Challenging fingerprint scanner

Vidar Ajaxon Grønland, Håvard Hasli, Jon Fredrik Pettersen

October 16, 2005

Abstract

This project, studys former articles on making fake fingers to fool a fingerprint system. Based on these articles we will set up some experiments that we think might work. In authentication systems it is crucial that the finger being read is indeed a real finger, and not a produced fake finger made from an authentic user of the fingerprint system. In this project we will look at ways to fool a fingerprint reader. Through several experiments we show how to make a fake fingerprint, using products that are easily available to the public. The fingerprints we used was voluntary extracted from members of the group writing this project report. The experiments were done at the Authentication laboratory at NISLab at Gjøvik University College.

Contents

1 Introduction

In today's society, we are very dependent on computer systems and their ability to keep our information from others. Therefore, authentication has become a very important tool in securing computer systems. There are many different approaches on how to authenticate users, i.e. something you know (password,PIN[1]), something you have (Smartcard[2], token) and something you are (biometric[3]). Biometric systems are very convenient because they only need something you are, and not something you know. What this mean is that you do not have to walk around remembering passwords and PIN's, you just bring along your body. In this project we are going to look into fingerprints, which is a biometric authentication method.

Fingerprints are one of the most widespread biometric systems used today. The reason for this is most likely because the fingerprint scanners have become quite affordable, are small in size and people find them quite convenient to use. The downside of fingerprint authentication is that they are allegedly easy to fool[3]. The goal of this project is also to try to fool two types of fingerprint scanners that we have access to in our laboratory created by NISLab[4].

Fingerprints are a unique marker for a person, even an identical twins have different prints. While two prints may look basically the same at a glance, a trained investigator or an advanced piece of software can pick out clear, defined differences. This is the basic idea of fingerprint analysis, in both crime investigation and security. A fingerprint scanner's job is to take the place of a human analyst by collecting a print sample and comparing it to other samples on record. In section 4.2.1 and 4.2.2, the two types of scanners we will use are explained.

There are basically two methods of approach when it comes to duplicate fingerprints, with or without co-operation. Because of the limited time we have, we will only duplicate fingerprints made in co-operation with the owner, meaning we will try to fool these scanners by making fake fingers based on our own fingers. This also makes it much easier for us to conduct the experiments when our time schedule allows us to. The reason we will only use our own

[1] A personal identification number (PIN) is a numeric value that is used in certain systems to gain access, and authenticate. PINs are a type of password.

[2] Smartcard = A smart card, or integrated circuit(s) card (ICC), is defined as any integrated circuitry embedded into a flat, plastic body.

[3] Biometric = Biometrics is the science and technology of authentication (i.e. establishing the identity of an individual) by measuring the subject person's physiological or behavioral features.

[4] NISLab = Norwegian Information Security Laboratory at Gjøvik University College

fingers is also of ethical and legal issues discussed in chapter 3. In [3]there is explained how to make a fake finger without co-operation.

2 Literature study

A lot of papers have been subject to test if fingerprint scanners are vulnerable to attack by fake fingers. A lot of these have found that it's indeed possible to fool a fingerprint authentication system. One of the earliest articles showing that fingerprint scanners are not very reliable is [1]. In this article the authors describe two methods of making a fingerprint, one with owner co-operation and the other without co-operation. The method of co-operation uses a plaster cast of the finger that is filled with silicon rubber to create a wafer-thin silicon dummy of the finger. To duplicate a fingerprint without the cooperation of the owner, one possibility is to lift the latent fingerprint from a fingerprint scanner. To capture this fingerprint, use fine powder to enhance the fingerprint and remove it with scotch tape. To create a mould of the fingerprint it should be transferred to a photo sensitive PCB. You can use a Dremmel-tool to make the mould deeper, before you create the fingerprint with silicon[1].

In [2], there are several fingerprint scanners that is put to the test. In the test they find that breathing on the fingerprint sensor activates the sensor, making the fat from former fingerprints being scanned. They also use a plastic bag of water, to reactivate the latent fingerprint.

It has been proven that faking both volunteer and prints taken from a surface, can successfully be reproduced by using supplies bought at any grocery store. The results can be found in a study[3], written by Tsutomu Matsumoto et al. This paper reports that gummy fingers, namely artificial fingers that are easily made of cheap and readily available gelatine, were accepted by extremely high rates by particular fingerprint devices with optical or capacitive sensors. It also fooled the liveliness detection that many producers of equipment implemented after a study[4] that concluded it was possible to fool fingerprint sensors with artificial fingers made out of silicone.

3 Ethical and legal issues

Because of the increased terrorist activity the last few years, biometric authentication methods have been more frequently used[5]. This is because biometric methods is know to be a good measure of who you are, and can be used with good certainty to recognize you from other persons. People's threshold to accepting stronger security measures and less privacy has also been lowered, due to these terror attacks.

But still people may have personal or religious reasons for not liking the use of biometric. This is both the application of the devices and the usage of them. Especially elder people don't like to use new technology and retina scan may seem hard to accept for them. Also people from non-technology countries may fear the use of such technology, just as the native Americans feared that taking a photograph of them would steal their soul. Finally there are philosophical objections to the perceived loss of autonomy and control if the use of biometrics is so wide spread as to become virtually required to conduct the day-to-day aspects of one's life[6].

Biometric technologies don't just involve collection of information about the person, but rather information of the person, intrinsic to them[7]. Many people see the process of scanning fingerprints as analogues to crime and police business.

Fear of disease

Having several people touch the same biometric equipment will in peoples minds, (probably true), increase transfer of bacteria and possibly diseases. The equipment will also get smudgy leading to greater FRR[5], and possibly queues. Clean environment and information to the public to clean their hands before and after scan would possibly dampen this fear. Another solution would be UV light on top of the sensor when its not in use. UV light kills most of the bacteria, by removing its ability to replicate itself[8].

Fear of criminal activity

Watching too many movies most public presumably believes that cutting a finger of you will be enough to circumvent fingerprint censors. This is a false consumption since most high level security sensors implements liveliness detection additionally to the scan itself. The criminal will probably force you to authenticate yourself by means of threats or other methods.

While using biometrical access methods all day people fear the "BigBrother"-effect leaving traces of where you have been/done. Already today you may trace many people by simply tracing their credit card records, so biometrical data wouldn't increase the possibility to trace you significantly. Giving records to third parts also concern people, but good "contracts" or laws should prevent this. One possibility is that you carry your own id card with

[5] False Rejection Rate is the expected propotion of transactions with truthful claims of identity(in a positive ID system) or non-identity(in negative ID system) that are incorrectly rejected[10]

your biometric information unlocking the code to whatever place/terminal you need to enter, so your biometrics wouldn't have to be stored any other place than your card.

Laws
Most countries have laws that protect people against misuse of personal information, some weaker than other. Ann Cavoukian explains this in a good manner in her report as follows[6]: The rights to privacy and fair information practices are part of the legal framework of most countries and come into play when dealing with any identification system like the biometrics technologies mentioned here. There are other, non-criminal, legal issues that may surround biometric systems. Labour laws in many jurisdictions limit the information that employers may require employees to provide. Privacy laws limit the disclosure of information to third parties for a purpose not consistent with the purpose of the original collection. Privacy laws may also restrict the merging of disparate databases. This would limit the ability to match biometric and other electronic information to develop a comprehensive profile about an individual. One problem with this is that the general public does not know how the biometric methods work. It is a well known phenomenon that people is not found of using technology that they don't understand or seem intimidating[6].

The reason we only used our own fingers in this project
Gathering personal data is regulated by law[9] in Norway, it states that gathering and storing personal information of an individual requires that individual's acknowledgement. When gathering such information as fingerprints one should present the candidate with a paper (consent paper) which states the purpose of the use of the data and ensure that the data won't be used in other purposes than the tests[10]. Further the test data should be anonymized by adding candidate numbers instead of names. Due to the limited time we had finishing this project we consequently decided to use ourselves as test persons, taking all responsibility of our actions.

4 Rules and planning

4.1 Rules

The experiments will take place in the NISLab laboratory located at the college. We will use the two fingerprint scanners listed in section 3.2. All tests will be performed by the same persons in the same environment. Because of the time-consuming activities in the experiments there will only be two test persons, both using their right index finger during the testing. If we were to have more test persons, we would have done what is stated in the ethics section regarding the consent paper. We also would have had to create some rules regarding storing the biometrics of the other persons. The results of the experiments do not have a scientific value due to the few people involved and the fact that we reproduced experiments already performed by others. Having said that, our goal was only to fool the fingerprint scanners in the lab just to se how easy it really is, and the how much it would cost.

4.2 Available resources

The biometric sensors we have used in the experiments are:

- Digital Persona U.are.U 4000(Optical sensor)
- Billionton(Capacitive sensor)

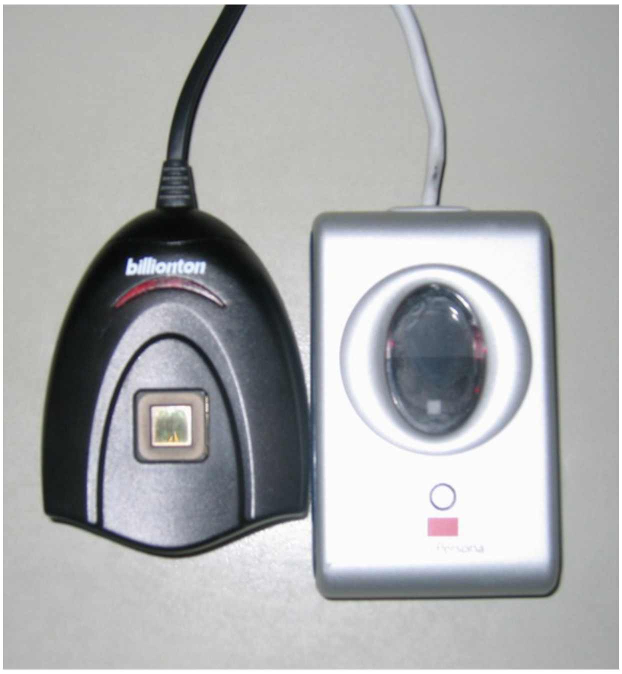


Figure 1: The two fingerprint scanners we used(Billionton to the left)

4.2.1 Optical sensor: Digital Persona U.are.U 4000

The heart of an optical scanner is a charge coupled device (CCD), the same light sensor system used in digital cameras and camcorders. A CCD is simply an array of light-sensitive diodes called photosites, which generate an electrical signal in response to light photons. Each photosite records a pixel, a tiny dot representing the light that hit that spot. The light and dark pixels form an image of the scanned scene. The Digital Persona U.are.U represents the picture in 8bit grayscale. The scanning process starts when you place your finger on a glass plate, and a CCD camera takes a picture. The scanner has its own light source, typically an array of light-emitting diodes, to illuminate the ridges of the finger. The CCD system actually generates an inverted image of the finger, with darker areas representing more reflected light (the ridges of the finger) and lighter areas representing less reflected light (the valleys between the ridges).

The manufacturer claims that this reader has latent print rejection and counterfeit finger rejection. We will try to disprove these properties later in the report. Some key specifications on the reader are:

- Pixel resolution: 512 dpi
- Scan capture area: 14.6 mm x 18.1 mm
- 8-bit grayscale (256 levels of gray)

This fingerprint sensor is priced in the range around 100-120 US Dollars. This makes it affordable for even the smallest companies and private persons.

4.2.2 Capacitive sensor: Billionton

This scanner is in the category of solid state sensors. Like optical scanners, capacitive fingerprint scanners generate an image of the ridges and valleys that make up a fingerprint. But instead of sensing the print using light, the capacitors use electrical current.

The sensor is made up of one or more semiconductor chips containing an array of tiny cells. Each cell includes two conductor plates, covered with an insulating layer. The cells are tiny, smaller than the width of one ridge on a finger. The small electrical charges that is made between the finger and each of the silicon plates, is used by the scanner to see whether the current came from a ridge or a walley on the finger[11]. This scanner has a much smaller area of which the finger is read than the U.are.U scanner. Because of this we believe that this scanner will be harder to fool since it only scans

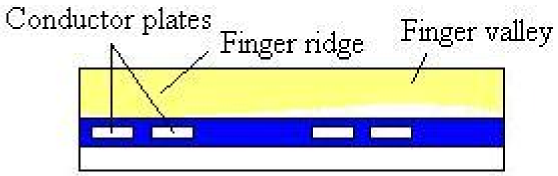


Figure 2: Capacitive reader

a little part of the finger, meaning that the forged fingerprint must be of very good quality. This scanner is sensitive against electrostatic discharges (ESD), chemical corrosion and physical scratches to the sensors surface[11].

Some key specifications on the Billionton reader are:

- The sensor matrix is comprised of 16,384 individual elements arranged in a 128x128 Square Pattern (500 pixels per inch, ppi)
- FAR : False Acceptance Rate (FAR) : 0.015%
- FRR : False Rejection Rate (FRR) : 2.3%

4.2.3 NISLab authentication workbench

This is the software which we will perform the experiments. It is possible to choose which devices you want to use with the SW. We only used the two fingerprint sensors from Billionton and Digital Persona.

4.3 What we are planning to do, and what results we believe to find

We will try to reproduce some of the experiments found in the literature we have studied. The goal is to at least fool one of the sensors. We believe that using gelatine to represent the prints is the most likely material that will work, but we also have faith in silicone. Gelatine is the substance that resembles human skin the best when it comes to moist and resistance, so this is our best shot at fooling the capacitive sensor. We will conduct the experiments to find out which of the following hypothesis is true:

- H0: Can't fool the fingerprint scanner.
- H1: The fingerprint scanner can be fooled.

5 Fooling fingerprint sensors

Intro to the experiments

We were two test persons conducting the experiments, test person A and B. Each fingerprint in each experiment was tried 20 times on each sensor. The scanners was cleaned when they looked smudgy. We only used our right index fingers. All the experiments will be carried out in the NISLab at Gjøvik University College, using the NISLab Authentication Workbench software.

5.1 Making the moulds

Plastic clay

In experiment 1-5, we used plastic clay for moulds. They were made by first kneading the plastic clay, and then press the finger into it. On some of the moulds we had to improve the height of the edges so that the material pored into it did not leak out. Before we removed the fingerprints, we froze the mould over night so that it would be easier to collect the fingerprint without destroying it.

Plaster

Then in experiment 6-8, we used plaster for the moulds. One of the test persons (test person A) poured the plaster into a little cup, and waited until the plaster was almost dry. He then pressed his finger into it, at held it there until it was completely dry. The whole process took 20 to 25 minutes. The other test person (test person B) used plastic clay around the finger to create ”walls”, and then poured plaster into it. This approach was used to be certain that the finger did not move while the plaster hardened. This process also took about 20 minutes. The downside of using plaster as a mould is that it is highly unlikely to be used when making a fingerprint without cooperation. The plastic clay is also unlikely to be used, but you might be able to fool someone to play with the clay and hope they leave a good fingerprint.

Candle wax

In experiment 9, we lit two tea-lights and waited until it was completely melted. Then we dipped our right index finger several times until we had a fairly stiff mould. We then removed the mould very carefully.

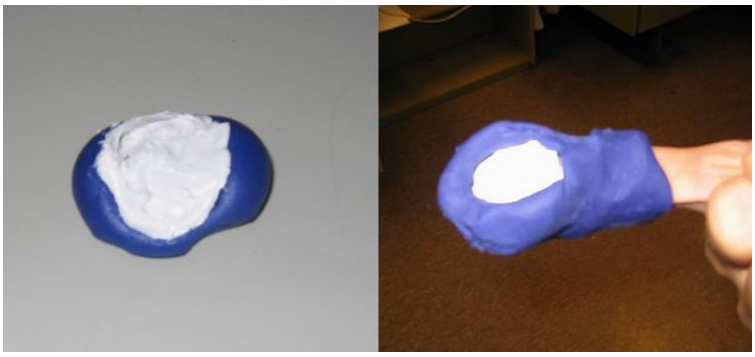


Figure 3: Plaster mould used by test person B to the right. Mould used by teste person A to the left.

5.2 Results

Experiment 1:
Plastic clay as mould, and gelatine as finger.
Gelatine mixture: 2 plates of gelatine and 0.5 dl of warm water.

- Test person A: Not able to activate any of the scanners.
- Test person B: Not able to activate any of the scanners, possibly because of bubbles in the gelatine and the fact that the gelatine was very hard.

Time consumed: 10min + 30 min for hardening the gelatine.

Experiment 2:
Plastic clay as a mould, and wood cement as finger.

- Test person A: Not able to activate any of the scanners
- Test person B: Activated the optical scanner, but got zero in similarity. Not able to activate the capacitive scanner.

Time consumed: 3min + 2 days for hardening the cement.

Experiment 3:
Plastic clay as mould and hot glue as finger.

- Test person A: Not able to activate any of the scanners
- Test person B: Not able to activate any of the scanners

Time consumed: 10min + 30 min for hardening he glue.

Experiment 4:
Plastic clay as mould and glass silicone as finger.

- Test person A: Activated the optical scanner, bad picture quality. Not able to activate the capacitive scanner.

- Test person B: Activated the optical scanner, very good picture quality but still got zero in similarity. Not able to activate the capacitive scanner.

Time consumed: 5min + 1 day for hardening the silicone.

Experiment 5:
Plastic clay as mould and bathroom silicone as finger.

- Test person A: Not able to activate any of the scanners

- Test person B: Partly picture on the optical scanner, but zero in similarity. Not able to activate the capacitive scanner

Time consumed: 5min + 1 day for hardening the silicone.

Experiment 6:
Plaster as mould and gelatine as finger.
Gelatine mixture: 2 plates of gelatine and 0.5 dl of warm water.

- Test person A: Activated both scannerss, but got zero in similarity.

- Test person B: On the optical scanner: Zero in similarity for the first 16 tries, but got 90 in similarity on the 17th try and 54 on the 18th try. Activated the capacitive scanner but got a very bad picture so it failed.

Time consumed: 25min + 30min for hardening the gelatine.

Experiment 7:
Plaster as mould and wood cement as finger.

- Test person A: Not able to activate any of the scannerss

- Test person B: Fingerprint broke when it was removed from the mould.

Time consumed: 25min + 2 days for hardening the silicone.

Experiment 8:
Plaster as mould and glass silicone as finger.

- Test person A: Activated the optical scanner, zero in similarity. Did not activate the capacitive scanner.

- Test person B: On the optical scanner: Success on all tries. Best result was a similarity of 165. Not able to activate the capacitive scanner.

Time consumed: 25min + 1 day for hardening the silicone.

Experiment 9:
Stearine as mould and wood cement as finger.

- Test person A: Fingerprint broke when it was removed from the mould

- Test person B: Not able to activate any of the scannerss

Time consumed: 20min + 2 days for hardening the cement.

Experiment 10:
Use latent fingerprint already on sensor and breathe on it to activate it. Time consumed: 3min. Also tried to use a bag with warm water, but it would not activate. This experiment was only performed on the optical scanner.

Experiment 11:
Two sided scotch tape with fingerprint on it, put it on the sensor and use a transparent to activate it. Time consumed: 3min. Only performed on the optical sensor. Failed to activate the sensor most of the times. When we managed to activate it, we got something that looked like a double print. This was not very surprising since the scanners probably recorded the finger used to push the transparent in addition to the print on the tape.

See Appendix B for a table with the results.

5.3 Summary of experiments

As the results above show, we were able to fool only the optical scanner. Hence the H1 hypotesis is true for the Digital persona U.are.U 4000. As for the Billionton scanner we see that hypotesis H0 is true, which was not very surprising since the capacitive sensor uses a more advanced way of checking the finger (see 4.2.2). We were hoping to fool it with the gelatine finger, but we were only able to activate it but did not get a match. Reasons for failure to activate and failure in similarity are listed below.

Sources of fault

- Inhomogeneous quality of the moulds made by plaster and plastic clay.
- Differences in valley depths on the fingertips of the test persons.
- Unable to remove all the clay from the fake fingerprints without destroying it.
- Some of the materials were not completely dry inside when they were removed from the moulds.
- The gelatine evaporated during the hardening process, leaving us with a fingerprint that was impossible to remove from the mould. This could probably have been prevented by putting the moulds with the gelatine directly into the freezer right after it had been poured in.
- Bad choice of materials for the moulds should probably have used another type of clay that hardens in air or by heating in oven. This would have made it much easier to remove the materials from the mould.
- The mixture of gelatine and water is important to get the right consistence, especially when it comes to fooling the capacitive sensor.
- Latent fingerprints leaves noise on the sensor.

5.4 Other experiments

Other experiments we could have tested is to copy a fingerprint onto a transparent and then put a layer of glue on top of it to retrieve an imprint. This experiment was deemed wasted since none of the members of the project group thought it would work because the ridges probably would have been too small to create a copy of the imprint.

A solution to getting the ridges improved and larger would have been to use some sort of print card for electronics and make the imprint in the same way you would make an electronic circuit board[3]. Another possibility could be the use of a 3D-printer like the ones found at http://www.zcorp.com however the cost of such a device makes it out of range for most of the population.(HiG is planning to buy such a printer so trying to see if it may work would be a nice follow up task)

5.5 Ways to attack a biometric system

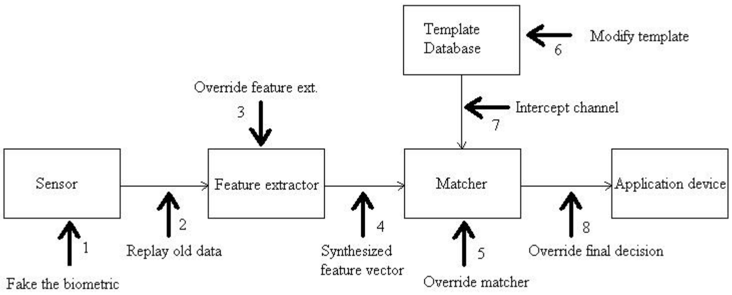


Figure 4: Ways to attack a biometric system

In this figure we see the ways of fooling a biometric system. In this project we have attacked using possibility 1 and 2. A more detailed overview of the eight ways of attacking the system can be found in[12].

6 Conclusion

The potential for spoofing a fingerprint system raises a number of questions related to the types of application best protected by this biometric. Firstly, identification by the fingerprint cannot provide conclusive proof of an individual's presence, which has been proven to some extent in our experiments. Secondly it is also the "only" system where the biometric characteristics can be stolen without the owner noticing or reasonably being able to prevent it. This certainly does not mean fingerprint technology is poor and unreliable, but each company considering installing one must think of the possibilities that could compromise the system. In high security systems fingerprints should be used in combination with tokens and/or passwords. By using a smartcard on which the user's template fingerprint is stored, the possibility of unnoticed access is reduced considerably. Another way of making it harder to fool the sensors is to acquire a sensor which has liveliness detection. One must also have in mind that anyone could break into a system if they put enough effort and resources into it. The problem with fingerprints, as we have seen, is that even amateurs as our selves were able to make dummy fingers good enough too fool at least the optical sensor. There is no need to say what an expert is able to do with better materials.

References

[1] Ton van der Putte and Jeroen Keuning, *Don't get your fingers burned*

[2] Lisa Thalheim, Jan Krissler, Peter-Michael Ziegler, *Body Check*

[3] T. Matsumoto et.al *Impact of Artificial "Gummy" Fingers on Fingerprint Systems*(2002).

[4] *Network Computing: Six biometric devices point the finger at security, reviews, pp. 84-96 (1998). Also to be referred at URL: http://www.networkcomputing.com, August.*(2000).

[5] *Wayne penny, A double edged sword - security and privacy*
http://www.sans.org/rr/whitepapers/authentication/137.php

[6] Ann Cavoukian, Ph.D. *Biometrics and Policing: Comments from a Privacy Perspective Commissioner*
www.ipc.on.ca/docs/biometric.pdf (1999).

[7] Roger Clarke *Biometrics and Privacy*
http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html

[8] *UV light kills bacteria http://en.wikipedia.org/wiki/Uv_light#Sterilization*

[9] Personopplysningsloven
http://www.lovdata.no/cgi-wift/wiftldles?doc=/usr/www/lovdata/for/sf/mo/mo-20001215-1265.html&dep=alle&kort+,+titt=personopplysning&

[10] A.J Mansfield et.al *Best practice in testing and reporting performance of biometric devices*(2002).

[11] Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhkar *Handbook of fingerprint recognition*(Springer 2003).

[12] Nalini K. Ratha, J.H Connell, R.M Bolle *An analysis of minutiae matching strenght*

Appendix

A Products

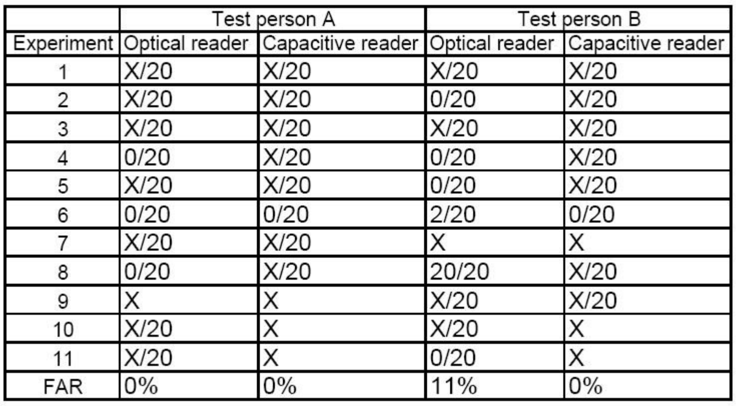
- Gelatine: Gelita Gelatine, price 7,80 NOK pr. packet
- Glass Silicone: Bostik Sillicone Glass, price 73,20 NOK 0,3l
- Wood cement: Bostik Super trelim 730 Ute, price 72 NOK 0,5l
- Plastic clay: Omya Patplume price 45 NOK
- Hot glue: panduro hobby smeltelim, price 39 NOK a 12 pcs
- Plaster: Global syntetisk gips, price 29 NOK 1kg
- Bathroom silicone: CASCO, price 62,40 NOK 0,3l
- Transparent, price free.
- Tealights: Firstprice by RIMI, 19 NOK 100pcs

Total cost: 363 NOK

These cost were divided between two groups that conducted the same experiments. This was made possible because of the small amount of material that is needed for each experiment.

Appendix

B Results



	Test person A		Test person B	
Experiment	Optical reader	Capacitive reader	Optical reader	Capacitive reader
1	X/20	X/20	X/20	X/20
2	X/20	X/20	0/20	X/20
3	X/20	X/20	X/20	X/20
4	0/20	X/20	0/20	X/20
5	X/20	X/20	0/20	X/20
6	0/20	0/20	2/20	0/20
7	X/20	X/20	X	X
8	0/20	X/20	20/20	X/20
9	X	X	X/20	X/20
10	X/20	X	X/20	X
11	X/20	X	0/20	X
FAR	0%	0%	11%	0%

Figure 5: Result table

- By X/20 we mean that we were not able to activate the reader.
- By 0/20 we mean that we were able to activate the reader, but did not get any similarity.
- By X we mean that the experiment was not perfomed.