Attacking Fingerprint Sensors

Anders Wiehe anders@wiehe.org
Torkjel Søndrol mail@torkjel.com
Ole Kasper Olsen mail@olekasper.no
Fredrik Skarderud fredrik@skarderud.net

NISlab / Gjøvik University College

15th December 2004

Abstract

We leave our fingerprints behind everywhere like when going to a café for a coffee or a soda, yet we never think of the possibilities that others might steal our prints from the cup or glass we just drank from.

In this report we have conducted several experiments of lifting such latent fingerprints, and later having used them to create artificial reproductions. We have tried to use several different materials and techniques to reproduce artificial fingers in both consensual and unconsensual scenarios. The artificial fingers have been tested on two different types of fingerprint sensors.

Contents

1 Introduction

Lately we have seen that the market for small and cheap fingerprint sensors has expanded [1]. Where fingerprint sensors and other biometric recognition devices previously were regarded as science fiction in most people's minds, they are now on their way to become a more commonly used method for fast and easy authentication.

The goal of the fingerprint sensor is in many applications to relive the user of the burden of having to remember one or often several passwords. The obvious question is then; are fingerprint sensors as secure as passwords? We will not attempt to answer that question in this paper, however what we will try to do, is establish just how easy it is to fool a couple of these new fingerprint sensors.

2 Literature Study

The testing of biometric authentication devices has been the subject of several papers. One of the first to be published was van der Putte and Keuning's description of two methods to create dummy fingers [2] in 2001; one method without cooperation and one with cooperation. Creating fingers with cooperation should be performed pressing the finger into plaster to create a mold, and then use silicon waterproof cement or liquid silicon to create a finger using the mold. When no cooperation, they recommend trying to get a latent fingerprint from the fingerprint reader itself, since the quality should be good and it would be the correct finger. The print should be enhanced using fine powder and removed from the reader using scotch tape. Then the print should be transferred to a photo sensitive copper plated circuit board (PCB) to create a mould. The mold might be deepened further using a Dremel multi-tool before the artificial finger is created using silicone.

Most of the work on fooling biometric authentication devices was kindled by the publishing of Thalheim et al. in the German computer magazine *c't* [3] in 2002. They described the easiness of fooling several types of fingerprint sensors, an iris camera and a face recognition solution. Among the discoveries they made are that it was possible to steal fingerprints from other surfaces by dusting them with fingerprint powder and capture it with an adhesive film before pressing the film gently to a capacitive or optical reader. They also managed to fool optical fingerprint readers using a silicon finger created by pressing a real finger into a wax mold.

Matsumoto et al. looked at ways of creating artificial fingers using silicone and gelatin in [4]. They first cloned the finger using a mould made of free-moulding plastic, and then filled it with both gelatin and silicone rubber to create the artificial finger. They managed to fool the optical scanner using the gelatin finger, but not the one made from silicone. In their next experiment, they cloned a residual fingerprint, which was captured on a glass plate and enhanced using a cyanoacrylate adhesive. This was transferred to a PCB, and a gelatin finger was created. All the verification systems tested accepted the artificial finger more than 67% of the time.

Then, in 2003, Kaseva and Stén performed several tests on the Precise Biometrics 100 SC capacitive fingerprint scanner [5]. They were unable to fool the scanner breathing on it as Thalheim did in [3]. They were also unable to reactivate latent fingerprints on the sensor by pressing gummy bears upon it. They managed however to fool the sensor using a gelatin finger made from a mould created by pressing the finger into hot glue. They also managed to steal a latent fingerprint from a mug using photocopier powder and transfer it to a PCB, which was used as a mould for a gelatin finger, which fooled the sensor.

Sandström published a report in 2004 on liveness detection in fingerprint systems [6]. She performed an experiment, in which she created an artificial finger from a latent fingerprint she enhanced using a soot powder mixture and a squirrel hair brush. The print was further enhanced in Adobe Photoshop and printed on a PCB, which was used as a mold for the gelatin finger. The fake finger was tested on several of the fingerprint systems at the CeBIT trade fair in Hanover, Germany in 2004, where she had a mean success rate of 67% when using this finger.

A common theme in the above articles seems to be that capacitive sensors can easily be fooled by using gelatin, since a real finger and gelatin has approximately the same capacitance.

The German computer club Chaos Computer Club Berlin has created a short video sequence [7] demonstrating the easiness of creating a fake finger from a latent fingerprint. They use instant glue to enhance the fingerprint, and then enhance it further using graphics software before they print it on a transparent. They then cover it with a thin layer of wood glue, which they can use as a fake finger, or as they so succinctly put it: *"Meine zweite identitet!"*

3 Testing Methodology

In 2002, Mansfield and Wayman created a series of best practises for testing biometric devices [8]. The purpose of this was to provide a framework for testing, help avoid systematic bias while testing and to help testers achieve best possible estimate of performance. However, the framework was created for evaluating sensors, measuring matching and decision errors using *zero-effort impostors*[1]. As we are aiming to completely fool the sensors we test, not merely evaluate their performance in a realistic scenario without active adversaries, the framework cannot apply to us.

We have also decided to not record any FAR or FRR statistics while testing the sensors. This is because we believe that the definitions of FAR and FRR as found in notable literature on the subject do not apply in our case. In [9], false acceptance is defined as pairs of different fingerprints found to match. In our case, we will not have pairs of different fingerprints, we will have the original fingerprint and an artificial copy of the original fingerprint. The definition found in [1] is in essence equal. The definition which can be found in [8] however, is a more general definition, indended to resolve some inconsitencies between different authors regarding FAR, FRR and positive and negative recognition systems. They define a false acceptance as a wrongful claim of identity that is incorrectly confirmed. This seems to match with the experiments we are going to be conducting. However, they then proceed to explicitly state that decision errors such as FAR and FRR "are due to matching errors or aquisition errors". In our case the false acceptance would be a result of neither a matching error

[1] An impostor who submits his biometric features to the system as if he was attempting a successful verification against his own template, i.e., no manufacturing of fake fingerprints.

nor aquisition error, but rather matching and aquisition success. Based on this, we will henceforth refrain from using such terminology as false acceptance and false rejection, as the literature do not define these terms properly for use in our situation.

We will try to duplicate some of the techniques from the articles described in the literature section. We will also try different combinations of moulds and substances for artificial fingers, and all of the fingers will be tested against the same fingerprint sensors using the same configurations.

4 Equipment

4.1 Software Packages

The software used for capturing fingerprints and comparing matching scores was NISlab Authentication Workbench, developed by two of the group's members for NISlab. Authentication Workbench is a testing suite for various authentication methods and devices, which includes fingerprint sensors.

Authentication Workbench can have many uses, like testing fake fingers which we are going to attempt. The main mode of operation, however, is to organise and help perform extensive evaluation experiments, providing FAR and FRR[2] statistics among other things.

4.2 Biometric Sensors

The sensors available to us in our experiments were one optical and one capacitive fingerprint sensor. Both used USB to interface with the computer running the acquisition software. Both sensors had built-in support in Authentication Workbench.

4.2.1 Optical Fingerprint Sensor: Digital Persona U.are.U 4000

The Digital Persona fingerprint sensor shown in figure 1a is a fairly cheap fingerprint sensor aimed at both the small business and the private market, priced at around $100.

As latent fingerprint and counterfeit image rejection are among the features reported by the manufacturer for this sensor, we are eager to test this fingerprint sensor. It is also supposed to be encrypting image data between the reader and the computer it is attached to. In other words, security seems to be a prioritised area for this manufacturer.

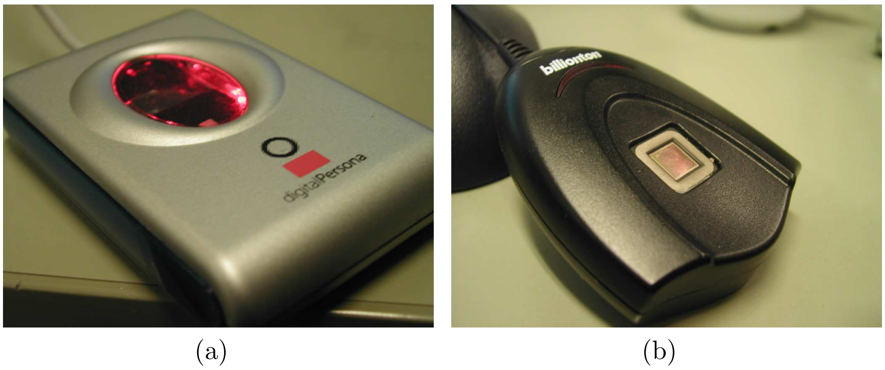
The sensor's resolution is 512 dpi with a 14.6x18.1 square millimetres fingerprint sensing area. As with most other optical FTIR[3] based fingerprint sensors, the images it produces are 8 bit grey-scale images (256 tones of grey).

4.2.2 Capacitive Solid-State Sensor: Billionton

The Billionton is a relatively cheap capacitive fingerprint sensor with a small 6.5x6.5 square millimetres sensor area. The sensor matrix is comprised of 16,384

[2] False Acceptance Rate and False Rejection Rate, see [1], page 13.

[3] Frustrated Total Internal Reflection, see [1], pages 59–61.



(a) (b)

Figure 1: Our sensors — (a) Digital Persona U.Are.U 4000 (b) Billionton capacitive fingerprint reader.

capacitive sensors, arranged in a 128 by 128 array, resulting in a 500 dpi resolution.

The manufacturer claims that the device's false acceptance rate is 0.015% and the false rejection rate is 2.3%. Given that these numbers are only meaningful at a certain match score threshold, we conclude that using a recommended threshold, FAR and FRR values will be as reported.

The sensor do not seem to be available for purchase anymore, but although not mentioned on the sensor's packaging or in its manual, we have reason to believe that the solid state chip which is mounted in the Billionton is an AuthenTec AES3400 of the EntréPad family.

The sensor is shown in figure 1b.

4.3 Materiel

Before starting our experiments, we went on a shopping spree in downtown Gjøvik. Based on our initial literature studies, we had written down a list of various related and unrelated household articles and other products.

Initially we went out and bought a couple of different types of silicone used for bathroom sealing, wood cement, instant glue, plasticine, air drying clay, gummy bears, gelatin, a makeup brush, wide transparent tape, candle lights and a glue gun. Just to get us started.

We were also wondering whether to contact the local police department to get some graphite powder to lift latent fingerprints, but we decided that nicking a used laser tone cartridge and shake and beat it until some toner powder fell out was sufficient.

5 Experiments – Consensual

The term *consensual* suggests the user we are stealing the fingerprint from is aware of the process and actively participates by pressing his finger into some kind of a mould.

Even though we have classified this approach as "consensual", there are unconsensual ways to go about achieving the same. For example, one can drug a victim and make an imprint of his or her finger or one can do some advanced social engineering and fool a person into giving away an imprint. There are a multitude of ways to do this, however very few can be done in such a way that the target does not know about it.

5.1 Procedure

5.1.1 Creating Moulds

Plasticine The first experiment we performed was to use plasticine as a mould. We knead the plasticine for a while to make it soft and easy to shape, before we gently pushed a finger into it to create the mould.

Candle Wax The next item we tried to use as a mould was candle wax. We lit the candles and let them burn until all the wax was melted. Then we removed the wick from the wax, let it dry for a little while, and pressed our finger into the wax. When the wax was dried, we had a nice mould.

Clay The next mould was made out of the kind of clay that dries in normal room temperature when exposed to air. We knead the clay while carefully adding a bit of water to it to make it nice and soft in which it was possible to gently press a finger. We tried to use this mold both moist and after it had dried over night.

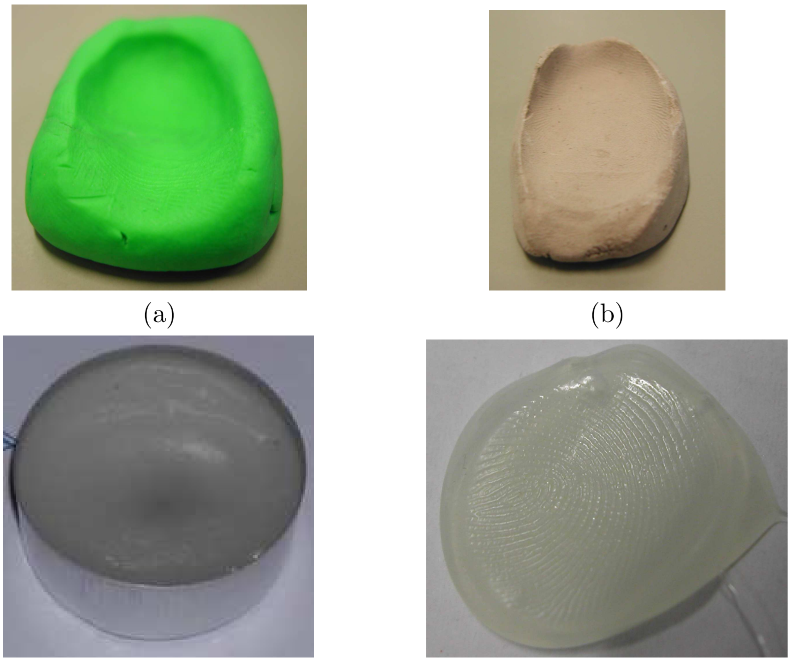
Hot Glue We also tried creating moulds using hot glue, which was pushed out of a glue gun onto a piece of paper and cooled down a bit. We could touch the underside of the paper to detect when the glue was cold enough to place the finger into. When the glue had cooled off, it was usable as a mould.

Ink and Transparency Last we tried capturing fingerprints like the police do by pressing the finger applied with ink on a piece of paper. This paper was scanned into the computer, and the further process of creating a working fingerprint mould using a transparency is identical to the procedure of creating a mould out of a latent fingerprint. See section 6.1.

5.1.2 Casting Artificial Fingers

Gelatin Solutions Gelatin is to be mixed with water to become a substance desirable in this kind of experiments. The thickness of this substance will vary with the ratio between gelatin and water. We tried three different substances of gelatin solutions. One thin solution with about 65% water and 35% gelatin, one solution with about 45% gelatin and 55% water and one solution with about 55% gelatin and 45% water.

Plasticine Mould We tried filling the plasticine mould with both silicone and gelatin. The problem with the plasticine was that it stuck to the valleys of the silicone finger when it was removed from the mold. This was solved by cooling the plasticine down before the artificial finger was removed. We let the silicone fingers dry for one day in their moulds before we carefully removed it. The silicone finger was usable after some serious cleaning with water and soap. The



(a)

(b)

(c)

(d)

Figure 2: Different kind of moulds — (a) Plasticine mould (b) Clay mould (c) Candle wax mould (d) Hot Glue mould.

gelatin finger, on the other hand, could easily be removed from the plasticine mould without any traces of plasticine in the valleys.

Candle Wax Mould The candle wax was filled with gelatin, which was a total failure. The gelatin shrunk while drying, which resulted in almost no fingerprints on the gelatin. We later tried using silicone in wax mould, which gave a much better result. The silicone could easily be removed from the mould by melting the wax under hot water.

Clay Mould The clay mould was filled with silicone. We tried both filling a wet and a dried clay mould with silicone. The silicone finger casted in wet clay was usable instantly without much residues of clay stuck in its valleys, but the one casted in dried clay had valleys filled with dried clay when the finger was removed. Only after some serious cleaning using water and soap, we were able to get a usable silicone finger.

Hot Glue Mould The glue mould was filled with both silicone and gelatin. The gelatin finger was easy to remove from the mould after it had dried, but the silicone got stuck to the mould, and was unfortunately impossible to remove without destroying the finger. We tried melting the mould using boiling water, but the silicone finger still had glue stuck firmly in the valleys.

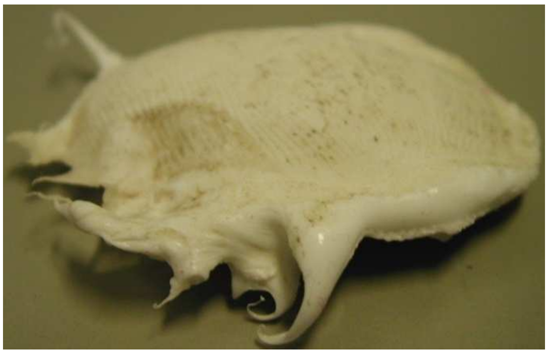


Figure 3: A working silicone finger, which was cast in a clay mould.

5.2 Results

The results from our consensual experiments have been listed in 1. The table shows the different combinations of moulds and castings we used along with which sensors it fooled.

Mould	**Casting**	**U.are.U 4000**	**Billionton**
Plasticine	Silicone	Fooled	Not fooled
Plasticine	Gelatin	Not Fooled	Not fooled
Candle Wax	Silicone	Fooled	Not fooled
Candle Wax	Gelatin	Not Fooled	Not fooled
Clay	Silicone	Fooled	Not fooled
Hot Glue	Gelatin	Not Fooled	Not fooled
Hot Glue	Silicone	Not Fooled	Not fooled
Ink/Transp.	Wood Cement*	Not Fooled	Not fooled

Table 1: Results from the consensual experiments. *) The procedure of using a wood cement as a cast is explained in section 6.1.

With regards to the gelatin results, all three solutions did fool the capacitive into thinking that a finger was placed on the sensing area. However the print on the sensing area were very smudged, and we were not able to get a positive match against the pre-stored template. In [6], a proportion of 44% gelatin and 56% water was used, claimed to be very successful. In our experiment we achieved the best results with the 55% gelatin solution. With this solution we at least managed to fool the optical sensor. However trying a bit harder, we probably would be able to fool the optical sensor with all of the three solutions.

5.2.1 Matching Score Statistics – Silicone

As shown in table 1, one of the combinations which we were able to fool the optical sensor with was a silicone finger cast from a moist clay mould. We conducted ten tries to measure the matching score for the fake silicone finger, and ten tries to measure the matching score for the genuine finger. We chose to make ten tries of fooling the sensor for many reasons. Firstly we wanted to be sure that it was not a fluke that we managed to fool the sensor with our fake finger. Further, we wanted to generate some data for analysis and comparison reasons. The ten attempts with the genuine finger was conducted to be able to differ between the result obtained by both the genuine and the fake finger. Even though ten tries is very little foundation to generate some FRR statistics for the genuine finger, the results could give a small indication of how stable the sensor results are. Table 2 shows the results from the experiment.

Try #	**Matching Scores, Genuine Finger**	**Matching Scores, Silicone Finger**
1	340	189
2	393	215
3	543	58
4	528	182
5	385	161
6	292	134
7	521	184
8	649	177
9	538	121
10	533	132
$\overline{x}$	472.2	155.3

Table 2: Results from the consensual experiment

The threshold value for validating a fingerprint is default set to 47 by the manufacturer of the sensor's software development kit (SDK). The strictest threshold value possible to configure the sensor to use is 63. The lowest value measured for the fake finger was 58, so if we had configured the strictest configuration, nine out of ten attempts to fool the sensor had succeeded. However, we operated with the default configuration with a threshold limit of 47, meaning that the sensor was fooled all ten times.

5.3 Analysis

As shown in the results table 1, we were only able to fool the U.are.U sensor, and only using silicone as a material for fake finger. We believe, however, that using a sufficient mixture of gelatin and water using the correct mould will give a finger capable of fooling the optical reader. As shown later in section 6.2, we were able to create working artificial fingers using gelatin and PCB, hence it should be feasible to use other moulds as well.

We believe that with a good silicone finger we will be able to completely fool our optical sensor into thinking we have an actual live finger, yielding matching scores upwards of 500. However, we achieved matching scores of only about 150. The reason is probably the plasticine and clay that got stuck in the valleys of the fingerprint, and was impossible to remove later using water and soap. Still, when the default threshold is set to 47 (and maximum adjustable being 63) we had no problems fooling the sensor.

6 Experiments – Unconsensual

This section deals with fingerprints obtained in a non-cooperative fashion. In our experiments, we have only obtained fingerprints from ourselves, however we have tried to do so in a realistic fashion yet without making things too difficult for ourselves (the latent fingerprints we made were not smudged in any way).

6.1 Procedure

The procedure from the discovery of a latent fingerprint to having an artificial recreation of the fingerprint is not trivial. First and foremost there is the problem of identifying the correct finger. Lifting a latent fingerprint from a finger not included in a fingerprint recognition process will obviously only be wasted effort. The easiest solution to this problem may be to simply obtain the latent fingerprint from the fingerprint sensor itself. We leave it as an exercise to the reader how to find other devious ways to obtain the correct latent fingerprint.

Assuming the correct latent fingerprint has been identified, we present various methods for obtaining it, which we have tried to do in our experiments. Generally speaking, the following have to be done.

1. **Latent Fingerprint Enhancement:** The fingerprint will have to be enhanced in some ways so that it can be lifted.

2. **Lifting a Latent Fingerprint:** After enhancement, the fingerprint must in some way be transferred to a different, but fitting, medium from which it was discovered and enhanced. In our case, this included different ways of digitising the enhanced fingerprint.

3. **Digitally Enhancing the Fingerprint:** After having lifted and digitised the fingerprint, it needs to be digitally enhanced, so that acceptable moulds can be made from the digitised fingerprint.

4. **Creating a Mould for Fingerprint Reproduction:** Next step is to create a mould which we can use, preferably over a long period of time if we have impure intentions, to create artificial fingers at will.

5. **Casting Artificial Fingers:** Final step is to make an artificial finger.

6.1.1 Latent Fingerprint Enhancement

Law enforcement agencies currently use chemical reagents [1] or graphite powder for latent fingerprint enhancement. These techniques require serious funding, and are thusly not available to us. We have tried the following techniques.

Laser Toner Powder Having read that copying powder from photocopiers were being used in [5], we figured that the toner powder which is found in normal cartridges for laser printers would have similar characteristics.

After having "borrowed" a toner cartridge from a waste bin outside the college's IT department we started bashing it around until toner powder started drizzling out. After having shaken out enough powder, we took an ordinary white ceramic cup which "accidentally" had a very nice fingerprint on it and blew some of the very fine-grained toner powder onto the cup. This approach

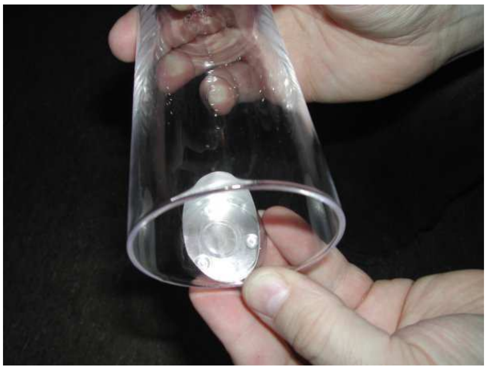


Figure 4: Enhancing latent print with instant glue fumes.

worked very well, although it is obviously dependent on the amount of powder blown onto the latent fingerprint. Too much or too little, and the print will be unusable.

We also tried to take some toner powder on the makeup brush we bought and brush it gently against a latent fingerprint. This approach was however not as good as the method of blowing the toner powder across the fingerprint. Most of the times, the brush destroyed the fingerprint, no matter how gentle we were. Much of this may be attributed to the brush itself, as we didn't want to spend an obscene amount of money on a brush which we were only going to "have fun with", and bought a really cheap one. Not nearly law enforcement quality, to say the least.

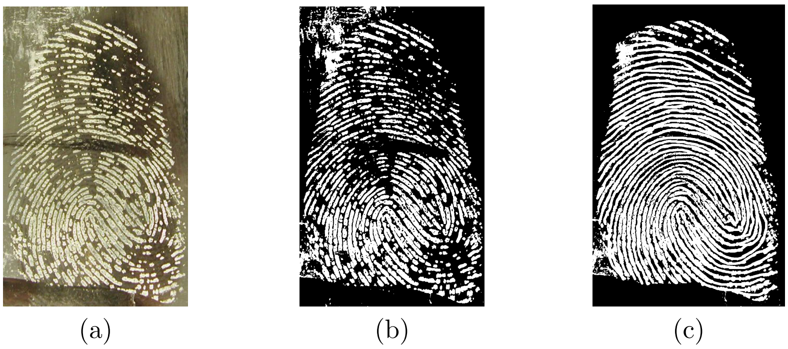
Ethylcyanoacrylate Fumes Having watched the video released by Chaos Computer Club Berlin [7] (see section 2), we learnt of another way of enhancing latent fingerprints. By encapsulating the latent print with a container containing instant glue, the working agent in the glue (ethylcyanoacrylate) will evaporate and fumes from the glue will be attached to the ridges of the latent fingerprint, and make it possible to lift it.

Figure 4 shows how we had some instant glue in a small container previously holding a candle light, which we held up to a glass with a latent fingerprint. After 10 minutes, the fingerprint was clearly visible.

6.1.2 Lifting a Latent Fingerprint

Digital Camera The first method of fingerprint digitising we tried was by using a digital photo camera borrowed from the college's library which was able to take images up to 3.2 mega pixels in size (2048x1536 pixels).

Ideally, for a good fingerprint image, the image size should have been larger. However, we tried to do the best we could with the camera we had. It was important to be able to get close enough to the fingerprint while getting a clear shot. The camera had nice macro functionality which made it possible to get good, in-focus images of close objects. We had, however, no tripod or similar mounting device to get absolutely blur-free images, meaning we had to do with stacks of smart cards or other creative specialities.



(a) (b) (c)

Figure 5: Different versions of a fumed latent fingerprint image — (a) Original (b) Converted to 1bit (c) Retraced and converted to 1bit.

We believe that with a more expensive camera and a tripod, we could have made better images requiring less time spent in various graphics software suites.

Transparent Tape After having had somewhat limited success with our camera, we figured we could try a different approach. This method will only work on dusted fingerprints (e.g., laser toner powder). By using a broad transparent tape we are able to lift the laser toner powder which had stuck to the latent fingerprint, as done in [3]. Having the powder fastened to the tape, we then transfered it to a white sheet of paper by simply attaching the transparent tape onto it.

Having the latent fingerprint now transferred to a white sheet of paper enable us to easily digitise it using an ordinary flatbed scanner. We used a Canon CanoScan LiDE 50 at 1,200 dpi to digitise our lifted fingerprints.

6.1.3 Digitally Enhancing the Fingerprint

We used a rather diverse amount of graphics software suites to enhance the fingerprint images. None of the group's members had any particular experience with such mammoth programs, so we did the best we could.

Among the group members we tried Adobe Photoshop CS which was available at the college's lab, a trial version of Jasc Paint Shop Pro 9 and The Gimp, a free and powerful graphical suite for Linux.

The goal of the enhancement process is to reduce the 24 bit true colour images (as seen in figure 5a) to a colour depth of one bit, resulting in an image with only two distinct colours—black and white. Doing just this transformation without somehow enhancing the ridges and/or luminance values will result in a very poor and unusable fingerprint image—see figure 5b.

We tried different techniques for achieving a good result. One that worked well was to retrace the ridges using for example Paint Shop Pro's clone brush tool. Even though not all ridges are retraced particularly carefully, the mask which can bee seen in figure 5c works very well.

Using localised thresholds (the luminance point where darker shades become black and lighter shades become white) when converting images to 1 bit was also very helpful.

6.1.4 Creating a Mould for Fingerprint Reproduction

Transparencies One way to create a mould is to use a transparency, which the enhanced digitised fingerprint is printed upon with a laser printer.

When printing, care must be taken so that the printed fingerprint is roughly the same size of the real-life fingerprint. The resolution of the printer is probably also an important aspect, however we did not experiment with adjusting the dpi of the printer. We used a HP LaserJet 4 Plus laser printer capable of 600 dpi resolution.

When the fingerprint is printed on the transparency, the laser toner powder which is burnt onto the transparency will create an impression some micrometres high. This enables us to use it as a mould.

Photosensitive Circuit Board The second approach we explored with intent to create a mould for fingerprint reproduction, was to try developing a mould out of a photosensitive circuit board, something we first read about in [5]. The PCB which we kindly got from the college's electrical engineering laboratory had a 35 μm thick copper layer.

The procedure for creating a PCB for use as a fingerprint mould is roughly as follows.

1. Make a transparency with fingerprint masks as previously described.

2. Cut a PCB die to match with the fingerprints on the transparency.

3. Expose the PCB to ultraviolet radiation, using the transparency as a mask. The parts of copper which are not covered by the radiation absorbing black parts of the mask will be less resilient towards later etching. Make sure to get the mask correctly as inverted and mirrored fingerprints are hardly useful. Figure 6a depicts our PCB getting ready for a tan. Leave it in for about 2–3 minutes.

4. After ultraviolet radiation, we need to develop the mask by applying lye (NaOH) onto the PCB. Just brush it on in generous strokes.

5. We then proceeded to bathe the PCB in ferro chloride, which etches away the copper which was not masked when we exposed the PCB to ultraviolet radiation. Leaving the PCB in the etching bath for about 10 minutes seemed to erode most of the unmasked copper. Figure 6b depicts the PCB in the middle of the etching process.

Figure 7 shows the final, rinsed PCB. The resulting circuit board may be used as a very permanent long-term fingerprint mould, which—if used with care—will be able to produce many artificial fingers for our fairly non-malicious use.

6.1.5 Casting Artificial Fingers

Silicone Having had fairly good success with using silicone in our other moulds (see section 5.1.1), silicone was the first thing we tried on our newly created circuit board. Obviously, as we should definitely have understood, the silicone

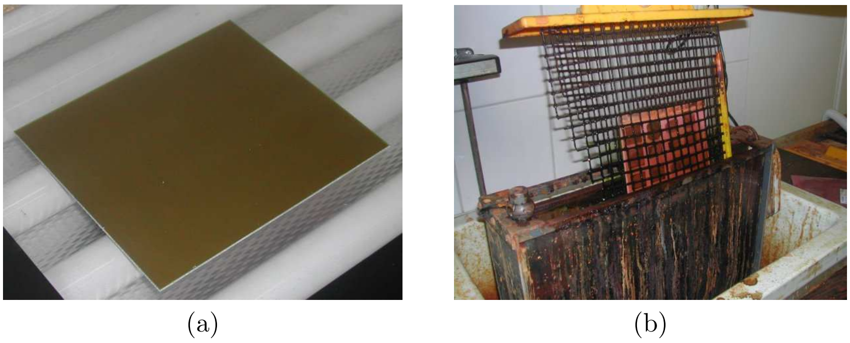

(a) (b)

Figure 6: Photosensitive circuit board under development — (a) Ultraviolet radiation (b) Etching in ferro chloride.

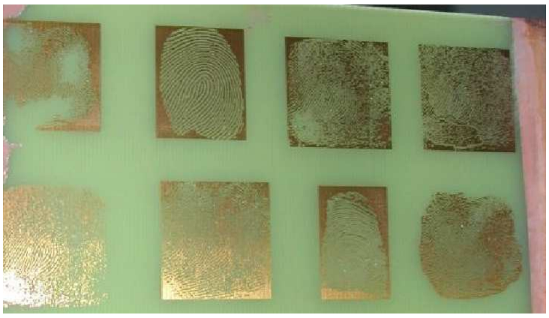


Figure 7: Finished PCB fingerprint mould.

fastened very tightly to the circuit board, and it was nigh impossible to get it off even with a special silicone-removing solvent.

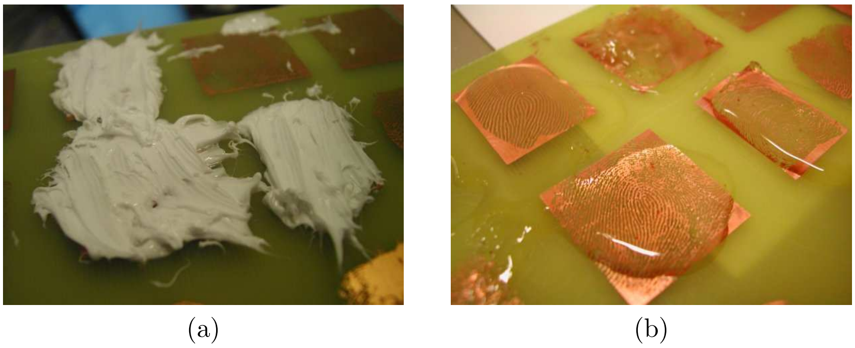
Silicone may have worked if we had rubbed in the circuit board with some sort of very fine oil (like sewing machine oil). We did however try to apply just a tiny bit of silicone-removing solvent before adding silicone. The result was that the silicone never dried enough to be able to pull a whole finger off of the circuit board.

We have also tried applying a very thin layer of silicone to a transparency mould.

Gelatin By applying gelatin (solution made as described in section 5.1.2), we were able to make some pretty nice-looking finger casts from the PCB.

Additionally we also tried applying gelatin to a transparency mould as we did with the silicone.

Wood Cement This was a method we learnt from [7]. By carefully applying a very thin layer of wood cement to the printed transparency, we are able to make artificial finger casts. By allowing the wood cement to dry just enough so that it can be removed with the help of a plain butter knife as a whole sheet, we are able to create great-looking casts, with almost surprisingly clearly pronounced valleys and ridges.



(a) (b)

Figure 8: Casting using the photosensitive circuit board — (a) Silicone (b) Gelatin.

We also tried applying some wood cement to our circuit board. We used more or less the same approach as described above, only in this case we didn't have to be equally careful with the amount of wood cement.

Plasticine Just to have tested it, we quickly wrapped some plasticine around a finger and pressed it into the circuit board to make a cast.

Hot Glue We also tried to use the glue gun on our circuit board. The heated glue easily filled the ridges in the mould. We peeled the glue off before it solidified too much.

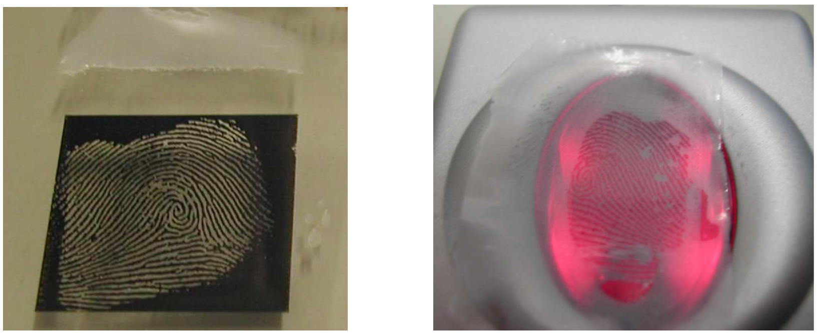
6.1.6 Summary

The process proved to be fairly tedious and time consuming, especially the digital enhancement phase. We required at least 20 and upwards to 60 minutes to properly enhance a fingerprint. When they in [7] exclaim that a new identity can easily be obtained in "a couple of minutes" (from latent fingerprint to finished artificial finger), we are somewhat sceptical. Granted, the quality of the latent fingerprint, the proficiency with which we lift it and experience with the software suites in question do have a significant impact on the time spent, however squeezing the entire process in under 30 minutes seems to be relatively hard.

6.2 Results

As is evidenced by the previous section, the different combinations of lifting fingerprints and casting artificial fingers are numerous—way too numerous for us to try all combinations within a limited time-frame. Rather than going through every combination we tried, this section will therefore only briefly summarise the highlights of our results. For an extensive matrix of everything we've tried, the reader is referred to appendix A.

The first thing we tried was to use the circuit board with a variety of casting substances. As mentioned earlier, we started with silicone first, something which resulted in much frustration as we had severe problems when trying to get it off. Having learnt from our mistakes, we proceeded with gelatin. The first few



(a) (b)

Figure 9: (a) The transparency after the wood cement was removed (b) The wood cement on the top of the sensor.

times we were unable to fool any of the readers with the gelatin fingers. Rather frustrated with the fact that nothing worked, we also tried plasticine. To our joy, this actually fooled the optical sensor, albeit with a very low matching score of 54 which is just above the default threshold value (47). Later, we also managed to fool the optical sensor with both gelatin, wood cement and hot glue artificial fingers based on the circuit board mould.

Moving on to our other type of mould, the transparency, we tried applying wood cement to cast artificial fingers. At first, this method didn't yield any working fingers, but after becoming more proficient with the method, we started cranking out working fingers. We were very successful fooling the optical sensor with latent fingerprints enhanced by instant glue and lifted using the digital camera, and also powdered latent fingerprints which was lifted using transparent tape and later scanned.

Having read that solid state capacitive sensors, like the one we have at our disposal, are exceedingly easy to fool with gelatin artificial fingers, we had hoped for a better success ratio than the one we obtained, which is an astounding 0%. None of our gelatine fingers, or fingers based on other casts for that matter, fooled the capacitive reader.

6.2.1 Matching Score Statistics – Wood Cement

We did some tests on a wood cement finger measuring the matching score values achieved for the wood cement generated fingerprint. The fake finger was produced using the following procedure. First we enhanced a fingerprint from a cup using the laser powder technique. Then we digitised the fingerprint by using the transparent tape approach. After we had digitally enhanced the fingerprint, we printed a transparency of the fingerprint. The fake finger was then created by applying the wood cement technique as described in section 6.1.5. Figure 9 shows the transparency mould and the wood cement finger cast from it.

The fingerprint sensor used in the test was the U.are.U 4000 optical sensor. During the experiment a series of ten tries with the wood cement finger and the genuine finger was conducted. When measuring the matching score achieved with the fake finger all participants of the group had at least one try to fool the sensor. It might have been easier for one member of the group to fool it as he might have had more experience trying to fool the sensor than other members. The results are displayed in table 3.

Try #	**Matching Score, Genuine Finger**	**Matching Score, Wood Cement Finger**
1	336	345
2	470	340
3	617	352
4	458	357
5	422	342
6	416	243
7	425	322
8	451	387
9	464	397
10	459	260
$\overline{x}$	451.8	334.5

Table 3: Results from the unconsensual experiment

The threshold value for validating a fingerprint is default set to 47 by the sensor SDK manufacturer. The most strict threshold value possible to configure the sensor to use is 63. This means that the matching score values we achieved with our wood cement finger made from an unconsensual gathered fingerprint was way over the limit of 47. In fact, 70% of the matching scores we achieved with our wood cement finger was higher than the lowest matching score gathered from the genuine finger! The experiment was a complete success, and if we had spent even more time with digital enhancement techniques, we might have gotten even better results with our fake wood cement finger.

6.3 Analysis

The most interesting of our finding were perhaps the fact that if only the valleys and ridges were prominent enough, the optical U.are.U scanner was easily fooled. The sensor pro ably has some liveness checking, as simply printing a fingerprint on a white sheet of paper does not work, however it seems to accept any object with enough differences between ridges and valleys. It is not perfectly clear to us what the manufacturer means by "counterfeit image rejection", but it obviously cannot have anything to do with three-dimensional objects being introduced to the sensor area. We even managed to fool this sensor with a slab of glue which was heated, then pressed onto the circuit board mould before introduced to the sensor.

When it comes to the capacitive sensor, we didn't have much luck. As we had read that gelatin could easily fool such sensors, we are surprised by this result, as we have gone to great lengths to make a gelatin solution which would work. It is still unclear to us why nothing worked, however the amount of water added to the gelatin seems to be the key, as the lower the amount of water, the better imprint we got on the sensor (see figure 10). With more time, we might have been able to mix a gelatin solution which had low enough water content to actually pass as a finger to the capacitive sensor.

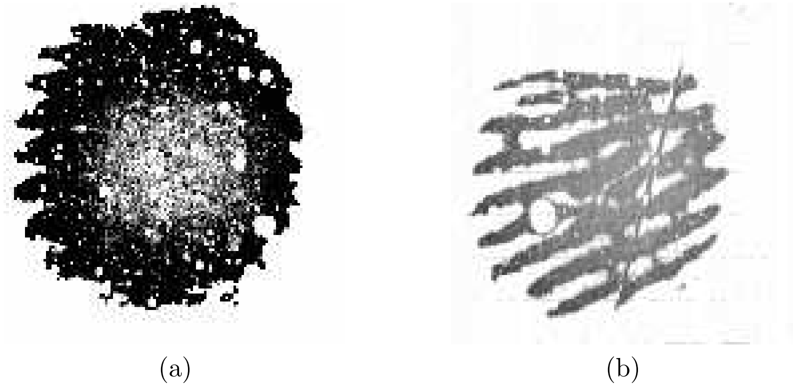


Figure 10: Results on capacitive fingerprint sensor with varying degree of humidity in gelatin solution — (a) Very moist solution (b) Our thickest solution.

Another reason for our failures may be that the valleys of the mould were too shallow, and that the capacitive sensor was more picky about ridges and valleys than the optical sensor. We did however also try gelatin with plasticine moulds (see section 5.1.2) which should definitely have equal height differences between ridges and valleys as a human finger. However, as mentioned, we were not able to fool the capacitive using these either.

Another reason for our failures with the Billionton sensor, may also be that the sensor itself has a high false rejection rate. We have not been able to do proper FRR testing during our experiments, but rudimentary tests do indicate that the FRR is higher than the 2.3% Billionton operates with.

There's also the remote possibility that we are not to blame at all, and that AuthenTec's capacitive fingerprint sensors are among the best on the market. Unfortunately, without access to other brands of capacitive fingerprint sensors we are unable to do the necessary comparisons.

As a closing observation, it is to be said that many of our failures were conducted early in the project, and as the project progressed we got bettter at mixing gelatin, enhancing images on the computer, and peeling off wood cement. In other words, many of our failures, both in unconsensual and consensual experiments may not have been failures if we had tried to do them again. But, alas, time does not permit us to go back and retry every one of our failed experiments.

7 Future Work

We have only tested our fake fingers on the Billionton fingerprint sensor and the Digital Persona U.are.U 4000 sensor. This is obviously not representative for the whole market of fingerprint sensors, and hence, to test more readers would be interesting. It would be very interesting to test more capacitive devices, since we were unable to fool the Billionton sensor. This might give the answer to the question; are capacitive sensors better than optical sensors?

We have tried several different approaches to create fake fingers, like silicone and gelatin. However, there are a lot of other materials with the potential of replicating a real finger fairly well. For instance, we would like to test how well liquid latex works, but due to the limited time, we did not manage to do this.

Appendix A shows a summary of the different combinations of moulds and fingers we tried. There are a lot of combinations we did not try, and it would be interesting to know whether these combinations would work.

When we carried out our unconsensual experiments, we tried creating an as clearly as possible fingerprint on the surface before enhancing it using toner powder or ethylcyanoacrylate fumes. It was hard enough for us to get a clear fingerprint to lift even from this basis, but it would be interesting to determine the work factor of enhancing a fingerprint left behind by an person ignorant of the threats of fingerprint lifting (e.g. by stealing a used coffee cup from the café).

Acquiring a fingerprint from a victim can also be done by sniffing[4] the fingerprint image while it is transferred from the fingerprint reader to the PC. This can be done while the user is doing a genuine enrol or verify attempt. An attacker can then make a fake finger with the fingerprint image sniffed from the USB bus using the methods described in this report. Another possibility is for the attacker to launch a replay attack by replacing the fingerprint reader with a device that pretends to be the fingerprint reader and sends the captured image when asked to do a fingerprint scan. Determining the easiness of acquiring an fingerprint image these ways would be interesting.

8 Conclusion

Obtaining fingerprints from both cooperating and non-cooperating persons is possible with relatively low resources. With all the different combinations of experiments we tried, we had about 600 NOK (currently about $96) in various expenses, not counting the photosensitive circuit board. The most successful artificial finger we made, based on toner powder, tape, transparencies and wood cement can be made for almost no cost at all, provided a decent printer and a scanner are available.

We feel we have proven that obtaining a fingerprint from a target in a non-cooperative fashion and crafting a working artificial finger from it is a fairly easy process. The big question is then whether the process is easy enough to render fingerprint recognition as an authentication method useless or not, especially where a certain degree of security is required and supervised scanning is not possible. We can only hope that our findings with the optical sensor is not representative for higher-level sensor devices based on the same technology.

While we have shown that it is easy to fool the optical fingerprint sensor U.are.U 4000, fooling the capacitive Billionton sensor proved to be much harder. In fact we didn't manage to do that at all, but others claim to easily be able to fool capacitive sensors.

It seems to us that fingerprint recognition systems for small business and private use still have a long way to go before being considered to be secure. As sensors such as the ones we have tested are becoming more and more commonplace, we feel that extensive tests of a wide array of different sensors and

[4] Sniffing can be done with for example a hardware sniffer like the CATC Inspector available from `http://www.catc.com/products/usb.html` or a software-based sniffer like USB Snoop available from `http://benoit.papillault.free.fr/usbsnoop/`

brands should be conducted to try to establish the general level of security of such devices.

9 Acknowledgements

There are some people and institutes we would like to thank for making these experiments possible. We would thank NISlab for funding and equipment to realise the experiments, Arne Myhre at the college's electrical engineering lab for helping us with the PCB card and The Gjøvik University College Library for providing the digital camera.

References

[1] Davide Maltoni, Dario Maio, Anil K. Jain, and Salil Prabhakar. *Handbook of Fingerprint Recognition.* Springer Verlag, 2003.

[2] Ton van der Putte and Jeroen Keuning. Biometrical fingerprint recognition: don't get your fingers burned. In *Proceedings of the fourth working conference on smart card research and advanced applications*, pages 289–303. Kluwer Academic Publishers, 2001.

[3] Lisa Thalheim, Jan Krissler, and Peter-Michael Ziegler. Biometric access protection devices and their programs put to the test. *c't*, 2002. `http://www.heise.de/ct/english/02/11/114/`.

[4] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino. Impact of artificial "gummy" fingers on fingerprint systems. In Rudolf L. van Renesse, editor, *Proceedings of SPIE, Optical Security and Counterfeit Deterrence Techniques IV*, volume 4677, pages 275–289, April 2002.

[5] Antti Kaseva and Antti Stén. Fooling fingerprint scanners - Biometric vulnerabilities of the Precise Biometrics 100 SC scanner, 2003. `http://citeseer.ist.psu.edu/695069.html`.

[6] Marie Sandström. Liveness detection in fingerprint recognition systems. Master's thesis, Linköping Tekniska Högskola, 2004. `http://www.ep.liu.se/exjobb/isy/2004/3557/exjobb.pdf`.

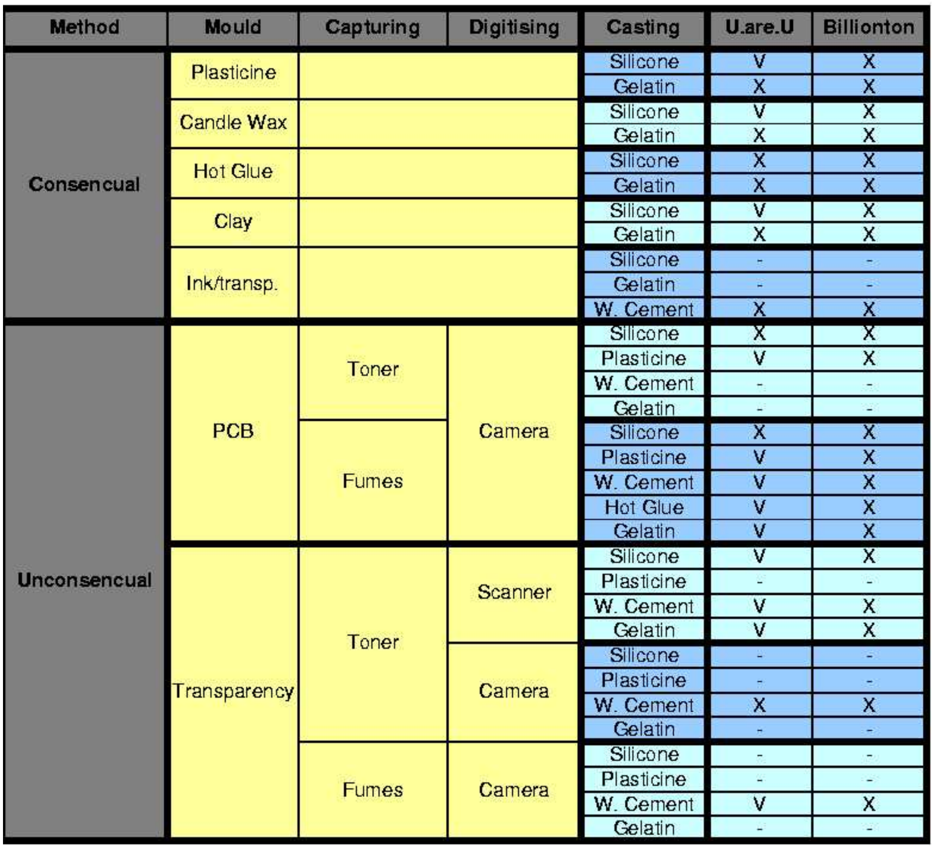
[7] Frank Rosengart / Chaos Computer Club Berlin. Fingerabdruck, 2004. `ftp://ftp.ccc.de/pub/video/Fingerabdruck_Hack/fingerabdruck.mpg`.

[8] A.J. Mansfield and J. L. Wayman. Best practices in testing and reporting performance of biometric devices, August 2002. `http://www.npl.co.uk/scientific_software/publications/biometrics/bestpr%ac_v2_1.pdf`.

[9] Lawrence O'Gorman. Fingerprint verification. In Anil K. Jain, Ruud Bolle, and Sharath Pankanti, editors, *Biometrics: Personal Identification in Networked Society*, pages 43–64. Kluwer Academic Press, 1999.

A Artificial Fingerprint Matrix

Figure 11 shows the different combinations of casts, moulds and lifting techniques we tried. “V” indicates successful fooling of the device, “X” indicates unsuccessful fooling and “-” indicates that we have not tried the particular combination.



Method	Mould	Capturing	Digitising	Casting	U.are.U	Billionton
Consencual	Plasticine			Silicone	V	X
				Gelatin	X	X
	Candle Wax			Silicone	V	X
				Gelatin	X	X
	Hot Glue			Silicone	X	X
				Gelatin	X	X
	Clay			Silicone	V	X
				Gelatin	X	X
	Ink/transp.			Silicone	-	-
				Gelatin	-	-
				W. Cement	X	X
Unconsencual	PCB	Toner	Camera	Silicone	X	X
				Plasticine	V	X
				W. Cement	-	-
				Gelatin	-	-
		Fumes		Silicone	X	X
				Plasticine	V	X
				W. Cement	V	X
				Hot Glue	V	X
				Gelatin	V	X
	Transparency	Toner	Scanner	Silicone	V	X
				Plasticine	-	-
				W. Cement	V	X
				Gelatin	V	X
			Camera	Silicone	-	-
				Plasticine	-	-
				W. Cement	X	X
				Gelatin	-	-
		Fumes	Camera	Silicone	-	-
				Plasticine	-	-
				W. Cement	V	X
				Gelatin	-	-

Figure 11: A matrix of tried combinations.

B Last Minute Tests and Results

Very late in our project period, we got access to a number of new fingerprint sensor devices. Rather than rewriting our entire report in less than a day, we present our preliminary results with these devices in this appendix.

B.1 The Sensors

B.1.1 Solid State Capacitive Sensors

We got two sensors made by the Taiwanese manufacturer CanSecu (or CanSeuc, depending on whether the device itself or the accompanying software is used as reference). Much as Billionton, they have just wrapped the following solid state sensors in a rubber wrapping with a USB connection.

Fujitsu MBF200 This is a capacitive solid state sensor with a 12.8x15 square millimetres sensing area comprising of 78,600 capacitive sensors arranged in a 256x300 array. The sensor generates a 500 dpi image of the fingerprint.

AuthenTec AES4000 This is the big brother of the solid state chip which was used in the Billionton sensor described in the report proper. The AES4000 has a larger sensing area than AES3400, but a lower dpi. Its sensing area is 9.75x9.75 square millimetres and with 9,216 capacitive sensors organised in a 96x96 array it yields 250 dpi images.

B.1.2 Optical Sensors

Biometrika FX2000 This is probably the first sensor we have tried which is not aimed at the small business or private market. It has a built-in 32 bit RISC CPU which handles tasks like encrypting the communication channel and fingerprint feature extraction. The sensor has a fairly large sensing area of 25x13.2 square millimetres and an acquisition hardware which yields 569 dpi, the highest of the sensors we have tried.

Tacoma Technology CMOS Desktop USB Scanner Little is known about this sensor's manufacturer, however the retailer operates with the following specifications: sensing area of 13x13 square millimetres and a CMOS camera yielding a resolution of 500 dpi.

B.2 Results and Discussion

Given the late arrival of these sensors, we have only tested them using three of our already made artificial fingerprints. We tested the silicone finger shown in figure 3 which was cast in a moist clay mould (from the consensual experiments), and a couple of weeks old and rather crusty wood cement finger which was made from a dusted fingerprint lifted with broad transparent tape and a scanner, then printed on a transparency (from the unconsensual experiments).

As a last test, we also used the artificial finger we got when we applied silicone to the same transparency mould we used for the wood cement artificial finger (from the unconsensual experiments).

Our results with the new sensors are summarised below in table 4.

Sensor	Sample	Result
AuthenTec AES4000	Cons. Silicone	Not Fooled
AuthenTec AES4000	Wood Cement	Not Fooled
AuthenTec AES4000	Breath	Not Fooled
Fujitsu MBF200	Cons. Silicone	Fooled
Fujitsu MBF200	Wood Cement	Fooled
Fujitsu MBF200	Breath	Fooled
Biometrika FX2000	Cons. Silicone	Fooled
Biometrika FX2000	Wood Cement	Fooled
Biometrika FX2000	Uncons. Silicone	Fooled
Biometrika FX2000	Breath	Not Fooled
Tacoma Optical	Cons. Silicone	Fooled
Tacoma Optical	Wood Cement	Fooled
Tacoma Optical	Uncons. Silicone	Fooled
Tacoma Optical	Breath	Fooled

Table 4: Results from the last-minute experiments.

Yet again, it seems that the sensor from AuthenTec is very resistant towards artificial fingers. Nothing we tried worked.

Just dry silicone and wood cement did not work on the solid state Fujitsu sensor, however it was easily fooled using both artificial fingers once we applied a tiny amount of saliva onto them, making it possible for them to build up capacitance. Being on a roll, we figured we could try breathing on it as well. To our incredible astonishment, it worked! We also tried this on the AES4000, which did not react to the breathing at all. We would never have thought that latent fingerprint reactivation was possible in this time and day.

Unfortunately we did not have enough time to be able to test the two solid state sensors against gelatin, something which would have been very interesting to try.

As for the optical sensors, the rather expensive Biometrika FX2000 ($254) was fooled by our now very degraded wood cement artificial finger, which was rather surprising to us. We got matching scores between 50 and 370. It is to be said however, that in the case of the FX2000, the threshold for accepting a fingerprint should possibly be set higher than 47 as is the case with the U.are.U sensor. We believe this because when testing against a genuine finger, we consistently got higher matching scores than with the U.are.U sensor. We attribute this to the FX2000's superior resolution and larger sensing area.

Both optical sensors were also fooled by the thin silicone finger from the unconsensual experiments. This is an artificial finger with just a minimum of height differences between ridges and valleys.

Given that the Tacoma optical sensor does not have any form of finger recognition (i.e., it's camera is always on even if there is no finger on the sensing area), we figured it couldn't hurt to try breathing on it, as we did with the Fujitsu solid state sensor. Given our astonishment when the solid state sensor was fooled, we were totally floored when we actually managed to fool the optical sensor by simply breathing on it.

It is to be noted that the Digital Persona, Tacoma, Biometrika and AuthenTec sensors included in this report all use the same extraction and matching software, namely the VeriFinger SDK. This may or may not be a disadvantage when doing comparisons between sensors. Personally, we believe that this can only be helpful when doing comparative evaluations between the sensors, as the fingerprint feature extraction algorithms will be static while the scanners themselves and the fingerprint images they deliver will be varying. The matching scores will then be directly comparable. We believe that it is either up to the device itself or its drivers to implement liveness detection and reject fingerprint images which are of too low quality.

On a related note, we would also like to state that the results in this appendix were obtained via the VeriFinger SDK's demo implementation software, as support for these new sensors is not implemented in NISlab Authentication Workbench at the time of writing. However, as the Fujitsu sensor was not supported by the VeriFinger SDK, we tested it by using the accompanying log-on manager software. As this software also supported the Tacoma optical sensor, we double checked our findings with the Tacoma sensor using this software. We obtained the same results.