Spoofing and anti-spoofing methods for fingerprint sensors

Lodrova Dana
Gjovik University College, Brno University of Technology
ilodrova@fit.vutbr.cz

version 1.0, 27. November 2008

Contents

1 Introduction

Nowadays more and more sensors contain some liveness testing method which measure some of the characteristic properties of live human body. But it is not easy to create and implement such method. It has to fulfill several security requirements. Firstly, it is necessary to measure same part of body which is captured. In case of fingerprint it means, that it is possible to use only such property, which can be measured through a fingertip. It is also necessary to test liveness approximately in the same time when the biometric sample is captured (both processes may not interfere). If this requirement is not fulfilled, an attacker can circumvent this protection by putting an artificial finger in fingerprint capturing phase and his/her live finger in liveness testing phase. Another requirement is, that the measurement of this property has to be easily software or hardware implemented, otherwise costs of such sensor or decision time can be for end-users unacceptable. And of course it is necessary to choose such property, which can not be easily simulated.

This review report is organized as follows. Section 2 contains overview of most widely-used methods for spoofing fingerprint sensors. In the third section there is a description of characteristic properties of live human skin/finger, which can be used for liveness testing purposes, and also overview of methods based on them. Last section describes an present trend: Security by obscurity.

2 Spoofing fingerprint sensors

In previous few years researches demonstrated variety of methods for spoofing different types of fingerprint sensors. The most known and the most used methods and their results are presented in next six subsections.

2.1 Reactivation of latent fingerprint

The simplest option for spoofing fingerprint sensors is reactivation of a latent fingerprint. In 2002 Ms. Thalheim et al. [18] proposed and tried three methods for fooling capacitive fingerprint sensors. When an attacker will breathe on the sensor area or apply a plastic bag filled by water, it causes reactivation of a latent fingerprint which rest on the sensor area. It is also possible to use the latent fingerprint from another place and dust a graphite powder over it. Then the attacker can use an adhesive tape for capturing the fingerprint and place the tape on the sensor area and apply gentle pressure.

Ms. Thalheim et al. tested Siemens' ID mouse (Infineon's FingerTIP), Cherry G83-14000 keyboard, Eutron's Magic Secure (STMicroelectronics' TouchChip) and Veridicom's 5th Sense Combo. It was possible to spoof all these sensors by breathing or using the plastic bag with water in few attempts when the latent fingerprint had a good quality. And they were able to spoof sensors even when the security was set at maximum level. The spoofing by the graphite powder was even more successful.

Mr. Ligon from Siemens published an article [8] as reaction to previously described tests. He claims, that Siemens ID mouse contain latent print rejection (LPR) algorithm, which reject every fingerprint which is identical with the previous one. He used latent fingerprints form 40 thumbs and also 40 index fingers. According his results, it was not possible to spoof sensor by the plastic bag filled with water and it was also impossible to fool it by breathing with LPR algorithm. When the fingerprint was created before mouse

activation, the breathing method had 5 percent successful rate in normal security mode and 2.5 percent successful rate in extended security mode. The usage of graphite powder was little more successful (10% in normal and 2.5% in extended security mode).

2.2 Image of fingerprint

The second option is the usage of a printed image of papillary lines or even a detailed picture of finger. It is supposed that this method can work only by the optical fingerprint sensors.

2.3 Professionally-made fingers

Another option is a usage of professionally made finger or fingerprint, for example a stamp [9]. This method is easier and without effort (in comparison with creating home-made artificial fingers). It is necessary to obtain the latent fingerprint, enhance it e.g. in Photoshop and go into stationer's shop. Stamp is finished after 2 days and it costs only 4 Euro (in the Czech Republic in 2007).

Figure 1: Left fingerprint: The stamp captured by the thermal fingerprint sensor Bergdata FCAT 100. Middle fingerprint: The stamp captured by the optical fingerprint sensor Suprema SFM3020-OP. Right fingerprint: The stamp captured by the capacitive fingerprint sensor Suprema SFM3050-TC1. Right picture: Picture of the stamp.

We tried to test this option by the common office stamp. It is possible to spoof optical, capacitive and thermal fingerprint sensors by it. In Fig. 1 you can see three fingerprints captured using this stamp by different types of sensors and in the right part of Fig. 1 you can find the picture of the stamp. This stamp is used as an example of vulnerabilities of fingerprint sensors in exercises in subject Biometric systems at Brno University of Technology, Faculty of Information Technology. It was no problem for students to work with this stamp, the only one difference between using live finger and the stamp is that with the stamp it is necessary to press harder on the sensor surface. In some cases the captured image from capacitive sensor can have small contrast, so for improvement of result it is good to breath on the stamp just before it is used. The most difficult thing is to fool thermal sensor with this stamp but it depends on the dexterity of attacker.

2.4 Home-made fingers

The widely used option how to spoof fingerprint sensors is the utilization of a home-made artificial finger. There are two possible situations: an invader can create the artificial finger with or without assistance of an enrolled user of biometric system.

2.4.1 with assistance of enrolled user

In this case the invader can create a mold with the aid of user and after it he can fill this mold with an appropriate substance. There are a lot of possibilities which material to use for the mold and which for the artificial finger. For example Prof. Matsumoto et al. [11] used a free plastic for the mold and a gelatin for the artificial fingerprint (so called "gummy fingers"). These fingers were tested by the help of 5 persons on 7 optical and 4 capacitive fingerprint sensors. Fingerprints was captured in 4 sessions; in the first session live finger was enrolled and also live finger was used for verification, in the second session it was enrolled live finger against artificial one, in the third enrolled artificial finger against live one and finally the enrolled artificial finger against artificial one. In all cases the successful rate was in the interval from 68 to 100 percent.

Another option chose Ms. Thalheim et al. [18], who used a wax mold from small common tea-warming candle and a silicon fingers for spoofing optical sensors (Identix's Bio-Touch USB 200 and Cherry's G81-12000 keyboard) and one thermal sensor (IdentAlink's FPS100U based on Atmel's CMOS-Finger-Chip sensor FCD4B14). It was no problem to spoof these sensors at all.

Prof. Schuckers et al. [16] used the mold from a dental impression material and play-doh fingers. They tried to spoof capacitive DC, opto-electric, optical, and capacitive AC sensors. Ten users were enrolled by their live finger and then each of them tried to enroll with six artificial play-doh fingers. The successful rate was 77 percent for capacitive AC, 63 percent for optical, 30 percent for opto-electric and only 13 percent for capacitive DE technology.

It exist a lot of other materials which are used for spoofing, for example Latex [1], Lukopren, glue etc.

2.4.2 without assistance of enrolled user

When an attacker has not possibility to cooperate with an enrolled user; he can create the mold for the artificial fingerprint e.g. by using a photosensitive printed circuit board (PCB) [13, 11]. Firstly it is necessary to obtain a latent fingerprint, for example from a glass or CD. Sometimes it is better to enhance its contrast by using a dactyloscopic powder, graphite powder or cyanoacrylate. The picture of fingerprint has to be adjusted, converted into black and white color range and printed by laser printer on a slide. [1] Than the slide is put on photosensitive PCB and illuminated with ultraviolet light. Finally it is developed and it can be used as the mold for artificial fingers. This procedure is documented in Fig. 2.

This method for creating mold was used for example by Prof. Matsumoto et al. [11] for their gummy fingers. The results of experiments did not show any difference in acceptance level between artificial fingers from the mold created with assistance of enrolled user and the mold made from PCB.

2.5 Thin artificial finger

The fifth and most difficult option is to use a very thin artificial fingerprint glued on the real finger. This thin artificial fingerprint is usually made from the same materials

[1] Sometimes it is also possible to use the slide with printed fingerprint as a mold.

Figure 2: Left: the fingerprint enhanced by cyanoacrylate. Middle: the fingerprint enhanced in Photoshop and printed on slide. Right: the photosensitive PCB after developing – the mold prepared for usage.

as thick (whole) artificial fingers. Because these artificial fingerprints are very thin, it is almost impossible to reveal such attempt by using cameras or a human supervision. It is also possible, that some methods for liveness detection can penetrate through such thin artificial fingerprint and test the liveness of the live human finger behind it.

2.6 Cutted finger

The last but worst option is, when an attacker tries to use a human finger which is separated from the hand. Prof. Schuckers et al. [16] tried to test the vulnerability of sensors against such type of attack and tried to spoof fingerprint sensors with cadaver fingers. The successful rate was quite high; 90 percent for capacitive DC, 86 for optical, 93 for capacitive AC, but only 40 percent for opto-electronic sensor technology.

3 Liveness testing method

The previous section shows, that it is very easy to spoof fingerprint sensors. Fortunatelly, it also exist a variety of properties and methods which are or can be used for liveness detection. It also exist few approaches how to sort all possible methods into groups. One approach was created by Ms. Valencia et al. [19], who divided all methods into three groups according to tested property. In first group, there are intrinsic properties of live human body/finger (e.g. color or electrical properties). Generated signals (e.g. pulse or perspiration) belong into second group and in the third group there are responses to a stimulus.

Another approach was presented for example by Mr. Wei-Yun et al.[20]. The methods are divided also into three groups. First group contains purely software based methods, which analyze only one picture from the sensor for liveness testing purposes (but these methods usually need big image resolution). In the second group there are hardware based methods (e.g. odor analysis or impedance measurement) and the last group contains methods which need more pictures or measurements to test liveness like a pulse or perspiration measurement.

In the next subsections I introduce you several known, widespread or just remarkable methods. Some of them were widely discussed on conferences and others are patented.

The numbers of patents are written in the references at the end of this review report.

3.1 Color

Detection of color itself can not be used as liveness testing method because it is quite easy to create artificial finger which color is indistinguishable from the real one. But Mr. Wei-Yun et al.[20] proposed the liveness testing method based on color change. When the finger is pressed on surface; the color of skin in the area of pressure changes from red to white. When an attacker uses a cut off finger or some kind of artificial finger, this change doesn't occur. It is assumed that this property can be used for people of different age, ethnicity, gender and type of skin.

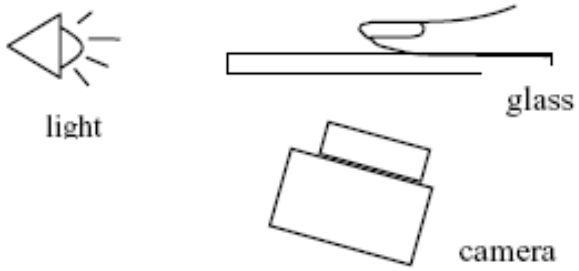

Figure 3: Prototype of sensor for detection of color change (picture was taken from [20]).

Mr. Wei-Yun et al. constructed a prototype with a white light source (see Fig. 3). They tested it with the help of group of 25 volunteers and 25 thin artificial fingers which was made form gelatin. This method achieved 80% accuracy in detecting the fake finger as not alive.

Nowadays they are working on the use of different light source and on collecting more data. Because this approach is useful only for optical fingerprint sensors, they are going to work on possibility to use this approach with other sensor types/technologies. They are going to use side view through small digital camera.

3.2 Spectral properties

Another characteristic property of live human finger is used by Lumidigm Inc. [5, 14]. Their LightPrint^{TM}technology utilizes spectral properties of various layers of skin/finger. The finger is illuminated by LED diodes with different wavelengths in sequence. The light from diodes is linearly polarized and is reflected back from finger. Each wavelength corresponds with different layer of finger. Reflected light is modified by lens and another polarizer and the resultant light is captured by common CMOS or CCD camera. In one configuration sensor contains 72 LED diodes and a common monochrome CCD camera with resolution 640x480. The scheme of multispectral imaging (MSI) sensor/process is in the Fig. 4.

This principle was tested with the help of 10 people (6 men and 4 women) against a lot of types of artificial fingers. Artificial fingers was made from latex, clear gummy bear candy, clear silicone, flesh colored latex, home-made play-doh, and putty. Color matched

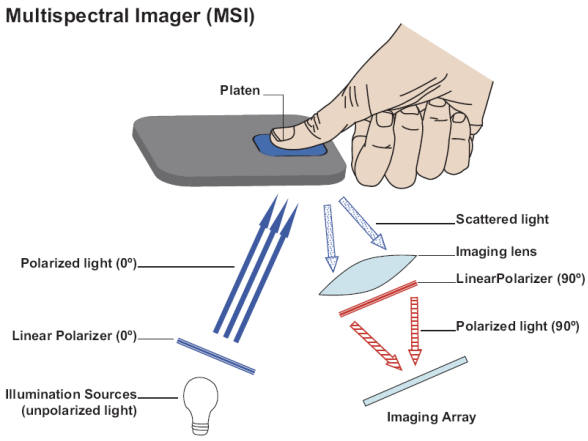

Figure 4: Schema of multispectral imaging process (picture was taken from [5]).

prosthetic finger was also used. Results of test showed good separation between set of live fingers and the set of artificial fingers.

Sensor was also tested for usage of dry or wet fingers and for situation, when user touch sensor surface only slightly. In all these cases the multispectral imaging sensor had much better results than compared optical sensor. Another advantage is the possibility to use this sensor outdoors, because water, dryness or city grime does not influence its work.

Lumidigm's MSI sensor is protected through many international or US patents. One of them [15] claims, that MSI technology is also capable to detect level of alcohol in blood, which can be useful in some situations.

3.3 Elasticity

Mr. Jia et al. [7] proposed and tested a liveness testing method based on skin elasticity analysis. At first sensor captures a sequence of fingerprint images (see Fig. 5), which shows skin deformation process. Same sequence is also used for identification/verification purposes. Afterwards algorithm computes correlation coefficient of fingerprint area, average signal intensity and extension of fingerprint area and decides if the finger is alive or not.

Figure 5: Sequence of fingerprint images illustrating elasticity of skin (picture was taken from [7]).

This method was tested with the help of 15 volunteers (two fingers per each of them) and 47 gelatin fingers. Each finger was tested ten times on Veridicom Fps200 fingerprint

sensor. This method achieved 4.78% EER.

3.4 Electrical properties

Another approach is to use electrical properties for liveness testing purposes. These methods can be based on capacitance, resistance, impedance, conductivity or dielectric constant measurement [19, 13]. Capacitance is normally measured by capacitive fingerprint sensors, but also there was one implementation of this method for optical sensor. In 2001 Sony was selling optical sensor FIU-500 with capacitance measurement [19]. Nowadays this sensor is not in the market and it is not known whether present optical sensors from Sony contain this method or not.

Another discussed property is conductivity of live human skin [13]. However problem is, that conductivity of finger is dependant on the type of skin and it can vary from several kilo Ohm for wet skin (e.g. in summer period) through about 200k Ohm for ordinary skin to several mega Ohm for extremely dry skin (e.g. in freezing winter period). This interval is so large that this method can be hardly used.

Problematic method is also a measurement of relative dielectric constant (RDC). Putte et al. [13] describe a method to fooling RDC measurement. They proposed to prepare dilution of alcohol (90%) and water (10%) and put it on the artificial finger. RDC of finger lies between RDC of water and RDC of alcohol. Because alcohol evaporates more quickly than water, the RDC of dilution goes up until it falls into interval for live human finger.

Mr. Shimamura et al. [17] presented proposal of sensor with liveness testing capability based on impedance sensing. The proposed sensor is based on standard capacitive sensor, but in the middle there is a cross-shaped fraud-detection electrode replacing few fingerprint sensing circuit (see scheme in Fig. 6). Because this electrode is very small (1800 μm x 400 μm), it is not necessary to increase chip size and the quality of captured fingerprint doesn't change too.

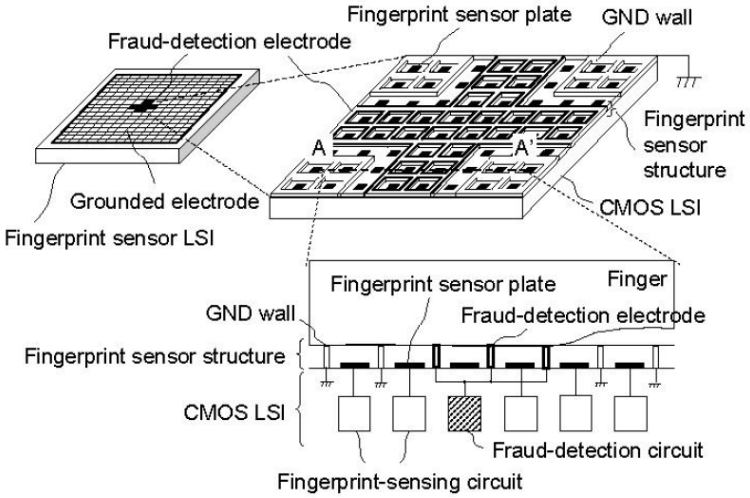

Figure 6: Scheme of electrode and circuit for fraud detection (picture was taken from [17]).

The chip can operate in two modes/phases. In the first phase the fingerprint is captured as by normal capacitive sensor and the fraud-detection circuit is switched off (con-

nection with ground potential). In the second phase the fraud-detection circuit is switched on and detects impedance between the fraud-detection electrode and the GND wall. In this phase all fingerprint sensing circuit are on stand by. Finally the user is identified through the use of information from both phases. The chip was tested through the use of gelatin and silicone artificial fingers and it was able to distinguish between them and live fingers.

Mr. Martinsen et al. [10] from IDEX ASA proposed another method based on impedance measurement. Proposed sensor contains an array of at least 4 electrodes, which are arranged for usage in at least two four-point configurations. By switching between these configurations it is possible to measure characteristics of different layers of live human finger.

3.5 Blood oxygenation

Another property, which can be used for liveness testing purposes, is blood oxygenation. The measurement of blood oxygenation can be for example based on principle of a pulse oximeter, which is nowadays widely-used in hospitals. Its principle is based on Lambert–Beer's law, which claims, that absorption of the light of some wavelength is directly proportional to the concentration of corresponding substance. For detection of saturated and unsaturated hemoglobin, the pulse oximeter use the red (660 nm) and infrared (940 nm) light. The amount of saturated and unsaturated hemoglobin is also periodically changed because of the pulse.

Disadvantage of this method is quite long detection time (about 5 seconds) and possibility to be fooled by very thin artificial finger. Nowadays I don't know about any implementation of this method in fingerprint sensors on the market.

3.6 Pulse

For detection of pulse it is also possible to use the method based on the principle of pulse oximeter, which was described in section 3.5 with the same disadvantages. But in case of pulse measurement the method needs also to deal with big differences in pulse frequency between different people and also between different sessions of one human [13]. Pulse is dependant not only on a health status, but also on an emotional status and previous physical activity (when somebody run up the stairs, he can not have the same pulse frequency as when he slowly came to the sensor).

Dr. Drahansky et al. [3, 4] proposed two different approaches for detection of pulse. The basic idea of these two methods is to measure small volumetric changes caused by pulse. First approach is based on optical principle. CCD camera with macro lens acquires a video sequence of zoomed views of finger. Then it is necessary to find unique points (e.g. minutiae or sweat pores) in all images. These points are further used as reference points. Due to pulse, distance between papillary lines is periodically changing in average with difference of 4.5 μm.

The second approach is based on a laser distance measurement. The laser sensor based on triangulation principle is able to detect very small changes in distance. In case of finger, the change of distance caused by pulse is approximately 6.5 μm. The resultant curve obtained from the laser sensor can be seen in Fig. 7.

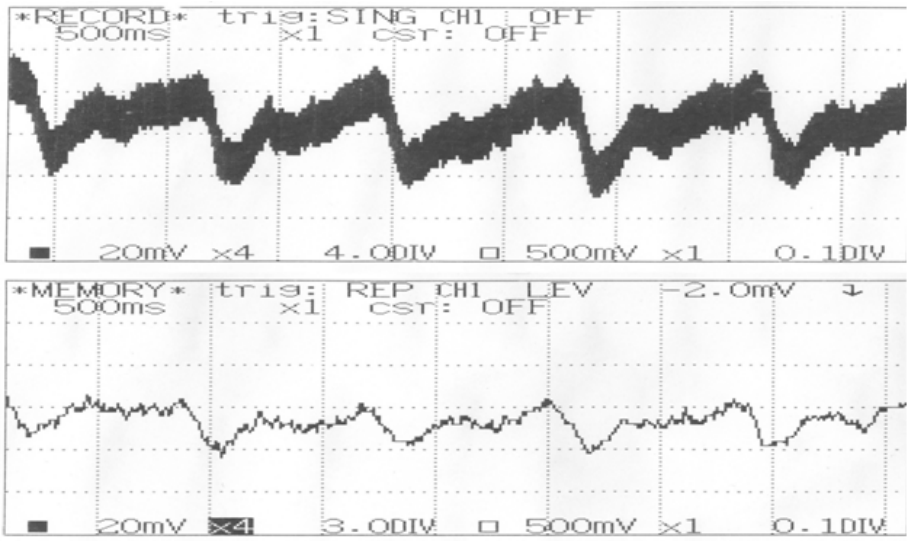

Figure 7: Curve of distance measured by the laser distance sensor (picture was taken from [3]).

3.7 Perspiration

Prof. Schuckers et al. created liveness testing method based on perspiration. This method is based on a measurement of moisture in time (see Fig. 8). First image is captured when the finger is put on the sensor surface. It usually contains a lot of dots, because the sweat is in the neighborhood of sweat pores. After putting the finger, the sweat starts to spread along papillary lines and after few seconds sensor captures the image again. You can see that each image in the Fig. 8 is darker than previous one.

Figure 8: Spreading of sweat along papillary lines (picture was taken from [16]).

However this principle looks easy, the algorithm itself is quite difficult. It begins with an image preprocessing phase because of removing the noise and increasing the quality of image. After that the image is transferred into a signal, which value represents a level of grey in image. When both images are plotted in the same graph (as in Fig. 9), it can be seen the spreading of sweat along papillary lines.

Afterward one static and few dynamic measures are computed. Static measure commutates distances between sweat pores and dynamical are based on computation differences between both captured images. Finally the results from all classifiers are input variables for a neural network, One R method or Discriminant Analysis, which decide if the finger is alive or not.

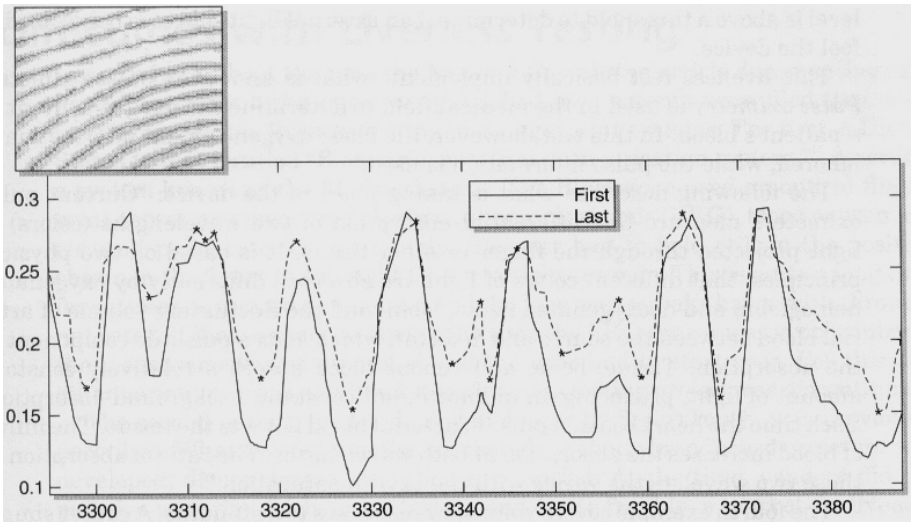

Figure 9: Signals corresponding to the level of grey in papillary lines (picture was taken from [19]).

This method was tested on capacitive (Precise Biometrics), optical (SecuGen) and opto-electric (Ethentica) sensors. The neural network and One R classification was performed using the WEKA software tool and for Discriminant analysis was used SAS tools. The results show approximately 90 percent of successful rate.

Advantage of this method is the purely software implementation and its possible usage for more types of fingerprint sensors. But the disadvantage is quite long time which is necessary for the perspiration process.

3.8 Body odor

Another approach is based on an odor analysis. Baldisserra et al. [1] proposed to use an electronic nose for liveness testing purposes. The electronic nose contains an array of chemical sensors which are able to detect molecules evaporated from tested object. The advantage of these sensors is low size and cost, so the sensors can be easily integrated into various types of fingerprint sensors. However, sensors have to be located carefully so, that the same part of skin, which is sensed for identification/verification purposes, will be also sensed by chemical sensors.

The acquisition of odor sample and decision take usually 10-15 seconds. When there is not any finger pressed on sensor surface, sensors sense the background because of possible environmental changes. The finger has to be pressed few seconds and after it sensor have to restore itself to the initial conditions.

Several odor sensors were tested and the most promising was sensor FIGARO TGS 2600. It was tested by the help of 15 volunteers (2 fingers 10 sessions) and 9 artificial fingerprints made from silicone, latex and gelatin (also 10 sessions). However, there was a problem with gelatin fingers, because the sensor response was similar to the response obtained in presence of human skin, so that the EER was 7.48%.

3.9 Ultrasound

Ultrasonic fingerprint sensors are in different situation (in comparison with other fingerprint sensors technologies). Mr. Bicz from Optel [2] claims that ultrasonic sensors contain inherent liveness detection capability. A signal scattered from finger contains information about various layers of finger (in dependence on the time, when it is received, and on the nature of received wave). The differences between the signal from live finger and the signal from artificial finger can be seen in their amplitude and "character" (e.g. after FFT).

Optel also claims, that its ultrasonic fingerprint sensor is capable to detect pulse (through volumetric changes in the blood vessels) and some biological changes, which are typically associated with level of stress. Results from stress detection can be used as notification on potential security problem.

3.10 Other properties

It exist a lot of properties which was discussed in articles [19, 13] and which can be used for liveness testing by fingers. One of the discussed properties is temperature. Finger temperature is (in normal environment) 8-10 degrees higher than room temperature. This property is also dependant on a health status (e.g. fiber or poor blood circulation), so it will be necessary to have quite wide interval of accepted values. Sensors, which are capable to work outside, should have even bigger interval. However, it is no problem to heat up the artificial finger to the hand temperature. Consequently the temperature itself can not be used as liveness testing method, but it is supposed, that can be used a thermal gradient.

Another discussed property is blood pressure. However all current noninvasive blood pressure measurement methods need to use two different places on the body, which is in the opposite with initial requirements for liveness testing methods. [2]

Some articles noticed also skin exudation (shedding of dead skin cells), but it does not exist any serious study on this topic.

4 Security by obscurity

Nowadays more and more manufacturers include into their sensors liveness testing capability (see Table 1 in appendix A). But in a lot of cases it is almost impossible to figure out on which principle their liveness testing method is based. This situation is often called "Security by obscurity". It means, that the manufacturers thing that they increase security of their solution by hiding its principle. But it is (in most of cases) not correct presumption. If the method is published, a lot of people (scientist, experts etc) can study the principle and also can try to circumvent it. They can find the mistakes which manufacturer overlook and give him the chance to improve this method.

On the other side, when the method is not published, it is wrong to assume, that it is so secret, that nobody (except its authors) know its principle. There is always some way (e.g. poorly secured computer network, blackmailing or corruption) to obtain specific

[2] It is available a sensor which need only one place for measuring, but it has to be entered directly into a vein.

information. In this case, if there is some mistake in this method, it will be known only to exclusive group of people. Such "back doors" can be really big problem especially for high security application.

5 Conclusion

In the first part of this review report I presented basic overview of spoofing methods for various types of fingerprint sensors. In the second part there was described the known, widespread or just remarkable methods for liveness testing. These methods are based on detection of various properties characteristic for live human body/finger. Some of them are software based another need additional hardware. At the end I described another new trend: Security by obscurity.

Nowadays more and more sensors in the market contain liveness testing capability. This is a very good trend because (as has been said before) there exist a lot of very easy sensor spoofing methods. On the other side, these liveness testing methods was tested mostly only by theirs producers. As far as I know, it doesn't exist any serious independent study which would verify their functionality or compare their successful rates with one another.

References

[1] Baldissera, D., et al.: Fake Fingerprint Detection by Odor Analysis. ICB 2006, LNCS 3832. 265–272 (2005)

[2] Bicz, W.: The impossibility Of Faking Optel's Ultrasonic Fingerprint Scanners. Optel. (December 2003)

[3] Drahansky, M., Lodrova, D.: Liveness Detection for Biometric Systems Based on Papillary Lines, Proceedings of Information Security and Assurance, Busan, KR, IEEE CS. 439–444 (2008)

[4] Drahansky, M., et al.: Method and Apparatus for Detecting Biometric Features. International patent WO 2007/036370. (April 2007)

[5] Ennis, M. S., et al.: Multispectral Sensing for High-Performance Fingerprint Biometric Imaging. Lumidigm, Inc.

[6] Gilenko, M., et al.: Method and Device for Recognition of Natural Skin. International patent WO 2002/101668.

[7] Jia, J., et al.: A New Approach to the Fake Finger Detection Based on Skin Elasticity Analysis. ICB 2007, LNCS 4642. 309–318 (2007)

[8] Ligon, A.: An Investigation Into the Vulnerability of the Siemens ID mouse Professional Version 4. Siemens. (September 2002)

[9] Lodrova, D.: Liveness Testing by Fingers. Master thesis. Brno University of Technology, Faculty of Information Technology. (2007)

[10] Martinsen, O. G., et al.: Live Finger Detection by Four-Point Measurement of Complex Impedance. International patent WO 2004/049942. (June 2004)

[11] Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S.: Impact of Artificial "Gummy" Fingers on Fingerprint Systems. Proceedings of SPIE, Vol. 4677, Optical Security and Counterfeit Deterrence Techniques IV, San Jose. 275–289 (February 2002)

[12] Michelin, J.-L.: Optical Measuring Device Using Optical Triangulation. International patent WO 2006/097645. (September 2006)

[13] Putte, T. van der, Keuning, J.: Biometrical Fingerprint Recognition: Don't get your fingers burned. IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications. Kluwer Academic Publishers. 289–303 (2000)

[14] Rowe, R. K.: A Multispectral Sensor for Fingerprint Spoof Detection. Sensors. (January 2005)

[15] Rowe, R. K., Harbour, R. M.: Noninvasive alcohol sensor. US Patent 7,386,152. (June 2008)

[16] Schuckers, S., et al.: Time-Series Detection of Perspiration as a Liveness test in Fingerprint Devices. BC 2004. (September 2004)

[17] Shimamura, T., et al.: A Fingerprint Sensor with Impedance Sensing for Fraud Detection. ISSCC 2008. (2008)

[18] Thalheim, L., Krissler, J., Ziegler P.-M.: Body Check, Biometric Access Protection Devices and their Programs Put to the Test in c't magazine. 114 (2002)

[19] Valencia, V. S., Horn, Ch.: Biometric Liveness Testing. Biometrics. 139–149 (2003)

[20] Wei-Yun, Y., et al.: Fake Finger Detection by Finger Color Change Analysis. ICB 2007, LNCS 4642. 888–896 (2007)

A Sensors

Table 1: Sensors with liveness testing capability. The question mark means, that this company did not publish principle of their liveness testing solution.

Producer	Tested property	Sensors
Lumidigm	LightPrint™(spectral)	J110, Venus series
Optel	(ultrasound)	
Sagem	(optronic ?[1])	MA521, MSO201, 301, 351, etc
Dermalog	(?[2])	ZF1
TST Biometrics	(optical ?[3])	BiRD 3
Upek	(?)	TCS5
AuthenTec	TrueFinger™(?[4])	EntrePad 1610
Sony	(capacitance)	FIU-500[5]

[1]Sagem's sensors contain patented optronic technology. This method is probably described in [12] in French. In English abstract there is written, that this method is based on optical triangulation measuring and it uses two light beans with different wavelengths along the same path.

[2]Dermalog claims that its liveness testing method is based on analysis of variety typical finger characteristic.

[3]TST Biometrics' sensor contains patented technology. This technology is probably described in [6] in German. In abstract there is written, that this method is based on illumination of skin at an irradiation point and on detection of scattered light.

[4]AuthenTec claims that its sensor dynamically measures the properties of the skin during scanning process.

[5]Sensor Sony FIU-500 was in the market approximately in year 2001.