Available online at www.sciencedirect.com

ScienceDirect

Procedia Engineering 100 (2015) 169 – 176

Procedia Engineering

www.elsevier.com/locate/procedia

25th DAAAM International Symposium on Intelligent Manufacturing and Automation, DAAAM 2014

Security of Biometric Systems

Milan Adámek*, Miroslav Matýsek, Petr Neumann

Faculty of AppliedInformatics, Tomas Bata University in Zlin, Czech Republic

Abstract

There are many ways how to identify people and to provide their authorization of access to a specific area. This article describes the reliability of biometric systems that are commonly used to identify of people. The article aims to highlight the ways in which to disturb the security of biometric systems. There are describes techniques that can impair the reliability of equipment for fingerprinting. To test the reliability of the fingerprint was made series of measurements; the results are presented in the article.

Peer-review under responsibility of DAAAM International Vienna

Keywords: Fingerprint sensor; biometric systems; reliability; attack; fake fingerprint

1. Introduction

Currently growing demand to increase the safety of not only persons, objects and data, but also the reliability of the identification of persons. Traditional identification technologies (check identity documents, standard access systems based on subject or password authentication) are now at their limits. To increase the reliability of the identification of the person contributes biometric identification. Biometric identification is understood as a discipline that is interested in describing and measuring of anatomical - physiological features and behavioral traits. Commonly used methods of biometric systems include identification of fingerprint, palm, face, iris of the eye. Commonly used methods of biometrics include fingerprint identification, palm, face, iris of the eye.

* Corresponding author. Tel.: +420576035220; fax: +420576035555.
E-mail address: adamek@fai.utb.cz

Peer-review under responsibility of DAAAM International Vienna
doi:10.1016/j.proeng.2015.01.355

Typical areas where biometric identifications are used include:

- Criminology
- Tourism (Customs clearance and passport control)
- Control of movement of persons, counter-terrorism measures, monitoring the crowds
- Attendance and access systems
- Data protection, PC and other data sources
- Electronic banking, online payment transactions and more [1].

The general structure of a biometric identification system is shown in Fig. 1.

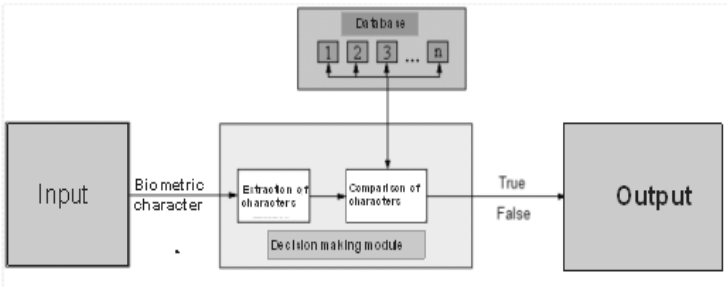

Fig. 1. Structure of a biometric identification system [2].

The basic component of a biometric identification system is a sensing module that ensures scanning of biometric characters. The major part is the decision-making module that compares the biometric features defined in the database. The output of the biometric identification system is the communication interface or lock allowing access to the space provided.

2. Access control systems using fingerprints

A fingerprinting is one of the best known biometric identification method. Usually the fingerprints are used in criminology, now they are widely used in commercial security. This method is based on the identification of the friction ridges of fingers (papillary lines). There are three basic patterns of classification of papillary lines, which are shown in Fig. 2.

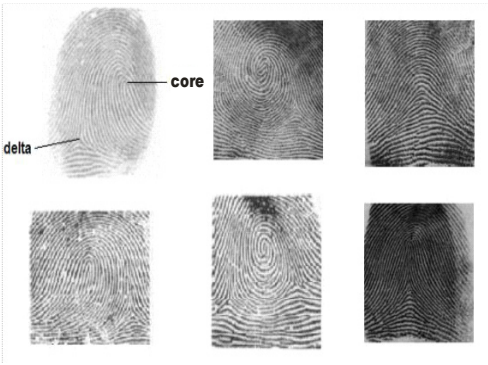

Fig. 2. Basic patterns (from left loop, swirl, arch) [2].

1. Loop - papillary lines are in the shape of a loop. The loop is approximately 65% of all fingerprints
2. Beliefs – papillary lines are in the shape of a circle, an oval, a spiral with a core. The vortex forms are approximately 25% of all fingerprints
3. Arch - papillary lines are in form of simple arcs. It is minimum number of occurrences - approximately 5-10% of occurrence.

Besides the basic shapes of papillary lines the interruption or termination of the papillary lines is used in the dactyloscopy approach. These marks are called minutiae. They can be in this form: starting / ending line, point, eye, hook, bridge crossings, forks, broken lines, side suspension, termination, etc.

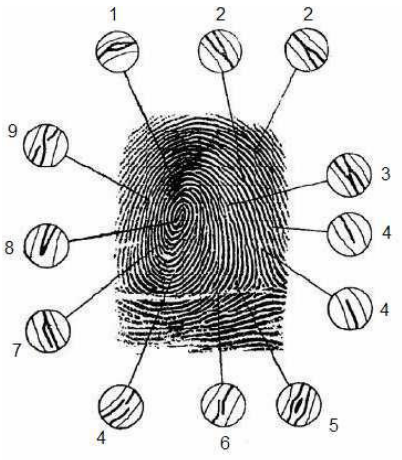

Fig. 3. Examples of minutiae.
(1 eye, 2 forks, 3 bridge, 4 starting / ending line, 5 point, 6 side break, 7 hook, 8 termination, 9 crossings) [1]

3. Principles of fingerprint sensors

3.1. Optical fingerprint sensor

The optical fingerprint sensors are based on reflectance or transmittance of light. These sensors use a different reflection of light from the ridge lines and the space between these lines. Reflected light is evaluated through a CCD or CMOS sensor.

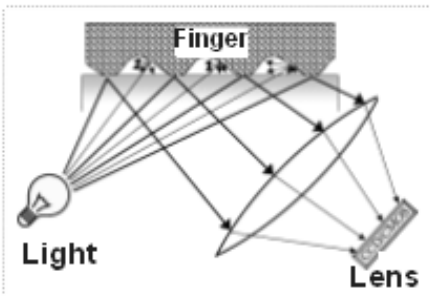

Fig. 4. The optical sensor on the principle of reflections [2].

An optical sensor using light transmission is based on the backlight finger from the upper part (from the nail) and on recording the image sensor on the opposite side.

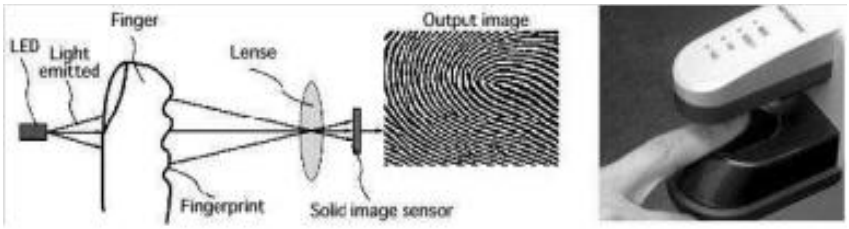

Fig. 5. Optical sensor based on a scanning transmission [3].

3.2. Capacitive fingerprint sensor

The principle of this sensor is based on measuring differences in capacity between the sensor plate and finger. Sensing area is equipped with a large number of sensor microelectrodes to evaluate the difference capacity between the peak and recesses in the finger.

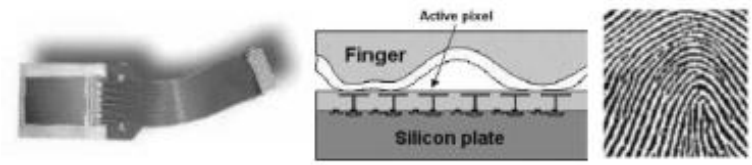

Fig. 6. The principle of the capacitor sensor [3].

3.3. Thermal fingerprint reader

Thermal fingerprint scanners use a small pyrodetector as a heat-sensitive element. The principle of this technology is based on measuring the temperature difference between the peak and valleys in papillary lines in the finger.

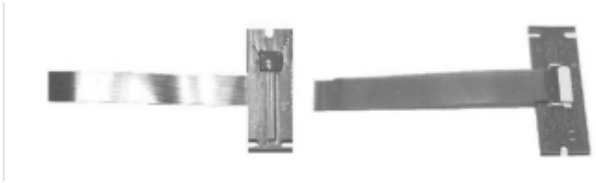

Fig. 7. The principle of the thermal sensor [4].

3.4. Ultrasonic fingerprint reader

For this sensor an ultrasonic signal is transmitted from the transmitter to the fingerprint. There are captured the reflected and deformed waves by rotating transmitter or receiver. There are evaluated farther and flatter the line.

Fig. 8. The ultrasonic reader [3]

4. Testing the reliability of fingerprint sensors

To test the reliability of fingerprint sensors two basic functions are used. The first function called FAR is a rate of false accepted reads. This function can be defined by:

$$FRR = \frac{N_{FR}}{N_{EIA(EVA)}} \cdot 100[\%] \quad (1)$$

where:

NFR - the number of false rejection

NEIA - number of attempts to identify the beneficiaries

NEVA - number of beneficiaries of all attempts to verify.

The second function FRR is a rate of false rejected reads. This function can be defined by:

$$FRR = \frac{N_{FA}}{N_{IIA(IVA)}} \cdot 100[\% \quad (2)$$

where:

NFA - the number of unauthorized adoption

NIIA - number of attempts by unauthorized persons to identify

NIVA - number of attempts by unauthorized persons for verification.

The relationship between FRR and FAR is shown in the picture below.

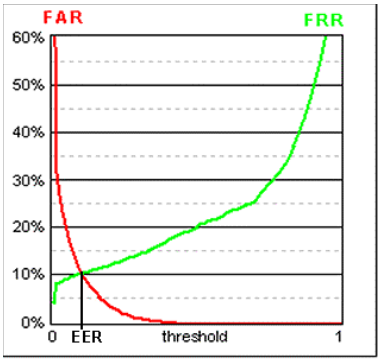

Fig. 9. The relationship between FRR and FAR [3].

Point EER - Equal Error Rate represents the point at which FAR and FRR have same value. This crossing is a good measure of overall performance of biometric devices. Smaller means better EER performance of a biometric device.

5. The attack of biometric identification systems

Generally, there are several possible of attack of identification systems. The whole system is so "safe" as resistant is its weakest part. An attack of identification systems can be divided into three groups:

- attack of system input
- attack of evaluation system
- attack of challenge decisions - output parts.

The following figure summarizes the possible points of attack.

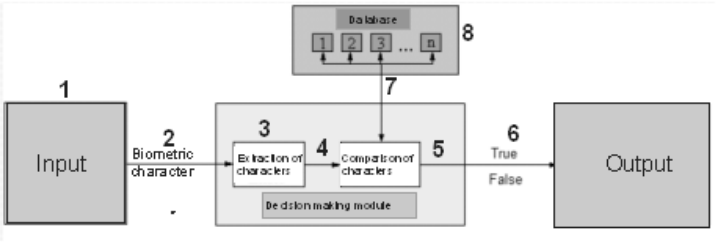

Fig. 10. The infection of a biometric identification system [5].

From Fig.10 it is clear that the attack of identification system can be made at least in 8 places:

1. Using a fake biometric characteristics
2. Attack on the transmission channel between the sensor and evaluation system
3. Disruption of searching of characters.
4. Disruption of transmission of characters.
5. Disruption of comparing of characters.
6. Distortion of the output system.
7. Shutdown, disruption, diversion routes of communication with the database reference templates.
8. Replacement of the template in the database.

6. Method of making of false fingerprint

For the production of false fingerprint can be used two approaches:

1. Fake fingerprint can be created directly in the mass. To create of a fake fingerprint there can be used several materials with regard to preservation of papillary lines, including their characters. For production granulated plastic be can used, this material is malleable after warming up. A similar properties has a plastic material. The original fingerprint is pressed into plastic material, by this way can be made the template of fake fingerprint. The template of fake fingerprint is filled with materials such as gelatin, silicone or plastic.

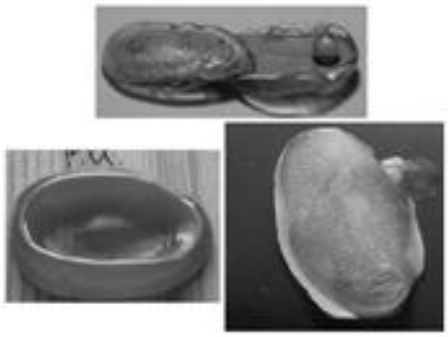

Fig. 11. Plastic finger prints (gelatin, silicone, plastic mold) [3].

2. A false impression created by the secured latent. For the production of a fingerprint is a latent need to

highlight and take pictures, scan. The resulting image is inverted to trim and two shades of black and white, enhanced image transfer material designed to create a form. You can use screen printing of plastic material or rubber stamps to create, etc.

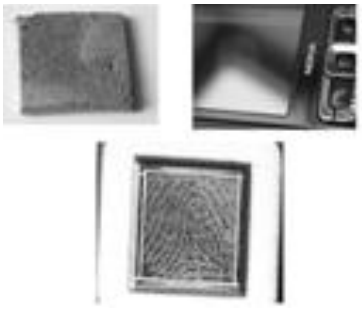

Fig. 12. Fake fingerprint, a latent fingerprint on mobile phone [2].

Both procedures can create relatively high-quality fingerprints but they have not a long shelf life. They can´t be used with scanners that use control vibrancy. For example, gelatin or silicone can´t be applied to all touch sensors because some methods do not meet the properties of these materials remain close to the properties of human skin, etc.

7. Testing of the reliability of fingerprint sensors with the use of fake fingerprints.

Through the false fingerprints the immunity of fingerprint sensors was measured. For testing of the false fingerprints was used capacitive fingerprint sensor. Fake fingerprints were made from a stamp rubber and a plastic.

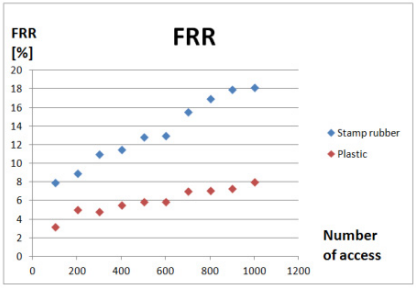

Fig. 13. FRR of capacitive fingerprint sensor: the fake fingerprint made from stamp rubber.

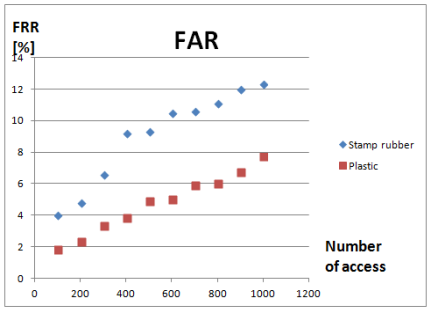

Fig. 14. FRR of capacitive fingerprint sensor: the fake fingerprint made from plastic.

Conclusion

The aim of the paper was to show that access systems using fingerprints can be a relatively simple way to break through. This paper describes the methods you can use to create a "fake" fingerprint. To create these fake fingerprints can use a plastic or rubber material. In order to increase safety it is necessary to amend system access. Most hotkey can be used with other biometric systems, e.g. scanner face.

Acknowledgement

The work was performed with financial support of research project NPU I No. MSMT-7778/2014 by the Ministry of Education of the Czech Republic, by the European Regional Development Fund under the Project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089, and by the European Social Fund under the project No. CZ.1.07/2.3.00/30.0035.

References

[1] O. Bitto, Encryption and biometrics: or arcane bits and touches.: Computer Media, 2005. ISBN 80-86686-48-5.
[2] R. Rak, Biometrics and identity of people: the forensic and commercial applications, BEN, Prague, 2008. ISBN 978-80-247-2365-5.
[3]Fingerprint structure imaging based on an ultrasound camera [online]. 2012 [cit. 2012-06-23]. <http://www.optel.pl/article/english/article.htm>.
[4] T. Coufal, What is FingerChip [online]. 2007 [cit. 2012-04-29]. <http://hw.cz/teorie-praxe/art2020-co-je-fingerchip.html>.
[5] Nobility Series FP2 Flash [online]. c2007 [cit. 202-05-03].
<http://www.adata.com.tw/en/product_show.php?ProductNo=AFP2ZZZWH>.
[6] D. Ševčík, M. Adámek, L Juříková: A mindreader system for improved security in crowded areas. In Annals of DAAAM for 2011 & Proceedings of the 22nd International DAAAM Symposium "Intelligent Manufacturing & Automation: Power of Knowledge and Creativity". Vienna : DAAAM International Vienna, 2011, s. 1455-156. ISBN 978-3-901509-83-4.