9

Liveness Detection in Biometrics

Martin Drahanský
Brno University of Technology, Faculty of Information Technology
Czech Republic

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 we are 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.

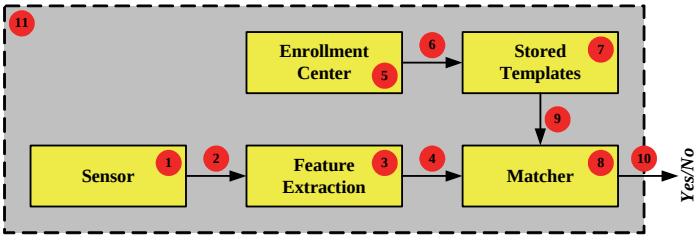

Fig. 1. Basic components of a biometric system.

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 (Fig. 1) (Dessimoz et al., 2006; Jain, 2005; Ambalakat, 2005; Galbally et al., 2007):

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 the database, is replayed to the system, thus circumventing the acquisition device.
3. *Overriding the feature extraction process*. A pre-selected 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 to 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 pre-selected 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, PKI (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 (Kluz, 2005).

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 (Matsumoto et al., 2005; Ambalakat, 2005; Roberts, 2006):

- *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 non-effort forgery. Commonly, the accuracy of authentication of fingerprint systems is evaluated by the false rejection rate (FRR) 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 (Collins, 2001). 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 (Matsumoto et al., 2005). 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 (LN, 2008). 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 (Matsumoto et al., 2005) that the production of a fake finger(print) is very simple (Drahanský, 2010). 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 post-processed, 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 (Kluz, 2005). 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 fool-proof (Kluz, 2005). 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; other require a hardware support. Methods which combine both approaches can also be used.

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 (Drahanský et al., 2006; Drahanský, 2007). 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 (Matsumoto et al., 2005; Tan et al., 2008). 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 (Drahanský et al., 2006; Drahanský, 2007). 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.

2.1 Perspiration

A non-invasive 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 (Schuckers et al., 2003). 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 Fig. 2).
It is worth noting that the outmost layer of the human skin houses around 600 sweat glands per square inch (Schuckers et al., 2003). These sweat glands diffuse the sweat (a dilute sodium chloride solution) on to the surface of the 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.

Fig. 2. Example of live fingerprint images acquired some time apart (Schuckers et al., 2003).

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.
The sweat creation and ascent from sweat pores during the scanning with 4× zoom factor could be seen in Fig. 3.

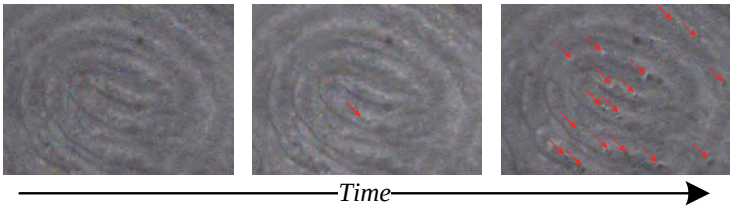

Fig. 3. Ascent of sweat from sweat pores on a fingertip (4× zoomed).

2.2 Spectroscopic characteristics

The technology discussed in this section was developed by the Lumidigm company (Rowe, 2005; Kluz, 2005) 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 (Rowe, 2005; Rowe, 2008). By collecting images generated from different illumination

wavelengths passed into the skin, different subsurface skin features may be measured and used to 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.

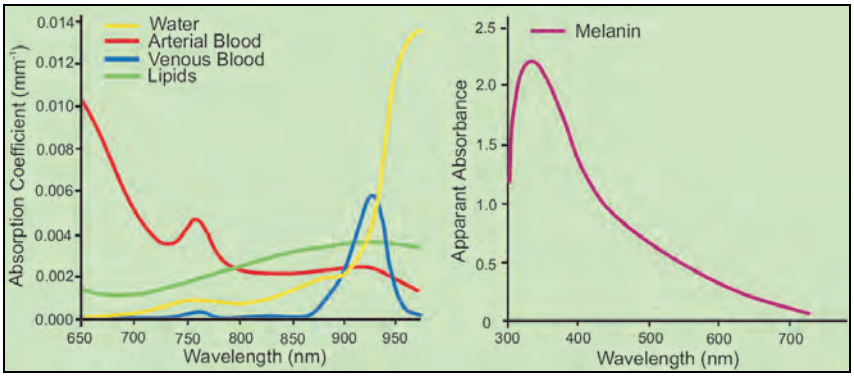

Fig. 4. Spectrographic properties of different components of living tissue (suitable for detection of spoofing attacks on iris recognition) (Toth, 2005).

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. 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 (Kluz, 2005). 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. The measurements can be transformed into a graph (Fig. 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 5 shows the layout of an optical fingerprint sensor that combines a conventional frustrated total internal reflection (FTIR) fingerprint reader with a multispectral imager.

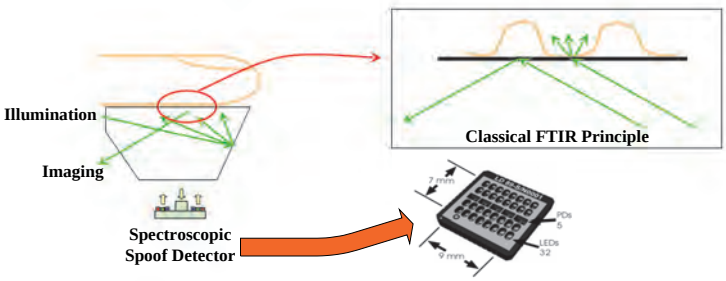

Fig. 5. FTIR and multispectral imager (Rowe, 2008).

The key components of a multispectral imager (Rowe, 2008; Rowe, 2005) suitable for imaging fingers are shown in Fig. 5. 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 CMOS or CCD detector.

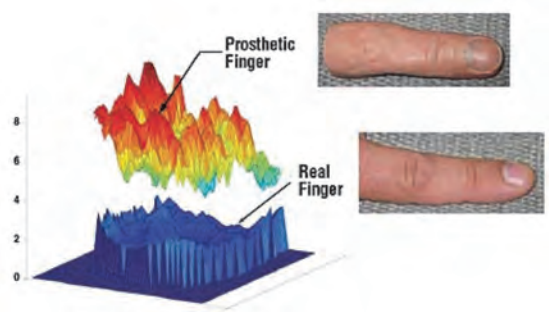

Fig. 6. Multispectral image data can clearly discriminate between a living finger and an ultra-realistic spoof. The graphs on the left side show how similar the spectral content of each image is to that expected for a genuine finger (Rowe, 2005; Toth, 2005).

A highly realistic artificial finger made by Alatheia Prosthetics (Rowe, 2005) 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 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 (Schuckers et al., 2004).

2.3 Ultrasonic technology

In this paragraph, a biometric system using an ultrasonic technology with inherent liveness testing capability will be described. This technique is being 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 Ultra-Scan from the USA, which is the second and last vendor of this technology principle in the market at the moment.
Standard ultrasonic methods (Kluz, 2005) 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 (Fig. 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

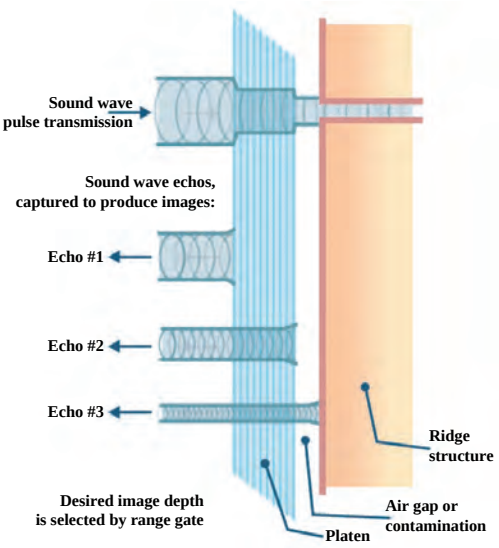

Fig. 7. Schematic of ultrasonic pulse/echo principle (UltraScan, 2004).

transformation. This phenomenon is called contact scattering (Kluz, 2005) 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.
The ultrasonic device reached the following conclusions (Kluz, 2005; Bicz, 2008):

- 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 (Bicz, 2008).

2.4 Physical characteristics: temperature

This simple method measures the temperature of the epidermis during a fingerprint acquisition. The temperature of the human epidermis of the finger moves in the range of approximately 25–37°C (see Fig. 8). However, this range usually has to be wider to make the system usable under different conditions. 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 (Drahanský, 2008) 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.

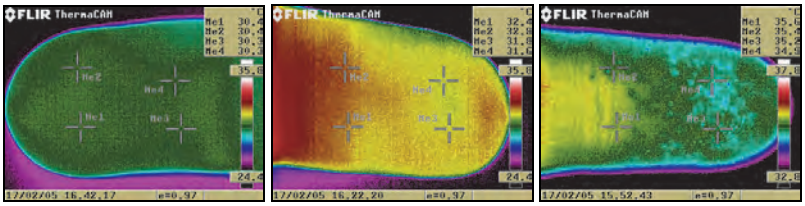

Fig. 8. Thermo-scans of the fingertips acquired using a thermo-camera FLIR.

2.5 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, non-living material.

The designed liveness testing module (Kluz, 2005; U.S. Patent 6,314,195) 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 (U.S. Patent 6,314,195).

2.6 Physical characteristics: 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 (Kluz, 2005; U.S. Patent 5,088,817). 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 not under pressure is usually reddish but becomes whitish when pressure is applied to the skin of the finger. 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) (U.S. Patent 5,088,817) does not show a substantial difference between the pressed state and the non pressed 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) (U.S. Patent 5,088,817) 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 Fig. 9).
A liveness testing module is proposed in (U.S. Patent 5,088,817) 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 towards the finger and receiving the reflected light. The light source projects a light beam towards the surface of the placed finger. Next, depending on the pressure or non-pressure state, the reflected light is measured by the light detection unit.

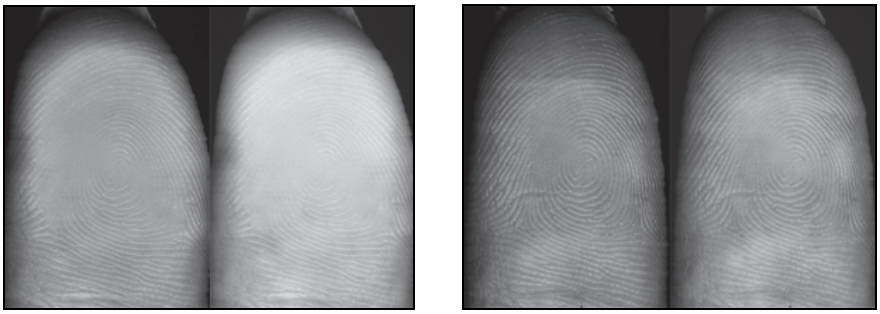

Fig. 9. Images of the fingertips pressed tightly (left subpart) and slightly (right subpart) to the sensor (Drahanský et al., 2008).

Based on such measurements the determining section returns the right decision, i.e. as the finger changes its state from non-pressure 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 (U.S. Patent 6,292,576), but unlike the method described in the previous paragraph, this technique employs the change in fingerprint ridges width. When the fingerprint changes its state from non-pressure 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 (Jia et al., 2007). 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 Fig. 10) can be used for fingerprint authentication.

Fig. 10. A sequence of fingerprint images describing the deformation of a real finger (Jia, 2007).

2.7 Physical characteristics: 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 (Kluz, 2005). 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 (Kluz, 2005) 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) (Kluz, 2005) 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 (Pute et al., 2000) 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 10 people, each finger, horizontal and vertical measurement strips, and 5 measurements per finger – conductivity (resistance) measurements. The range of values we found was from 20 kΩ to 3 MΩ (Drahanský, 2008). A paper copy or an artificial finger made of non skin-like material have higher electrical resistance, but for example, soft silicon (moisturized) shows resistance values close to the range found in our experiments.

2.8 Physical characteristics: bio-impedance

Bio-impedance (Martinsen et al., 1999; Grimmes et al., 2006; BIA, 2007) 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* (Grimmes et al., 2006) 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) (Grimmes et al., 2006), 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 DC (Direct Current) current flow.

The body tissue is composed of cells with poorly conducting, thin-cell membranes. Therefore, the tissue has capacitive properties (Grimmes et al., 2006): 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.

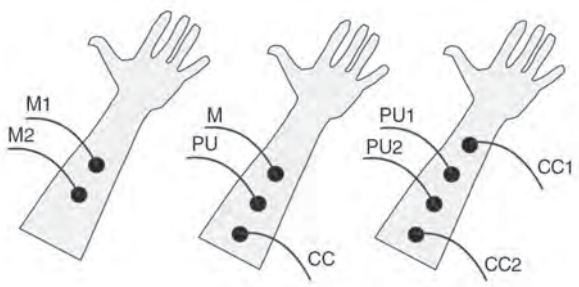

Fig. 11. Three skin surface electrode systems on an underarm (Grimmes et al., 2006).
Functions: *M* – measuring and current carrying, *CC* – current carrying, *PU* – signal pick-up.

Fig. 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 (Grimmes et al., 2006): the signal is not picked up from the sites of current application.

Fig. 12 shows a typical transfer impedance spectrum obtained with the 4-electrode system from Fig. 11. It shows two dispersions (Grimmes et al., 2006). The transfer impedance is

related to, but not solely determined by, the arm segment between the 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.

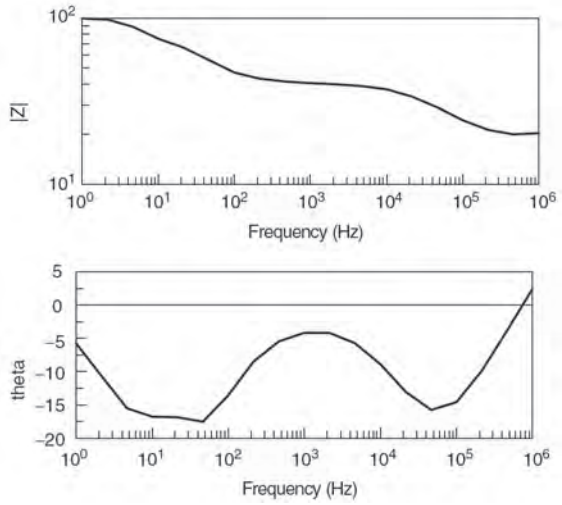

Fig. 12. Typical impedance spectrum obtained with four equal electrodes attached to the skin of the underarm (Grimmes et al., 2006).

2.9 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 (Kluz, 2005). 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 (Kluz, 2005). 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 (Kluz, 2005).

Our skin is semi-permeable 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 (Drahanský et

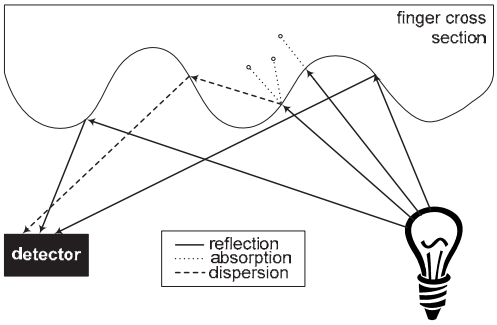

Fig. 13. Light absorption, dispersion and reflection by a fingerprint (Drahanský et al., 2006).

al., 2006; Drahanský et al., 2007). The light illuminating the finger surface is partly reflected and partly absorbed (Fig. 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.

Another example for optical skin feature is the saturation of hemoglobin (Drahanský et al., 2006; Drahanský et al., 2007), 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 non-oxygenated 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 non-oxygenated blood, respectively (Drahanský et al., 2006; Drahanský et al., 2007). 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 (Drahanský et al., 2006; Drahanský et al., 2007) 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 (Drahanský et al., 2006; Drahanský et al., 2007) 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 one or two seconds to the overall authorization process interval.

In (Drahanský et al., 2006; Drahanský et al., 2007), two approaches for measuring of fine movements of papillary lines, based on optical principles, are suggested (Fig. 14). The first solution is based on a close-up view of the fingertip acquired with a 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 Fig. 15 and Fig. 16, may significantly influence the hardware requirements imposed on the complete system.

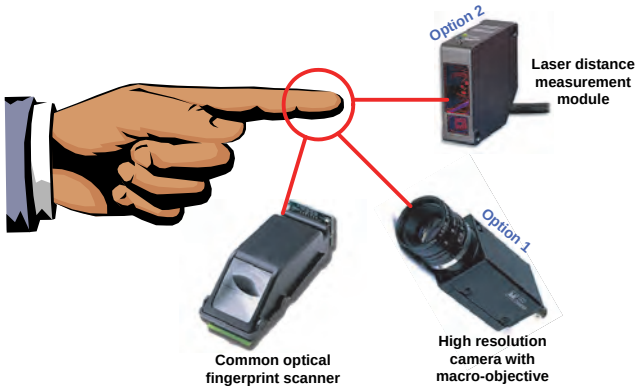

Fig. 14. Integrated liveness detection – scanner + optical and laser solution (Lodrová et al., 2008).

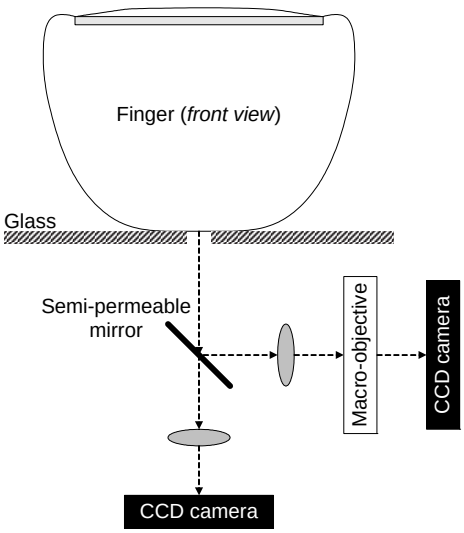

Fig. 15. Possible integration of a camera-based measurement system for liveness detection with optical fingerprint sensor (CCD/CMOS camera) (Drahanský et al., 2006).

2.9.1 Camera solution

The camera solution scheme is outlined in Fig. 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. The latter part of the system is used to acquire a video sequence for the liveness detection analysis.

2.9.2 Laser solution

The second optical method for the liveness testing is based on laser distance measurements (Drahanský et al., 2006; Drahanský et al., 2007). Fig. 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 Fig. 15. However, unlike the solution shown in Fig. 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.

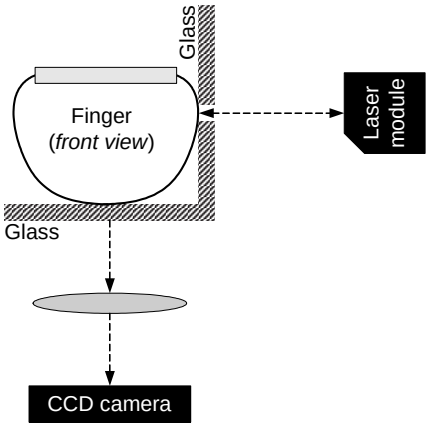

Fig. 16. Possible integration of laser distance measurement for liveness detection with optical fingerprint sensor (CCD/CMOS camera; aperture approx. 6 mm) (Drahanský et al., 2006).

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 (U.S. Patent 6,292,576) and (U.S. Patent 5,088,817). They coincide in principles (both are optical) but differ in monitored physical characteristics.

2.10 Physical characteristics: blood oxygenation

Sensors which measure blood oxygenation (Kluz, 2005) 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. Secondly, 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).

2.11 Other methods

There are some other methods based on the medical science characteristics which have been suggested for liveness testing purposes (Kluz, 2005). Nonetheless, they are mostly inconvenient and bulky. One example can be the measurement of blood pressure (Drahanský et al., 2006) 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 (www.healthandage.com; Drahanský et al., 2006); 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 mm Hg (lower values mean hypotension) and the value of the systolic blood pressure should not be below 120 mm Hg (again, lower values mean hypotension). People with hypertension have higher blood pressure values, with critical thresholds 140 mm Hg for the diastolic blood pressure and 300 mm Hg for the systolic blood pressure. In fact, diastolic and systolic blood pressure values are bound up with the ranges from 80 mm Hg to 140 mm Hg and from 120 mm Hg to 300 mm Hg, respectively (www.healthandage.com). On one hand, blood pressure values outside these normal ranges can indicate a fake fingerprint (Drahanský et al., 2006). 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 (Drahanský et al., 2006).

3. Conclusion

The topic of this chapter is oriented towards the liveness detection in fingerprint recognition systems. At the beginning, certain basic threats, which can be used in an attack on the

biometric system, are described in general. One of them is the use of fake finger(print)s. Of course, the security of the biometric system is discussed here too, however, this is rather out of scope of this thesis. This is followed by a detailed introduction to the liveness detection and to all known methods and related principles; these include perspiration, spectroscopic characteristics, ultrasonic principle and many physical characteristics.

4. Acknowledgment

This work is partially supported by the grant "*Information Technology in Biomedical Engineering*", GA102/09/H083 (CZ), by the grant "*Advanced secured, reliable and adaptive IT*", FIT-S-11-1 and the research plan "*Security-Oriented Research in Information Technology*", MSM0021630528 (CZ).

5. References

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

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

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

Das BIA-Kompendium – Data Input GmbH, *Body Composition*, 3rd Edition, 2007, p. 70, www.data-input.de.

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.

Drahanský M.: *Fingerprint Recognition Technology: Liveness Detection, Image Quality and Skin Diseases*, Habilitation thesis, Brno, CZ, 2010, p. 153.

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.

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.

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, http://www.wipo.int/pctdb/en/wo.jsp?wo=2007036370&IA=WO2007036370&DISPLAY=STATUS.

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

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.

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.

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

Jain, A.K.: *Biometric System Security*, Presentation, Michigan State University, p. 57, 2005.

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.

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

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

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.

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.

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.

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.

Roberts, C.: *Biometric Attack – Vectors and Defences*, 2006, p. 25.

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

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

Schuckers, S., Abhyankar, A.: *Detecting Liveness in Fingerprint Scanners Using Wavelets: Results of the Test Dataset*, In: BioAW 2004, LNCS 3087, 2004, Springer-Verlag, pp. 100-110.

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

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

Toth, B.: *Biometric Liveness Detection*, In: Information Security Bulletin, Vol. 10, 2005, pp. 291-297, www.chi-publishing.com.

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

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

U.S. Patent 6,292,576 – *Method and Apparatus for Distinguishing a Human Finger From a Reproduction of a Finger*, September 2001.
U.S. Patent 5,088,817 – *Biological Object Detection Apparatus*, February 1992.