FINGERPRINT DAMAGE SIMULATION

Ondřej Kanich

Master Degree Programme (2), FIT BUT

E-mail: xkanic00@stud.fit.vutbr.cz

Supervised by: Martin Drahanský

E-mail: drahan@fit.vutbr.cz

Abstract: This paper describes a design of application for synthetic fingerprint damage simulation. For this task, literature regarding image processing, fingerprint and the ways of generating them was studied. State of art of projects regarding creation of synthetic fingerprint were examined. The focus was laid mainly on the project SFinGe which is a pioneer in this area. There were described different phenomena influencing real fingerprints image. Area of interest was set to two ways of damaging of fingerprints dependent on sensor and user. Methods for simulation of specified damage to synthetic fingerprint that it looks more like a real one was design.

Keywords: fingerprints, synthetic fingerprint, damage, sensors

1. INTRODUCTION

Fingerprint technology is being used almost everyday and with its massive usage various problems emerge. New security elements like liveness detection are added as well as elements that increase convenience of the fingerprint recognition. Due to that algorithms that extract features become more sophisticated. These algorithms have larger demand on testing. Testing requires large fingerprint databases that are difficult to obtain. Instead of using real fingerprints it is better to generate synthetic ones. Generated synthetic fingerprints are usually perfect for fingerprint recognition. To thoroughly test the algorithms damaged synthetic fingerprint are needed.

2. SYNTHETIC FINGERPRINT GENERATOR - SFINGE

According to input variables synthetic fingerprint creation is either fingerprint reconstruction that takes fingerprint minutia as an input and reconstruct fingerprint from them or fingerprint generation that takes, in extreme case, no input (usually some input data are provided e.g. fingerprint class). There are several methods how to generate synthetic fingerprints. Method described here is part of the SFinGe application which seems to be the oldest one and also commonly best known. [1]

For better understanding you can look at the upper part of figure 1 to see process of fingerprint generation. Generating part ends with so called master fingerprint (a perfect fingerprint). First, fingerprint shape is determined. In second step fingerprint class and position of cores and deltas is chosen. Third step creates density map with respect of cores and deltas. Last step is ridge pattern generating. Image with initial seeds is iteratively refined with Gabor filter. Filter orientation and frequency is adjusted according to the previous steps. Minutiae are automatically generated at random places. After that phase master fingerprint is created. [1]

For more realistic fingerprint some damage simulation methods are applied (see the bottom part of figure 1). First step is selection of the contact region. To simulate different placement of the finger on the sensor area random translation of fingerprint pattern is made. Next step is variation of the ridge thickness. It is modified to simulate various skin dampness and finger pressure. Next phase is fingerprint distortion. In this phase skin deformation according to different finger placement over sensor is simulated. Skin plasticity and different force applied on each part of the finger creates non-linear distortion. Next step is noising and rendering. This step is simulating many various

factors. These include irregularity of the ridges, non-uniform pressure of the finger, different contact of the ridges with the sensor, presence of pores and other noise. Another phase is global translation and rotation. This phase simulates imperfectly placed finger on the sensor. Last step is generation of the realistic background. At the end of that step a fingerprint impression is finished. [1]

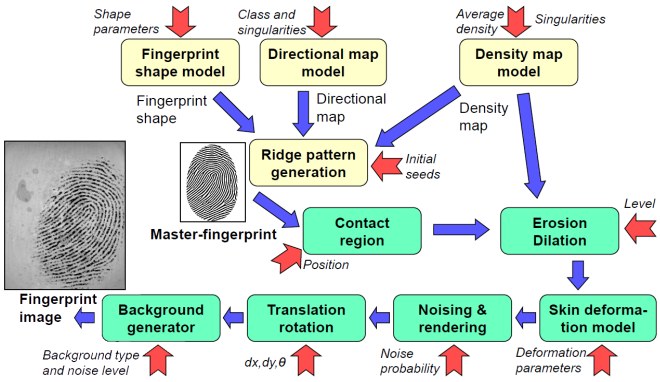

Figure 1: SFinGe process of the fingerprint generation

3. PHENOMENA INFLUENCING FINGERPRINT

This chapter sums up all phenomena that can influence a fingerprint. All damage done to the real fingerprint can be divided into three main groups: effect of a user, a sensor and an environment.

3.1. Effect of a User

All fingerprint scanners are influenced by *dirt on the finger*. Conductive materials and liquids are usually 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 case of damage done to a fingerprint. This is usually playing a huge role in optical, capacitive and e-field sensors. *Physical damage of the finger* like cuts or abrasions is obviously damaging the fingerprint. If the wound isn't deep to influence papillary lines forever ultrasonic and e-field technologies scan finger in deeper dermis layer where fingerprint is undamaged. *Skin diseases* can change papillary lines. In these cases only ultrasonic and e-field technology can sometimes reconstruct original fingerprint of that user. *Pressure* is influencing fingerprint similarly like dampness. Only contactless sensors are fully immune to this kind of damage. *Non-cooperative behaviour of the user* is typical when user hates biometric technology or simply tries to find the limits of its functionality. It covers unexpected pressure moves when device is scanning and/or is placing finger in wrong place or wrong rotation. None of technologies are fully resistant to these types of behaviour. [2]

3.2. Effect of a Sensor

Dirt on the surface has the same effects as the dirt on the finger. In addition to the fingers there are more types of dirt than can pollute the sensor area, for example metallic, wooden and earth dust, fine sand, etc. In addition to ultrasonic and e-field technologies every sweep sensor is resistant to this type of damage. The *latent fingerprints* are closely related to previous topic (for example same technologies are resistant to it). More than damaging a new fingerprint there is a security hazard. These fingerprints can be copied or reactivated to breach the biometric device. *Physical damage* is extreme but possible influencing factor of the resulting fingerprint. Damage of the sensor will have different effects on every technology. [2]

3.3. Effect of an Environment

Vibration can slightly change position of finger. This movement as it was described in user influencing factor can blur fingerprint image. Only sensors using sweep technology are, to a degree, resistant to this type of damage. Thermal and ultrasonic technology are only ones that are influenced by different *temperature* of sensor, finger or environment. *Surrounding light* is affecting only optical and electro-optical technologies because they use light sensing unit. *Electro-magnetic radiation* is

influencing factor that affects every technology. The device as whole can be influenced by electromagnetic radiation. Some devices for example will create a blurred image. [2]

4. DESIGN OF AN APPLICATION

Because of high number of the various factors that influence fingerprint individual methods of damage simulation will be added one by one. For this to work properly it is needed to make high modular design also there must be a way to set order of individual simulations. Some damage methods have been chosen. Figure 2. gives an examples of real fingerprint where dampness and/or pressure and influence of background is very easy to see. Left images shows very low pressure caused by using pinkie and high dampness on the same finger. Right image shows high susceptibility of an optical sensors to surrounding light.

Moisture and pressure have same impact on the real fingerprint. The stronger pressure on the finger the thicker the papillary lines on the fingerprint are. To simulate these effects morphological operators of an image processing are used. Size of the window allows us to control magnitude of damage. White background of places where there are no ridges in generated fingerprint image is glaring. It is possible to use one static background image. Interesting approach on background images generation has SFinGe. From set of only background images (i.e. without fingerprint on it) it uses KL transform (also known as eigenvalue decomposition) known from Principle Component Analysis to randomly generate new background images from given training set. [1]

Figure 2: Examples of real damaged fingerprints.

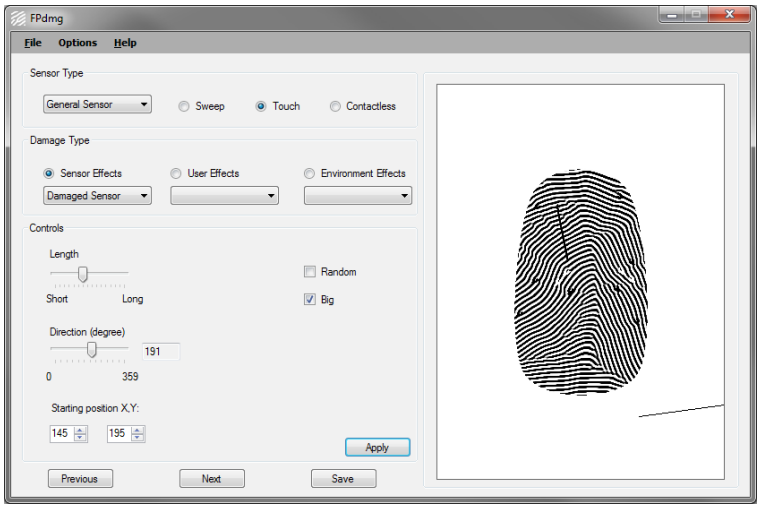

Figure 3: Screenshot from the application.

5. CONCLUSION

Methods of the generating synthetic fingerprint were discussed and shown on SFinGe generator. There were also listed supposedly all phenomena that influence real fingerprints. According to the described design of the application there is ongoing implementation. Currently implemented parts of the application respect needs for high modularity and clear Graphical User Interface which will ensure that user won't be overwhelmed by quantity of the sensors and damage types. It also contains very simple simulation of damaged sensor. In figure 3 there is a screenshot of the result - the implemented application. Database of a touch optical sensor for creation of the training set of the background images generation was taken.

REFERENCES

[1] Maltoni, D., Maio, D., Jain, A.K. and Prabhakar, S.: *Handbook of Fingerprint Recognition.* Springer, 2009. p. 494. ISBN 978-1-8488-2254-2.

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