
Interim Report for CPSC 601.20 Term Project:
“Fingerprint Spoofing”

Title:

Fingerprint Spoofing

Deadline:

November 5th, 2006

Author:

René Haahr Hemmingsen

Supervisor:

Dr. Marina Gavrilova

Number of pages: 21

Number of appendices: 0

Total number of pages: 21

Abstract:

This interim report begins by describing how fingerprint scanners work. The description includes an account for how current fingerprint scanners sense fingerprints as well as how various parameters such as resolution and pixel depth affect the resulting fingerprint image.

The second main part of this report deals with fingerprint spoofing techniques. A description of four different spoofing techniques from literature is given as well as a description of a technique proposed by the author.

In the last part of this report the planned experiments and tests are described.

With the underlying theory in place, future work will focus on: a) the actual experiments, and b) a brief survey of the techniques proposed to counter fingerprint spoofing.

René Haahr Hemmingsen

November 5th, 2006

Contents

1	Introduction	1
2	Fingerprint Scanners	3
2.1	Introduction	3
2.2	Fingerprint Images	4
2.2.1	Spatial Resolution	4
2.2.2	Pixel Resolution	5
2.2.3	Pixel Bit Depth	5
2.2.4	Geometric Accuracy	6
2.2.5	Signal-to-Noise Ratio	6
2.3	Live-Scan Technologies	6
2.3.1	Optical Sensors	7
2.3.2	Solid-State Sensors	9
2.3.3	Ultrasound Sensors	10
2.4	Live-Scan Acquisition Techniques	10
3	Fingerprint Spoofing	12
3.1	Duplication with Cooperation	12
3.1.1	The Free Molding Plastic Technique	12
3.1.2	The Plaster Technique	13
3.1.3	The Fingernail Polish Technique	14
3.2	Duplication without Cooperation	15
3.2.1	The Transparency Slide Technique	15
3.2.2	The Photo-Sensitive PCB Technique	16
4	Planned Experiments and Tests	17
4.1	Planned Experiments with Fingerprint Duplication	17
4.2	Planned Tests	17
5	Summary and Future Work	19

Chapter 1

Introduction

IT is playing a larger part in our everyday lives and the ubiquity of the Internet has grown to a point few would have foreseen. Further, events like 9/11 and other terrorist attacks in the western world, e.g., the bombings in London and Madrid, have made government agencies all over the world demand security improvements. These developments has brought forward a need for IT security and in particular a need for authentication. The question asked is if this person, server, or application is who it claims to be. The traditional way for humans to authenticate themselves is to use passwords or PINs. However, PINs and passwords can be disclosed to others, willingly or not, or they can be forgotten and have to be reset. If users get to choose they own passwords they are likely to choose ones that are easy to remember which most likely will also make it easier for the attacker to guess. Biometrics, on the other hand, seem to be able to mend these deficiencies. A biometric is something you *are*, thus, it cannot be lost, forgotten or divulged to others.

The current call for better and stronger security has generated a huge push towards biometrics with a lot of the attention being focused on fingerprint technologies. The interest in the area generated by multinational corporations and government agencies is colossal but is the technology really ready, i.e., will relying on fingerprint readers instead of passwords increase security? At the moment techniques such as password cracking, social engineering, etc. are common ways to try and break in to systems but is it really much harder to steal latent fingerprints and use those to fool the fingerprint reader? The problem is that even though fingerprints have a number of attractive properties compared to other biometrics, it does entail a few problems as well.

Above it was stated that biometrics: a) cannot be lost, b) cannot be forgotten, and c) cannot be divulged. That is not entirely true. With regards to fingerprints, for example, you can injure a finger damaging the epidermis or perhaps even lose the finger all together. Another and more serious problem with fingerprints is the fact that it *can* be divulged, both intentionally and unintentionally. People leave fingerprints where ever they go and these latent fingerprints can be used to fool fingerprint readers. This has been proven by several people, e.g., Putte and Keuning in [8] from 2001 and by Matsumoto et al. in [7], the now famous paper from 2002. In these papers, the authors proved that contemporary fingerprint readers could be easily fooled by dummy fingers and they were even able to develop dummy fingers from latent fingerprints that would also fool the test equipment. With that in mind, the current push towards replacing passwords with fingerprint readers seems like not such a good idea.

The object of this project is to find out whether fingerprint readers are still as easy to fool as shown by Matsumoto in 2002. In order to do that the project contains the following four main parts:

1. an in-depth study of how different types of fingerprint readers work in order to understand the technology,
2. a brief study of fingerprint spoofing and the techniques developed to illustrate the reality of the spoofing problem,
3. performing real-world experiments with the spoofing techniques described earlier to try and illustrate the current state of the publicly available fingerprint technology, and finally
4. a study of measures to mend the problem of fingerprint spoofing based on literature research and industry approaches.

These main parts will correspond to chapters in the final report. This interim report, however, only contains the two first parts, corresponding to Chapters 2 and 3, respectively. Furthermore, Chapter 4 contains a description of the planned experiments and tests. Finally, Chapter 5 summaries this interim report and outlines the future work.

All in all, the contents of this report is not overly technical. However, it does presuppose that the reader is familiar with the basics of fingerprint characteristics, i.e., ridge characteristics such as delta points etc. If not, [10], [6], or [3] might be good primers.

Chapter 2

Fingerprint Scanners

This chapter describes how fingerprint scanners work. The chapter begins with a brief introduction. Following this, Section 2.2 describes the properties of a fingerprint image and how these properties affect the quality of the image. Section 2.3 describes the different scanner technologies currently available and the following Section 2.4 brief outline two different scanning techniques.

The material presented in this chapter is mainly based on [10], [5], [6], and [2].

2.1 Introduction

The traditional method for fingerprint acquisition is the so-called ink-technique. This technique, dating back more than a century, requires that ink is equally applied to the subject's fingertip. The finger is then pressed—actually, it is rolled in a nail-to-nail fashion—against a paper card producing an imprint of the ridge pattern of the epidermis on the subject's fingertip. The emergence of computers eventually brought about the need for digitized storage of the fingerprints, thus, the manual acquisition process was extended to also include subsequent scanning of the ink-print cards to produce a digital image of the ink-print. This kind of process is referred to as *off-line* fingerprint acquisition.

With respect to biometrics the off-line technique described above has some inherent problems: a) it is a slow manual process, b) the inconvenience associated with inking the fingertips, and c) the stigma related to ink-prints due to the affiliation to law enforcement. To remedy these issues *live-scan* technologies were developed. The live-scan technologies rely on directly sens-

ing the fingerprint pattern using a type of electronic scanner thus rendering the use of ink superfluous.

Though originally designed for *automated fingerprint identification systems* (AFIS), the live-scan acquisition scanner technology have since made its way into the non-AFIS market. This development is mainly due to two factors. Firstly, the cost of the live-scan devices has dropped. According to [5], the cost of the live-scan capture devices fell more than one order of magnitude—from approximately \$1500 US to \$100 US—from the early to the late 1990s. Secondly, the size of the devices has also decreased to a point where it is now possible to incorporate scanning sensors in smart-cards etc. And this development is predicted to continue. According to the International Biometric Group the annual revenue of the biometric industry for 2006 is estimated to be 2,176 million US dollars and that figure is projected to climb to 5,749 by 2010 [4]. With fingerprint technology currently constituting 44% of the biometric market there is abundant impetus to fuel further advancements in scanner technology. According to [5], manufacturers promise that the cost of scanner devices will experience close to another order of magnitude decrease within the next few years

2.2 Fingerprint Images

In order to understand the parameters given when describing fingerprint scanners one needs to grasp some general properties of digital images, e.g., the *resolution* and the *dynamic range* of an image. These are described in the following subsections.

2.2.1 Spatial Resolution

In this context, the spatial resolution, generally just referred to as the *resolution*, describes the level of detail at which the scanner is capable of scanning a fingerprint. Here, the resolution is normally given in *dots per inch* (dpi) though using *samples per inch* (spi) would, arguably, be more correct. However, since the term dpi is so widely in biometrics literature it is also the terminology adopted by this report.

Since the dpi is a measure for how detailed the scanned image will be higher dpi is obviously better. Scanning a fingertip at 500 dpi instead of 300 dpi will thus produce an image with higher *pixel* resolution and therefore a higher level of detail. The minimum for scanners compliant with the specification issued by the *US Criminal Justice Information Services* (CJIS), which is a department within the FBI, is to scan at 500 dpi [2].

2.2.2 Pixel Resolution

The pixel resolution of an image refers to the number of pixels in the image. There are overall two ways to represent the pixel resolution. One way is to give the total number of pixels in the image represented as mega pixels. This is done by multiplying the image height in pixels with the image width in pixels divided by a million. This approach is commonly used in the field of digital cameras. In most other cases, the resolution of a digital image is represented as a set of two positive integers indicating the width and the height of the image, respectively.

As indicated in Section 2.2.1, the pixel resolution of an image is closely related to the spatial resolution of the scanner and the physical size of the area scanned. A scanner working at r dpi scanning an area of size $w \times h$ will output an image with pixel width and height equal to wr and hr , respectively. Therefore, a scanner with a scan area of 1 inch \times 1 inch, as is required by the CJIS specification (see Appendix G in [2]), and working at 500 dpi will result in an image with a resolution of 500×500 pixel.

2.2.3 Pixel Bit Depth

The pixel bit depth, or *dynamic range*, denotes the number of bits used to encode the intensity value of each bit. The higher the pixel depth is the higher is the number of colours it is possible to represent. However, since colour is not regarded useful for fingerprints, these are acquired using gray-scale images and the pixel bit depth thus determines how many levels of gray the resulting image contains. The CJIS specification requires that compliant scanners capture images with a pixel depth of 8 bit. Figure 2.1 depicts a 8, 6, 4, and 2 bit gray-scale image with 256, 64, 16, and 4, levels of gray, respectively.



Figure 2.1: Illustration of 8, 6, 4, and 2 pixel bit depth, respectively

According to [6], some contemporary fingerprint scanners actually only capture 2 or 3 bits of pixel depth information. Software is instead used to map the 2 or 3 bits into the 8 bits required. It is understood that a pixel depth of more than 1 bit is required, but according to [6] no definitive results

have been published documenting that recognition performance suffers when the pixel bit depth decreases.

2.2.4 Geometric Accuracy

The geometric accuracy is used to express the maximum distortion a fingerprint scanner is allowed to introduce and is usually given as a percentage with respect to the x and y directions. Due to the way most optical scanner devices are constructed these introduces a significant amount of distortion which must be compensated. The CJIS specification mandates that for compliant fingerprint images the maximum difference d between the actual distance x , between any two points on the finger, and the distance y , between the same two points on the output image of the given fingerprint, must conform to the following:

$$\begin{aligned}d &= 0.0007 \text{ inches} && \text{for } 0 \leq x \leq 0.07 \\d &= 0.01x \text{ inches} && \text{for } 0.07 < x < 1.5\end{aligned}$$

This means that the require positional accuracy is $\pm 1\%$ for distances between 0.07 and 1.5 inches (1.778mm and 38.1mm, respectively), and a constant ± 0.0007 inches (0.01778mm) for distances less than or equal to 0.07 inches. Given these requirements, compensating for even minor optical distortion is clearly paramount.

2.2.5 Signal-to-Noise Ratio

The signal-to-noise ration (S/N) is the ratio between a given transmitted signal and the background noise. The S/N is often used to qualify less tangible notions such a “good image quality” or “high image fidelity”. The CJIS mandates that the S/N for compliant devices is at least 125:1 [2].

2.3 Live-Scan Technologies

The most important element of a fingerprint scanner is the *sensor*. The sensor is the part of the scanner responsible for reading the surface of the fingertip. This analog information is then transformed into a digital fingerprint image using an analog-to-digital converter. According to [6], almost every fingerprint scanner currently available uses one of the following three sensor technologies: optical, solid-state, or ultrasound. In the following each of these technologies are described.

2.3.1 Optical Sensors

Optical sensors can be further subdivided into a number of different categories. Below is given a description of some of the optical technologies most commonly used.

Frustrated Total Internal Reflection (FTIR): FTIR is probably the most used optical sensor technology in use today and works by capturing light reflected of the ridge pattern on the epidermis. The process is illustrated in Figure 2.2. The term *total internal reflection* refers to

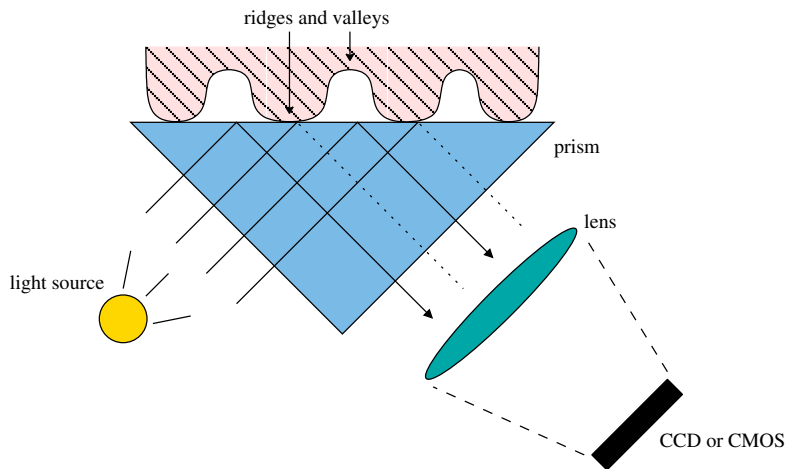


Figure 2.2: FTIR-based fingerprint sensing with an ordinary glass prism

an optical phenomenon that occurs when light is refracted, i.e., bent, at a medium boundary to a degree where it is sent backwards effectively reflecting all of the light.¹ *Frustrated* total internal reflection occurs when a medium—in this case the ridges on the epidermis—with a higher *refractive index* comes in contact with the surface of the glass prism. At this point light will leave the prism and be absorbed by the medium—in this case the ridge. In the valleys of the fingerprint, however, the light is refracted by the boundary of the glass prism. The resulting refracted light is then lead through a lens thus focusing it on either a CCD or CMOS image sensor. This creates an inverse image of

¹See <http://freespace.virgin.net/gareth.james/virtual/Optics/Refraction/refraction.html> for a very illustrative example of how light is refracted in glass and how the amount of light refracted is dependent on the angle at which it enters the glass.

the fingerprint where ridges are represented as dark areas (since they refract no light) and the valleys as bright areas.

One of the advantages of FTIR is that it senses a 3D-surface thus making it harder to fool it using a printed image of a fingerprint. A problem with the FTIR setup described above is that the prism imposes some constraints on how small this type of sensing devices can be. To mitigate this issue, an alternative approach has been introduced using a number of small prisms next to one another instead of a single large one. This allows the size of the mechanical assembly to be reduced somewhat, however, the resulting image will generally be of inferior quality when compared to traditional FTIR techniques [6].

Optical Fibers: This technique uses a fiber-optic platen instead of FTIR's prism and lens (see Figure 2.3). As shown in the figure the finger is in direct contact with the fiber-optic platen. The residual light from the ridges is conveyed through the optical fibers down onto the underlying CCD or CMOS. The compactness of this scheme makes it possible to

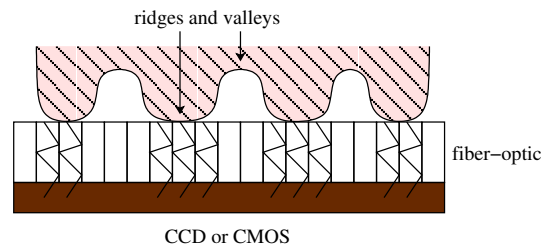


Figure 2.3: Fingerprint sensing based on optical fibers

build very thin sensing devices. However, because this technique does not use a lens to focus the light the CCD or CMOS sensors must be as big as the sensing area and since producing large sensors is costly and increases the chance of producing defective sensors this is a significant issue.

Direct Photograph: Perhaps the most obvious way to get an image of the ridge pattern on the epidermis is simply to take a photograph of the fingertip. This technique does not require the fingertip to actually touch the sensing device but some user guidance is needed to place the finger at uniform distance from the camera. Though this may seem like an uncomplicated way to acquire fingerprint images it can, however, prove quite difficult to get high-contrast and properly focused images.

2.3.2 Solid-State Sensors

Solid-state sensors, sometimes referred to as silicon sensors, have the advantage that they can very small. However, since the silicon sensor must be equal to the sensing area the price of a solid-state sensor is more or less the same as for the optical ones [6]. A solid-state sensor works by the user placing the fingertip directly on the silicon thus conveying the physical characteristics of the finger directly to the sensor. There have been proposed a number of different ways to convert this information into digital data and in the following three of these are described further.

Capacitive: The most commonly used solid-state sensor is the capacitive-based type which uses electrical current to sense the fingerprint. A capacitive sensor consists of a 2D-array of micro-capacitors where the fingerprint forms the other part of each individual capacitor. Small electrical charges are formed between the chip surface and the fingerprint and distance to the skin at a given point will then be commensurate with the magnitude of the charge thereby indication either a ridge or a valley. The scheme is illustrated in Figure 2.4. Since the fingertip

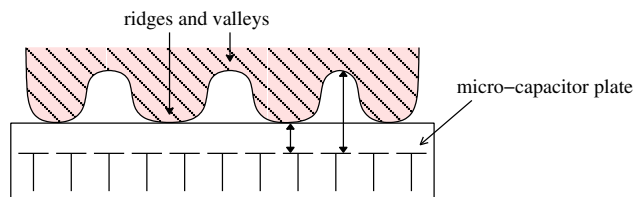


Figure 2.4: Capacitive fingerprint sensing

is placed directly on the solid-state sensor the silicon needs to be coated to protect it from chemicals like sodium, that are commonly found on fingertips. However, because the distances measured by the sensor is already so small, too thick a coating will make the difference between ridge and valley proportionally smaller and thus harder to detect. On the other hand, a coating too thin will not provide proper protection against mechanical abrasion—especially if the device employs *sweeping* (see Section 2.4). Furthermore, electrostatic discharges form a serious threat to the sensitive capacitive sensors so proper grounding is paramount.

Thermal: A thermal sensor is made of pyro-electrical material that generate electrical current based on temperature differences. By placing the

finger on the sensor the ridges and valleys of the print will produce different differences and thus an image of the ridge pattern can be extracted. However, since thermal equilibrium is quickly reached the image produced by this thermal method is transient. To mitigate this issue the sweeping method described in Section 2.4 may be used.

Piezoelectric: This technology is based on sensors that produce electrical current when mechanical stress is applied to them. The magnitude of the current depends on the amount of pressure applied thus ridges and valleys produce different amounts of current. As with the capacitive sensors the thickness of the protective coating is an important issue since too thick a coating will effectively blur the already minimal pressure differences thus impeding the performance of the piezoelectric sensor.

2.3.3 Ultrasound Sensors

A third approach to sensing fingerprints is to use ultrasound. This technology is based on sending sound waves towards the finger and capturing the echo signals that bounce off the fingerprint surface. Based on the echoes received an image of the subsurface skin is created and since the pattern of the subsurface skin is identical to the pattern on the epidermis, the image created will be that of the actual fingerprint. Since the subsurface skin pattern is used ultrasound sensing is less sensitive to some of the things that cause problems than using other technologies, e.g., dry fingers, dirt and oil accumulation on the epidermis, etc. The problem with ultrasound sensing, however, is that the scanners are large and expensive, thus, it is not as mature a technology as, for example, the optical and capacitive technologies described above.

2.4 Live-Scan Acquisition Techniques

Most of the live-scanners in use today employ either the *touch* method or the *sweeping* method.²

The touch method simply involves placing the finger on the sensing area of the device and waiting for the scan to complete (usually 1 or 2 seconds).

²A third method uses the rolling technique where the finger is rolled nail-to-nail. This method ensures that the whole fingertip print is captured but normally requires user guidance and is thus mostly used by law enforcement.

Though it is simple, this method has a few disadvantages. Some of these are listed below:

- The sensing area may become dirty through continuous use which may affect the sensing results, thus, regular cleaning is required to keep the device clean.
- Since fingers are carefully placed on the sensing area they are sure to leave latent fingerprints. These prints may then be used to subsequently fool the scanner.
- The cost of the sensor is commensurate with the size of the sensing area.

The sweeping method addresses all of the three drawbacks listed above. This is accomplished by simply sweeping the fingertip over the sensing area instead of holding it still. Thereby no latent prints are left on the sensing area of the device and the underlying sensor, usually a solid-state sensor, is only required to be as wide as the area that is being scanned. Decreasing the required size of the sensor makes the scanning device a lot cheaper and smaller in size making it feasible to incorporate them into a wider array of equipment. The result of a sweep is a number of slices that are then subsequently processed and combined to form the resulting fingerprint image.

Though the sweeping method has a number of attractive properties it also has a few drawbacks, e.g., it is likely to require a bit of practice before users learn how to perform the sweep properly and the mechanical abrasion caused by the sweeping increases the wear and tear on the sensor coating.

Chapter 3

Fingerprint Spoofing

As mentioned in the introduction, papers have been published documenting the feasibility of spoofing fingerprint scanners by developing artificial fingers. The most well known of these papers, arguably, being [7] by Matsumoto et al. from 2002. This chapter describes a number of techniques for creating fake fingers either with or without the cooperation of the given person.

The techniques described here are mainly based on [7], [8], [9] and [1].

3.1 Duplication with Cooperation

This section describes the case where the fingerprint is duplicated with the cooperation of the person to whom the finger belongs. This is obviously somewhat simpler than the other case, where the duplicate has to be reconstructed from a latent print left incidentally and the methods described below are thus more likely to produce good quality fake prints.

The following describes two techniques used in [7] and [8], respectively. Furthermore, a simple alternate technique devised by the author is suggested at the end of the section.

3.1.1 The Free Molding Plastic Technique

This is the technique used by Matsumoto et al. in [7]. It is a rather simple technique and the only materials required are free molding plastic, available at most hobby stores, and gelatine leaves, available at almost any supermarket. There are two steps in the duplication process: a) the creation of the mould, and b) the subsequent creation of the artificial finger. The process is as follows:

Creation of the mould:

1. Put the free molding plastic into hot water, i.e., water with a temperature of more than 60°C, and leave it there for a moment. Heating the plastic this way will soften it and make it easier to work with.
2. Take the plastic out of the water and let it cool down a bit before molding it into a ball.
3. Press the target finger against the plastic in a manner such that the fingertip creates a well-defined indentation in the plastic.
4. Hold the finger in that position and wait for the plastic to harden. Depending on the temperature of the plastic, this will take about ten minutes.

Creation of the gelatine finger:

1. Add 30cc of boiling water to 30g of solid gelatine and mix them in a bottle. Cap the bottle and wait for the resolution to form a gel as it cools down. Reheat the gel in a microwave oven to form a *sol*¹ and then let it cool down again to allow it to gelatinate. Repeat this reheating and subsequent cooling down process several times to reduce the amount of bubbles in the substance.
2. Pour the sol into the mould prepared as described above. Remember to carefully remove any bubbles that might form along the bottom of the mould.
3. Let the sol gelatinate by cooling it down, e.g., by placing the mould in a freezer for about ten minutes.
4. Carefully pull the gelatine finger out of the mould.

The result of the steps given above should be a ready-to-use gelatine finger containing the fingerprint of the given finger.

3.1.2 The Plaster Technique

This is the technique used by Putte and Keuning in [8]. The materials required and the fabrication process itself is a bit more complex than the technique used by Matsumoto et al. but it is still reasonably simple. As

¹A sol is a liquid substance that can be gelled to form a solid (gel).

opposed to creating a dummy finger, this technique aims at creating a thin silicon coating that subsequently can be glued on to a real finger. The process is as follows:

1. Create a kind of bowl by pressing the nail-side of the target finger into a ball of modelling-wax. The bowl should cover the tip of the finger whilst leaving a hole where the actual fingerprint is. This hole is then filled with good quality plaster.
2. Once the plaster dries it forms a bowl with the fingerprint on the inside.
3. Create a plaster pouncer that fits the plaster mould, save for about 1mm thus leaving room for the silicon layer.
4. Pour silicon waterproof cement or liquid silicon rubber into the plaster mould and press the created pouncer firmly on top of the silicon.
5. When the silicon has hardened the silicon layer holding the fingerprint should be very carefully removed from the plaster mould.

The result of this process is a thin silicon coating that holds the fingerprint.

3.1.3 The Fingernail Polish Technique

This technique is inspired by a comment made in [9], suggesting that one might be able to use half-dried fingernail polish to create a fingerprint mould. Based on that, and the two other techniques described above, the author has devised a very simple method for creating a duplicate silicon fingerprint. The process suggested is as follows:

1. Place a fairly thick layer of fingernail polish on a level completely smooth glass surface and wait until it starts to dry.
2. Carefully place the fingertip of the target finger on the layer of nail polish and press it softly down. Then lift the finger again and leave the nail polish on the glass to harden completely thus creating a mould of the fingerprint.
3. Pour a sol, either silicon- or a gelatine-based, prepared as described in Section 3.1.1, onto the mould on the glass. Use a spoon or something similar to level the sol and wait for it to harden.
4. Carefully remove the hardened dummy fingerprint from the glass.

The result of this process should be a thin layer holding the fingerprint that can then be glued onto a real finger. If this technique proves feasible, it will be a very low tech way to duplicate a fingerprint.

3.2 Duplication without Cooperation

This section describes how to duplicate a fingerprint without the cooperation or knowledge of the fingerprint's originator. Duplicating a fingerprint in this manner involves using a latent fingerprint to make a physical duplicate of the print. The process generally consists of four steps: a) making the latent fingerprint visible, b) capturing an image of the print, c) transforming the image of the print into a physical mould of the print, and d) using the mould to create a physical duplicate of the fingerprint.

The first of the two techniques described below is from [1] where as the latter, which is somewhat more complex, is documented in both [8] and [7], although with some minor discrepancies.

3.2.1 The Transparency Slide Technique

As described above, the first step of the process is about making the latent fingerprint visible. To accomplish this [1] suggests using one of the following two techniques: a) fingerprint dusting using a fine powder and a soft brush, or b) cyanoacrylate fuming using super glue.²

Once the latent print has been made visible it is captured with a digital camera. The picture of the latent print is then processed using an image processing software to enhance the ridge features. The result of the processing is a white print, i.e., the ridges are white, on a black background.

Creating the mould then just involves printing the processed image on a transparency slide using a laser printer. The toner will form a relief in which ridges appear as indentations (since they are the white areas of the picture). Ergo, the relief is a mould of the fingerprint.

The fourth and final step is to create the physical duplicate of the print. This is accomplished by carefully rolling a thin layer of wood glue onto the picture on the transparency slide. In [1], it is suggested to mix in a bit of glycerin to the wood glue as to improve the humidity and workability of the resolution. When the wood glue dries up the thin hardened layer of glue is carefully removed and the duplicate fingerprint is a reality.

²See [3] for a detailed description of these techniques.

3.2.2 The Photo-Sensitive PCB Technique

This technique is a bit more complicated than the one described above and it requires a bit of technical ingenuity since it, amongst other things, involves using chemicals to etch the copper of a printed circuit board (PCB).

In [7], the first three steps are identical to the first three steps described in Section 3.2.1, i.e., enhance the latent print, photograph it and process it, and finally print the image on a transparency slide. The only difference is that the ridges on the image should now appear as black and not white.

The mask produced in the previous step, i.e., the image on the transparency slide, is then attached to a PCB coated with a photo-sensitive layer of *photo-resist* which is then subsequently exposed to an UV light source for about 6 minutes. The result of this process is, that the part of the PCB that the fingerprint mask does not cover is exposed to the UV light and will thus disappear during the subsequent development process.

Developing the PCB is done by placing it in either a 0.6% solution of caustic soda (NaOH) or in dedicated PCB developer. When the excess photo-resist is etched away the PCB is placed in another etching bath containing a solution of fine-etch crystal which will remove the excess copper. What is left is a very slim copper profile of the fingerprint. The valleys on this PCB mould, which represents the ridges of the original print, can afterwards be made deeper manually to better reflect a real fingerprint.

Having created a mould of the fingerprint all that is left is to create the actual dummy. In [7], this is done using the gelatine technique described in Section 3.1.1 where as in [8], the duplicate fingerprint is created using waterproof silicon cement.

Chapter 4

Planned Experiments and Tests

In order to be able to comment on the effectiveness and feasibility of fingerprint spoofing a number of experiments will be conducted. This chapter gives a brief account for the planned experiments and subsequent tests.

4.1 Planned Experiments with Fingerprint Duplication

In Chapter 3, a number of techniques for duplicating fingerprints were described. Of the five techniques described four will form the basis for the experiments performed. These four are the three duplication techniques with cooperation, described in Sections 3.1.1-3.1.3, and the transparency slide technique described in Section 3.2.1. The technique using photo-sensitive PCB has opted out due to its complexity and extensive use of highly toxic chemicals.

4.2 Planned Tests

The duplicated fingers created in experiments described above will be tested using three different devices: a) a high-end Heimann fingerprint scanner, b) a consumer-level capacitive sweeping scanner build into an IBM laptop, and an ordinary flatbed scanner. With each of the dedicated fingerprint scanners the bundled fingerprint matching software will be used to determine match or non-match. With regards to the flatbed scanner software will be used to match images of the duplicates and the real fingers. However, which specific software this will be, is at the moment of writing yet undetermined.

The tests planned can be divided into four different types: live-live, live-duplicate, duplicate-live, and duplicate-duplicate. Each pair of fingers (F_L, F_D), i.e., a live and a duplicate, go through each type of test resulting in the scheme illustrated in Table 4.1.

Type	Enrolment	Verification
1	F_L	F_L
2	F_L	F_D
3	F_D	F_L
4	F_D	F_D

Table 4.1: The test scheme

For each of the pairs, (F_x, F_y) , in Table 4.1 the finger F_x will be enrolled and finger F_y will be tried verified 50 times and the results recorded. With regards to the experiments involving the flatbed scanner this number may end up being less depending on the degree of automation afforded by the software chosen.

Chapter 5

Summary and Future Work

In this interim report fingerprint scanner technologies and fingerprint spoofing techniques have been described. The remainder of this term will be spend on performing the planned experiments and subsequent tests. Furthermore, since it is anticipate that the experiments will show that it indeed is possible to fool the fingerprint scanners, the experiments will be followed up with a brief survey of some of the techniques proposed to counter the threat posed by fingerprint spoofing.

Bibliography

- [1] *How to fake fingerprints?* Chaos Computer Club e.V., October 2006.
@ http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml?language=en.
- [2] *Electronic Fingerprints Transmission Specification*. Department of Justice - Federal Bureau of Investigation, January 1999.
@ http://www.fbi.gov/hq/cjisd/iafis/efts_70.pdf.
- [3] René Haahr Hemmingsen. *Latent Fingerprint Recovery*. University of Calgary, October 2006.
- [4] *Biometrics Market and Industry Report 2006-2010*. International Biometric Group, January 2006.
@ http://www.ibgweb.com/reports/public/market_report.html.
- [5] Anil K. Jain, Arun Ross, and Sharath Pankanti. Biometrics: A Tool for Information Security. *IEEE Transactions on Information Forensics and Security*, 1(2):125–143, June 2006.
- [6] Davide Maltoni, Dario Maio, Anil K. Jain, and Salil Prabhakar. *Handbook of Fingerprint Recognition*. Springer-Verlag New York, LLC, 2003.
- [7] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, and Satoshi Hoshino. Impact of Artificial Gummy Fingers on Fingerprint Systems. In *Optical Security and Counterfeit Deterrence Techniques IV*, volume 4677, January 2002.
@ <http://cryptome.org/gummy.htm>.
- [8] Ton van der Putte and Jeroen Keuning. Biometrical fingerprint recognition: Don't get your fingers burned. In *Fourth Working Conference on Smart Card Research and Advanced Applications*, pages 289–303, 2001.
@ http://www.keuning.com/biometry/Biometrical_Fingerprint_Recognition.pdf.
- [9] *Biometric Devices and Fingerprint Spoofing*. Washington & Jefferson College, January 2006.

@ <http://www.washjeff.edu/users/ahollandminkley/Biometric/index.html>.

- [10] James Wayman, Anil K. Jain, Davide Maltoni, and Dario Maio. *Biometric Systems: Technology, Design and Performance Evaluation*. Springer-Verlag New York, LLC, November 2002.