) be used with real finger to use appropriate strength, (b) be almost unable to be used with swipe sensor technology, (c) be even with careful usage used only few times and (d) probably leave some residue on the sensor.

If the spoof material has not skin like properties, then it will possibly need special technique to present to sensor like using strong pressure, cropping spoof to exactly match sensing area, etc. There will probably exist sensor technology or liveness detection based on missing properties. If that is the case then usually combination of real finger and spoof have to be used. That means trying to use real finger for liveness detection and spoof for sensing the image. That generally results on very thin spoofs glued to real finger or using a real finger on a small part of sensing area and spoof in the remaining regions of sensing area.

Some technologies are acquiring fingerprint images from deeper layer of the skin. If that is the case, then it can also ignore the spoof and scan the real fingerprint below the spoof. In that case, it is better not to use real finger with the spoof.

Each combination of material and sensor is unique and needs different approach to use effectively. Some spoof materials can be enhanced with other materials to make them better when using specific sensor (e.g., adding coloring to spoof which has not naturally a skin color to overcome optical technology). To our best knowledge, there is not a sensor which cannot be overcome (although using special enhanced spoofs and excellent present technique).

15.4 2D/3D hand spoofs

The large advantage of hand geometry-based biometry technologies is the affordability. The current commercially available devices such as HandKey and HandPunch series from Schlage use single downward facing camera as the sensory input and store the features in 9 kB template. While this in comparison with retina scanner for example allows for lower cost of device, the system can be fooled even via trivial means.

In [42] a spoof was created using a simple paper silhouette. This spoof was then successfully accepted by HandKey system. From this paper, we can infer that the system does not perform any form of liveness detection. For even a texture analysis would prevent the spoofing of the system using this way (Figure 15.24).

The current generation of hand-based biometry sensors could be spoofed using this technique, however, in the upcoming generation, this approach should prove to

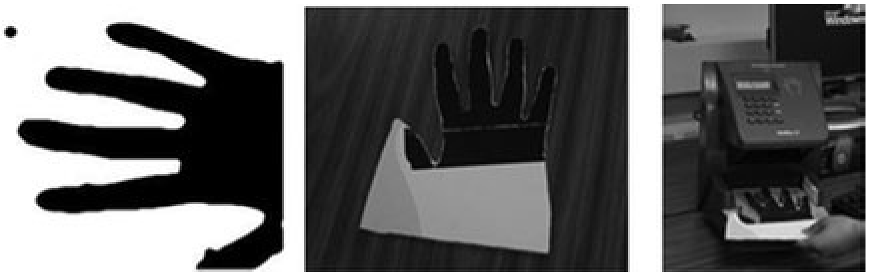

Figure 15.24 Paper silhouette spoof used to bypass commercial device [26]

be obsolete. As the liveness detection is covered in another part of this chapter, we will concentrate on spoofs based on increase in detail.

If the resolution of acquisition is increased substantially, the level of detail acquired increases as well. When the level of detail is low, such as in low resolution hand geometry verification, the matter of gathering the biometric information form uncooperative even unaware subject is a trivial matter. However, if the detail is increased enough during data gathering, the retrieval of source data from uncooperative subject becomes nontrivial, since the position, orientation, even movement can make the data gathering process fail. The spoof development then needs to integrate data from multiple acquisitions for spoof to contain all the data that are retrieved during calibrated acquisition.

Other direction that can increase the complexity of spoof development is an increase in dimensionality of used biometric. With increased computing power, it is now possible to perform a 3D reconstruction in real time, this allows for expansion of previously 2D biometric features into 3D feature, or using both of them. The increase in computing power, however, makes the creation of high detail spoof possible as well.

In Figure 15.25, we can see an example of mold casted spoof, this kind of spoof would not only overcome the 2D technologies, but also low detail 3D technologies. The shortcoming of this spoof lies in the acquisition process, which requires cooperation from the target, especially if the scanning devices, relies on pin guided approach, this would make it further complex, as the target's hand would need to be in a precise position during mold creation.

The more universal approach however, utilizes 3D printing technologies. In this case, no mold creation is required, as the data can be acquired, and the model reconstructed without the knowledge of the target, either by using the 3D scanning or by reconstructing the 3D model from an array of 2D images.

In Figure 15.26, we can see a model of hand printed using a commercially available low-cost 3D printer, with nozzle size of 0.3 mm and layer size of 0.125 mm, we can achieve a precision of up to 200 DPI in one axis. And on industrial scale, with infrared-laser-based 3D printer, the resolution can be as low as 15 μm [43]. If the texture analysis is not performed, a surface finish can be applied.

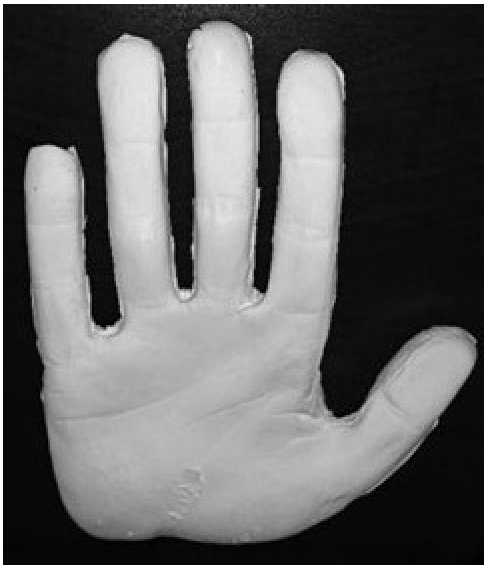

Figure 15.25 Mold casted hand spoof

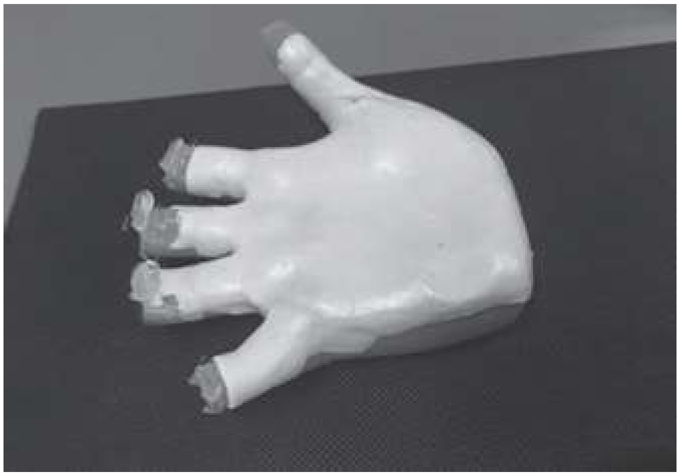

Figure 15.26 Hand spoof from 3D printer

The capabilities of these technologies need to be considered when designing the security system. Otherwise, there is a danger that newly created system is obsolete from the beginning, as the technology to create spoofs offers higher level of detail than the security technology can successfully verify or even observe.

To the knowledge of the authors, there is not at the moment a commercially available micrometric 3D printing technology, capable of simultaneous support of multiple printing materials. This would suggest that for creation of 3D spoof that integrates layers of material with different spectral absorption characteristics, necessary to overcome a vein detection-based liveness verification system on a 3D hand geometry-based biometrics system, new technology would have to be developed.

15.5 Conclusion

In this chapter, we discussed antispoofing and spoofing methods for hand-based biometrics. Generally, the methods which are based on skin properties could be used not only on fingers, but on the whole hand or even body.

It is very easy to produce a finger(print) fake, just based on fingerprint acquired from any object the person of interest touched. There are three ways how to produce such finger(print) fakes—2D/3D print, use a form (e.g., PCB) or to use a laser burner. The quality and use possibilities very strongly depend on the technology, which is used for antispoofing. Some of the fakes degrade after some time, i.e., are not usable after some days, weeks or months.

Regarding the antispoofing methods, a lot of them were proposed; however, on nearly all of them, at least one attack have been found. The most promising technology is very probably the multispectral illumination and sensing. This technology acquires real skin reaction to the illumination with a concrete wavelength, which is hard to simulate for a combination of more wavelengths. Another very promising technology is to use the electrical properties of the human finger, i.e., combination of charging and turbulent flow (induction). However, some fakes have been found for this technology as well. Also, some fingerprint acquisition technologies include automatic antispoofing detection – these are for example, ultrasound scanning and optical tomography. These methods penetrate beneath the skin and acquire the underlying structures of the skin. Therefore if there is any fake glued on the fingertip surface, these technologies show artifacts on the image, which means that a finger(print) fake is in use.

It is fully clear that antispoofing methods need to be used in a real world. The possibilities of how to attack a biometric system using fakes are wide. Therefore these attack attempts could be avoided just using such antispoofing methods.

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] Dessimoz, D., Richiardi, J., Champod, C., Drygajlo, A.: Multimodal Biometrics for Identity Documents, Research Report, PFS 341-08.05,

Version 2.0, Université de Lausanne & École Polytechnique Fédérale de Lausanne, 2006, p. 161.

[2] Jain, A.K.: Biometric System Security, Presentation, Michigan State University, East Lansing, MI, 2005, p. 57.

[3] Ambalakat, P.: Security of Biometric Authentication Systems, In: 21st Computer Science Seminar, SA1-T1-1, 2005, p. 7.

[4] Galbally, J., Fierrez, J., Ortega-Garcia, J.: Vulnerabilities in Biometric Systems: Attacks and Recent Advances in Liveness Detection, Biometrics Recognition Group, Madrid, Spain, 2007, p. 8.

[5] Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S.: Impact of Artificial "Gummy" Fingers on Fingerprint Systems, In: Proceedings of SPIE Vol. 4677, Optical Security and Counterfeit Deterrence Techniques IV, 2005, p. 11.

[6] Roberts, C.: Biometric Attack – Vectors and Defences, 2006, p. 25.

[7] Collins, C.G.: Fingerprint Science, Copperhouse/Atomic Dog Publishing, p. 192, 2001, ISBN 978-0-942-72818-7.

[8] LN: Němečtí hackeři šíří otisk prstu ministra (German Hackers Distribute the Minister's Fingerprint), Lidové noviny (newspaper), March 31, 2008.

[9] Drahanský, M.: Fingerprint Recognition Technology: Liveness Detection, Image Quality and Skin Diseases, Habilitation Thesis, Brno, CZ, 2010, p. 153.

[10] Straus, J., Porada, V., *et al.*: Kriminalistická daktyloskopie (*Criminalistics dactyloscopy*), Police academy of Czech Republic and Criminalistic Institute Prague of the Police of Czech Republic, Praha, 2005, p. 286, ISBN 80-7251-192-0.

[11] Kluz, M.: Liveness Testing in Biometric Systems, Master Thesis, Faculty of Informatics, Masaryk University Brno, CZ, 2005, p. 57.

[12] Drahanský, M., Funk, W., Nötzel, R.: Liveness, Detection Based on Fine Movements of the Fingertip Surface, In: IEEE – The West Point Workshop, West Point, New York, USA, 2006, pp. 42–47, ISBN 1-4244-0130-5.

[13] Drahanský, M.: Methods for Quality Determination of Papillary Lines in Fingerprints, NIST, Gaithersburg, USA, 2007, p. 25.

[14] Tan, B., Lewicke, A., Schuckers, S.: Novel Methods for Fingerprint Image Analysis Detect Fake Fingers, SPIE, 10.1117, 2.1200805.1171, 2008, p. 3.

[15] Schuckers, S., Hornak, L., Norman, T., Derakhshani, R., Parthasaradhi, S.: Issues for Liveness Detection in Biometrics, CITeR, Presentation, West Virginia University, Morgantown, WV, 2003, p. 25.

[16] Rowe, R.K.: A Multispectral Sensor for Fingerprint Spoof Detection, www.sensormag.com, January 2005.

[17] Rowe, R.K.: Spoof Detection, In: Summer School for Advanced Studies on Biometrics for Secure Authentication, Alghero, Italy, 2008, p. 43.

[18] Toth, B.: Biometric Liveness Detection, In: Information Security Bulletin, Vol. 10, 2005, pp. 291–297, retrieved from on 2017-08-13: www.chi-publishing.com.

[19] Abhyankar, A., Schuckers, S.A.C.: A Wavelet Based Approach to Detecting Liveness in Fingerprint Scanners. In: Proceedings of the SPIE Vol. 5404, Biometric Technology for Human Identification, 2004, p. 9.

[20] Qualcomm, Qualcomm Fingerprint Sensors, 2017-10-04, retrieved from on 2017-10-08: https://www.qualcomm.com/products/features/security/fingerprint-sensors.

[21] Sonavation, Ultrasound Biometric Sensor, 2017-10-04, retrieved from on 2017-10-08: http://www.sonavation.com/ultrasound-biometric-sensor/.

[22] InvenSense, InvenSense and GLOBALFOUNDRIES Collaborate on Industry-Leading Ultrasonic Fingerprint Imaging Technology, 2017-10-04, retrieved from on 2017-10-08: https://www.invensense.com/news-media/invensense-and-globalfoundries-collaborate-on-industry-leading-ultrasonic-fingerprint-imaging-technology/.

[23] Mainguet, J.F.: Ultrasonic Fingerprint Sensing, 2017-10-04, http://biometrics.mainguet.org/types/fingerprint/fingerprint_sensors_physics_ultrasound.htm.

[24] UltraScan: The Theory of Live-Scan Fingerprint Imaging (Breaking the Optical Barriers with Ultrasound), UltraScan, USA, 2004, p. 8.

[25] Bicz, W.: The Impossibility of Faking Optel's Ultrasonic Fingerprint Scanners, Optel, Poland, http://www.optel.pl/article/english/livetest.htm, 2008.

[26] Drahanský, M.: Experiments with Skin Resistance and Temperature for Liveness Detection, In: Proceedings of the Fourth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Los Alamitos, US, IEEE CS, 2008, pp. 1075–1079, ISBN 978-0-7695-3278-3.

[27] U.S. Patent 6,314,195 – Organism Identifying Method and Device, November 2001.

[28] U.S. Patent 5,088,817 – Biological Object Detection Apparatus, February 1992.

[29] Drahanský, M., Lodrová, D.: Liveness Detection for Biometric Systems Based on Papillary Lines, In: Proceedings of Information Security and Assurance, 2008, Busan, KR, IEEE CS, 2008, pp. 439–444, ISBN 978-0-7695-3126-7.

[30] U.S. Patent 6,292,576 – Method and Apparatus for Distinguishing a Human Finger From a Reproduction of a Finger, September 2001.

[31] Jia, J., Cai, L., Zhang, K., Chen, D.: A New Approach to Fake Finger Detection Based on Skin Elasticity Analysis, In: S.-W. Lee and S.Z. Li (Eds.): ICB 2007, LNCS 4642, 2007, pp. 309–318, Springer-Verlag Berlin Heidelberg, 2007, ISSN 0302-9743.

[32] Putte, T., Keuning, J.: Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned, In: IFIP TC8/WG8.8 4th Working Conference on Smart Card Research and Advanced Applications, Kluwer Academic Publishers, 2000, pp. 289–303.

[33] Martinsen, O.G., Grimnes, S., Haug, E.: Measuring Depth Depends on Frequency in Electrical Skin Impedance Measurements, In: Skin Research and Technology No. 5, 1999, pp. 179–181, ISSN 0909-752X.

[34] Grimnes, S., Martinsen, O.G.: Bioimpedance, University of Oslo, Norway, Wiley Encyclopedia of Biomedical Engineering, John Wiley & Sons., Inc., 2006, p. 9.

[35] Das BIA-Kompendium – Data Input GmbH, Body Composition, 3rd Edition, 2007, p. 70, retrieved from on 2017-09-17: www.data-input.de.

[36] Drahanský, M., Funk, W., Nötzel, R.: Method and Apparatus for Detecting Biometric Features, International PCT Patent, Pub. No. WO/2007/036370, Pub. Date 05.04.2007, Int. Application No. PCT/EP2006/009533, Int. Filing Date 28.09.2006, retrieved from on 2017-10-10: http://www.wipo.int/pctdb/en/wo.jsp?wo=2007036370&IA=WO2007036370&DISPLAY=STATUS.

[37] Lodrová, D., Drahanský, M.: Methods of Liveness Testing By Fingers, In: Analysis of Biomedical Signals and Images, Brno, CZ, VUTIUM, 2008, p. 7, ISBN 978-80-214-3612-1, ISSN 1211-412X.

[38] Online Canadian Pharmacy Drugstore, retrieved from on 2017-11-10: www.healthandage.com.

[39] Spurný, J., Doležel, M., Kanich, O., Drahanský, M., Shinoda, K.: New Materials for Spoofing Touch-Based Fingerprint Scanners, In: Proceedings of International Conference on Computer Application Technologies 2015, IEEE, Matsue, 2015, p. 15, ISBN 978-1-4673-8211-3.

[40] Kanich, O., Mézl, M., Drahanský, M.: Use of Creative Materials for Fingerprint Spoofs, In: The 11th IAPR International Conference on Biometrics, 2018, Queensland, p. 8.

[41] Schuckers, S.A.C.: Spoofing and Anti-Spoofing Measures, Information Security Technical Report, Vol. 7, No. 4, 2002, pp. 56–62. DOI doi:10.1016/S1363-4127(02)00407-7.

[42] Chen, H., Valizadegan, H., Jackson, C., Soltysiak, S., Jain, A.K.: Fake Hands: Spoofing Hand Geometry Systems, Biometric Consortium 2005, Washington DC, 2005.

[43] DMP60 Series. 3D MicroPrint, retrieved from on 2017-11-10: http://www.3dmicroprint.com/products/machines/dmp60-series/.