BRNO UNIVERSITY OF TECHNOLOGY
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

RESEARCH IN FINGERPRINT DAMAGE SIMULATIONS

VÝZKUM V OBLASTI SIMULACÍ POŠKOZENÍ OTISKU PRSTU

EXTENDED ABSTRACT OF DOCTORAL THESIS
ROZŠÍŘENÝ ABSTRAKT DISERTAČNÍ PRÁCE

AUTHOR Ing. ONDŘEJ KANICH
AUTOR PRÁCE

SUPERVISOR prof. Ing., Dipl.-Ing. MARTIN DRAHANSKÝ, Ph.D.
VEDOUCÍ PRÁCE

BRNO 2018

Abstract

The goal of this research is to develop methods for fingerprint damage simulations. In the first part of this thesis the emphasis is placed on a summary of the current knowledge of synthetic fingerprint generation and the damage to these fingerprints. Moreover, general information about fingerprints, fingerprint recognition, and phenomena that damage fingerprints including skin diseases are stated herein. This thesis contains the design and implementation of the SyFDaS application for generation and modular damaging of fingerprints. The next part is a description of methods for damage by swipe mode, narrow sensor, damaged sensor, pressure and moisture, skin distortion, warts, atopic eczema, and psoriasis. Several other types of damage, including fingerprint spoofs, are analysed. Overall, there are 43 basic damages which were visually verified. Due to damage combinations, there are 1,171 types of damage and 348,300 fingerprint images generated, which were evaluated by four different quality measurement methods.

Abstrakt

Cílem této práce je vyvinout metody simulací poškozování otisků prstů. V první části je kladen důraz na shrnutí stávajících znalostí v oblasti generování syntetických otisků prstů a jejich poškozování. Dále jsou uvedeny informace o otiscích prstů obecně, jejich rozpoznávání a vlivy, které otisky poškozují, včetně onemocnění kůže. Práce obsahuje návrh a implementaci aplikace SyFDaS pro generování a modulární poškozování otisků prstů. Další částí je popis metod pro poškozování vlivem průtahového režimu, zúženého snímače, poškozeného snímače, přítlaku a vlhkosti, zkreslení pokožky, bradavic, atopického ekzému a lupénky. Dále je analyzováno několik dalších typů poškození včetně falzifikátů otisků prstů. Celkově je uvedeno 43 základních poškození, která jsou vizuálně verifikována. Díky kombinování poškození je využito 1 171 typů poškození a vygenerováno 348 300 obrázků otisků prstů, které jsou vyhodnoceny čtyřmi různými metodami posuzování kvality.

Keywords

fingerprint, synthetic fingerprint, fingerprint generation, damage simulation, sensors, skin disease, fingerprint spoof, Petri net

Klíčová slova

otisk prstu, syntetický otisk prstu, generování otisku prstu, simulace poškození, senzory, onemocnění kůže, falzifikát otisku prstu, Petriho síť

Citation

Ondřej Kanich: Research in Fingerprint Damage Simulations, doctoral thesis, Brno, FIT BUT, Brno, Czech Republic, 2018

Research in Fingerprint Damage Simulations

Declaration

I hereby declare that this thesis is my original work and has been created under the supervision of prof. Ing., Dipl.-Ing. Martin Drahanský, Ph.D. Some results were achieved in cooperation with bachelor's or master's degree students led by my supervisor or myself. Where other sources of information have been used, they have been duly acknowledged.

……………………
Ondřej Kanich
May 30, 2018

Acknowledgements

I wish to thank Martin Drahanský for his support, advice, and his valuable and inspiring consultations during his supervision of this work. I would also like to thank my whole family for their endless support, great hints, strong motivation, and ceaseless patience. I appreciate Eva Březinová for her advice and insight of the medical part of my work. I acknowledge all students that have helped with this work, namely Milan Bárta, Tomáš Oravec, Štěpánka Barotová, and David Košťák. Last but not least, I wish to thank all former and current members of the STRaDe research group for fruitful discussions, advice, and other assistance which was immensely helpful.

This thesis was supported by several projects: *New solutions for multimodal biometrics – enhancement of security and reliability of biometric technologies* (COST LD14013), *Reliability and Security in IT* (FIT-S-14-2486), *IT4Innovations excellence in science* (LQ1602), *Tools and methods for video and image processing to improve effectivity of rescue and security services operations* (VI20172020068), *Secure and Reliable Computer Systems* (FIT-S-17-4014).

Contents

1 Introduction

In the past decade, fingerprint technology has experienced an incredible boom. They moved from sci-fi movies to just about every personal device. Nowadays, almost every smartphone has a fingerprint reader and their placement in laptops now comes standard. The usage of these technologies in civil areas, like access control or security systems, is now a reality. With this massive expansion, however, there are problems that emerge. Mobile devices are focusing on minimalistic solutions. That usually means the cheapest (for example, the sensor has to be as small as possible), but still workable solutions. On the other hand, security and access control systems are focusing on the highest level of security. [1]

Keeping the performance with the smaller sensors means that algorithms must use every possible information in the sensing area. Cracking these devices (usually smartphones) is a prestigious thing. Producers of biometric systems have to react with new or better liveness detection subsystems. Algorithms that extract features then have to work with liveness detection as well. As a result, algorithms are becoming more sophisticated and complex. This leads to larger demands on testing and testing requires fingerprint database – large databases with not only many fingerprints from one finger but also many fingers. That means that many people (volunteers) are involved in the creation of various databases. The capture of so many fingerprints is a very time-consuming operation. It might seem like that when the database is finished, it can be used everywhere and everything is solved, but that is not true. And that is because fingerprints are considered as personal data and as such they are protected by various laws. The details of these laws can differ from country to country, so generally it can be said that usage of these databases is difficult. [1]

If only there would be a way to get huge databases without these legal concerns, with a lot of challenging fingerprints, and so on. There is one possibility and that is a synthetic fingerprint database. There are already ways to generate a synthetic fingerprint. It is not connected to any real person, thus it is not protected by legislation. The only problem is that they are usually perfect or only slightly damaged. What is needed is challenging fingerprints – damaged ones, and not only with some damage but with a specific damage. The challenge for mobile usage is small sensors (small sensing area); for security and access systems it could be skin disease. When someone has a skin disease that influences the fingerprint, the situation can occur where this person cannot use the access system or cannot get past the security. Fingerprint spoofing is also a problem for all applications. The potential damage done by successful spoofing to break into a smartphone or a highly secure building is different, but it is the same problem.

There are fingerprints that are not so common in the population and these should be in the databases as well. The situation where some kind of fingerprint has not been tested because it just did not appear in the database is unthinkable. This topic is closely related to the so-called Doddington's zoo [2] [3], which stated that the difficulty of comparing two biometric traits is not the same. The fingerprint on a user's left thumb could be easy to compare and the fingerprint on the user's right thumb could wreak havoc for the algorithms. Synthetic database could be prepared so it only contains the worst from the worst. This challenging database could be very beneficial for all types of testing. The usage of synthetic databases is not constricted only to test the algorithms – they can also be used as an educational tool. Police experts on dactyloscopy can learn what diseased fingerprints look like, developers of new systems can see the most challenging fingerprints in advance, etc.

This work focuses on how to specifically damage the perfect synthetic fingerprint so it can be used in these exemplary applications. The main aim is to describe the present technology in generating synthetic fingerprints with an emphasis placed on the simulation of a damaged fingerprint and to design and implement methods that take the perfect fingerprint and transform it into a more realistic damaged representation. These methods take in the input from various types of sensors as well as other phenomena in order to simulate a very specific damage done to a real fingerprint when it is acquired. This way it cannot only simulate a specific damage but also generate a fingerprint exposed to different environments.

In the second chapter research goals of this work are described. The third chapter is dedicated to the current state of the art. There is information about fingerprints, the process of fingerprint acquirement, methods for generating synthetic fingerprints, and the phenomena influencing them. In the fourth chapter there is the design and implementation of the SyFDaS application. Starting with the theoretical Petri net background to the core design of the application, there are some basic touch-based damages and database generation methods listed. The fifth chapter is dedicated to damage simulations for swipe sensors. It shows the way in which the swipe sensor influences the phenomena created for touch sensors and describes new phenomena that are specific only to swipe sensors. Methods for implementation of these phenomena are included as well as examples and their evaluation. This chapter also includes an extensive introduction of evaluation methods. In the sixth chapter, skin diseases that influence fingerprints are described. This chapter also contains information about the simulations of some diseases and their examples and evaluations. The seventh chapter is an introduction to other potential damages. The last chapter is the conclusion, which sums up all essential information.

2 Research Goals

There are three main innovative goals of my research:

(i) Theoretical analysis of swipe fingerprint sensor effects on fingerprint acquisition and simulation of these effects on synthetic fingerprints. This approach will uniquely simulate fingerprint images from swipe fingerprint sensors – this simulation will consist of the following damages (for more details see Chapter 5):

   a. Narrowing of the fingerprint.
   b. Skin distortion in swipe mode.
   c. Pressure and moisture in swipe mode.
   d. A physically damaged finger and sensor in the swipe mode.
   e. Narrowing of the fingerprint in swipe mode.

(ii) Analysis of skin disease effects on fingerprint images. Sophisticated simulation of the chosen skin diseases on synthetic fingerprints, consisting of (for more details see Chapter 6):

   a. Simulation of warts.
   b. Simulation of atopic dermatitis.
   c. Simulation of psoriasis.

(iii) Analysis of other chosen factors which could have significant impact on the fingerprints (for more details see Chapter 7):

   a. Effects of produced fingerprint spoofs from various materials.
   b. Effects of lotion and detergent.

The theoretical model for the damage simulator (and generator) is the first part of the work. This model is based on Petri nets. Afterwards, available databases (our own DBs in the team STRaDe and DBs available online) of specifically damaged fingerprint have been analysed. After that theoretical models with mathematical background have been prepared. Based on these models, simulations mentioned in (i) and (ii) have been implemented. Simulations have been verified by several methods: (i) if it is possible, by visual comparison of a fingerprint – with and without this specific type of distortion, (ii) using the NFIQ standard, VeriFinger fingerprint recognition software, and experimental new algorithm, (iii) if it is possible, by comparison performed by expert. Quality estimation of damaged and undamaged fingerprints have been calculated. Comparison scores based on verification of perfect and damaged fingerprint have been also determined. A large-scale database with specifically damaged synthetic fingerprints has been generated.

3 State of the Art Fingerprint Technology

This chapter describes the general information needed to understand the rest of the work that was done in this research. The main goal of this thesis is closely related to the fingerprints used in biometrics, thus the basic knowledge of biometrics with an emphasis on fingerprints and methods to acquiring them is covered. An integral part is also the way the recognition of fingerprints works, i.e. the processes that are necessary to acquire a fingerprint. All terms related to biometrics are consulted with [4]. [1]

3.1 Fingerprints

This work is mainly focused on *fingerprints*, therefore, this subchapter studies them in more detail. The fingerprint, since 1880, is one of the biometric characteristics that has been used to identify people. Almost a hundred years earlier, it was already known that fingerprints are unique. Francis Galton counted the likelihood of two fingerprints being the same as 1 in 64 billion. That is one of the reasons why it is one of the most basic and widespread biometric characteristics that can be seen in everyday life. In comparison with other biometric characteristics, its main advantages are its uniqueness, permanence, performance, circumvention, and price. It is pretty decent in other properties as well, but there are better characteristics for that (e.g. retina, DNA). [1] [5]

3.1.1 Ridges (Papillary Lines)

A fingerprint is created by capturing *ridges (papillary lines)*[1], [5] [6] [7] [8] which are protrusions in the internal side of hands (and feet as well). In Figure 3.1 the structure of the top side of the skin can be seen. In the *epidermis* portion, some types of minutiae and sweat pores are shown, which are described in Subchapter 3.1.2. The curvatures of the ridges are formed in the deeper layer – the *dermis*. The real

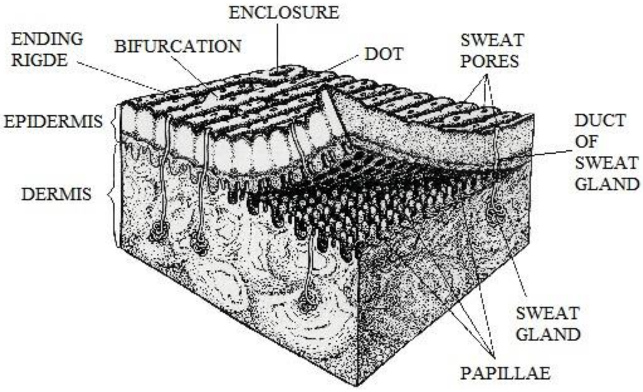

Figure 3.1: Skin Structure (taken and modified from [5]).

[1] According to Harmonized Biometric Vocabulary (http://www.christoph-busch.de/standards.html)

ridges in the epidermis, which can be seen and captured as a fingerprint, are just a projection from the deeper layer (for example, wrinkles are formed in the same layer). This means that one cannot alter or delete the fingerprint by damaging the epidermis, for instance by a burn, abrasion, or cut. If damage like that is done, it will regenerate with the growth of skin in the surface of the finger. The only way to change ridges is by damaging the dermis. This will permanently alter that part of the ridges, thus creating new unique pattern. [1] [3] [5] [7] [9] [10] [11] [12] [13] [14] [15]

3.1.2 Classification of Fingerprints

By simply comparing two images, the identification would be a difficult task, therefore fingerprints can be divided into several particular classes. Using this classification system, it is possible to quickly reject fingerprints from another class, which greatly accelerates the identification. IAFIS (Integrated Automated Fingerprint Identification System), [16] uses the *Henry's classification system* [5], which contains three classes. These are *arch*, *loop*, and *whorl*. Nowadays, extended versions, where these three classes are split into more specific ones, are used. All these classes are not equally frequent in fingers. [1] [5] [8] [9] [17]

To understand how these classes can be distinguished, it is necessary to define some objects of interest. The first of them is *delta* [5] [6]. It is a place where ridges run in three different directions; it forms a triangular shape. The second of them is *core* [5] [6]. Core is the centre of the fingerprint and it can be found in the innermost loop or in the middle of the spiral in the whorl class. All classes differ in the quantity of cores and deltas or in the direction of the cores. [1] [5] [6] [8] [9] [18]

Classes alone are not sufficient enough to identify a person. The characteristic that is detailed enough to distinguish every finger in the world is the *fingerprint minutia*. Minutia [5] is a special formation created by ridges. In dactyloscopy huge amounts of these formations are distinguished. Each type of minutia has a different likelihood of appearance in the fingerprint. In automated processing only two basic types of minutiae are recognized: *ridge ending* and *bifurcation*. [1] [5] [8] [9] [19]

3.2 Fingerprint Acquirement

Nowadays, when fingerprint recognition technology is used, regardless of the precise usage (i.e. verification or identification) the first thing to do is to get a fingerprint from the finger to the computer. There are several methods of obtaining a digitalized fingerprint. The traditional dactyloscopic card, where the fingerprint is obtained by moistening the fingertip in ink or a chemical substance (clean fingerprinting), can be scanned. This method leaves fingers dirty and there is no certainty of making a good fingerprint. It is better to have fingers scanned directly into the computer. The principle of these direct methods can be found in the following subchapters. [1] [5] [7]

Fingerprint capturing sensors are divided into three main categories. They are swipe, contactless, and touch (or area) sensors. When using **touch sensors** the finger is placed on the sensor area and left there for a few seconds without moving it. These sensors are very easy to use, even for inexperienced users. The only thing that could go wrong is a bad rotation or position of the finger. A bad rotation often occurs when the thumb is being scanned (20° is usually enough for matching algorithms to stop working). People with longer fingers frequently do not properly estimate the sensor’s area, and then the core of the fingerprint is not scanned or appears in the edge of the scan, which is not an optimal position for many matching algorithms. The biggest disadvantage of touch sensors is that latent fingerprints can remain on them. Some technologies can get tricked by the reactivation of the last finger from a latent fingerprint. In this matter, a related problem is that the sensor gets dirty with each scan and must be cleaned, depending on the frequency of scanning. Dirty sensors produce dirty fingerprints, which can result in a higher false rejection rate [7]. A good sensor should also have an area large enough to fit everyone's finger. However, a larger area usually means a higher cost. [1] [7]

Swipe sensors are usually a little bit wider than a finger, but their height is only several millimetres. When using swipe sensors, the finger is swiped vertically over the sensing area. The sensor will then reconstruct the fingerprint from each smaller part captured when the finger was swiped. The advantage of this type of sensor is its lower cost, because of the much smaller area. Also, there is no latent fingerprint available (only the last part of it) and finger movement basically cleans the sensor each time it is used. The rotation of the fingerprint, thanks to the vertical movement, is almost non-existent. On the other hand, the sensor is harder to use. There are many things that can go wrong when swiping a finger. The exact speed, position, and steadiness of the movement have to be maintained. In case of the wrong speed or unsteadiness of the finger movement, the final image is discontinuous or unrealistically long. In addition, when the finger is in the wrong position, the final image is simply only half of a fingerprint. The sensor must be able to scan very quickly to permit a suitable swiping speed. The image reconstruction is time-consuming and it is also a source of inaccuracy and errors in the final image. The first swiping sensor was used with thermal technology, but nowadays the most widely used technology is capacitive or RF capacitive. [1] [7] [20] [21] [22] [23] [24] [25] [26]

The last type of *sensor* is a **contactless** one. These sensors scan ridges even without a finger touching the sensor. Usually they work in a similar way to touch sensors. Because of that, there are no worries of a latent fingerprint, dirt on the sensor, or a bad speed or unsteadiness of the fingerprint movement. On the other hand, the device is usually placed around the whole finger, which implies a higher cost and a lower acceptability. The only thing that is needed is the right position of the finger in the device.

In Figure 3.2 an overview of fingerprint recognition process can be seen. First, a digitalized image of a fingerprint is needed. Nowadays, sensors tend to have liveness detection (anti-spoofing) as a part of the scanning process. The next phase is the enhancement of image quality. This phase can be divided into smaller ones – the orientation field estimation for each point, the estimation of the block orientation field, and then the final mapping on the original image. Using this information, the image is then enhanced. In this step many various methods can be applied on the image. The next step is binarization. It is usually done by some thresholding method, e.g. by regional average thresholding or by adaptive thresholding. At the end of this step is a binary image, where ridges are black and valleys white. The following process is minutiae detection, and for this purpose only ridges are needed. So in this step the ridges are thinned to be only one pixel wide. The last phase is minutiae detection and extraction. After that, different approaches for recognition could be used; for example, global and local minutia alignment, minutia cylinder-code, etc. [27]. [1] [5] [7] [8] [12]

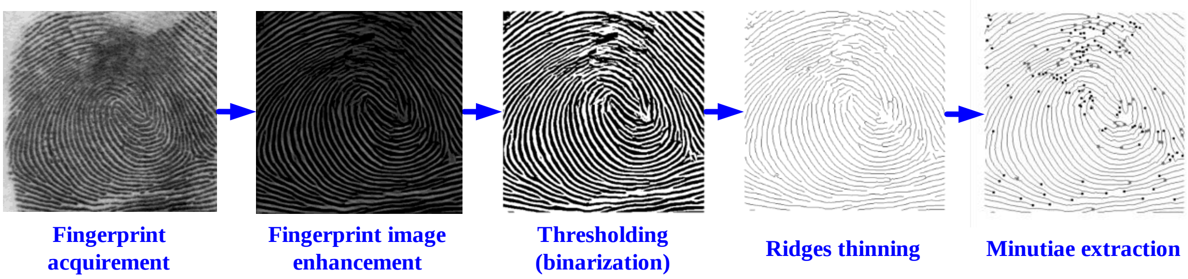

Figure 3.2: An overview of fingerprint recognition process (taken and modified from [17]).

3.3 Methods for Generating Synthetic Fingerprints

Synthetic fingerprint generation is an inverse biometrics problem [28]. According to input variables, it is essentially the fingerprint recognition process (Subchapter 3.2) from the end to the start. Several methods of how to generate a synthetic fingerprint can be found in [6] [9] [29] [30] [31] [32] [33], and when these methods are thoroughly studied, one can find that they are all based on the same principle. The method used by the SFinGe seems to be the oldest one and also the most commonly known, so it will be described as a template for others. For example, very similar methods are used by Anguli, which is an Indian Institute of Science fingerprint generator. [1] [14] [34]

The generating part ends with the so-called master fingerprint (a perfect fingerprint, equivalent to the phase extracted lines from Figure 3.2). First, the fingerprint's shape is determined The second step is the directional field model. In this step the fingerprint class is chosen together with the position of cores and deltas. The third step creates a density map. The last step is ridge pattern generation. This phase uses all previous steps along with some initial seeds. Iteratively, the image with the initial seeds is refined with the Gabor filter. Minutiae are automatically generated at random places with random types. After that phase, the master fingerprint is finished. [1] [9] [14] [29] [30] [34] [35]

As can be seen, the SFinGe generating process is not exactly an inverted recognition process. If this process is strictly followed, so-called fingerprint reconstruction is then performed. These are methods that focus on the creation of a whole fingerprint from only the minutiae saved as a template in fingerprint recognition [36] [37]. Another method lies between these two. It states that fingerprint features are dependent on each other [29]. This method firstly determines singular points, after that it is the orientation field, and finally the minutiae. Each step is dependent on the previous one. After all of the steps are completed, the master fingerprint is made with the use of the AM-FM (amplitude modulation, frequency modulation) method. The last described method (from SyFDaS generator) uses minutiae as an input. The creation of a whole fingerprint is based on only these minutiae. Note that instead of the initial seeds, this method uses minutiae as these seeds and the generation starts with them, so precisely defined minutiae do not change in the generation process. [1] [9] [14] [29] [32] [34]

3.4 Phenomena Influencing a Fingerprint

Information in this subchapter is needed in order to fully revert from the master fingerprint to a realistic looking. There are three main groups of phenomena that can damage the quality of a fingerprint. They are finger condition, sensor condition, and environment. Almost all fingerprint scanners are influenced by **dirt on the finger**, be it a small particle, a few grains of dust, or simply an oily finger. Conductive materials and liquids are usually the most problematic types of dirt. The **dry** or **moist finger** is one of the most typical cases of damage done to a fingerprint. Whether it is because the users wash their hands, if they are nervous and their fingers are sweating, or if they have very dry hands and lotion was applied. The **physical damage of a finger**, such as cuts or abrasions, is obviously damaging to a fingerprint. There is a combination of physical damage and non-cooperative behaviour, which is often called **altered fingerprints** [38] [39] [40]. This category includes surgeries that alter or replace ridges, intentional cuts, mutilation by acid, attempts to change fingerprint class, or scorching. There are numerous **skin diseases** [10], but it is hard to tell how many people are affected by these. Skin diseases are explained further in Chapter 6. **Pressure** can turn the fingerprint into a big black oval. The change of pressure, a very big or a very low pressure, is also considered to be part of the next category: non-cooperative behaviour. All these activities lead to very thick, thin, or blurred images. The **non-cooperative behaviour of the user** is typical when the user exerts unexpected pressure, moves when the device is scanning, or places the finger in the wrong place or with a wrong rotation. The **contact region** is a phenomenon which occurs when the user presents their finger to a sensor in such way that only a part of it can be acquired. [1] [7] [8] [13] [14] [15] [34] [38] [39] [40] [41] [42] [43]

Another group of factors affecting the fingerprint images are those connected to the sensor. **Dirt on the surface** has the same effect as dirt on the finger. Apart from fingers, there are other things that can pollute sensor area: metallic dust, wooden dust, earth dust, fine sand, or excrement (in outdoor use). The **latent fingerprint** is closely related to the previous topic. In some way it is a type of dirt on the surface of the sensor. **Physical damage** is an extreme but possible influencing factor of the resulting fingerprint. **Sensor technology** itself has a large impact on how the fingerprint looks (there are a lot of things that could go wrong [44]). For instance, some technologies like ultrasonic or optical tomography can access an image from a deeper level of skin and the resulting image is then shown without shallow scars. [1] [7] [8] [13] [14] [15] [34] [41] [42] [43]

The last category of influencing factors are those that can be found in the surrounding environment. **Vibration** in some degree is not a problem, but when the vibrations have a high amplitude they can unfasten some internal components, causing the device to break down. Sometimes they can also slightly change the position of a finger. This movement, as it was described in the user influencing factors, can blur the fingerprint. The **temperature** can be different for the sensor, the finger, and the environment. Taking into account extreme temperatures, it is possible to have very dry or very moist fingers which can affect the resulting image. **Surrounding light** only affects optical and electro-optical technologies because they have a light-sensing unit. **Electro-magnetic radiation** is an influencing factor that affects every technology. The device as a whole can be influenced by electro-magnetic radiation. Some devices will, for example, create a blurred image. [1] [7] [8] [13] [14] [15] [34] [41] [42] [43]

4 SyFDaS – Synthetic Fingerprint Damage Simulator

When designing an application for damaging synthetic fingerprints, it was determined to first create a simulation of this application using P/T Petri nets. This simulation is called Fingerprint Generation Petri Net (FGN). After that, the application is described; the primary focus is laid upon the core design and graphical user interface. In this chapter, the enhancement of the generator is described. The biggest portion of this chapter is dedicated to touch-based damages. Lastly, database generation options are discussed.

4.1 Fingerprint Generation Petri Net

Petri nets [45] are specific modelling techniques. They can be defined either by graphs or by a purely mathematical notation. The graphic notation is usually easily understandable, while the mathematical one can be used for various analyses and proofs. Petri nets are primarily used in distributed and discrete

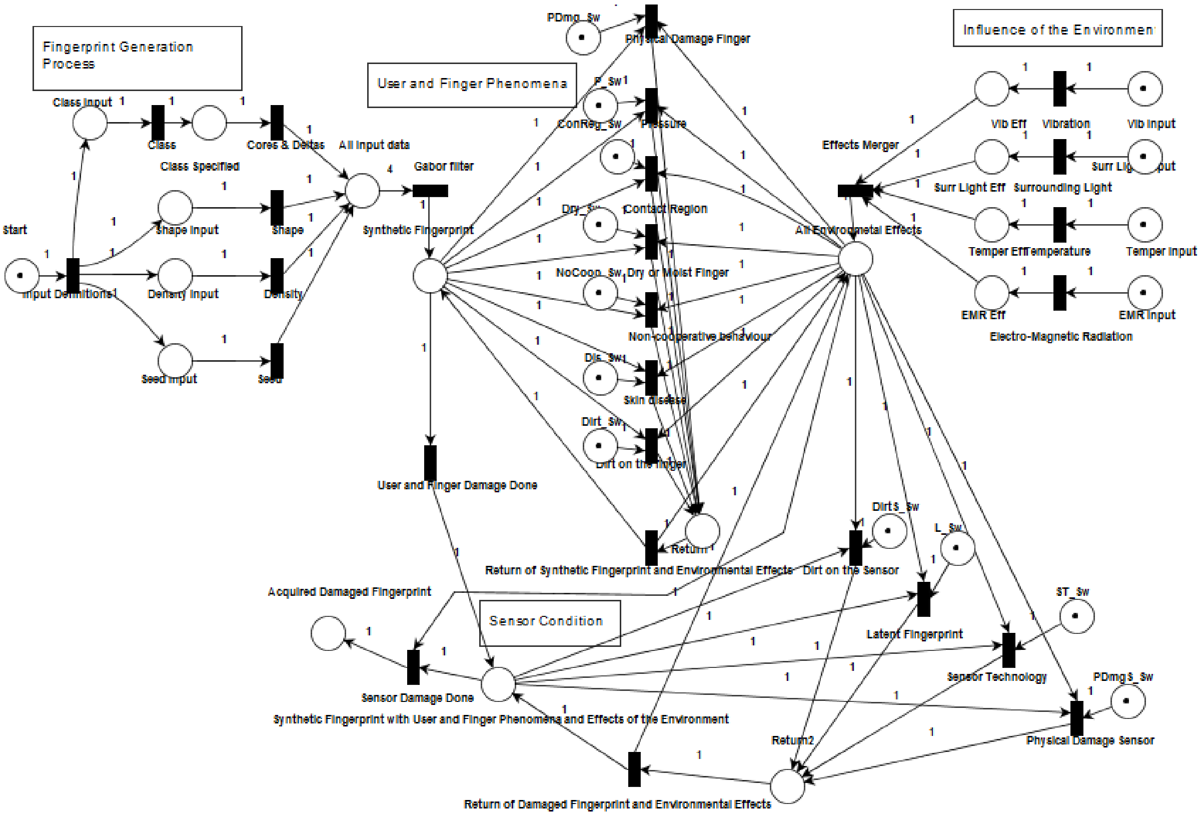

Figure 4.1: The whole proposed Fingerprint generation Petri net.

systems. The goal of this subchapter is to create a Petri net that will simulate the generation of a synthetic fingerprint. It is important to know that the Petri net only simulates the fingerprint generation process. It is advantageous to use them as a clear way of showing all of the possibilities in synthetic fingerprint damage simulation. They can also be used to show specific scenarios. To make Petri net creation clearer, the generation process will be divided into four distinct parts. The first part is the master fingerprint generation, the second part simulates the state of the environment, the third part simulates the user and finger condition with the respective fingerprint damage, and the last part simulates the sensor conditions that affect the fingerprint (as can be seen in Figure 4.1). [34]

4.2 SyFDaS Core Design

Following the simulation in Subchapter 4.1, the application can be divided into two parts. The first part creates the synthetic fingerprint, and the second part takes care of all damage simulations. For the purpose of fingerprint generation, the base generator (Chaloupka's fingerprint generator) from [9] is used. This generator is using minutiae as an input (as covered in Subchapter 3.3). Unfortunately, it was hard to create realistic looking fingerprints because of that. Too often the orientation field was not from one of the fingerprint classes, which had a great impact on the look of the generated image. It was decided to add the desired fingerprint class as one of the inputs for the generator. The methodology of generation had to be preserved – the main inputs should be defined as minutiae. The original algorithm started with an orientation field at 0° in point of the field, after that it was changed based on the given minutiae. The new version changes this part of the algorithm. If a fingerprint class is given an orientation field, it is first processed by the field generation for that particular class. By setting the filter, orientation (with fingerprint class), mask, and density in their respective parts of the GUI, the generation is prepared. Consequently, all possible damage simulations must be held in one clean interface. To do that, it is essential to use the modular approach on this interface. The information about a sensor, a type of sensor, damage and all the controls related to it has to be easily accessible. [1]

4.2.1 Damaged Sensor

There are databases (specifically with optical sensors) where this type of damage is clearly shown. It is a thin black line usually connected to the edge of the acquired fingerprint. This line corresponds with the crack on the protective glass. In extreme cases there could be a web of broken glass instead of one crack. Some types of dirt on the sensor look like this crack. For example, an eyelash of straight hair leaves the same trace on the acquired fingerprint. This phenomenon was also listed in Subchapter 3.4. It is simulated by simply drawing a line in the desired area on the fingerprint. [1]

4.2.2 Pressure and Moisture

When it comes to applying intentional damage to the fingerprint, too much pressure is the first thing that comes to mind. Similarly, as in the simulation of a damaged sensor, moisture influences the final image in the same way as pressure. Both dampness and pressure increase the thickness and the contrast of the ridges. The more pressure the user applies or the damper their finger is, the thicker the lines are. In extreme cases almost no lines are visible on the fingerprint, because the fingerprint is either entirely black or white. This factor was also mentioned in Subchapter 3.4. Morphological operations of erosion and dilation [46] will be used to simulate these effects. [1]

4.2.3 Fingerprint Distortion

Fingerprint distortion is typically done unintentionally. It is created due to skin deformation and the non-orthogonal finger pressure to the sensor. In fact, every little finger movement when touching the sensor glass creates this distortion. To make a non-distorted image the major focus would have to be on not moving the finger and on applying the pressure exactly orthogonally. Even this might not be enough, because two-dimensional images are created out of a three-dimensional finger, so the skin is stretching and compressing and thus creating distortion. In Subchapter 3.4 the non-cooperative behaviour of the user is described. The same distortion model as in SFinGe will be used to simulate this distortion. In [47] a model was designed and also verified. The model divides the fingerprint into three areas. The internal area where the finger is pushed so hard that the skin cannot be deformed. The second is the external area where the pressure is so low that the skin is maximally distorted. And the third area is the transition area, which combines the two previous areas. [1]

4.2.4 Database Generation

In addition to a single image processing it is often required to have a possibility to create a database (or a batch) from several images. Massive processing is one of the biggest advantages of synthetic fingerprints. The preparation of damage could be time-consuming (especially for swipe sensors) because there has to be a way to save the damage. All input data (sensor information, damage information, etc.) is saved. Often it is interesting to combine damages. For this, there is the **full combination** setting. This means that all damages will be combined to all damages. If one image is taken then all one damage combinations are done to it, all two damages combinations, etc.

If the full combinations of given damages are done then it could be problematic if the same type of damage cannot be applied to the same image, i.e., it makes no sense that the image would be distorted in two different ways at the same time. That is the reason for the **restricted combination** setting. This setting allows only one of each damage type in each combination.

When discussing possible damage combinations, fingerprint sensors could be damaged in two places at once. In that case the image should be damaged by two damages of the same type. Without explicit semantics of the combinations of all damage types, there is no general solution to this problem. Because of that, the last level of combinations was introduced – it is **no combination**. Using this, all damages that are loaded will be made in that order to all images. In this setting all images only have one damage impression.

5 Swipe Sensor Damage Simulation

This chapter is focused on altering existing synthetic fingerprints in the master fingerprint phase to a synthetic fingerprint that will look like a real fingerprint created by a swipe fingerprint sensor. At the moment, there is no conclusive research on sensor specific variations of synthetic fingerprints. The only efforts made in this area were some projects that tried to create a sensor specific background. A description of swipe sensors could be found in Subchapter 3.2. The primary point is that the image acquired by swipe sensors is a combination of several smaller images. These smaller images are from different parts of the finger which is doing a swipe motion over the sensor unit. The reconstruction algorithm [20] [21] [22] [23] [24] [25] [48] then merges these images into one final image.

5.1 Damage Analysis

The complexity of fingerprint acquirement using a swipe sensor is reflected in determining the new influential factors for this type of sensor, and a skilled and trained user is capable of creating high-quality results with it. That is because a reconstruction algorithm, which is merging individual acquired images, can repair some damages done by the user. On the other hand, unskilled users can in the same way create more damages because of bad cooperation between them and the algorithm. It was found that it is possible to simulate a swipe sensor similar to the touch sensors. The main difference is that each factor can appear in each small image, which are later merged to the final acquired image. Influential factors can be divided into two groups: the first one with the factors that are altering damages common with the touch sensors, and the second group with factors that are completely new in swipe sensor usage. The first group contains already known damages like *pressure*, *contact region*, and *skin distortion* used in swipe mode (see Subchapter 5.2). In the second group, this work focuses only on *narrowing* the fingerprint image. Successful simulation of these factors leads to creating a fingerprint which will be close to a fingerprint taken from the swipe sensor.

5.2 Swipe Mode

This group focuses on the already created touch fingerprint damages, however, those are used in a swipe mode. Swipe mode is basically the recreation of a reconstruction algorithm. The algorithm works in this way: the sensor usually acquires a short and wide part of fingerprint (based on the size of sensing unit). This small image is called a *slice*. By swipe motions, the sensor gets a lot of slices and it stores them in the order of their acquirement. Its responsibility is to reconstruct the fingerprint image based on correlation, the swipe speed, and the known parameters of sensing unit (as can be seen on Figure 5.1). Synthetic fingerprints are generated without slices. It is necessary to take steps in the inverse order. Synthetic images will be divided into slices. Each of them will be treated as an independent image. After that, all slices will be merged together.

An important issue is how the input data will be transferred to these slices. There are several solutions. **Fully-automatic settings** will be defined by the first (seed) settings as well as some optional information about the trend of the values. **Semi-automatic settings** will be defined by the input data spread out on a set of slices. **Manual settings** will be defined by providing input data for each slice. Manual settings will be used in this work.

Generally, there are only a few boundaries regarding how many slices there are in one image. It is dependent on user swipe speed and sensing unit height. This general swipe mode would be difficult to use, and the user would have to pay attention if another slice is a few pixels away or shifted to the right or really far down. For that reason, swipe mode is simplified. Slices are uniformly distributed in the image, and they are not moved in horizontal axis. After this simplification, the variables needed for this swipe mode can be defined. Primarily, it is the *height* and *overlap* of the slices. After knowing all this information, the image can be easily divided into slices. All of them are damaged independently. Now all there is left to do is to merge all of the damaged slices together to one image.

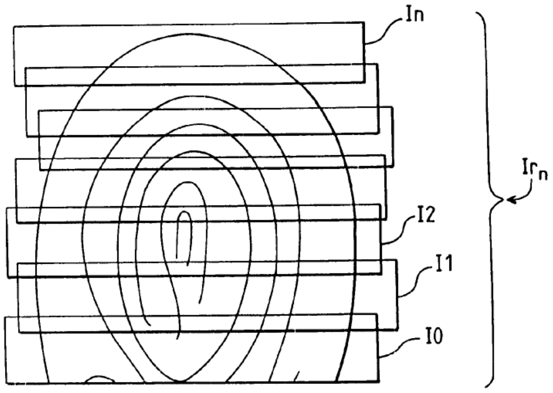

Figure 5.1: Example of assembled slices to create a fingerprint (taken from [43])

5.3 Damages Exclusive to Swipe Sensors

This category describes the damages that are typical for swipe sensors. Of course, with some extra effort and *non-cooperative behaviour* some of these damages can be replicated on touch sensors. Further restriction is that damages in this category are not altered touch damages – these will be described in Subchapter 5.2. The most important damage is the **narrow sensor**. The greatest advantage of this technology is its price. To further leverage this advantage, the sensing unit is not only short, but also narrow. Only a portion of the width of the finger is scanned. If the finger is swiped askew then the behaviour is dependent on the reconstruction algorithms. Some of them are able to detect this anomaly and move the next slice down and to the side (so translation in *x* and *y* axis). This results in images that have higher widths than the sensing unit. Closely connected to the movement and unskilled user is the acquirement of **another phalange**. Acquired images often start in the middle of the fingerprint and continue over the joint as the user is trying to make a long swipe. This is a very special type of “damage”. To simulate this, it is needed to add a ridge line print from the inner side of the joint and the second phalanx. When prolonging a synthetic fingerprint image, one can rely on the fact that the next phalange of the finger usually has a very flat arch class. **Faults** or **exploitation** of reconstruction algorithm is heavily dependent on the specific implementation and properties of the algorithm used inside of sensor. Whenever the motion of capture is done slow at the start and then swiftly accelerates, it is possible to also create unrealistically long images or ridges. The last damage to be discussed is **motion blur**. Damage can be often seen on the edges of the fingerprint. Motion blur can be caused by changing skin distortion or movement (translation, rotation) of the finger during the swipe, causing problems with the reconstruction algorithm. On the other hand, it could be caused by a fall of precision when a finger is getting out of range on the edge of the sensing area.

5.3.1 Narrow Sensor

This subchapter describes the implementation of damage done by the narrow sensor. The most important part is to determine how much the image should be narrowed (*narrow cut*). There is a small overlap between the clear image and the blank space where the sensor cannot take an image. Width of the overlap is the next input to this damage simulation (*smooth width*). The last piece of information is the position of the centre of the sensor (*central width*). Figure 5.2 shows how the fingerprint will be narrowed along with the resulting image.

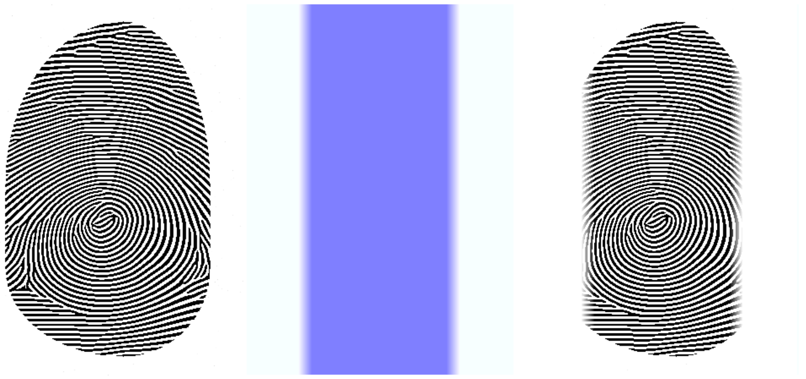

Figure 5.2: Narrow sensor simulation (before damage, preview and after applying the damage).

5.4 Examples of Damages

As stated in Subchapter 5.3, swipe sensors are usually narrow. On the contrary, synthetic fingerprints are usually generated as undamaged live prints (oval shaped) [32]. To create realistic-looking fingerprints it is better to have them narrowed. For that, a *narrow sensor* touch-based damage is used.

Pressure and moisture damage is one of the easiest to see. In addition, a change of pressure is very frequent in a swipe motion. There are a lot of combinations of greater or lower pressures in the database. In the end, these seven were chosen. **All low (pm0)** Figure 5.3bc, **Extreme (pm1)** Figure 5.3de, **High to normal (pm2)** Figure 5.3fg, **Low to high to low (pm3)** Figure 5.4ab, **Normal**

to low (pm4) Figure 5.4cd, **Recurrent normal to low (pm5)** Figure 5.4ef, **Slowly high to low (pm6)** Figure 5.4gh.

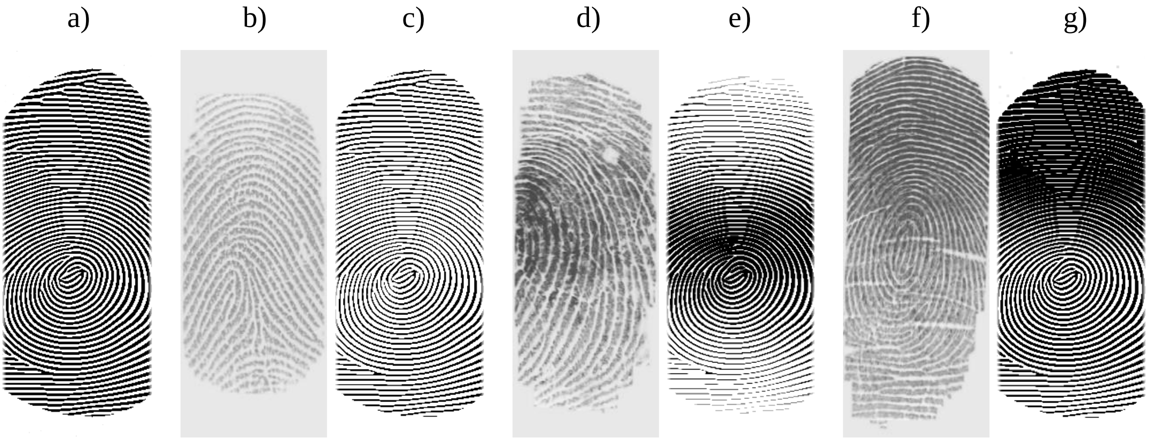

Figure 5.3: Examples of pressure damage images (a – original, b, d, f – real, c, e, g – damaged).

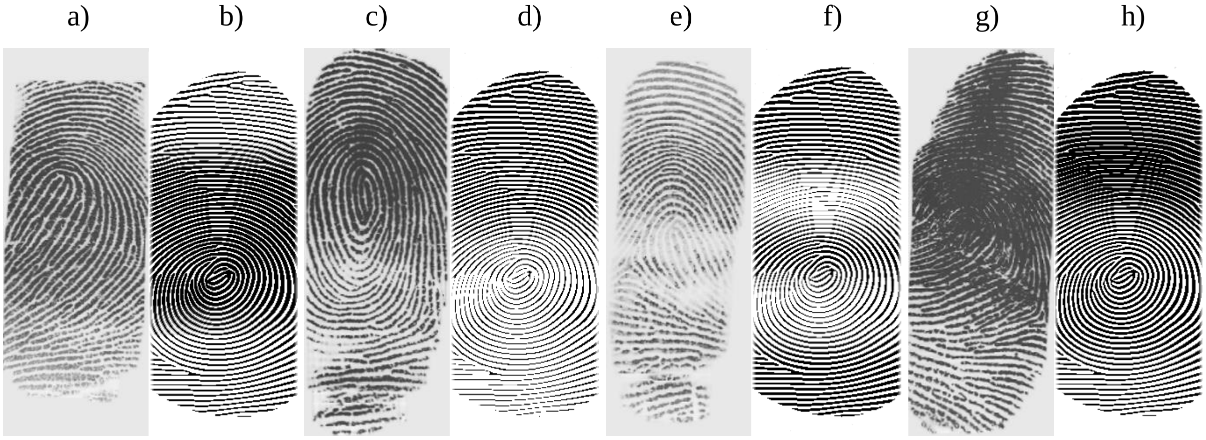

Figure 5.4: Examples of pressure damage images 2 (a, c, e, g – real, b, d, f, h – damaged).

Usage of the **narrow sensor** in swipe mode can simulate different contact regions. The exact results of contact region damage in swipe sensors are dependent on the used reconstruction algorithm. In this case (same as in the acquired database), fixed sensing region is assumed. Wrong (not complete) contact regions are in a high percentage of images. The use of non-traditional fingers in databases leads to a lot of these damages. These are often made by the little finger or thumb. In the end, 11 damages were chosen. **All sideways sharp (narr0)** Figure 5.5bc, **All sideways steady (narr1)** Figure 5.5de, **Cutdown (narr2)** Figure 5.5fg, **One side (narr3)** Figure 5.6ab, **Side zigzags (narr4)** Figure 5.6cd, **Tip bottom jumpy (narr5)** Figure 5.6ef, **Tip bottom one side (narr6)** Figure 5.6gh, **Tip bottom standard (narr7)** Figure 5.7ab, **Tip both sides (narr8)** Figure 5.7cd, **Tip top round (narr9)** Figure 5.7ef, **Tip top sharp (narr10)** Figure 5.7gh.

Swipe **sensors** are more resistant to **damage**. Based on the previous damages and the simplification of fixed sensing, region expected behaviour can be simulated. Two types of damage were chosen for this simulation. This damage is the one which has the same settings for all slices. If the sensor is damaged it will be in all slices and in the same place. **Long, narrow (dmg0)** Figure 5.8b, **Long, wide (dmg0)** Figure 5.8c, **Short, narrow (dmg1)** Figure 5.8d, **Short, wide (dmg1)** Figure 5.8e.

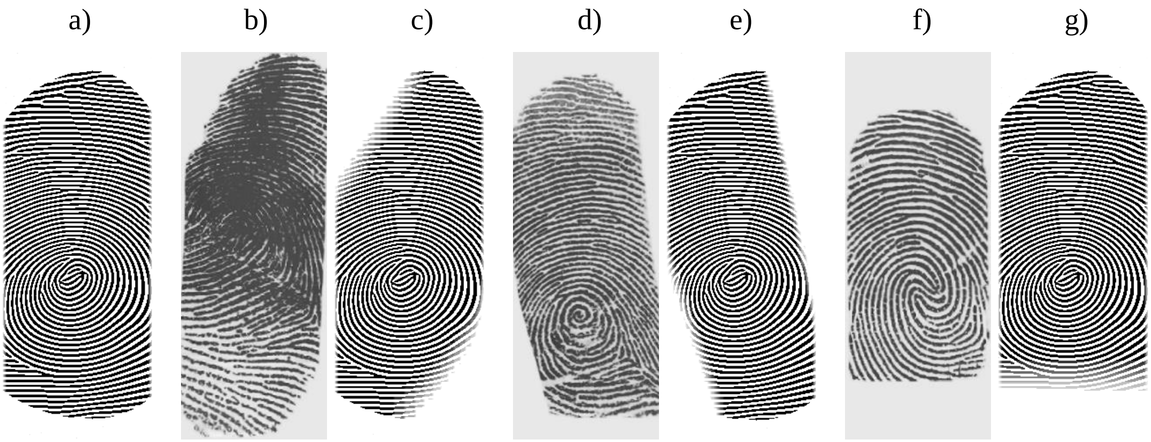

Figure 5.5: Examples of narrow damage images (a – original, b, d, f – real, c, e, g – damaged).

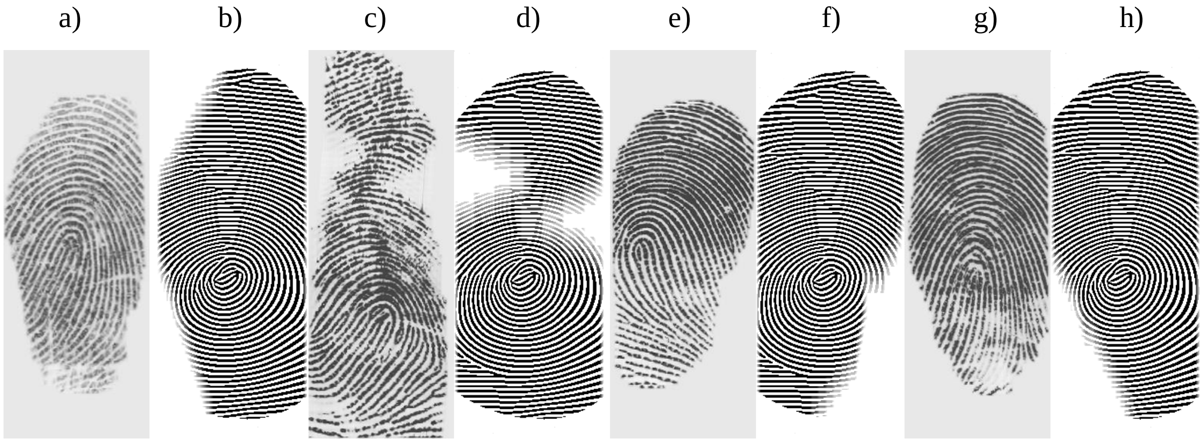

Figure 5.6: Examples of narrow damage 2 (a, c, e, g – real images, b, d, f, h – damaged impressions).

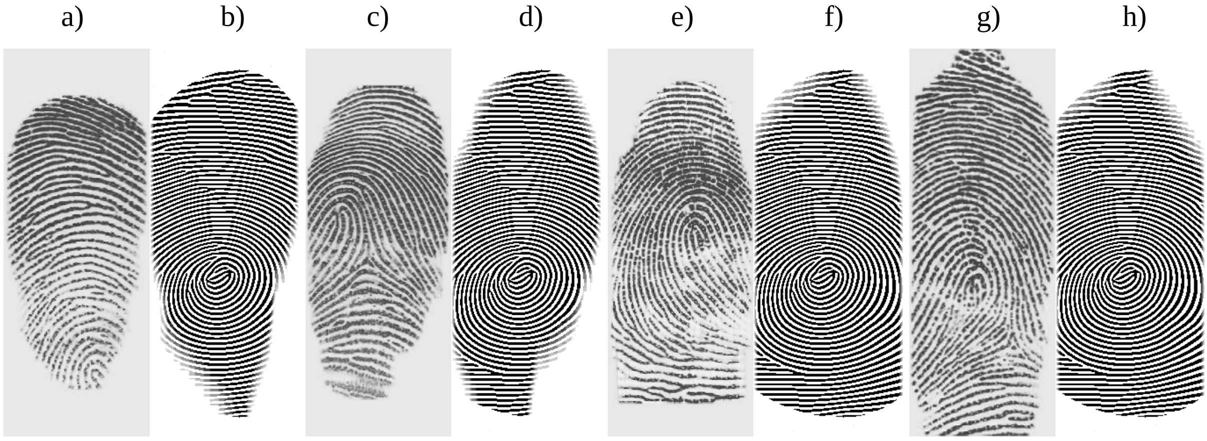

Figure 5.7: Examples of narrow damage 3 (a, c, e, g – real images, b, d, f, h – damaged impressions).

The final example is using **skin distortion**. This damage is probably the worst to correctly simulate. It is certain that skin has to be distorted when doing the swipe motion. Distortions are also hard to see in real images. On the other hand, if the finger is moving sideways or too fast, for example, there has to be distortion and it can be seen as motion blur. That is because the correlation part of the

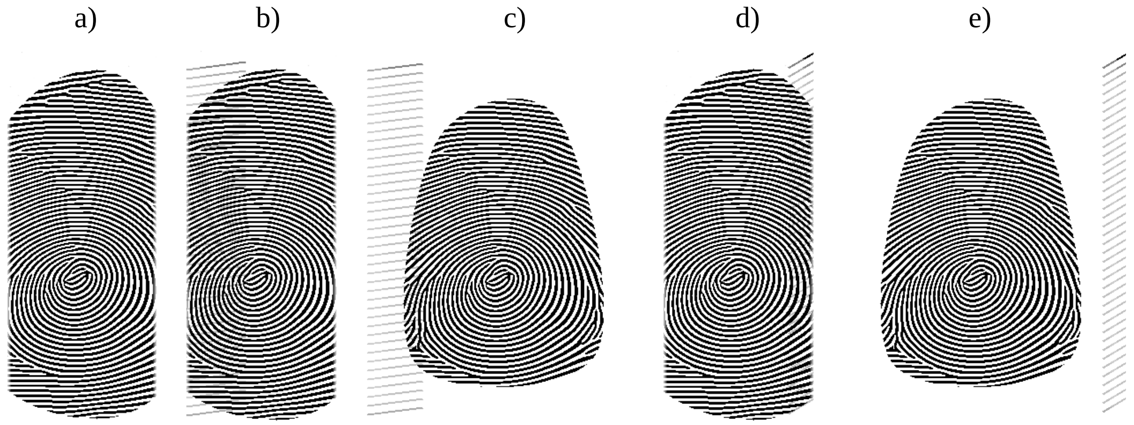

Figure 5.8: Examples of damaged sensor images (a – original, b, c, d, e – damaged impressions).

reconstruction algorithm finds non-distorted parts which are consistent with previous slices as well as the distorted parts which are not. Some mistakes or inaccuracies will be surely made when this happens. Distortion could also mean that part of the skin is not touching the sensing area, thereby creating contact region damage. The chosen examples are a little extreme. On the other hand, they can be easily seen and the motion blur (with translation or rotation) is obvious in each example. Real images with motion blur and other damages can be seen in Figure 5.9efg. **Extreme (dis0)** Figure 5.9b, **Move X (dis1)** Figure 5.9c, **Move Y (dis2)** Figure 5.9d.

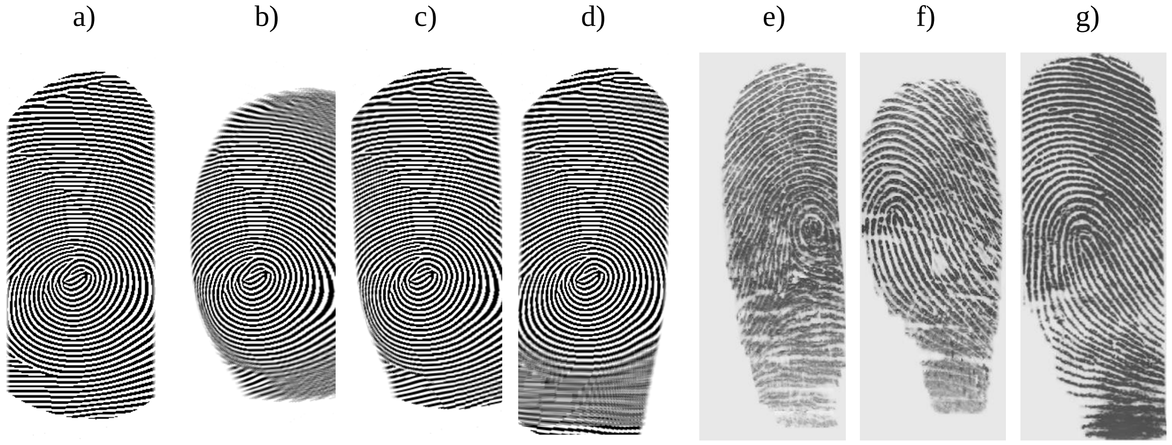

Figure 5.9: Examples of skin distortion damage (a – original, b, c, d – damaged, e, f, g – real).

5.5 Evaluation

The first part of the evaluation can be found in the previous subchapters. It was done by describing the solution and its similarities with real applications and also by comparing damaged images with real ones. However, in order to quantify how much damage was done to the synthetic fingerprints, it is necessary to find out the quality of them. Several methods for quality determination are used. Even before that, however, it is necessary to present the testing database. All available synthetic generators were used to generate testing databases. This database has 150 synthetic images: 60 from SFinGe [30], 60 from Anguli [31], and 30 from SyFDaS. Fingerprints were used in the state of master fingerprint.

Quality measurement is the second step of verifying the results. The premise is simple; damaged fingerprints should be of lower quality than original images. Three different measurement methods are used here. The first one is the *NEUROtechnology VeriFinger* – it is commercial software used primarily for fingerprint recognition, however, a part of the algorithm quality is also determined. This quality measurement and comparison score are used. The second method is from the National Institute of Standards and Technology (NIST) called *NFIQ* (NIST Fingerprint Image Quality). This algorithm is the only standard used for quality measurement. The last method used is the algorithm of quality measurement designed by Mr. *Oravec* [49].

Evaluation is structured to all basic options (as described in Subchapter 5.4.) and then to extreme damages (the most damaging combinations of basic options). There are graphs that show the minimal value for all fingerprint images, the maximal value (red dots), and the median (shown as black dash). It is important to note that damage which has the worst score (closer to minimal quality) has done a higher damage to an image, thus is treated as the best damage.

Example images and more information about **pressure and moisture** damages can be found in Subchapter 5.4. Figure 5.10 shows results in the comparison score. An enormous gap between *no damage* and damaged images can be seen. The lowest values for the median are practically the same for *pm0* (all low), *pm1* (extreme), and *pm3* (low to high to low) – the exact numbers being 1005.5, 1009, and 1007.5, respectively. By the minimal score values it can be declared that *pm1* is the best in this metric. Both damages with high pressure (*pm2* – high to low and *pm6* – slowly high to low) have shown bad results in the comparison score. Generally, the best results are achieved by *pm0* (all low), *pm1* (extreme), and *pm2* (high to low). For most of the metrics, there is a substantial difference between *no damage* and damaged images, which is another proof of verification.

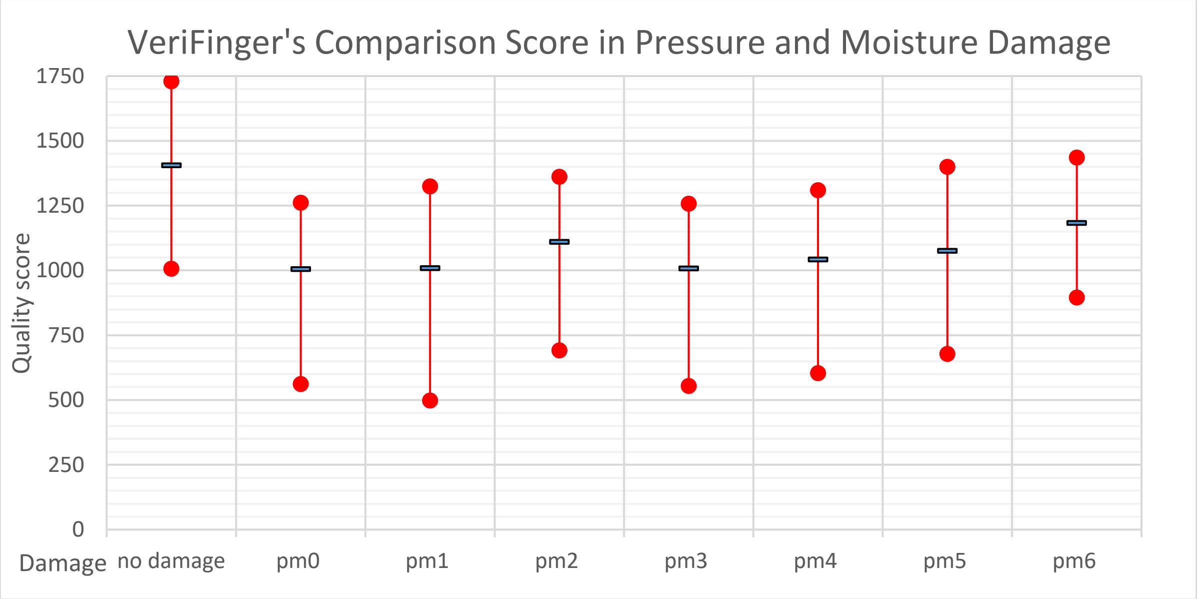

Figure 5.10: Graph of VeriFinger's comparison score in pressure and moisture damage (narrow).

Example images and more information about **sensor damage** and **skin distortion** can be found in Subchapter 5.4. Similar to previous subchapters, the focus is on the best damage. In Figure 5.11 VeriFinger's comparison score (with the exception of *no damage*) sorted damages from the best to the worst (from left to right). *Dis0* (extreme) shows all basic damages with the worst results. The clear winner of the best damage in this category is the *dis0* (extreme). Since this distortion was prepared as extreme, this result is not a big surprise. On the other hand, pressure damage and the edge parts of distortion look similar. This suggests that it is the rotation of minutiae points, which made this damage so much worse. From the damaged sensor category, the better one would probably be *dmg0* (long), but only narrowly. To sum up, all damages have lower results than the images without damage. It is close in some metrics, but the difference is there.

Narrow damage is very interesting to examine. Deleting part of the image means deleting some of the minutiae points, which should immediately result in a worse quality score. There are 11 basic damages in this category, which means that there are two graphs (part 1 and 2) instead of only one. Nevertheless, graphs are shown one after another and the results are discussed together. Images and more information about specific damages are in Subchapter 5.4. The best damages by the comparison score (Figure 5.12 and Figure 5.13) are *narr4* (side zigzags), *narr7* (tip bottom standard), and *narr1* (all sideways steady) in this order. *Narr4* has the lowest median score (barely), *narr7* has the lowest minimal score, and *narr1* is very close to these values. There are not any damages that would be better than the *no damage*. This is probably because in the comparison score information about the missing minutiae points in the edges of the damaged images is available. Thus, this small area reduction is influencing the score. *Narr4* is the only damage that could directly damage the fingerprint core. That is a crucial point not only because of its importance for fingerprint classification, but also because there is usually the highest density of minutiae points. *Narr1* presumably has the biggest area cut, but that is heavily dependent on the exact location of the fingerprint.

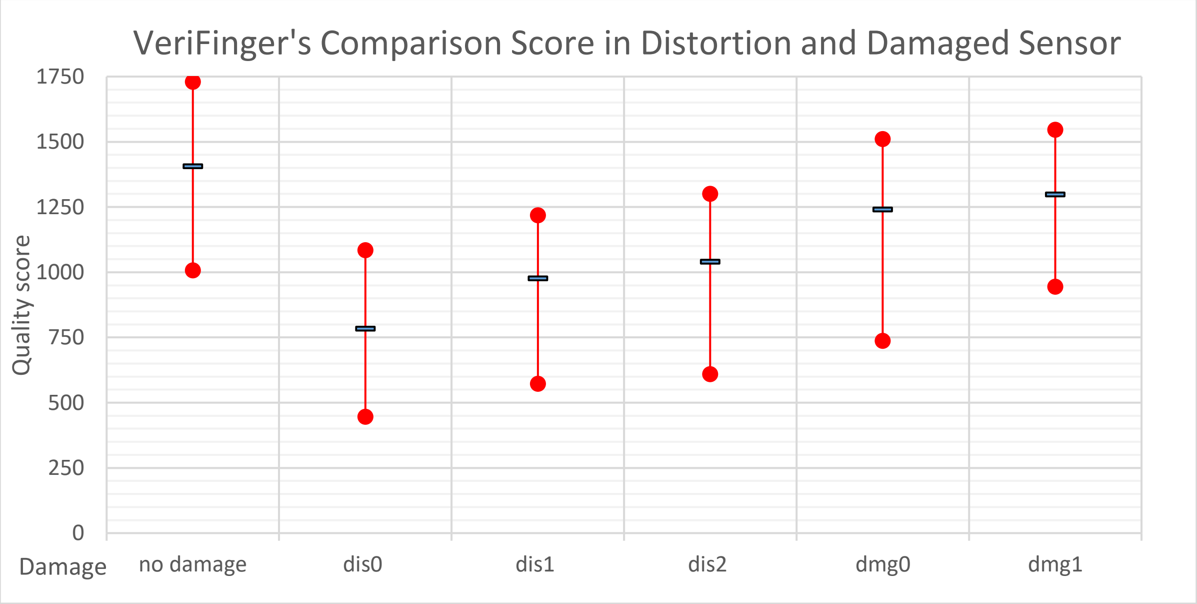

Figure 5.11: Graph of VeriFinger's comparison score in distortion and damaged sensor (narrow).

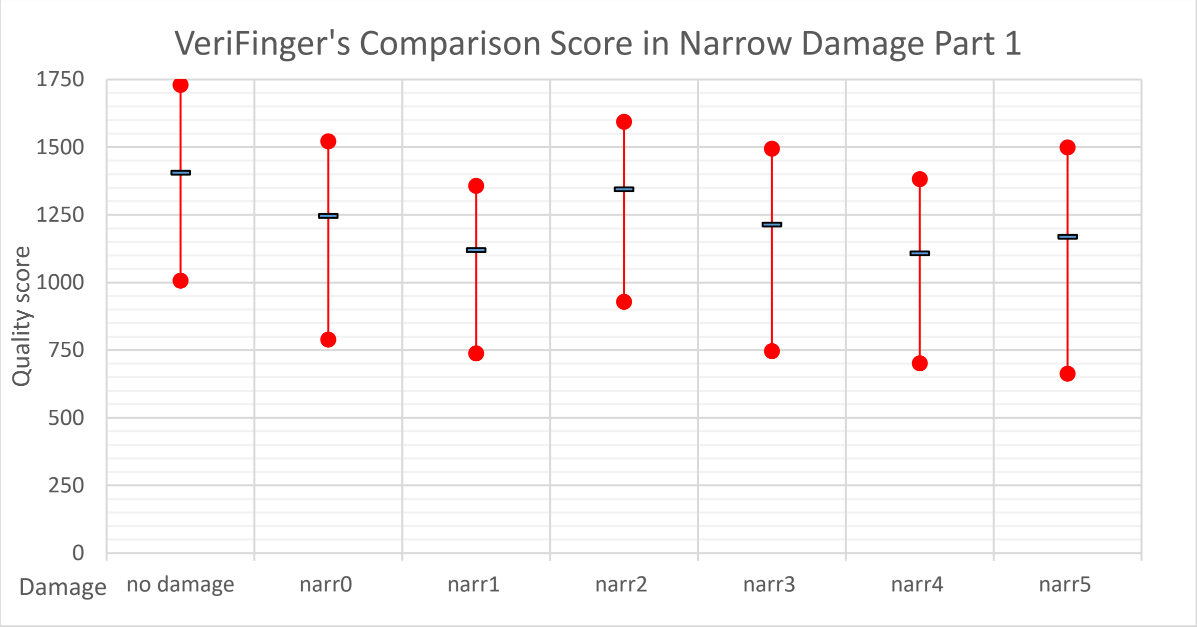

Figure 5.12: Graph of VeriFinger's comparison score in narrow damage – part 1 (narrow).

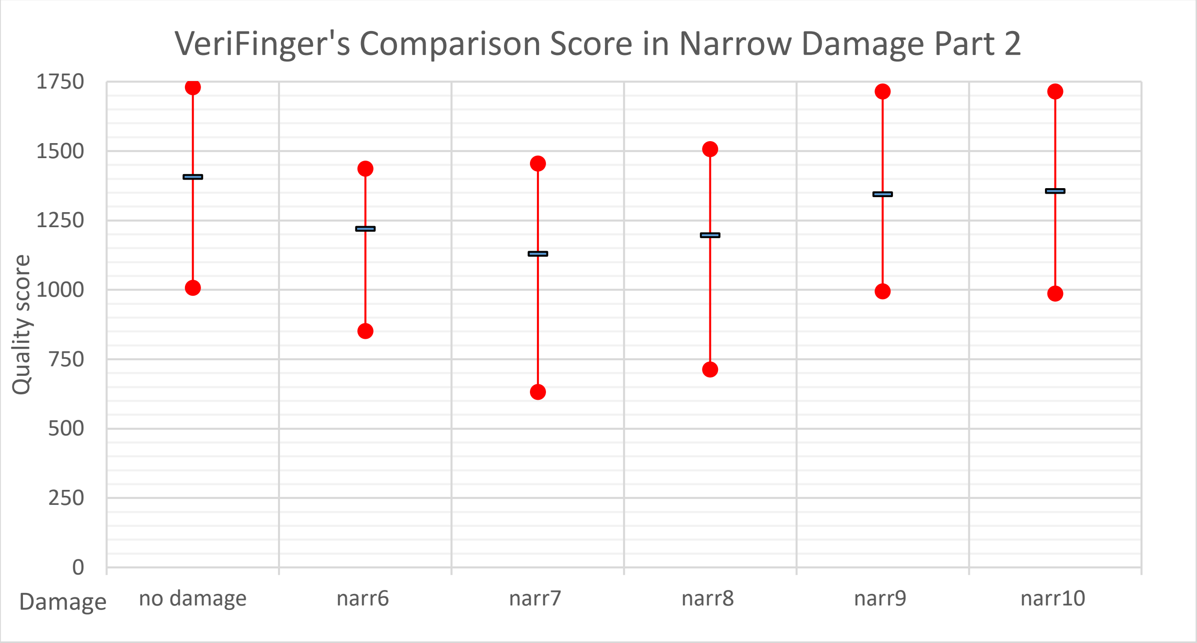

Figure 5.13: Graph of VeriFinger's comparison score in narrow damage – part 2 (narrow).

The database generated for the evaluation was composed of basic damages and also from the combinations of these damages (**extreme damages**). Restricted combination settings were used (for more information see Subchapter 4.2.4). This resulted in 1,152 combinations. From Subchapter 5.5 it is known that there were 150 source images in the database. 150 image – each has 1,152 impressions, which gives 172,800 images in total. This subchapter picks the seven best damage combinations to evaluate. **Pm2 dis0 narr4 dmg1** Figure 5.14b, **Pm2 dis0 narr4 dmg0** Figure 5.14c, **Pm2 dis0 narr1 dmg1** Figure 5.14d, **Pm1 dis0 narr4 dmg1** Figure 5.14e, **Pm2 dis0 narr5 dmg0** Figure 5.14f, **Pm2 dis0 narr8 dmg0** Figure 5.14g, **Pm2 dis0 narr1 dmg0:** Figure 5.14h.

The top 3 in the comparison score (Figure 5.15) are “*pm2 dis0 narr4 dmg0*” followed by “*pm2 dis0 narr4 dmg1*” and “*pm1 dis0 narr4 dmg1*”. Based on the occurrences of damages in the chosen combinations it is certain that *dis0* is the most important (it appears in all combinations); the second in that regard is *pm2* (in all but one). On the contrary, *dmg0* and *dmg1* are doing some damage, but because they are evenly spread they are not so important. In the case of a narrow category, it could be said that *narr4* and *narr1* are better than others, but perhaps not so much. Basically, if the best of the individual damages are combined they create one of the most damaging combinations. There are, of course, different weights for each damage category. Some damages which were not so good individually could excel in combinations, but there is no specific combination that would cooperate so well to make the result vastly better then looking at parts of that combination.

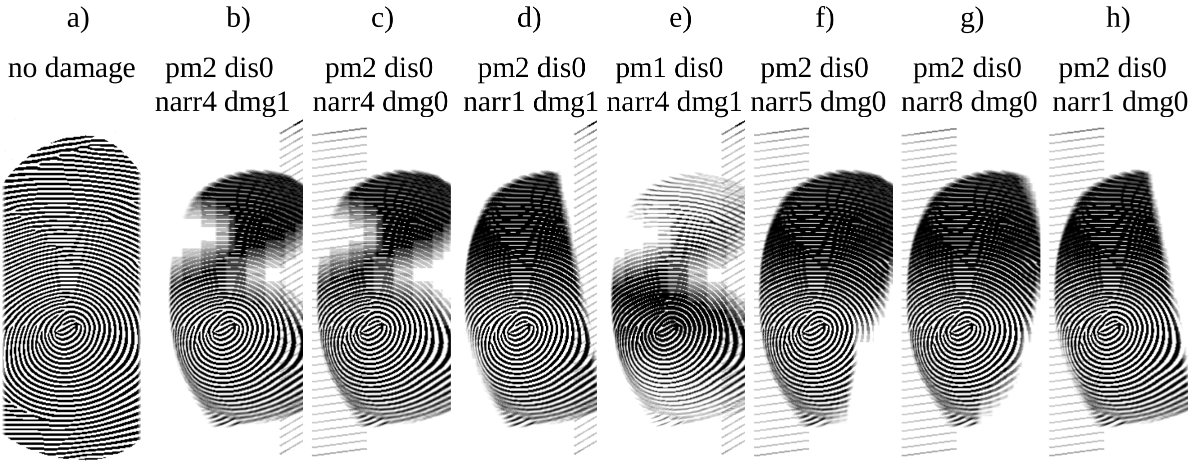

Figure 5.14: Examples of extreme damages in narrow width images.

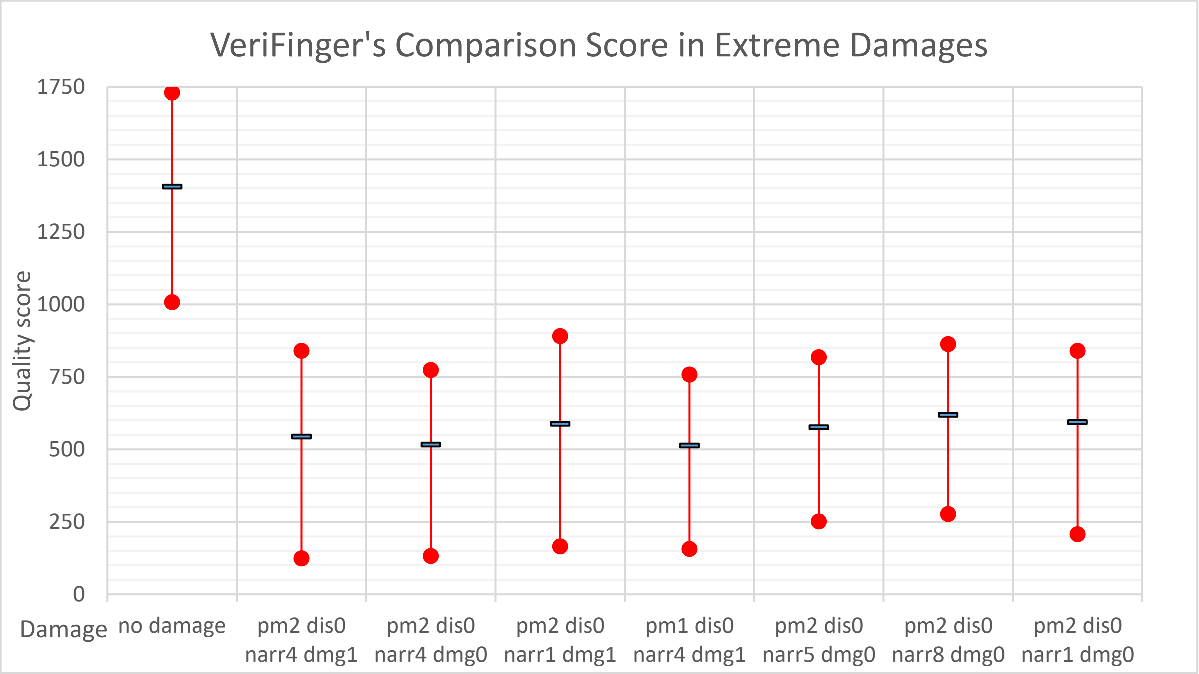

Figure 5.15: Graph of VeriFinger’s comparison score in extreme damages (narrow).

6 Skin Disease Simulation

The skin is the largest organ in the body, having a surface area of 1.8 m^2 and making up to 12-15 % of an adult's total body weight. It consists of three layers (see Figure 3.1) [50]: the *epidermis* (the outer layer), *dermis* („true skin") and *subcutaneous* (fatty) layer. Structure and thickness of the skin vary by site (e.g. thick epidermis on palms and soles due to mechanical protection – up to 1.4 mm). The first category of diseases that influence fingerprints are diseases causing **histopathological changes of the epidermis and dermis**. These diseases usually cause problems for all kinds of fingerprint sensors, because they can influence either the colour or internal structure of the skin. The second group are diseases that cause **skin discoloration**. These diseases may cause problems for optical fingerprint sensors and also for sensors that use a fingerprint liveness detection checks based on the colour or spectral analysis of the human skin [13]. The third and final category consists of diseases that cause **histopathological changes in the junction of the epidermis and dermis**. These diseases could cause structure changes underneath the skin in the junction between the dermis and epidermis – i.e. in the area from which ultrasonic fingerprint sensors acquire fingerprint pattern images. [10] [11] [14] [15] [43]

6.1 Database of Fingerprints with Skin Diseases

It is rather difficult to get a fingerprint database with skin-diseased users along with information about their disease. The creation of this type of database is even harder because of the cooperation required of technicians, medical doctors, and patients. On the other hand, there is no other reasonable method of testing how recognition algorithms can cope with skin diseases. The workspace which was sent to several institutions to acquire fingerprints contains a three-dimensional touchless and touch optical sensor, a swipe and touch capacitive sensor, and a digital microscope. Some institutions also acquired fingerprints using a dactyloscopic card. Each image in the database has anonymized information about the patient, severity, and type of disease. [14] [15] [42] [43] [51] [52]

6.1.1 Database Analysis

The raw, diseased fingerprint database was first analysed in order to provide a solid foundation for future research. For every disease, common signs among all fingerprint images affected by this disease were found, and a general description of each disease and its influences were defined. By observing and comparing the fingerprint images, 12 common features were defined and seven of them are local features [51]: *straight lines* (SL), *grid* (G), *small ridges disruptions* (SRD), *small "cheetah" spots* (CS), *larger round/oblong spots* (ROS), *large irregular spots* (IS) and *dark places* (DP). The other five are global image patterns [51]: *blurriness of (parts of) the image* (B), *significantly high contrast of the image* (HC), *the entire fingerprint area affected* (EA), *total deformation of the fingerprint image* (TD), and *significantly high-quality and healthy fingerprint* (HQ). [43] [51] [53]

6.2 Directly Simulated Diseases

To create the impression of fingerprints having a skin disease it is necessary to implement an algorithm that is designed to damage the master fingerprint and make it look like the fingerprint from a diseased finger. The first method is to base the algorithm on the findings from Subchapter 6.1.1. That means simulating the seven local and five global markings that can be found on the diseased fingerprints. After that, the damage done to a fingerprint with these markings is based on the **probabilistic distribution** of markings in the specific diseases. The second method for creating algorithms that will damage the fingerprints is based on **study of the diseases** one by one. By conducting a thorough analysis of a specific type of damage a unique algorithm can be created. There could even be a few algorithms based on, for example, disease severity. Sometimes the effects of diseases are difficult to generalize. In that case, it might be enough to **adapt damage from the existing** fingerprint images to a synthetic one. This subchapter focuses on the algorithms based on the second approach.

6.2.1 Verruca Vulgaris (Warts)

The first skin disease chosen for simulation are warts, specifically common warts (verruca vulgaris). The disease is described in detail (adapted mainly from [54] [55] [56]). Warts are caused by the human papillomavirus (HPV), which belongs to a group of papovaviruses. Common warts are the most-spread variant of warts (affecting approximately 10 % of the population [57]) and usually cause frustration on the part of the patient. Common warts are usually located on the hands, favouring the fingers and palms. Lesions range in size from pinpoint to more than 1 cm, most averaging about 5 mm. They grow in size for weeks to months and are usually present as elevated, rounded papules with a rough, greyish surface. In some instances, a single wart (mother wart) appears and grows slowly for a long time, and then suddenly many new warts erupt. The database contains fingerprint images acquired by various methods and sensors. To study the possible differences between images acquired by different sensors, three fingerprints of the same finger affected by warts have been chosen (see Figure 6.1). In Figure 6.1ab, it can be seen that the wart is located just on top of the whorl. It is a white oval with an irregular border. Inside the oval are black dots. The ridge structure is completely disrupted by the wart. However, the ridge flow continues normally around the border of the wart. Figure 6.18c, acquired by the UPEK sensor, cuts the wart out of the image completely. [10] [11] [55] [56] [58]

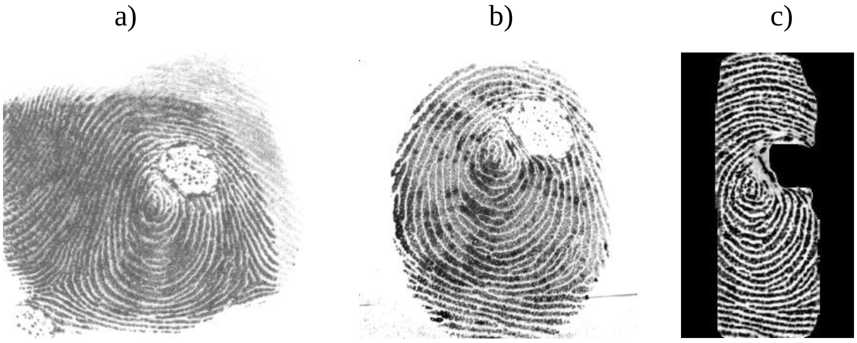

Figure 6.1: Same fingerprint affected by warts acquired by a) dactyloscopic card, b) Sagem MSO 300 and c) UPEK Eikon II.

Based on the analysis of the existing fingerprints with warts, a design of a method of disease simulation is proposed. The algorithm consists of the following steps:

1. Localise the fingerprint area in the image.
2. Determine the new wart size and locate its centre point on the fingerprint.
3. Draw the wart into an image buffer.
    a. Create an empty image buffer.
    b. Generate a number of small circles around the centre point of the wart.
    c. Draw the generated circles into the buffer.
    d. Draw dark dots inside the wart.
    e. Determine the final colour of each wart pixel.
    f. Blur the wart in the buffer
4. Draw the wart from the image buffer into the fingerprint image.
5. Generate possible secondary warts.

Five different settings of warts were simulated. Real images of warts can be seen in Figure 6.1, images with generated impressions in Figure 6.2. **Small warts with no secondary warts (warts0)** Figure 6.2a, **Small warts with up to two secondary warts (warts1)** Figure 6.2bc, **Large warts with no secondary warts (warts2)** Figure 6.2d, **Large warts with up to two secondary warts (warts3)** Figure 6.2ef, **Extreme (warts4)** Figure 6.2gh.

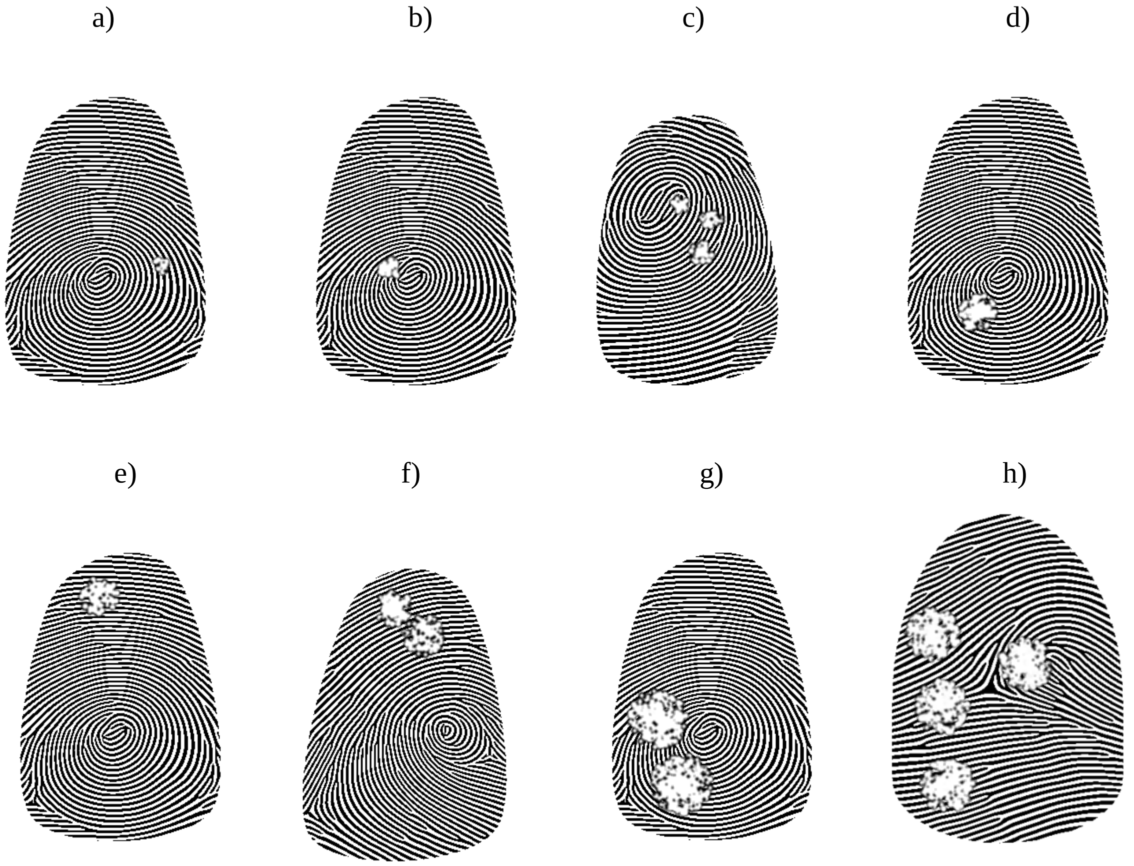

Figure 6.2: Examples of warts damage (a) warts0, b) c) warts1, d) warts2, e) f) warts3, g h) warts4).

6.2.2 Atopic Dermatitis

The second chosen skin disease is atopic dermatitis (also known as atopic eczema). In the following subchapters, this disease is described in detail with a focus on hand eczema (adapted from [54] [55] [56]). Atopic dermatitis [54] is a chronic, inflammatory skin disease that is characterized by pruritus and a chronic course of exacerbations and remissions. As in the case of wart-affected fingerprints, in order to study the differences between the images acquired by different sensors, three fingerprint images of the same finger have been selected (see Figure 6.3). [10] [11] [55] [56] [58] [59]

The comparison of the three images shows no significant difference in the quality among them. Abnormal white lines can be seen on all three of them, as well as patches of light and dark colours. Light patches are located mainly on the outer parts of the fingerprint, while dark areas are concentrated mostly in the centre of the fingerprint. [55] [56]

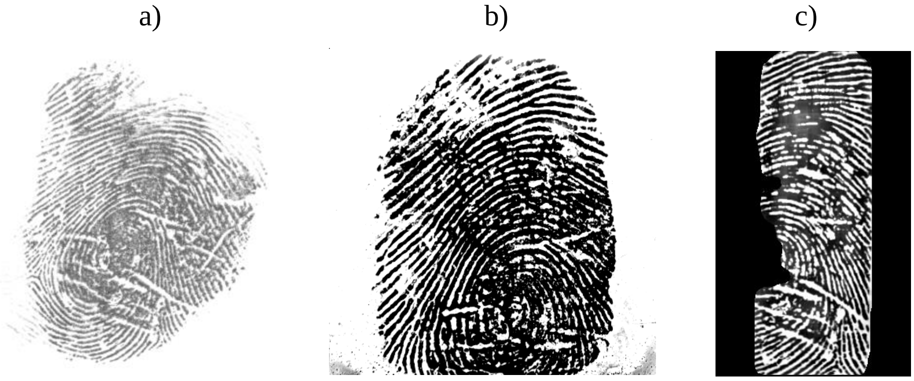

Figure 6.3: Same fingerprint affected by atopic dermatitis acquired by different sensors – a) dactyloscopic card, b) Sagem MSO 300 and c) UPEK Eikon II.

Based on the analysis of existing fingerprints affected by atopic eczema, the design of a method for generating similarly damaged synthetic fingerprint images is proposed in this section. The algorithm consists of the following steps: [55]

1. Localise the fingerprint area on the image.
2. Create an empty image buffer.
3. Draw eczema patches into a buffer.
    a. Determine the centre and size of the patch.
    b. Draw the patch of the determined type (light or dark).
4. Determine the final colour of each pixel of the patches.
5. Blur the patches in the image buffer.
6. Draw eczema white lines into the buffer.
    a. Determine the starting point, direction, and length of the line.
    b. Generate line points in the given direction and length.
    c. Interpolate the generated line points.
    d. Draw the lines in the determined thickness.
7. Blur the lines in the image buffer.
8. Draw the buffer into the fingerprint image.

Nine different settings of atopic dermatitis have been simulated. **Few horizontal lines only (eczem0)** Figure 6.4a, **A lot of horizontal lines only (eczem1)** Figure 6.4b, **Few vertical lines only (eczem2)** Figure 6.4c, **A lot of vertical lines only (eczem3)** Figure 6.5a, **Horizontal and vertical lines only (eczem4)** Figure 6.5b, **Horizontal and vertical lines, half thickness (eczem5)** Figure 6.5c, **Small number of patches only (eczem6)** Figure 6.6a, **High number of patches only (eczem7)** Figure 6.6b, **All factors together (eczem8)** Figure 6.6c.

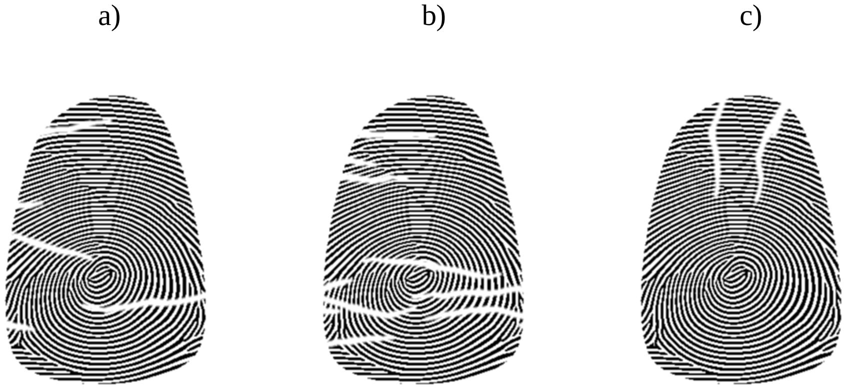

Figure 6.4: Examples of atopic dermatitis disease damage (a) eczem0, b) eczem1, c) eczem2).

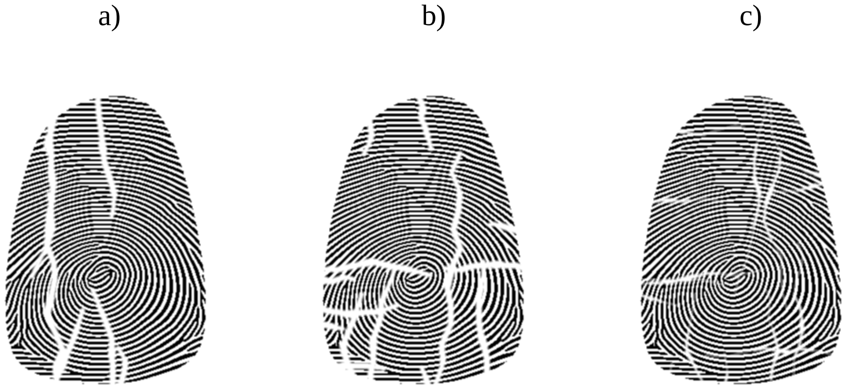

Figure 6.5: Examples of atopic dermatitis disease damage (a) eczem3, b) eczem4, c) eczem5).

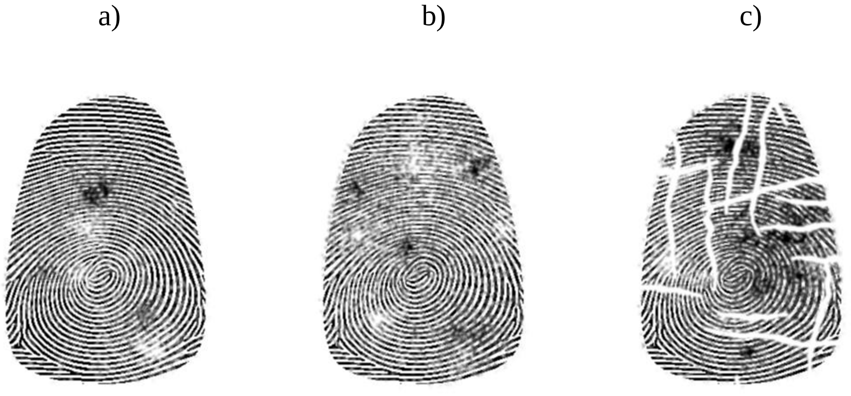

Figure 6.6: Examples of atopic dermatitis disease damage (a) eczem6, b) eczem7, c) eczem8).

6.3 Simulation Based on Learning from Diseased Images

As stated in Subchapter 6.2, some diseases are hard to describe and have very different effects based on disease severity. It would be obvious to use some neural network or machine-learning methods for their simulation. On the other hand, as stated in Subchapter 6.1, it is really difficult to get diseased fingerprint images. The database used is not big enough to utilize these kinds of methods (e.g. deep neural networks). Nevertheless, the core idea of these methods could still be used.

6.3.1 Psoriasis

To test this concept, psoriasis was chosen as a sample disease. It is the second most frequent disease in the database. Also, it is one of the most frequent skin diseases. Around 2-3 % of the population suffers from this disease. Psoriasis is caused by a failure of the immune system. It is too active, so skin cells are created not in 28-30 days, but in three to four days. The body is not prepared for such an influx of cells, so the old cells are accumulated on the skin's surface as a result. Itchy, silver flakes known as plaque are created. The more severe the disease is, the more plaque is created and the more the fingerprint is damaged. Unlike other disease simulations, there is no need of a deep description of individual damages done to a fingerprint. Anyway, in Figure 6.7 the images acquired by the dactyloscopic card are shown. [10] [11] [58] [60] [61]

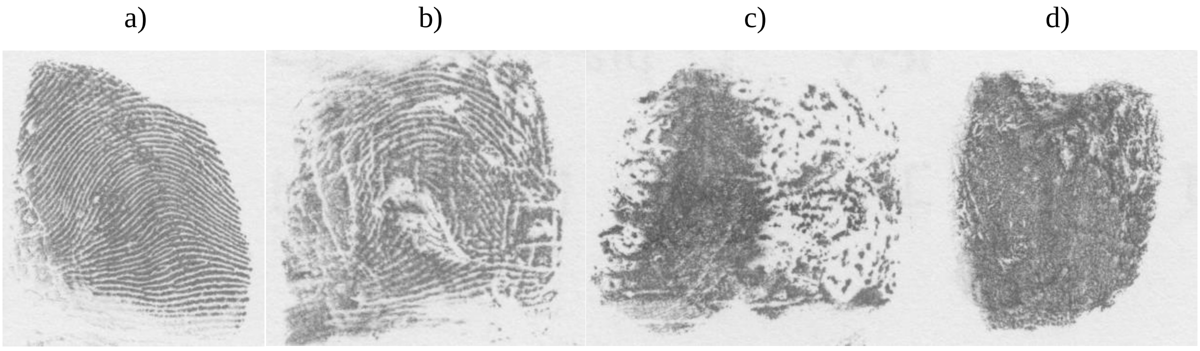

Figure 6.7: Different fingerprints affected by psoriasis acquired by dactyloscopic card.

Based on the described details of the disease, the idea of an algorithm for the damage extraction from existing images can be designed. For the simpler processing of input images, only one of the acquirement methods was chosen. The chosen method is the dactyloscopic card (as can be seen on Figure 6.7). Algorithm consists of the following steps:

1. Load an input (real) image.
2. Detection, extraction, processing, and storage of subjects (Figure 6.8) from the image.
3. Repeat steps 1-3 until there are no input images.
4. Load the synthetic image.
5. Localize the fingerprint area.
6. Load the damage subject.

7. Insert subject into the image.
8. Until there is a defined number of subjects in the image, repeat step 6-8.

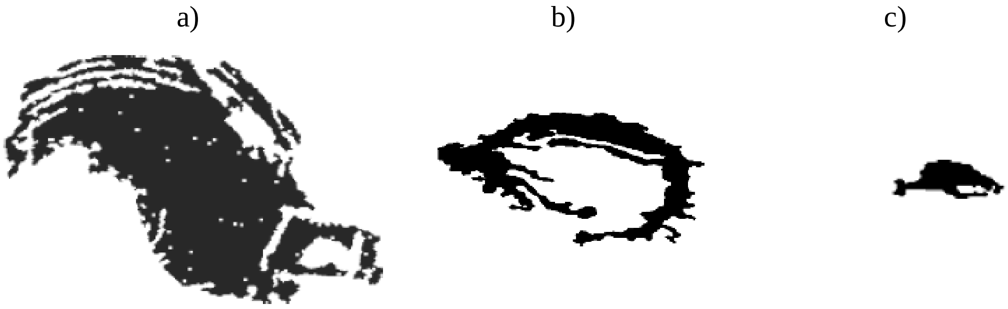

Figure 6.8: Enlarged and coloured subjects - a) black, b) large white, c) small white.

In this case, six different settings of psoriasis are simulated. The real images of psoriasis can be seen in Figure 6.7, generated impressions in Figure 6.9. **Small number of subjects (psor0)** Figure 6.9a, **Small number of subjects plus one black subject (psor1)** Figure 6.9b, **Small number of subjects plus two black subjects (psor2)** Figure 6.9c, **Moderate number of subjects plus three black subjects (psor3)** Figure 6.9d, **High number of subjects plus three black subjects (psor4)** Figure 6.9e, **Enormous number of subjects plus four black and one larger white subject (psor5)** Figure 6.9f.

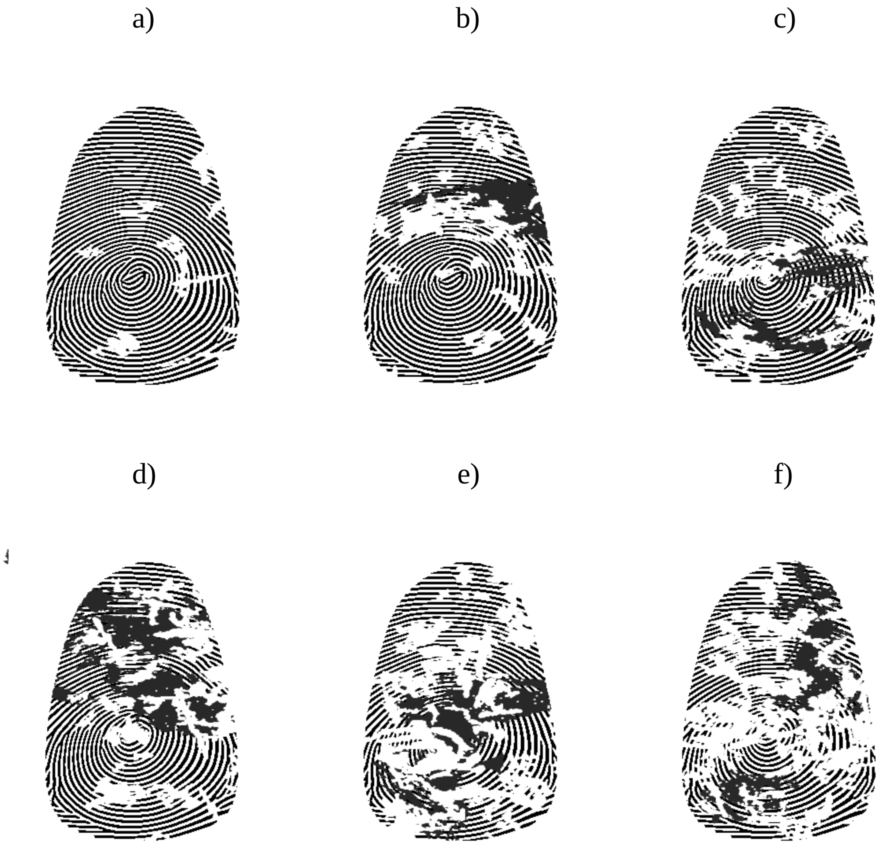

Figure 6.9: Examples of psoriasis damage (a) psor0, b) psor1, c) psor2, d) psor3, e) psor4, f) psor5).

6.4 Evaluation

Introduction to the evaluation process is the same as it was in Subchapter 5.5. The only difference is that only basic damages are evaluated. The first part of the evaluation process can be found in the previous subchapters. That is a visual comparison of the damaged fingerprint images and source fingerprint images with skin diseases. To ensure that not only the images look similar to real one, but that they really resemble the image of the disease, they were also discussed with doctors. Methodologies and some example images were consulted with a dermatologist.

Information about the specifics of the **warts damage** and example images can be found in Subchapter 6.2.1. It is possible to place the wart on different spots which could have an effect on the final score. This graph (Figure 6.10) is a nice presentation of random effect evaluation. There is a stable reduction in median quality score based on the severity of the damage. However, the minimal and maximal values are scattered. *Warts4* (extreme) confirmed the role of the best damage. In conclusion, all damages have the same or lower quality scores than the reference damage.

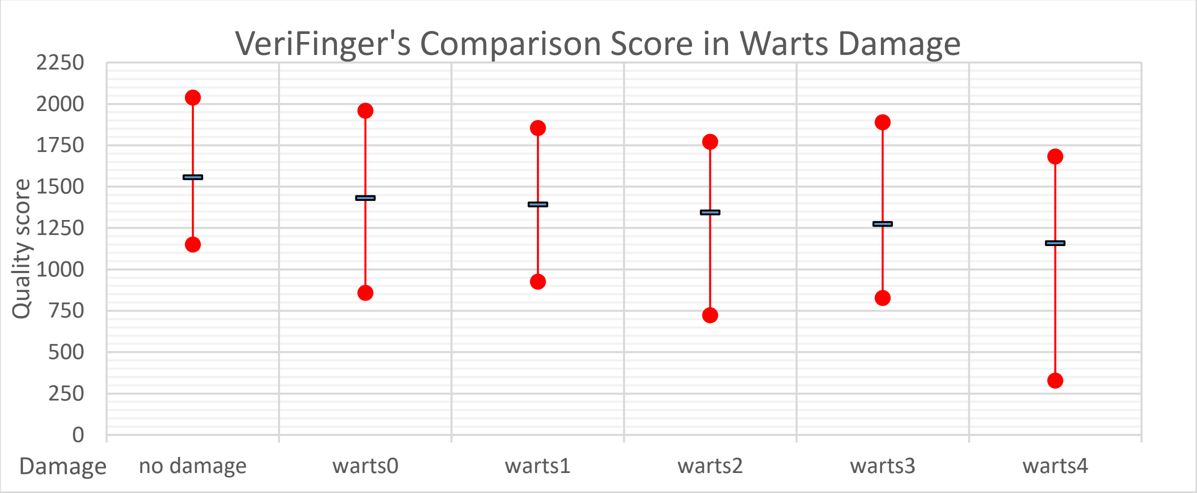

Figure 6.10: Graph of VeriFinger's comparison score in warts damage.

The structure of the **atopic eczema damage** is a little bit different than the other damages. The last damage (*eczem8*) combines all previous damages. All this information and example images are in Subchapter 6.2.2. Algorithms that create these damages have some parts that are stochastic. For example, in one fingerprint it could randomly damage the core with a lot of minutiae, but in another fingerprint it could randomly damage only a marginal. The system of damage composition can be clearly seen in Figure 6.11 and Figure 6.12. First, the median reduction *eczem4* (horizontal and vertical lines only), combines previously tested horizontal (*eczem0* and *eczem1*) and vertical (*eczem2* and *eczem3*) lines. Second, a high reduction in quality is to be expected in *eczem8* (all factors together) because it combines the previous damages. This also means that lines and spots are posing different damages to the images, so their quality reduction can be almost added together.

Detailed information and example images for the **psoriasis damage** category are described in Subchapter 6.3.1. The severity of the damage should be sorted out (the higher number in the damage shortcut should mean more severe damage). The choice and position of generated subjects are stochastic, so again, a little bit of volatility in maximal and minimal values can be excepted. Figure 6.13 shows a clear quality trend. Nevertheless, the extreme minimal value for the *psor1* (small number of subjects plus one black subject) can be seen. In the comparison with the swipe mode, the *psor2* is on a par with the best swipe mode damage. *Psor3*, *psor4*, and *psor5* being the most damaging variants.

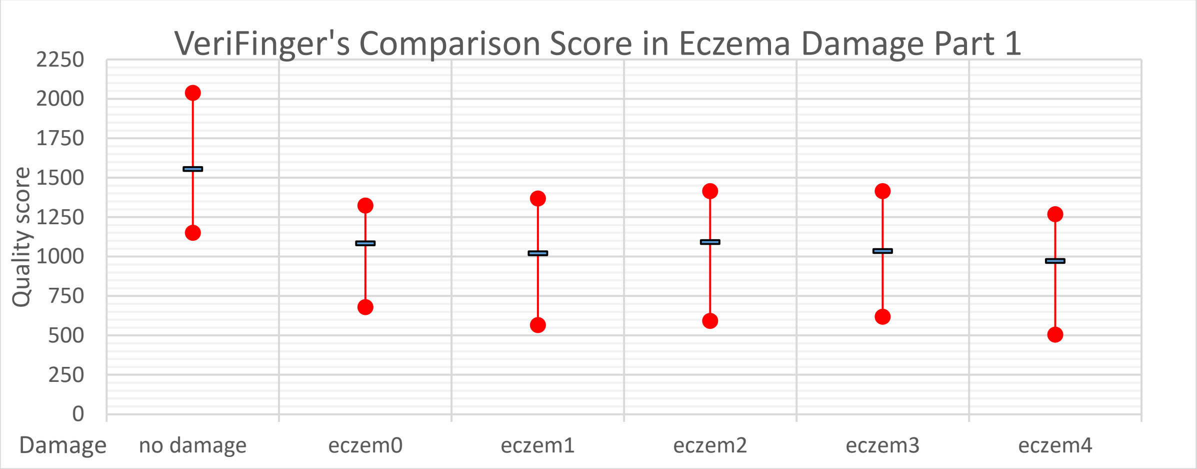

Figure 6.11: Graph of VeriFinger's comparison score in atopic eczema damage – part 1.

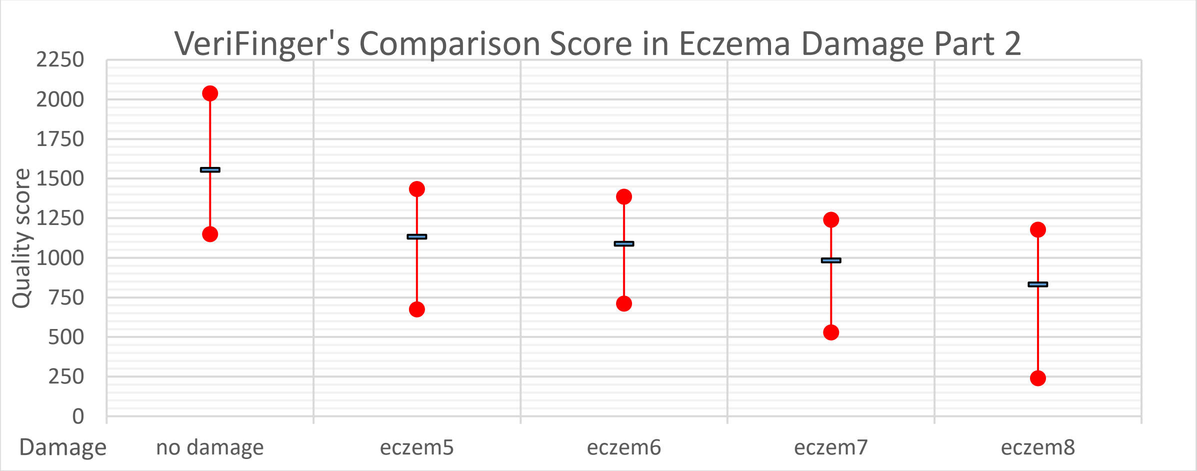

Figure 6.12: Graph of VeriFinger's comparison score in atopic eczema damage – part 2.

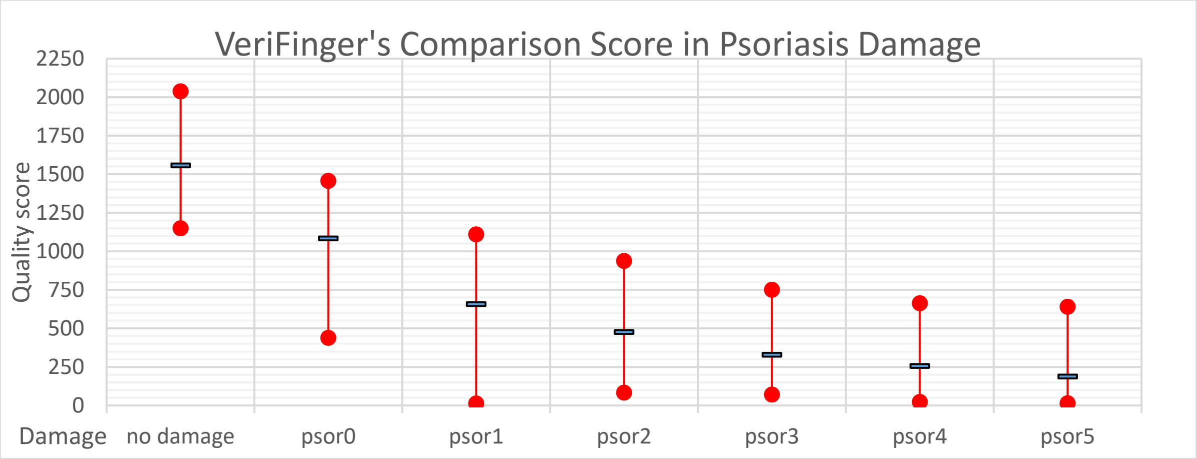

Figure 6.13: Graph of VeriFinger's comparison score in psoriasis damage.

7 Other Inspected Damages

Other researched areas are described in this chapter. Theoretically, any damage from any source can be simulated to the synthetic fingerprints. The simulation of a fingerprint spoof and the simulation of factors caused by the use of everyday detergents or lotions are described in this chapter. The exact influence on the fingerprint is determined and following that, a consideration of them as a possible extension of the application is described. In the scope of (other) specific damages, interesting work on altered fingerprints is shown in [62].

The simulations of factors that are specific for **fingerprint spoofs** can be useful in recognizing these spoofs directly from the fingerprint image they produce. First, however, a database of images to analyse the damage done to the fingerprint is required. In the following images and experiments, a PCB mould is used. With the prepared mould (using source fingerprint image), the only missing thing is the material from which the spoof will be created. Materials can be divided into three groups: **Technical industry:** aquarium silicon (black and transparent), epoxy resin kit for Epoxy CHS 1200, epoxy resin "Havel Composite L285", and epoxy resin "HobbyKing". **Food industry:** gelatine, aspic, and gummy bears. **Creative materials:** Fimo standard, Fimo air, Kera, WePAM, Oyumare, Play-Doh, Premo, glass colours, Cernit, gel wax, Kato, Siligum, latex, and wax sheets. When the material is in the required shape, i.e. it is dry, it supposedly perfectly fills the mould, then it is taken out and a fingerprint spoof is done. [42] [63] [64]

Fingerprint spoofs generally have a lower quality than real fingerprints, and these flaws in quality could be simulated as fingerprint damage done by using a spoof fingerprint. A couple examples of these flaws are: **air bubbles** in the material, **broken ridges** in the edge of the fingerprint, and **imperfect edges** of the fingerprint. Some of these imperfections can be avoided by the thorough creation of a mould and fingerprints spoofs, but some materials make creation of a fingerprint spoof without flaws almost impossible. There are several flaws described in the literature [65]: background noise, overall shape, clear external contours, missing sections, unreal distortion, unexpected appearance (residue from spoof material), air bubbles, absence of sweat pores, narrow valleys, and reproducible artefacts. Nevertheless, the difference between the damages of real, damaged fingerprint and an almost perfect spoof is a very difficult task. There are some software-based liveness detection systems (more recently called "presentation attack detection systems" [66] [67]). In summary, it was determined not to simulate this type of damage. There is some promising research going on regarding presentation attack detection using user-specific effects [68].

The last part describes fingerprints influenced by **detergents and lotions** used in everyday life. There are situations where the users are forced to clean their hands. On the contrary, it is really common that the user has unclean hands. The situation when a user is going through a fingerprint access device after washing their hands or using hand lotion can be very common as well as the situation when a user is unlocking his or her mobile phone or laptop, utilizing fingerprint technology with a polluted hand. Only a small preliminary database was acquired. Damage can be very specific, which can lead to either a specific simulation or to adapting the damages from the database. Overall, this is a promising area of future research. [43]

8 Conclusion

This extended abstract thesis covers the state-of-the-art techniques of fingerprint acquirement and recognition. What has also been described are the methods of generating a synthetic fingerprint and fingerprint reconstruction. This description was focused on the SFinGe generator and its methods. All of the phenomena that can supposedly damage the image of a fingerprint created by a biometric device are listed. Based on this information, a Fingerprint Generation Petri net was created. The SyFDaS application that was implemented follows the Fingerprint Generation Petri net. It contains a fingerprint generator and a damage simulator in a clear GUI, which is suitable for expansion. There are described algorithms for database generation, for basic damage simulations – a damaged sensor, pressure and moisture, and fingerprint distortion and for advanced damage simulations – a swipe mode, a narrow sensor, warts, an atopic dermatitis, and psoriasis.

The core of this extended abstract of doctoral thesis is the discussion of the phenomena that are specific to swipe sensors, skin diseases, and other interesting damages. A thorough analysis of the phenomena specific to swipe sensors are shown in two categories. The first category consists of the phenomena that are directly specific to these sensors, i.e. a narrow acquired fingerprint and a long fingerprint. The second category focuses on phenomena that are common to touch sensors but have to be simulated differently with a swipe sensor. The main idea is that the swipe sensor can be divided into small segments of a touch sensor that are merged together. Damage simulations have to be done for each segment with the acknowledgement that the input data of these simulations have to be similar and then merged together.

Skin diseases can be a big problem when using widespread biometric systems. The systems that are currently used are not capable of detecting skin diseases or enhancing the quality of fingerprints with diseases, which basically makes the biometric system unsuitable for some users. The main reason is that it is very difficult to obtain access to a database of fingerprints with skin diseases. The available database of skin diseases that influences fingerprints has been analysed. Skin diseases and an algorithm for their detection has also been proposed. The several possibilities regarding how to simulate the damage done by skin diseases to fingerprints is also described. The first possibility is to directly simulate the effects of a disease. Warts and atopic dermatitis are examples of this approach. A more thorough description of these diseases is given and algorithms to simulate them are proposed. The second possibility is to use machine learning or neural networks. An algorithm to simulate psoriasis is an example of using this method.

The last area of interest is fingerprint spoofing and detergents. The methods for the production of fingerprint spoofs have been described. Various materials which can and were used to produce spoofs have been analysed. The possible damages made when producing fingerprint spoof were discussed, and the next category deals with the effects of detergents or lotions on fingerprints. The preliminary database needed for research in this area is described.

As an input, there were 300 undamaged synthetic fingerprints (from three generators and in two width variants), 20 basic damages from diseases, and 1,151 basic and combined damages in swipe sensors used. Overall, 348,300 different damaged synthetic fingerprint images were generated. All of the 43 basic damages were visually checked and compared with real images with respective damage. Reference fingerprints with no damage and all 1,171 damages were verified using four different quality measurement methods (VeriFinger's quality score, VeriFinger's comparison score, NFIQ, and Oravec's quality metric). All damages have their median scores lower than the respective scores of the reference images. The best of the damage was extreme psoriasis damage (*psor5*), which has its average median scores only 38 % of the reference scores.

These results show that fingerprint images were successfully damaged. The generated database and all of the results can immediately be used for the analysis of quality measurements methods as well as for the creation of new methods for quality estimation. The size of the database (and the possibility to generate new data if needed) allows for the use of machine learning or neural networks to assist with this task. Fingerprint image enhancement methods could be analysed and their limitation could be found through a generated database. For both of these tasks there is the possibility to define new instances of damage (by changing the input values for the desired damage type, or in the case of swipe sensor simulation by giving different inputs to merging algorithms). There are a great number of possibilities in the area of public education regarding synthetic images and their damaged impressions. One of the reasons is that there is not a risk of revealing a person's identity with the exemplary images shown. Images mainly focused on diseases could be used for educating forensic experts and dermatologists. The achieved results are a stepping stone for other areas of research.

Future work can be focused on several areas. The first of them being the extension of simulated damages. Different diseases can be simulated (the probabilistic method could be used), some damages in swipe sensor simulation could also be done (the second phalange, faults of reconstruction algorithm, another approach on the merge algorithm), and generally some new damages can be simulated like the effects of sensor technology (or the background of the images in general), motion blur made by non-cooperative behaviour and effects of detergents, lotions, and other everyday products.

The second area of the future research could deal with synthetic images for the development of new algorithms or the enhancement of existing ones. Examples could be the development of the detection and extraction of the damaged regions in fingerprint images, the reconstruction and enhancement of quality in these damaged regions, or "only" the recognition and evaluation of severity of these damages. Created database of images could be used for this purpose right now, but it would be even better to have a precise annotation of the damage done to images (which is possible with the damage simulation done to perfect images). All these algorithms together could expand the usability of fingerprint recognition in general.

The final area of research could focus on using machine learning and neural networks. These approaches require a huge database as an input, but if these input images are provided they would show incredible results. A synthetic database is great for this. On the other hand, there is a risk of overfitting these synthetic damages (a method will then detect only synthetic damages and not generalized ones). Nevertheless, machine learning and neural networks could be used to address the problems mentioned in the second area. In addition, the method for presentation attack detection as an optional part of fingerprint image enhancement could be imagined with synthetic images damaged to look like spoofs, thus avoiding the question whether it is more important to detect a spoof or to enhance the quality of an image.

In summary, the theoretical description of fingerprint acquirement, recognition, synthetic generation, skin diseases, and other damages was given and a practical solution to synthetic fingerprint damage simulation (and generation) with a focus on swipe mode, narrow sensor, damaged sensor, pressure/moisture, fingerprint distortion, warts, atopic dermatitis and psoriasis was also described. A lot of damages were proposed, all of which were verified to inflict the assumed damage to the fingerprint image. New and interesting areas for future research were proposed, some of which are very promising and can be researched with some additional work. Other areas, however, can now be explored with the presented results.

Bibliography

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

[2] Lai, K.K., Kanich, O., Dvořák, M., Drahanský, M., Yanushkevich, S.N., Shmerko, V.P., *Biometric-Enabled Watchlists Technology*, IET Biometrics, 2017, p. 10, ISSN: 2047-4938.

[3] Li S.Z., Jain A.K.: *Encyclopedia of Biometrics*. Springer, 2015, p. 1651. DOI 10.1007/978-1-4899-7488-4.

[4] International Organization for Standardization: *International standard ISO/IEC 2382-37:2017 Information technology – Vocabulary – Part 37: Biometrics*. ISO/IEC JTC 1/SC 37 Biometrics, 2017, p. 27.

[5] Drahanský M., Orság F., Doležel M. et al.: *Biometrie (Biometrics)*. Computer Press a.s., 2011, p. 294. ISBN 978-80-254-8979-6.

[6] Maltoni D., Maio D., Jain A.K. et al.: *Handbook of Fingerprint Recognition*. Springer, 2009, p. 512. ISBN 978-1-8488-2254-2.

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

[8] Kanich O., Drahanský M.: *State of the Art in Fingerprint Recognition*. Hand-based Biometrics: Methods and Technologies, IET, 2018, p. 28. ISBN 978-1-78561-224-4.

[9] Chaloupka R.: *Generátor Otisků Prstů (Fingerprint Generator)*. Master's thesis FIT BUT, 2007, p. 47

[10] Březinová E.: *Outer Hand Physiology and Diseases*. Hand-based Biometrics: Methods and Technologies, IET, 2018, p. 26. ISBN 978-1-78561-224-4.

[11] Štork J. et al.: *Dermatovenerologie (Dermatovenerology)*. Galén, 2013, p. 502. ISBN 9788072628988.

[12] U.S. Department of Justice: *The Fingerprint Sourcebook*. CreateSpace Independent Publishing Platform, 2014, p. 428. ISBN 978-1502828422.

[13] Drahanský M., Kanich O., Březinová E. et al.: *Experiments with Optical Properties of Skin on Fingers*. International Journal of Optics and Applications, 2017, pp. 37-46. DOI 10.5923/j.optics.20160602.03.

[14] Drahanský M., Kanich O., Březinová E.: *Is Fingerprint Recognition Really so Reliable and Secure?*. Challenges for fingerprint recognition – spoofing, skin diseases and environmental

effects, Handbook of Biometrics for Forensic Science, Springer, 2017, p. 21. ISBN 978-3-319-50671-5.

[15] Drahanský M., Kanich O., Pernický R. et al.: *Verarbeitung von beschädigten Fingerabdrücken in der polizeilichen Praxis*. Datenschutz und Datensicherheit, Springer, 2017, pp. 407-414. ISSN 1614-0702, DOI 10.1007/s11623-017-0803-2.

[16] Federal Bureau of Investigation: *Integrated Automated Fingerprint Identification System – Web page* [online]. 2014. [cit. 2014-5-21]. Available online: http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis.

[17] Drahanský M.: *Biometric Systems* [online]. Course at the FIT BUT, 2017. [cit. 2017-7-28] Available online: http://www.fit.vutbr.cz/study/courses/BIO/.

[18] Cappelli R., Maltoni D.: *On the Spatial Distribution of Fingerprint Singularities*. IEEE Transactions on Pattern Analysis and Machine Intelligence, IEEE, 2009, pp. 742-748. DOI 10.1109/TPAMI.2008.243.

[19] Rak R., Matyáš V., Říha Z. et al.: *Biometrie a identita člověka (Biometrics and Person's Identity)*. Grada, 2008, p. 664. ISBN 978-80-247-2365-5.

[20] Du R.W., Yang C., Kou C.I.: *System for Fingerprint Image Reconstruction Based on Motion Estimate Across a Narrow Fingerprint Sensor*. U.S. Patent US7212658B2, 2004, p. 25.

[21] Ratha N.K., Govindaraju V.: *Advances in Biometrics: Sensors, Algorithms and Systems*. Springer, 2008, p. 503. ISBN 978-1-84628-920-0.

[22] O'Gorman L., Xia X.: *Method and System for Capturing Fingerprints from Multiple Swipe*. U.S. Patent US0123714A1, 2003, p. 20.

[23] Chou B.C.S.: *Sweep-type fingerprint sensors module*. U.S. Patent US7200250B2, 2007, p. 11.

[24] Xia X., O'Gorman L.: *Innovations in Fingerprint Capture Devices*. Pattern Recognition, Elsevier, 2003, pp. 361-369. DOI 10.1016/S0031-3203(02)00036-5.

[25] Mardiansyah A.Z., Bejo A., Hidayat R.: *Fingerprint Image Reconstruction for Swipe Sensor Using Predictive Overlap Method*. MATEC – the 2nd International Conference on Engineering and Technology for Sustainable Development, 2018, p. 4. DOI 10.1051/matecconf/201815401042.

[26] Kanich O., Drahanský M.: *Currently Used Swipe Fingerprint Sensors*. International Journal of Bio-Science and Bio-Technology, SERSC, 2016, pp. 381-386. ISSN: 2233-7849.

[27] Cappelli R., Ferrara M., Maltoni D.: *Minutiae-Based Fingerprint Matching*. Cross Disciplinary Biometric Systems, Intelligent Systems Reference Library, Springer, 2012, pp. 117-150. DOI 10.1007/978-3-642-28457-1_7.

[28] Yanushkevich S.N.: *Synthetic Biometrics: A Survey*. The 2006 IEEE International Joint Conference on Neural Network Proceedings, IEEE, 2006, pp. 676-683. DOI 10.1109/IJCNN.2006.246749.

[29] Zhao Q., Jain A.K., Paulter N.G. et al.: *Fingerprint Image Synthesis Based on Statistical Feature Models*. 2012 IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS), IEEE, 2012, pp. 23-30. ISBN 978-14-673-1384-1.

[30] Cappelli R.: *SFinGe: An Approach to Synthetic Fingerprint Generation*. In BT 2004 – International Workshop on Biometric Technologies, 2004, pp. 147-154.

[31] Ansari A.H.: *Generation and Storage of Large Synthetic Fingerprint Database*. Master's thesis Indian Institute of Science, 2011, p. 47.

[32] Feng J., Jain A.K.: *Fingerprint Reconstruction: From Minutiae to Phase*. IEEE Transactions on Pattern Analysis and Machine Intelligence, IEEE, 2010, pp. 209-223. ISSN 0162-8828, DOI 10.1109/TPAMI.2010.77.

[33] Kücken M., Newell A.C.: *A Model for Fingerprint Formation*. European Physical Society, EPL (Europhysics Letters), 2004, pp. 141-146. DOI 10.1209/epl/i2004-10161-2.

[34] Kanich O., Drahanský M.: *Simulation of Synthetic Fingerprint Generation Using Petri Nets*. IET Biometrics, IET, 2017, p. 17. ISSN 2047-4938, DOI 10.1049/iet-bmt.2016.0041.

[35] Cappelli R., Ferrara M., Maltoni D.: *Generating Synthetic Fingerprints*. Hand-based Biometrics: Methods and Technologies, IET, 2018, p. 24. ISBN 978-1-78561-224-4.

[36] Galbally J., Cappelli R., Lumini A. et al.: *Fake Fingertip Generation from a Minutiae Template*. 19th International Conference on Pattern Recognition, IEEE, 2008, p. 4. DOI 10.1109/ICPR.2008.4761456.

[37] Cappelli R., Maio D., Lumini A. et al.: *Fingerprint Image Reconstruction from Standard Templates*. IEEE Transactions on Pattern Analysis and Machine Intelligence, IEEE, 2007, pp. 1489-1503. DOI 10.1109/TPAMI.2007.1087.

[38] Feng J., Jain A.K., Ross A.: *Fingerprint Alteration*. MSU Technical Report, MSU-CSE-09-30, 2009, p. 13.

[39] Mihaiu A-I.: *Changes in the Papillary Structure (I)*. Romanian Journal of Forensic Science, Romanian Society of Legal Medicine, 2012, pp. 1148-1158. ISSN 2069-2617.

[40] Vinoth A., Saravanakumar S.: *An Analysis of Altered Fingerprint Detection, Recognition and Verification*. International Journal of Computer Science and Mobile Computing, 2006, pp. 178-182. ISSN 2320-088X.

[41] Tuč D.: *Testing of the Environmental Influences on Fingerprints Sensors*. Bachelor's project FIT BUT, 2005, p. 63.

[42] Drahanský M., Kanich O.: *Vulnerabilities of Biometric Systems*. Security and Protection of Information 2015, 2015, pp. 53-60. ISBN 978-80-7231-997-8.

[43] Heidari M., Kanich O., Drahanský M.: *Processing of Fingerprints Influenced by Skin Diseases*. Hand-based Biometrics: Methods and Technologies, IET, 2018, p. 34. ISBN 978-1-78561-224-4.

[44] Alessandroni A., Cappelli R., Ferrara M. et al.: *Definition of Fingerprint Scanner Image Quality Specifications by Operational Quality*. Biometrics and Identity Management, Springer, 2008, pp. 29-36. DOI 10.1007/978-3-540-89991-4_4.

[45] Reisig W.: *Understanding Petri Nets*. Springer-Verlag, 2013, p. 230. ISBN 978-3-642-3327-7.

[46] Gonzalez R.C., Woods R.E.: *Digital Image Processing (3rd Edition)*. Prentice Hall, 2008, p. 954. ISBN 978-0-1316-8728-8.

[47] Singh S., Murshed N., Kropatsch W.: *Modelling Plastic Distortion in Fingerprint Images*. Second International Conference on Advances in Pattern Recognition (ICAPR2001), Springer, 2001, pp. 369-376. ISBN 978-3-540-41767-2, DOI 10.1007/3-540-44732-6_38.

[48] Mainguet J.F.: *Fingerprint-reading System*. U.S. Patent US6459804B2, 1996, p. 11.

[49] Oravec T.: *Methodology of Fingerprint Image Quality Measurement*. Master’s thesis FIT BUT, 2018, p. 55.

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

[51] Barotová Š.: *Detector of Skin Diseases by Fingerprint Technology*. Bachelor’s thesis FIT BUT, 2017, p. 50.

[52] Doležel M., Drahanský M., Urbánek J. et al.: *Influence of Skin Diseases on Fingerprint Quality and Recognition*. New Trends and Developments in Biometrics, IntechOpen, 2012, pp. 275-303. DOI 10.5772/51992.

[53] Barotová Š., Drahanský M., Pernický R.: *Detection of Ridge Damages in Fingerprint Recognition Caused By Skin Diseases*. International Journal of Signal Processing, SERSC, 2016, pp. 125–146. DOI 10.14257/ijsip.2016.9.11.13.

[54] James W.D., Berger T.G., Elston D.M.: *Andrews‘ Diseases of the Skin Clinical Dermatology (10th Edition)*. Elsevier, 2006, p. 691. ISBN 0-7216-2921-0.

[55] Bárta M.: *Generation of Skin Disease into the Synthetic Fingerprints*. Master’s thesis FIT BUT, 2016, p. 60.

[56] Bárta M., Drahanský M.: *Generation of Skin Diseases into Synthetic Fingerprints*. International Journal of Image Processing, CSC Journals, 2016, pp. 229-248. ISSN 1985-2304.

[57] Schellhaas U., Gerber W., Hammes S. et al.: *Pulsed Dye Laser Treatment Is Effective in the Treatment of Recalcitrant Viral Warts*. Dermatologic surgery, 2008, pp. 67-72. ISSN 1076-0512.

[58] Khanna N., Singh S.: *Bhutani's Color Atlas of Dermatology*. Jaypee Brothers Medical Publishers (P) Ltd., 2015, p. 498. ISBN 978-93-5152-302-4.

[59] Ring J., Alomar A., Bieber T. et al.: *Guidelines for Treatment of Atopic Eczema (Atopic Dermatitis) Part I*. Journal of the European Academy of Dermatology and Venereology, 2012, pp. 1045-1060. ISSN 0926-9959.

[60] Košťák D.: *Generation of Skin Disease Effects into Synthetic Fingerprints from Anguli Generator*. Bachelor's thesis FIT BUT, 2018, p. 44.

[61] Kerkhof van de P.C.M.: *Textbook of Psoriasis*. Blackwell Publishing Ltd., 2003, p. 348. ISBN 1-4051-0717-0.

[62] Papi S., Ferrara M., Maltoni D. et al.: *On the Generation of Synthetic Fingerprint Alterations*. 2016 International Conference of the Biometrics Special Interest Group (BIOSIG), IEEE, 2016, p. 6. DOI 10.1109/BIOSIG.2016.7736930.

[63] Spurný J., Doležel M., Kanich O. et al.: *New materials for spoofing touch-based fingerprint scanners*. Proceedings of International Conference on Computer Application Technologies 2015, 2015, p. 15. ISBN 978-1-4673-8211-3

[64] Drahanský M., Kanich O., Dvořák M.: *Spoofing methods in hand-based biometrics*. Hand-based Biometrics: Methods and Technologies, IET, 2018, p. 32. ISBN 978-1-78561-224-4.

[65] Champod C., Espinoza M.: *Forgeries of Fingerprints in Forensic Science*. Handbook of Biometrics Anti-Spoofing, Springer, 2014, pp. 13-34. ISBN 978-1-4471-6523-1.

[66] Schuckers S.: *Presentations and Attacks, and Spoofs, Oh My*. Image and Vision Computing, Elsevier, 2016, pp. 26-30. DOI 10.1016/j.imavis.2016.03.016.

[67] Ghiani L., Yambay D., Mura V. et al.: *LivDet 2013 Fingerprint Liveness Detection Competition 2013*. 2013 International Conference on Biometrics (ICB), IEEE, 2013, p. 6. ISBN 978-1-4799-0310-8, DOI 10.1109/ICB.2013.6613027.

[68] Ghiani L., Marcialis G.L., Roli F.: *Fingerprint Presentation Attacks Detection Based on the User-specific Effect*. 2017 IEEE International Joint Conference on Biometrics, IEEE, 2017, p. 7. DOI 10.1109/BTAS.2017.8272717.

europass Curriculum vitae

PERSONAL INFORMATION

Ondřej Kanich

K Trati 765, 73934 Šenov (Czech Republic)

WORK EXPERIENCE

04/08/2014–Present

Simulation of manufacturing systems

Taurid, Ostrava (Czech Republic)

Simulation of production systems and lines

Optimization of production systems

01/07/2010–Present

Supervisor of hiking club

ATOM Klubka 19216, Šenov (Czech Republic)

Supervision of children

Preparation of games and program

Obtaining supplies for expeditions and camps

EDUCATION AND TRAINING

27/06/2014–Present

EQF level 8

Brno University of Technology - Faculty of Information Technology, Brno (Czech Republic)

Ph.D. student

12/06/2012–26/06/2014

Master's degree in Intelligent systems

EQF level 7

Brno University of Technology - Faculty of Information Technology, Brno (Czech Republic)

24/04/2016–26/06/2016

Research internship in Canada

University of Calgary, Calgary, Alberta (Canada)

Research on risk assessment of biometric sensors at the airport

PERSONAL SKILLS

Mother tongue(s)

Czech

Foreign language(s)

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken interaction	Spoken production	
English	C1	C1	B2	C1	C1
	First certificate of English (FCE) B2				
Spanish	A1	A2	A1	A1	A1
Polish	A2	A2	A1	A1	A1

Levels: A1 and A2: Basic user - B1 and B2: Independent user - C1 and C2: Proficient user
Common European Framework of Reference for Languages

Communication skills

Good communication skills gained by supervising hiking club

Regular communication with students in several courses

Organisational / managerial skills

Decent skills in team-leading gained in hiking club and by leading master's , bachelor thesis and group projects in Biometrics course.

Digital skills

Good knowledge of office software (text processor, spreadsheet, presentation software)

Good knowledge of programming languages (C#, C++, C)

Basic knowledge of operation systems Microsoft Windows (10, 7 - certification Microsoft® Certified Technology Specialist: Windows 7, Configuration)

Advanced knowledge of Siemens Plant Simulation software and SimTalk language

Basic knowledge of programming languages (Python, Prolog, Haskell, Lisp, JASON)

ADDITIONAL INFORMATION

Certifications

Participation in 12th and 15th Summer School for Advanced Studies on Biometrics (2015 and 2018).

Publications

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.

Spurný J., Doležel, M., Kanich, O., Drahanský, M., Shinoda, K.: *New materials for spoofing touch-based fingerprint scanners*, Proceedings of International Conference on Computer Application Technologies 2015. Matsue, p. 15. ISBN 978-1-4673-8211-3.

Drahanský, M., Kanich, O.: *Vulnerabilities of Biometric Systems*, Conference on Security and Protection of Information 2015. Brno, pp. 53-60. ISBN 978-80-7231-997-8.

Drahanský, M., Kanich, O., Březinová, E.: *Is fingerprint recognition really so reliable and secure?*, Challenges for fingerprint recognition – spoofing, skin diseases and environmental effects, Handbook of Biometrics for Forensic Science. Springer, p. 21, ISBN 978-3-319-50671-5.

Kanich, O., Drahanský, M.: *Currently Used Swipe Fingerprint Sensors*, International Journal of Bio-Science and Bio-Technology, 2016, pp. 381-386, ISSN: 2233-7849.

Drahanský, M., Kanich, O., Březinová, E., Shinoda, K.: *Experiments with Optical Properties of Skin on Fingers*, International Journal of Optics and Applications, 2017, pp. 37-46, DOI 10.5923/j.optics.20160602.03.

Kanich, O., Drahanský, M.: *Simulation of Synthetic Fingerprint Generation Using Petri Nets*, IET Biometrics, 2017, pages 17, ISSN: 2047-4938, DOI 10.1049/ietbmt.2016.0041.

Lai, K.K., Kanich, O., Dvořák, M., Drahanský, M., Yanushkevich, S.N., Shmerko, V.P., *Biometric-Enabled Watchlists Technology*, IET Biometrics, 2017, p. 10, ISSN: 2047-4938.

Drahanský, M., Pernický, R., Kanich, O., Barotová, Š.: *Verarbeitung von beschädigten Fingerabdrücken in der polizeilichen Praxis*, Datenschutz und Datensicherheit, 2017, ISSN: 1614-0702.

Kanich, O., Drahanský, M.: *State of the art in fingerprint recognition*, Hand-based Biometrics: Methods and Technologies, IET, 2018, p. 28, ISBN 978-1-78561-224-4.

Drahanský, M. Kanich, O., Dvořák, M.: *Spoofing methods in hand-based biometrics*, Hand-based Biometrics: Methods and Technologies, IET, 2018, p. 32, ISBN 978-1-78561-224-4.

Mona, H., Kanich, O., Drahanský, M.: *Processing of fingerprints influenced by skin diseases*, Hand-based Biometrics: Methods and Technologies, IET, 2018, p. 34, ISBN 978-1-78561-224-4.

Projects

New solutions for multimodal biometrics – enhancement of security and reliability of biometric technologies, COST LD14013 (CZ – 2014-2016).

Reliability and security in IT, FIT-S-14-2486 (CZ – 2014-2016).

IT4Innovations excellence in science, LQ1602 (CZ – 2016-2020).

Tools and methods for video and image processing to improve effectivity of rescue and security services operations, VI20172020068 (CZ – 2017-2020).

Secure and reliable computer systems, FIT-S-17-4014 (CZ – 2017-2019).

Modern and open engineering study, MOST, (EU – 2017-2022).

Others

Drahanský, M., Dvořák, R., Váňa, J., Goldmann, T., Dvořák, M., Kanich, O.: *A multispectral lifecycle detector especially suited for the fingerprint recognition technology* [Utility model], 2018.

Commenting of standard ISO/IEC: JTC 1/SC 37 N 6754 and JTC 1/SC 37 N 6756, 2018.

References

prof. RNDr. Pavel Danihelka, CSc. – VŠB – TUO, Faculty of Safety Engineering

prof. Ing., Dipl.-Ing. Martin Drahanský, Ph.D. – BUT in Brno, Faculty of Information Technology