Liveness Detection for Biometric Systems Based on Papillary Lines

Martin Drahansky, Dana Lodrova
Brno University of Technology, Faculty of Information Technology
drahan@fit.vutbr.cz, ilodrova@fit.vutbr.cz

Abstract

This paper deals with an add-on for biometric security systems, especially for the fingerprint recognition technology. This added part of such systems is the liveness detection. Our method is based on detection of optical characteristics of the finger surface (skin). The main idea is to detect the movements of papillary lines, but some another optical information could be extracted, what is outlined at the end.

1. Introduction

Fingerprints belong to one of the most widely used biometric characteristics and have been generally accepted in forensics for more than hundred years. Fingerprints are utilized presently in a large number of automated recognition systems for person identification and verification. Another frequently used biometric characteristic is hand geometry. Both, the fingerprints and hand geometry methods use hand as a biometric attribute.

Securing of the automated and unsupervised fingerprint recognition systems used for access control is one of the most critical and most challenging tasks in real word scenarios. Basic threats for a biometric security system are: repudiation, coercion, contamination and circumvention [3].

A variety of methods can be used to get unauthorized access to a system based on 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 paper copy, soft silicon, gummy, plastic material or similar substances [1][2][4]. The fingerprint of a person enrolled into a database is easy to acquire, even without the user's cooperation. Latent fingerprints on daily-use products or sensors of the access control system itself could be used as templates.

To discourage potential attackers from presenting a fake finger or, even worse, to force a legitimate user of the system to present his finger, or even to hurt a person to gain access, the system must be augmented by a liveness detection system: to prevent false acceptance we have to recognize whether the finger on the plate of the fingerprint sensor is alive or not.

This paper is organized as follows. In the second chapter we give a short overview of common methods used for the liveness detection in the finger- or hand-based technologies. In the third chapter we present a method of the liveness detection based on tracing of papillary line movements on a fingertip surface. In the fourth chapter, there is an outline of a new liveness detection method, on which we are working now.

2. Overview of Known Methods

For the purposes of the liveness detection, one or more characteristic properties of the living human body can be used. It is important to detect liveness of the part of the body which is being captured by a sensor. It is nonsense to test e.g. a pupil dilatation by the fingerprint sen-

sors – apparently, an impostor with an artificial finger would pass such system as well as a common user.

There are two requirements to be fulfilled to make the liveness detection system working safe. First, the liveness detection and the fingerprint scan have to be performed at the same time. If this requirement is not fulfilled, it is easy to deceive the sensor. E.g. an impostor knows that the system tests the liveness first and scans the fingerprint after. The impostor knows that he can put his real (and most probably alive) finger on the sensing area during the phase of the liveness detection and then he can replace his own finger by the artificial one before the scan of the fingerprint is performed (this presumes a good knowledge of the system, of course). Second, the method of the liveness detection itself must not influence the fingerprint scan and vice versa.

For the liveness detection, it is necessary to choose a property which is difficult or impossible to imitate. The chosen liveness detection method should be easy to implement either as a hardware or software solution, so that the final price of such security solution would be not too high. It is important to find an appropriate compromise among price, user-friendliness and security of the liveness detection solution.

Human body offers a vast amount of various characteristic properties, but not all of them comply with foregoing requirements and not all of them can be used with the fingerprint technology. The properties usable for the liveness detection systems can be split into three categories [5][6]: intrinsic properties, involuntarily generated signals and responses to a stimulus.

2.1 Intrinsic Properties

The intrinsic properties are based on characteristics of the living human tissue. In case of the fingerprint technology we can use e.g. properties of various skin layers or body fluids.

One of the possibilities of utilization of the intrinsic properties is analysis of the spectral characteristics (e.g. used in sensors made by Lumidigm, Inc.). The spectral characteristics of the skin are absorbance, transmittance and reflectance of the electromagnetic radiation of different wavelengths, which penetrate the skin surface to a different depth. Hence, electromagnetic waves of various lengths are reflected and absorbed in a different way. The spectral characteristics are unique for a variety of substances; they can even distinguish between alive and lifeless parts of body. The sensor made by Lumidigm Inc. illuminates finger by LEDs with wavelengths ranging from the blue light and finishing up on the red or infrared light. The wavelengths are carefully chosen to correspond with the individual parts of the living body (e.g. melanin, collagen, hemoglobin etc.).

The spectral characteristics can be measured by the ultrasonic sensors too. In this case, reflectance of the ultrasonic waves is measured. Amplitude and character of the reflected wave is unique, so we can distinguish between a living finger and other substances.

Other properties possible to use for the purposes of the liveness detection can be obtained from the body fluids. E.g. we can measure the blood oxygenation, which is based on a pulse oximetry and requires hardware with two light sources: red (660 nm) and infrared (940 nm) light. The amount of the absorbed light corresponds to the concentration of the oxygenated and deoxygenated hemoglobin. The advantage of this method inheres in its origin in the well known principle of pulse oximetry, which is especially used in medicine. One of the disadvantages is a long time of the scan. This method can be cheated by a very thin artificial fin-

gerprint too. The sensor could fail to notice the fake and the impostor could be accepted, since his own finger behind the artificial one was (properly) detected as living.

Another way is usage of the electrical properties of the living human skin, i.e. its conductance or dielectric constant. The living human skin has its unique electrical characteristics, so we can use it to distinguish from other substances. For a hardware implementation, it is necessary to join a system of electrodes and an evaluation unit to the sensor. Disadvantage of such methods is dependence on the ambient conditions, on moisture in the first place. The consequence of the dependence is a wide range of accepted values, which can be easily abuse. In case of liveness detection based on the dielectric constant measurement is sufficient to dip the artificial fingerprint into the 90% alcohol dilution. The alcohol is evaporating faster than water and dielectric constant is moving slowly into the range of accepted values.

For liveness detection, physical or visual properties can be used too. In this category we can include e.g. density, elasticity or color of skin. However, it is nonsense to test only the color of skin itself, because, at present, it is easy to make an artificial finger which looks exactly like a real one.

2.2 Involuntarily Generated Signals

Involuntarily generated signals are spontaneously and uncontrollably generated by a living human body.

The best known involuntarily generated signal is a pulse. One of the approaches to measure pulse is based on the pulse oximetry (see above); another one is based on fine movements of the skin (this method is described in Chapter 3). The pulsation differs from person to person and it is even not same for one person in various times. It strongly depends on emotional state and previous activity of the person being measured (such as physical activity). The normal pulse rate ranges between 60 and 90 heart beats per minute. The maximum pulse rate lies between 200 and 220 heart beats per minute. The disadvantage of these methods is, similarly to the disadvantage of the pulse oximetry, possibility of omission of a very thin artificial fingerprint attached on the real finger. In this case the method detects the heart rate of a real finger behind the artificial one.

Figure 1. Perspiration: change of captured fingerprint in time [7].

Other well known method is based on perspiration. This method is developed by Biomedical Signal Analysis Laboratory. When user's finger is put on the sensing area it is relatively dry, which results in a pale captured image. The finger is perspiring and the sweat is distributed along the ridges into the originally dry areas, hence the captured image becomes darker during some time. This process is clearly illustrated in Fig. 1.

Another involuntarily generated signal is for instance the temperature. It is quite easy to measure it, but not sufficient to detect liveness. Average temperature on fingertips ranges between 26°C and 30°C. However, the temperature depends on the health condition of the user (fever or poor blood circulation could influence the result of the liveness detection). This could make an impostor with a thin artificial fingerprint attached on his real finger be accepted and, on the other hand, a user with poor blood circulation or cold rejected, which is undesired behavior.

To the involuntarily generated signals can be included some exotic properties like shedding of dead skin cells or a body odor as well. However, those can not be easily used for the purposes of the liveness detection.

2.2 Responses to a Stimulus

In this category belong responses to a tactile stimulus given within the sensing area. A visual or an auditory response/stimulus has no sense to use in case of the finger liveness detection, because the stimulus has to be given within the sensing area.

First two possibilities are the witting responses, e.g. the sensing area is cooled down or warmed up and the user is asked to push a red button if the sensing area is warm or a blue button if the area is cold. However, in such scenario, the impostor can press the right button with a probability of 50%, which makes this solution inconvenient.

Another possibility is to detect an involuntary response. The temperature stimulus can be used again. Increased temperature causes enlargement of peripheral blood vessels, which can be measured as increasing amplitude of the blood flow. The response to decreasing temperature is reverse. The living human skin responds very sensitively to the temperature deviations. Knowing this, it is possible to design the sensor so that his temperature changes very slightly. The temperature alternation becomes undetectable for the user, but still measurable for the sensor due to the sensitivity of the skin.

3. Detection of Fine Movements

One of the proposed solutions is based on the analysis of fine movements of the papillary lines of the fingertips and on measurements of the distance of the fingertip surface to a laser sensor, respectively. The system is compact enough to be integrated with the optical fingerprint sensors.

One advantage of the implementation is that the finger is not required to have contact with the measuring device. Moreover, the costs of production of such implementation are low. This is of particular importance, as in most cases liveness detection will be an add-on that augments already existing robust and field-tested fingerprint scanners.

3.1. Measurement principle

There are two approaches to measure fine movements of papillary lines [1], both based on optical principles. The first solution is based on a close-up view of the fingertip acquired with a CCD camera; the second one is the distance measurement with a laser sensor.

The camera solution scheme is outlined in Fig. 2. The main idea is that a small aperture (approximately 6 mm) is created in the middle of a glass plate with mirror below the plate. The mirror has a permeable and an impermeable mode of operation. 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 camera. Next, for liveness detection the mirror is made impermeable and the part of the fingertip placed on the aperture is mirrored to the right and projected on the CCD camera by a macro lens. To acquire the whole fingerprint in the first step, we only need a single scan. The complete fingerprint can be used for fingerprint recognition. Next, we acquire a video sequence for liveness detection analysis. There is no need to scan the fingerprint in the acquirement phase – the hand could be scanned in place of a finger, but the zoomed view of fingerprint has to be acquired.

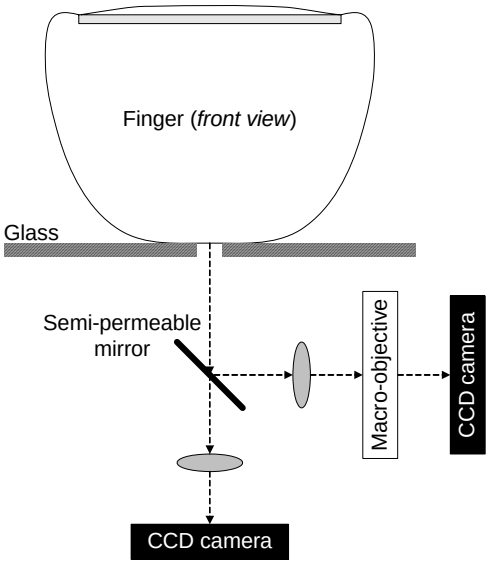

Figure 2. Liveness detection with CCD camera.

3.1.1. Camera system: An important aspect of the camera based liveness detection is analysis of the video stream. First of all, single frames of the video sequence are processed to find unique points (e.g. minutiae, sweat pores), which can be used as reference points to identify a region of the fingerprint that will be further analyzed.

Human's heartbeat causes small volumetric changes on the fingertip (these changes occur also in other areas of the hand). As the fingertip expands, the distance between the papillary lines grows (Fig. 3). These fluctuations are small, but measurable and show similarities to a cardiogram. The video stream (or the sequence of images) is analyzed and filtered so that these movements can be observed. Cheating this method by applying a silicon layer (or another attack method) on the finger should change these characteristics considerably, so that such attack can be easily detected.

Average volume changes of the fingertip (as measured by a laser range-meter) are 6.5 μm in the volume radius. According to the measured volume changes, the papillary lines move in average with a difference of 4.5 μm.

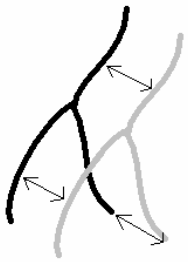

Figure3. Illustration of the movement of papillary lines.

The fingerprint (or the image respectively) must be zoomed so that the movements become detectable. Preliminary tests have been performed, but due to the low quality of the optics, the results are still ambiguous and the research is still going on.

The sequence of images captured by the camera has to be processed by various filters and edge detectors (e.g. Gaussian filter, Sobel and Laplace edge detector etc.) as you can see in Fig. 5. The edge detection algorithms sharpen the papillary lines and the Gaussian filter eliminates background noise and other unnecessary image information. The algorithms are demanding on computational resources and improvements in this area are a necessity. This technique still has to be further developed, but is promising. 4× zoom rate does not allow to detect enough distinct movement. Hence, a higher zoom rate must be used. 8× zoomed images significantly improve the detection and seem to be sufficient for this task.

Next step in the detection process is locating of the reference points on the fingerprint (e.g. minutiae, sweat pores). The reference points must be unique. These points serve the purposes of the papillary line identification and are necessary for the detection of the movements of the papillary lines on the fingertip.

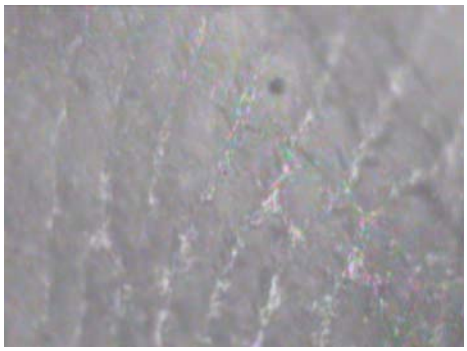

Figure 4. An example of a zoomed fingertip image (4×).

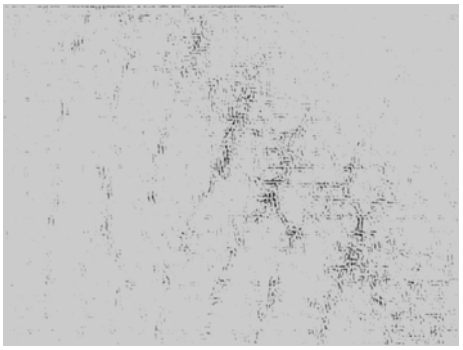

Figure 5. Image processed by the filters and edge detectors.

3.1.2. Laser system: The second optical method for liveness detection is a laser distance measurement, which is outlined in Fig. 6. The lens optical system and the CCD camera for acquisition of the complete fingerprint are the same as in Fig. 2. In contrast to the solution shown in Fig. 2 the laser distance measurement module, based on the triangulation principle, is placed to the right side of the glass plate, which is L-shaped here. The user places his finger such that it is in contact with the horizontal and the vertical side of the glass plate.

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 [1], 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 some μm). If the finger (the same for hand recognition) is positioned tight, i.e. jitter of the hand cannot influence the measurement (finger fixation), we obtain a measurement curve which is similar to the curve shown in Fig. 7.

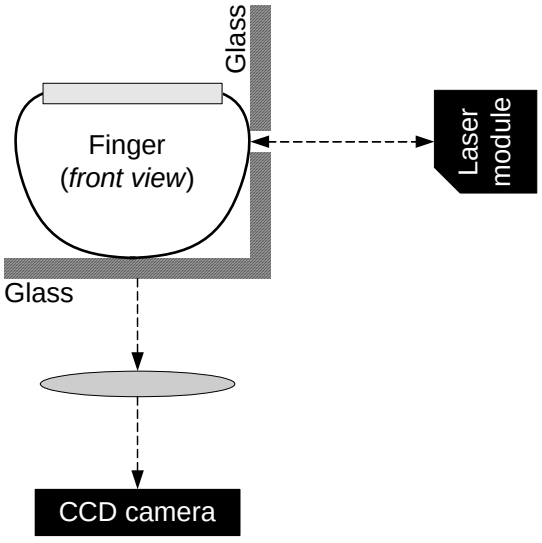

Figure 6. Laser distance measurement for liveness detection.

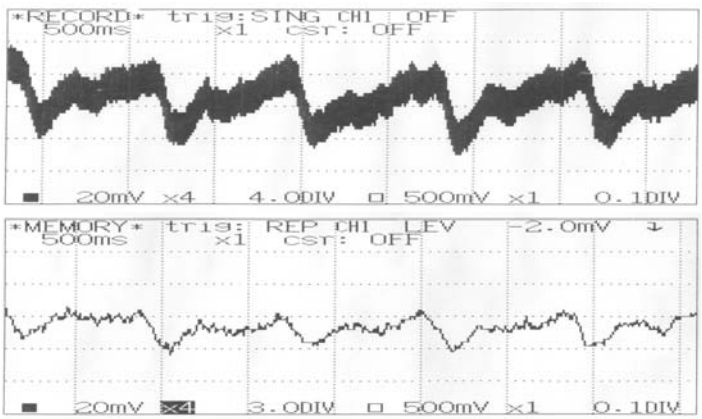

Figure 7. Distance measurement curves from triangulation laser sensor [1].

4. Future work

Our goal for the near future is to optimize the process of the laser module, so that we could create a first prototype of a device for fingerprint verification with integrated liveness detection.

There are other liveness detection methods based on optical principles like ours. Those are registered and described in the following patents:

- US Patent 5,088,817 (February 1992)
- US Patent 6,292,576 (September 2001)

These methods are also based on the optical principle. However, we found new characteristics of the fingertip, which we use for the purposes of the liveness detection and which differentiate from the methods described in the aforementioned patents.

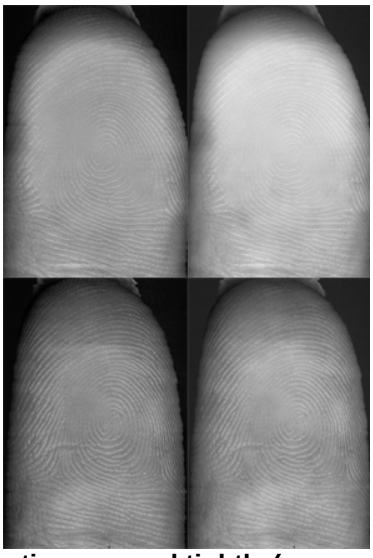

Figure 8. Images of the fingertips pressed tightly (upper row) and slightly (lower row) to the sensor.

In the Fig. 8 there are images of the fingerprints scanned in two various situations. In the upper row, there are images of the fingerprints of the fingertips pressed strongly to the surface of the scanner, whereas in the lower row, the fingertips were pressed slightly to the surface of the scanner. We found a way to detect liveness based on the pressure of the fingertip on the surface of the scanner. The patents mentioned before treat with the pressure of the fingertip too, in a different way, however. This liveness detection method is in the application process for a utility model by the Czech patent agency now.

Work on the new method based on the optical characteristics of the fingertip will continue and we shall finish the second prototype of such device in the near future.

References

[1] M. Drahansky, W. Funk, R. Nötzel, "Liveness Detection based on Fine Movements of the Fingertip Surface", Proceedings of IAW'06, IEEE, New York, USA, 2006, p. 19-21, ISBN 1-4244-0130-5.
[2] T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, "Impact of Artificial "Gummy" Fingers on Fingerprint Systems", Proceedings of SPIE, vol. 4677, SPIE, San Jose, USA, 2002, pp. 275-289.
[3] A. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, Handbook of Fingerprint Recognition, Springer, New York, 2003, ISBN 0-387-95431-7.
[4] T. Putte, J. Keuning, "Biometrical Fingerprint Recognition: Don't Get Your Finger Burned", Proceedings of 4th Working Conference on Smart Card Research and Advanced Applications, ACM, Bristol, UK, 2002, pp. 289-303, ISBN 0-7923-7953-5.
[5] V.S. Valencia, C. Horn, "Biometric Liveness Testing", Biometrics, LNCS, 2003, pp. 139-149, ISSN 1611-3349.
[6] M. Kluz, "Liveness Testing in Biometric Systems", Master thesis, Brno, Masaryk University, Faculty of Informatics, Brno, CZ, 2005, p. 57.
[7] S. Shuckers, L. Hornak, T. Norman, R. Derakhshani, S. Parthnasardi, "Issues for Liveness Detection in Biometrics", CEMR LDCSEE, West Virginia University, USA, 2006, p. 25.

Authors

Martin Drahansky graduated in 2001 at the Brno University of Technology, Faculty of Electrotechnics and Computer Science in Czech Republic and simultaneously at the FernUniversität in Hagen, Faculty of Electrotechnics, Germany. He achieved his Ph.D. grade in 2005 at the Brno University of Technology, Faculty of Information Technology in Czech Republic. Now he works as assistant professor at the Brno University of Technology, Faculty of Information Technology, Department of Intelligent Systems. His research topics include biometrics, security and cryptography, artificial intelligence and sensoric systems. For more information – see please http://www.fit.vutbr.cz/~drahan/.

Dana Lodrova graduated in 2007 at the Brno University of Technology, Faculty of Information Technology, Czech Republic. She is a Ph.D. student at the Brno University of Technology, Faculty of Information Technology at the moment. Her scientific orientation includes especially biometrics, intelligent systems and artificial technology. For more information – see please http://www.fit.vutbr.cz/~ilodrova/.