Vulnerabilities of Biometric Systems

Martin Drahanský

drahan@fit.vutbr.cz

Ondřej Kanich

ikanich@fit.vutbr.cz

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

Abstract

This article is focused on three vulnerabilities of biometric systems at a sensor level, presented on an example of fingerprint recognition. The first part is oriented on human diseases influencing the quality (and generally possibility) of acquired fingerprint. The second part introduces various other factors having an influence to the process of fingerprint acquisition. The last part is devoted to production of finger(print) fakes and herewith attacking the biometric systems in a spoof-use-way.

Keywords: biometrics, vulnerability, disease, influencing factor, spoof.

1 Introduction

Everybody knows and uses biometric systems not each day, but from sometimes to very often or daily. The most of us are in possession of biometric e-passports, where our biometric data (templates generated from samples of our fingerprint and eye iris; face is stored as image) is stored. When we read the popular or scientific articles (neglecting datasheets of products) about biometric systems, we can get the impression that all of these systems work properly with some exceptional troubles, which influence the error statistics. The reality is a little bit different. It is not necessary to consider an unexperienced user, who tries to work with a new biometric system – the results are not good at the beginning, because many factors play an important role and the user has to learn these. But we can speak about another phenomenon, maybe two phenomena strongly decreasing the quality of acquired biometric samples – (i) human diseases attacking concrete biometric characteristics; (ii) surrounding environment influencing the technology acquiring any concrete biometric characteristic. In the first case we have to consider various human diseases, which influence the concrete biometric characteristic and could change such properties that are relevant for feature extraction (generally recognition of the person). In the scope of the article, some of these diseases will be discussed. Furthermore, the surrounding environment influences the scanning technology, i.e.

sometimes it is not possible to acquire a good quality sample – the following processing of this sample fails. Some of concrete surrounding influences will be discussed. A short introduction into possible attacks on biometric systems using spoofing methods will be discussed as well. The reason is that any liveness detection method has contrary properties to the methods decreasing the influence of diseases and surrounding environment to biometric sample processing.

2 Skin Diseases on Fingertips

Skin diseases represent very important, but often neglected factor of the fingerprint acquirement. It is not possible to say in general how many people suffer from skin diseases, because there are so many various skin diseases [6][7]. In a general medical practice about 20-25 % of patients with skin complaints are referred. When discussing whether the fingerprint recognition technology is a perfect solution capable to resolve all our security problems, we should always keep in mind those potential users who suffer from some skin disease.

The situation after successful recovery of a potential user from such skin diseases is, however, very important for the possible further use of fingerprint recognition devices. If the disease has attacked and destroyed the structure of papillary lines in the epidermis and underlying dermis (so called dermoepidermal junction – connection of the top two layers of the skin), the papillary lines will not grow in the same form as before (if at all) and therefore this user could be restricted in his future life by being excluded from the use of fingerprint recognition systems, though his fingers do not have any symptoms of the skin disease anymore.

Skin is constantly being regenerated. A keratinocyte („skin cell") starts its life at the lower layer of epidermis (the basal layer), which is nourished by blood vessels and is supplied with nerve endings from dermis. The cell migrates upward from basal layer to stratum corneum (the outermost skin layer). During four weeks the cell undergoes a series of changes, gradually flattening out and moving toward the surface. Then it dies and is shed. This physiological process can be negatively affected in many diseases of the skin. The epidermis is not supplied with blood vessels, but has nerve endings. The shape of dermoepidermal junction basically forms the structure of papillary lines.

In the most cases of dermatological disorders we find a lot of changes in the ultrastructure of the skin, including epidermis and dermis. There is often inflammation (inflammatory cells), atrophy or hypertrophy, fibrotisation and many other changes visible in the microscope. These differences result in changes of color (optical characteristics), changes of dermal vessels and capillaries (blood perfusion), changes of elasticity and thickness of the skin (optical characteristics after pressure change).

The first group represent **diseases causing histopathological changes of epidermis and dermis** – these diseases usually cause problems for all kinds of fingerprint scanners, because they can influence either color or internal structure of the skin. The most common representatives of this group are [6][7]: *Hand and fingertip eczema*, *Dyshidrosis*, *Tinea*, *Pyoderma*, *Pitted keratolysis*, *Pyogenic granuloma*, *Systemic sclerosis* or *Raynaud's phenomenon*.

The second group represent **diseases causing skin discoloration** – these diseases may cause problems for optical fingerprint scanners and also for scanners which use a fingerprint anti-spoof detection check based on the color or spectral analysis of the human skin. Typical representatives are [6][7]: Macular drug eruptions and rashes in infectious diseases (*Hand, foot and mouth disease*, *Scarlet fever*, *Secondary syphilis*, *Kawasaki's disease*), *Pitted keratolysis*, *Raynaud's phenomenon*, *Xanthomas*, *Carotenosis* or *Hereditary hemorrhagic teleangiectasia*.

The third group represent **diseases causing histopathological changes in junction of epidermis and dermis** – these diseases could cause structure changes underneath the skin in the junction between dermis and epidermis – i.e. in the area from which ultrasonic fingerprint scanners acquire fingerprint pattern images. Typical representatives are [6][7]: *Hand eczema*, *Verruca vulgaris* (warts), *Psoriasis* or *Epidermolysis bullosa*.

For acquirement of diseased fingerprints we co-operate with the University hospital in Olomouc and collect these fingerprints. The workplace for diseases fingerprint acquisition is shown in Fig. 1.

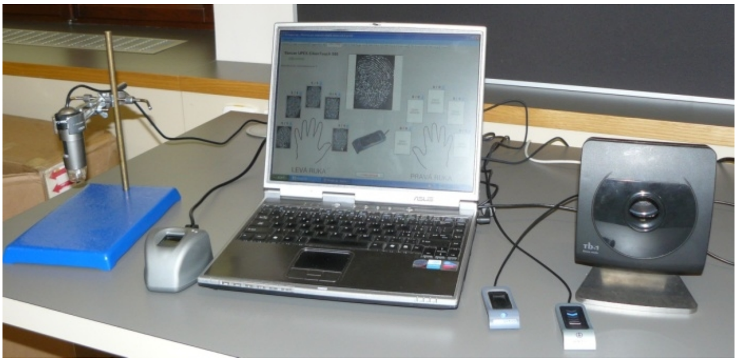

Figure 1: Workplace for diseases fingerprint acquisition.

3 Factors Influencing Fingerprint Acquisition

This chapter tries to sum up all the factors that can influence a fingerprint. Resulting fingerprint image without all these factors is quite different when compared to the realistic one. That is shown on Fig. 2 where we can see realistic fingerprint image one the left side and artificially generated on the right side. There are the three main groups of phenomena damaging the quality of fingerprint. It is finger condition, sensor condition and environment. At first influencing factors connected to the user and his finger will be described.

Almost all fingerprint scanners are influenced by the **dirt on the finger**, be it a small particle, a few grains of dust or just a greasy finger. Conductive materials and liquids are usually the most problematic types of dirt. Only ultrasonic, contactless and e-field technologies are resistant to this type of damage. **Dry or moist finger** is one of the most typical cases of damage done to a fingerprint. Whether it is because we wash our hands or we are nervous and our fingers are sweating or on the other hand we have very dry hands because of some lotion, our skin resistance can increase or decrease ten times the normal value. This usually plays a huge role in the recognition by optical, capacitive and e-field sensors.

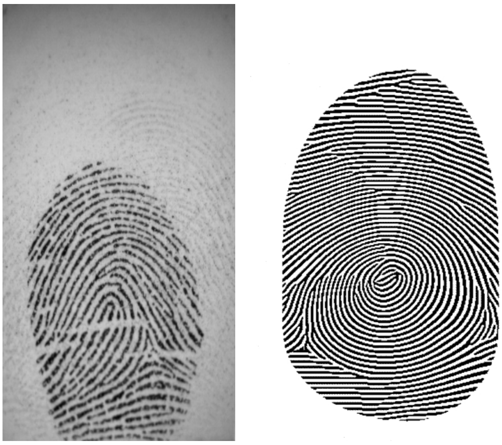

Figure 2: Realistic fingerprint vs. artificially generated.

Physical damage of a finger like cuts or abrasions is obviously damaging the fingerprint. If it isn't a deep wound that influences papillary lines forever, there are ultrasonic and e-field technologies that scan the finger in the deeper dermis layer where the fingerprint is undamaged. Closely connected to this type of damage are **skin diseases**. As it was described in Chapter 2 there are many of them and they have various effects on the finger. In some cases the ultrasonic and the e-field technology can reconstruct the original fingerprint from that user. And if the disease is severe enough to damage the dermis structure of papillary lines there is no way of getting the original structure.

Pressure can turn the fingerprint into a big black oval. Only contactless sensors are fully immune to the damage that the pressure can make. In these categories there are contactless, optical, ultrasonic and e-field technologies. The change of pressure, a very big or a very low pressure or moving is also considered being part of the next category non-cooperative behavior. All these activities lead to a very thick or thin and blurred images. **Non-cooperative behavior of the user** is typical when the user hates biometric technology or simply tries to find the limits of its functionality. The user usually uses an unexpected pressure, moves when the device is scanning and/or places the finger in a wrong place or a wrong rotation. None of the technologies is fully resistant to these types of behavior. [1][2]

Second, factors connected to the sensor will be described. **Dirt on the surface** has the same effects like the dirt on the finger. The problem is that it is affecting everyone who is using that device. So in the registration phase it can create a common error for every user and there is a danger that these users will not be able to be identified after cleaning up the device. In addition to fingers there are more types of dirt than can pollute the sensor area: for example metallic dust, wooden dust, earth dust, fine sand, excrements (in outdoor use). These could be on fingers too but there are easily pictured on the sensor. In addition to ultrasonic and e-field technologies, every sweep sensor is also more resistant to this type of damage.

Latent fingerprint is closely related to the previous topic. It is in some way a type of dirt on the surface of the sensor. More than damaging a new fingerprint there is a security hazard. These fingerprints can be copied or reactivated to breach the biometric device. The technologies, which are resistant to latent fingerprint, are the same like those in the previous topic. **Physical damage** is an extreme but a possible influencing factor of the resulting fingerprint. There is no easy way to prevent the sensor from damaging. The damage of the sensor will have different effects on every technology. In the optical technology, for example, the glass crack could be seen in the fingerprint. [1][2]

The last type of influencing factors is the surrounding environment. **Vibration** in some degree is not a problem, but when the vibrations are large, they can unfasten some internal components causing the device to break down. In another situation they can slightly change the position of finger. This movement, as it was described in the user influencing factors, can blur the fingerprint. Only sensors using the sweep technology are to a certain degree resistant to this type of damage.

Temperature can be different for the sensor, the finger or the environment. Typically there are no problems with the exception of the thermal technology. But when we think about extreme temperatures, we have to deal with very dry or very moist fingers which can affect the resulting image. Also it is known that the ultrasonic technology doesn't operate properly in extremely low temperatures. **Surrounding light** is only affecting optical and electro-optical technologies because they have a light sensing unit. Usually to keep the cost of the sensor low the sensor area is small so that the finger covers it. In that case there is no problem with the surrounding light. However, when the sensor area is larger, the finger of the user is smaller, a smaller finger like a pinkie is used or the contactless technology is used, the influence of the surrounding light can be huge. **Electro-magnetic radiation** is an influencing factor which affects every technology. The device as a whole can be influenced by electro-magnetic radiation. Wires inside or outside connecting it to other parts of biometric system and all electronic components can be influenced. Some devices for example will create a blurred image. [1][2]

4 Attacks on Biometric System

Nowadays it is well known that there do exist many various materials, which could be used for production of fingerprint fakes. The whole process of creation of the fingerprint fakes starts with creation of mold. This mold could be from wax, play-doh or printed circuit board.

Mold is created either directly from genuine user (cooperative method) or using latent fingerprint left by genuine user (non-cooperative method). In the first case we get almost perfect mold immediately. In the second case we can use several methods that reveals latent fingerprint. We can get fingerprint image by using powder and brush to reveal it and Scotch tape to take it. Other very fast method is based on usage of an electrospun nanofibre mat. If the fingerprint image can be saw by naked eye we can also only photographed it and get digital image that way.

Digital image can be improved in graphical software and after that the last step is to create mold. We can either create stamp with fingerprint or use it to similarly like direct mold (using, wax, play-doh etc.) or we can print negative image to printed circuit board. [3][4][5]

After that the mold is filled with desired material. When the material is in required shape i.e. it is dry, it supposedly perfectly fill the mold than it is taken out and fingerprint spoof is done. For better idea how creation of fingerprint spoof looks like there is Fig. 3. It shows printed circuit board with silicon mold. It is sad truth that there has been found minimally one material to each fingerprint scanner technology that can overcame it. That is of course where no liveness detection method is applied. [3][4][5]

Materials used for fingerprint spoofs came from two main sources. The first group contains materials used in a food industry. The following consumable materials are used: gelatin, aspic and gummy bears. The second group are materials used in technical industry: silicons and various types of glues. For additional improvement of the above mentioned materials to get better results in some fingerprint scanning technology it is used skin tone paint and the grated graphite. [3][4][5]

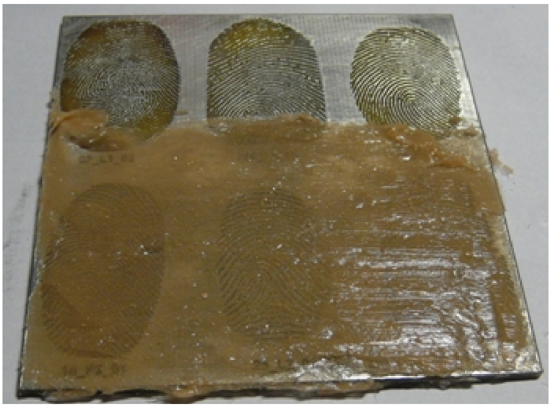

Figure 3: Mold and silicon material used for creation of fingerprint spoof.

5 Conclusion

In this article we discussed three main vulnerabilities of a biometric system at a sensor level. We presented these types of weak places at a sensor level on an example of fingerprint recognition. However, a general biometric system could be vulnerable at the sensor level using the same weaknesses – diseases (face, eye etc.), influencing factors (surrounding light for face acquirement etc.) and spoofs (3D fake for 3D face recognition, hand vein pattern spoof etc.). Therefore it is necessary to consider such weak places and try to take them into account when planning the use of a concrete biometric system at a before known population. Neglecting these factors can lead to the misuse of a biometric system (possible attack) or to very low functionality, which will cause that the biometric system will be refused and the users will not use the system (in some cases they will try to damage or destroy the biometric system).

Acknowledgments

This research has been realized under the support of the following grants: *"New solutions for multimodal biometrics – enhancement of security and reliability of biometric technologies"* COST LD14013 (CZ – 2014-2016); "*The IT4Innovations Centre of Excellence*" MŠMT ED1.1.00/02.0070 (CZ – 2011-2015) and "*Reliability and security in IT*" BUT FIT-S-14-2486 (CZ - 2014-2016).

References

[1] Drahanský M.: *Fingerprint Recognition Technology - Related Topics*. LAP LAMBERT Academic Publishing GmbH & Co. KG, 2011, p. 172, ISBN 978-3-8443-3007-6.

[2] Kanich O.: Fingerprint Damage Simulation – A Simulation of Fingerprint Distortion, Damaged Sensor, Pressure and Moisture, LAP LAMBERT Academic Publishing GmbH & Co. KG, 2014, p. 57. ISBN 978-3-659-63942-5.

[3] Rattani A., Ross A.: *Automatic Adaptation of Fingerprint Liveness Detector to New Spoof Materials*, 2014 IEEE International Joint Conference on Biometrics (IJCB), Clearwater, FL, IEEE, 2014, p. 8, DOI: 10.1109/BTAS.2014.6996254.

[4] Al-Ajlan A.: *Survey on Fingerprint Liveness Detection*, 2013 International Workshop on Biometrics and Forensics (IWBF), Lisbon, IEEE, 2013, p. 5, ISBN 978-1-4673-4987-1.

[5] Ghiani L., Yambay D., Mura V., Tocco S., Marcialis G.L., Roli F., Schuckers S. *LivDet 2013 Fingerprint Liveness Detection Competition 2013*, 2013 International Conference on Biometrics (ICB), Madrid, IEEE, 2013, p. 6, DOI 10.1109/ICB.2013.6613027.

[6] Habif T.P.: *Clinical Dermatology*, 4th Edition, Mosby, China, 2004, p. 1004, ISBN 978-0-323-01319-2.

[7] Wolff K., Johnson R.A., Suurmond D.: *Fitzpatrick's Color Atlas and Synopsis of Clinical Dermatology*, 5th Edition, McGraw-Hill, USA, 2005, p. 1085, ISBN 0-07-144019-4.