Norwegian University of
Science and Technology

Creating 3D-artefacts for spoofing fingerprint readers

Emil Volckmar Ry

Master in Information Security
Submission date: May 2018
Supervisor: Guoqiang Li, IIK
Co-supervisor: Patrick Bours, IIK

Norwegian University of Science and Technology
Department of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Creating 3D-artefacts for spoofing fingerprint readers

Emil Volckmar Ry

01-06-2018

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Information Security and Communication Technology
Norwegian University of Science and Technology,

Supervisor: Prof. Patrick Bours
Co-Supervisor: Dr. Guoqiang Li

Preface

This thesis concludes the two years Master in Information Security at NTNU Gjøvik. The idea came about whilst being an TA for Patrick Bours and trying to find a suiting demo for the biometrics part of IMT4113, introduction to Cyber and Information Security Technology. This thesis is intended for anyone interested in biometric fingerprint artefact generation and others interested in biometrics.

Gjøvik, 01-06-2018

Emil Volckmar Ry

Acknowledgment

I want to express my gratitude to my supervisor Guoqiang Li, whom since the start of the thesis work has been professional, helpful and encouraging. He has been a real teamplayer helping me to achieve the best result possible. Without him, this thesis would not be what it is. I would also like to thank Kjell Sandnes as well as all the other eager students at ADDLABS, whom has shared of their knowledge and joy for 3d printing which has been contagious. Adding to this, I would also like to thank Pål Erik Endrerud for his help with modelling when my own efforts are not enough (which has been many, many times). I would also like to thank Patrick Bours, which encouraged me and helped me through the early stages of planning, and connected me with Guoqiang Li.

I would also like to thank my colleagues, and specifically Kristian Dragerengen for lots of good two hour lunches as well as constructive feedback which has made my thesis much better ;)

Finally I would like to thank my girlfriend and my parents who have been really supportive through the work on my thesis.

E.V.R

Abstract

The advent of mobile phones have changed the way we use our phones. It is not only the way we use our phones that have changed, we now secure our devices using biometrics. The industry is also implementing biometrics into their applications which means that personal services such as banking and other financial applications are using biometric authentication. Thus the value of what we protect with biometrics is also increasing at a rapid pace. This makes the need for auditing of biometric modalities in mobile devices and sensors important. The focus of the thesis is on how vulnerable the system is to artefacts, made with limited resources using readily available filaments.The current state of the art research in biometric 3d printed artefact generation focuses on making durable artefacts for repetitive testing of different sensory devices. The problem with these artefacts are that they are expensive to produce. Thus the motivation of this thesis is to make production of artefacts more affordable by using less accurate and non proprietary materials to explore the possibilities with "off the shelf" filaments and printers.

In this thesis we propose a more affordable alternative to artefact generation using Prusa I3 MK IIs which can produce good results above 50 microns[1], is less accurate compared to the current state-of-the-arts 16 microns[2]. This is done with off-the-shelf filaments with time saving modelling techniques, which does most of the modelling based on 3d auto generation from an image. Artefacts made in different materials for different purposes are presented and tested on their respective sensory devices as well the materials themselves. An artefact generated from a self made capture is also made to describe how a full manufacturing process would look like. The effect of image enhancement is investigated. We use the artefacts we generated to look at similarity scores before and after enhancement. The interoperability between a enhanced artefact and a raw artefact is investigated. These two artefacts are then used to check for interoperability between several captures from the same subject in the FVC2002db2 database. Mobile sensory devices are tested using conductive materials.

Artefacts for optical sensory devices have shown great promise on this affordable printer. We are able to be recognized as a genuine user by the commercial comparator. The effects of image enhancement and interoperability between artefacts have shown to better for artefacts which has had been enhanced having a significantly higher average(120) similarity scores than raw artefact(50). Additionally, while our findings indicate that while artefact generation for devices such as the conductive sensor devices was not successful, we are able to craft artefacts which can be enrolled and authenticated on a phone. However, presented with the original human finger, it is not recognized as the same finger. This is most likely due to scaling.

Contents

List of Figures

List of Tables

1 Introduction

1.1 Topic covered by the project

Biometric recognition, or biometrics, refers to the use of distinctive anatomical and behavioural characteristics or identifiers like fingerprint, face, iris, voice or hand geometry to automatically recognize a person[4]. Biometric devices are gradually becoming intertwined into our daily lives and is quickly becoming an authentication device for "everyone", quickly getting adopted into systems such as smart devices, like the Iphone X and other phones. We are now, more than ever, relying on our devices' biometric capabilities. This is not coincidental. Biometric systems have the potential of being more secure than the existing systems to date, such as pin codes or other types of passwords. Pin codes and passwords, given good brute force capabilities, or other types of attacks, can easily be attacked on entropy alone. This can of course be done with fingerprints, but their entropy will be far greater than that of an eight character password.

Biometrics has gained prominence not only in our digital life, it has changed how border control operates. In US border control[9], a automated fingerprint recognition system is operational. In the EU this is set to be operational in 2020[10]. In India the Adhaar program[11] is the biggest biometric system in the world, involving around 1.19 billion Indians, capturing both their facial features as well as all 10 fingerprints per subject. Fingerprinting is becoming ubiquitous in the sense that almost all devices we carry has a fingerprint sensor of some variation. Biometrics is gradually being adopted into more security devices as well as our personal devices. Specifically the use of fingerprints has been gaining prominence in smart phones with over 700 million[12] devices delivered with a fingerprint sensor, and lately face recognition in the Iphone X[13].

Biometrics rely to a large degree on the seven characteristics of biometric functionality defined by Jain et al.. [14] such as:

- universality (everyone has one)
- uniqueness (different from all individuals)
- permanence (permanent in nature)
- measurability (can be easily collected and processed. It is easy to extract relevant feature sets)
- performance (speed, robustness of technology)
- acceptability (people are willing to use it)
- circumvention (hard to fool by either artefact or substitute)

To put these requirements into perspective, we can look at the fingerprint. In recent years, fingerprint recognition-based systems are becoming an accepted standard of authentication in smart devices. Based on Jain's functionality requirements this is not hard to understand.

In terms of universality, most people have at least one finger. Furthermore, the fingerprints uniqueness was determined in 1880 by Henry Fauld[4], and is today what we rely upon when signing into our digital devices. The notion of permanence of fingerprints, have been established by Herschel in 1888[4], and is a well known fact today. In terms of modern devices, the ease of fingerprint scanners is alluring, as collecting is easy, and performance is quite quick on most devices. It seems that fingerprints are well accepted in terms of acceptability; while people are sceptical to unlock their phones with their face towards the phone in public, most people accept the use of finger scanners.

To distinguish fingers, their ridges and valleys are interpreted. We can see ridges and valleys in figure 1. The ridges are the highest points and valleys are the low points in this image. Fingerprint scanners use these to find minutiae points.

Figure 1: Ridges and valleys in a photo[3]

There are many types of fingerprint scanners, but optical and capacitive sensing is the most widespread. Simplified, these sensors read your fingerprint line by line and differentiates between ridges and valleys in order to "read" the fingerprint. Depending on the sensor this is done differently. Optical sensors, like the one presented in figure 2, works when finger touches the top side of the glass/plastic prism and the ridges are in optical contact with the prism surface, but valleys remain at a certain distance. When light is directed through the prism it is reflected at the valleys while ridges absorb the light[4]. Since ridges absorb the lighting allows the ridges to be distinguished from the valleys, which appear bright.

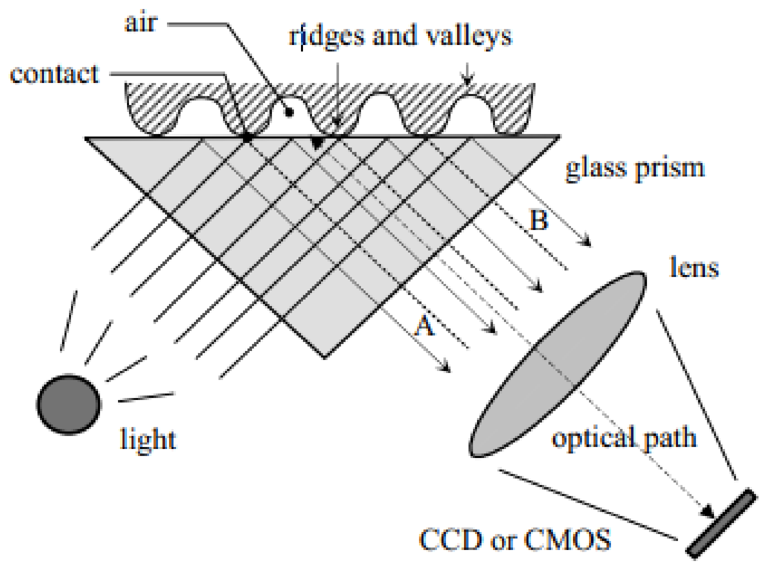

Figure 2: The inner workings of a FTIR optical sensor[4]

For touch less optical sensors, the captures are taken using the CCD or CMOS camera[5]. In figure 3 we see a capture performed by a traditional optical sensor as well as a touch less optical sensor. The fingerprint captured using the touch less optical sensor has much more noise, reflections and is generally more complex than the traditional capture.

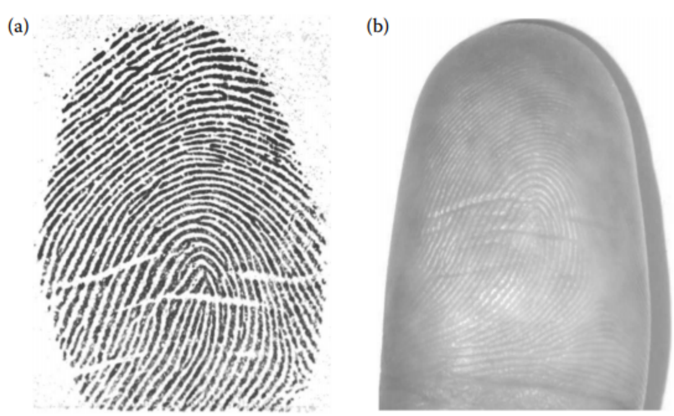

Figure 3: Showing captures from a traditional optical sensor(a) and a touch less optical sensor(b)[5]

Capacitive sensors work much the same way that optical sensor would, in that it senses the difference between ridges and valleys. These sensors can be described as a two-dimensional array of micro-capacitor plates, where the finger acts as the second dimension. This can be seen in figure 4. This means that when a finger, which is naturally conductive, touches the plate, the part of the array which the finger touches is filled with a electric capacity. This charge varies depending on the distance between the fingerprint surface and the capacitance plates [15]. In Figure 5 we see a capture from a Precise 250MC capacitive sensor[16].

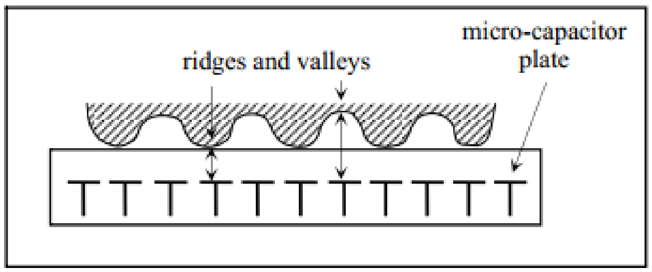

Figure 4: The inner workings of a capacitive sensor[4]

Figure 5: Precise 250MC capacitive sensor capture

While fingerprints are both unique and permanent, there exists a plethora of ways to circumvent a finger sensor. Depending on its capabilities of a sensor, spoofing such sensors or otherwise manufacture something which can fool basic sensors is not hard, and can be done with cheap materials. Examples of such attacks are many, such as The Verges Russell Brandom [17] which with the help of dentistry paste and some Play-Doh makes an artefact which is capable of unlocking a phone. Other examples of such attacks involve latent fingerprints from a high resolution image of the German ministry of defence to recreate her fingerprint[18]. Arora et al. [19] present a method for spoofing capacitive readers which could spoof capacitive readers successfully five out of five times on two different readers. These sensors are not as advanced, meaning they lack the ability to do liveness detection, the act of proving vitality, which requires the attacks to be more advanced.

1.1.1 Sensory devices

The problem with biometric recognition is the dependencies on which it relies. Presentation attack detection[20] is done either by hardware or modification of hardware or the use of specially crafted software, also including fingerprint sensing technology. There are many different types of sensors, but generally sensors used for smart phones and other devices are capacitive sensors and optical sensors. Sensors like these are not reserved for top tier phones any more, and are becoming a vital part of how we interact and authenticate with our devices. Capacitive sensors being the more advanced way of sensing fingerprints rely on an array of tiny capacitors to collect data about a fingerprint. These capacitors hold an electric charge, allowing them to retain information about a passing ridge over the single capacitor. This allows us to "paint" a picture of how a fingerprint looks, and also makes liveness detection possible. This is used to detect if the presented probe is alive based on if the human skin leads a current.

There are many types of presentation attacks, but most attacks are not being able to fool advanced liveness detection due to the not being able to lead a current. Using 3d printers, researchers have been able to make a artefact which leads enough current to fool presentation attack detection measures by using a D/C sputtering technique which infuses the artefact with small pieces of materials which leads a current, such as gold[19]. The accuracy of a 3d printer allows us to make an imprint which preserves the features of the finger and transfer them to an artefact [21]. However, there are several factors which needs to be taken into account to make a valid 3d printed spoof.

1.2 Keywords

FINGERPRINT, FINGERPRINT SPOOFING, ARTEFACT GENERATION

1.3 Problem description

As 3d printed technology has progressed, the feasibility of a 3d printed fingerprint is becoming increasingly less far-fetched; this work will look into the feasibility of a 3d generated artefact. Making such a fingerprint might sound like something which is easily done, but there are many different factors which needs to be explored in order to make a fingerprint that can be accepted by a fingerprint reader.

Modern fingerprint scanners do liveness detection based on if the skin conducts electricity. This means that the conductivity of different materials will need to be explored. If making the finger is feasible, there still remains the question on whether it is viable in terms of performance. Finally, the question of viability and feasibility of such a print will be discussed.

1.4 Justification, motivation and benefits

As the use of biometrics increase, the value they protect increase. People are increasingly relying on the fact that systems are secure - when they might not be. Given the plethora of ways of spoofing fingerprints, it is important to look at the feasibility of a 3d printed fingerprint. In [22, 23] the idea of spoofing is presented as something which is easily done. But how well can this be done? and for what types of sensors can this be done? Through performance analysis, there is a real chance to see whether it is feasible, and if this is viable. Stakeholders and others involved in making fingerprinting authentication devices could revise their methods if the 3d printed finger is proven to be viable.

According to Arora et al.. [24] there is precedent to research such a topic:

> "Given that state-of-the-art high-resolution 3D printers cannot fabricate 3D hand targets with rubber-like conductive materials, we are investigating methods to impart conductivity to the 3D printed hand targets. This would enable evaluation of capacitive fingerprint readers using these targets. "[24]

Furthermore, in [19], there is testing done on capacitive readers, while not having been done on optical sensors; which then would be novel research. In the fingerprint recognition field, there is a common sense that the majority of fingerprint readers are optical based[25], which adds to the motivation for this research.

Additional motivation for this also lies in the fact that most research already done in this field is primarily done using an expensive printer (200 000 USD)[26] and with the help of expensive materials, while still claiming that they are reasonable(writing PCS price, instead of bulk of materials + cost of printer). It is therefore interesting to investigate feasibility using the PRUSA i3 for doing this, which have a current price of 899 USD using cheap materials costing about 50usd. Additionally, the printers used in [24, 21, 19] are able to print details as small as 16 microns, where the Prusa I3 MK2 is limited to a layer height from above 50microns [1].

1.5 Research questions

We have categorized the research questions into 4 main questions, with a total of 6 subquestions pertaining to the main question:

- What is the existing research? (state of the art)
  - What is the current state of the art?
- What is the feasibility of such an artefact?
  - How can such an model be built?
  - what materials are needed?
  - how can we introduce conductivity?
- What is the quality of the generated fingerprint artefact?
  - Using similarity scores to measure its effect.

- Can the 3d printed fingerprint be matched to the original sample from the same subject? What similarity scores are we able to achieve?

These questions are the most relevant to answer should one get a fully working prototype of such a finger, and explore its potential.

1.6 Planned contributions

In this thesis we plan to show how artefacts using can be made using cheap materials and cheap printers. We will show how auto generated modelling helps us make models, as well as an exploration into different materials for making artefacts will be conducted. Several small scale experiments will be done to test several artefacts for different purposes:

- From FVC sample to 3D artefact
- From real finger to 3D artefact
- Checking conductivity and cohesion of materials
- Flexibility of materials
- Impact of scaling and artefact interoperability
- Mobile sensory technology

The final artefacts will be assessed using similarity scores to verify the artefacts quality. This will be further tested with interoperability between different samples of the same finger to validate its success as a complete artefact. The effects of pre-enhancement of the source image in model generation will be tested comparing assessing interoperability between a raw image and an cleaned image for modelling. Mobile phone sensors are tested as well as conductive artefacts.

1.7 Organization of thesis

The thesis will contain several chapters:

- Chapter 2: provides background knowledge
- Chapter 3: provides the proposed approach with aspects such as modelling
- Chapter 4: explores several small scale experiments and their research methodology.
- Chapter 5: provides the discussion of the results.
- Chapter 6: concludes the thesis and summarizes the results.
- Chapter 6.1: future work is discussed.

1.8 Ethical and legal considerations

Given that this thesis work will be done in a closed environment, within the offices of NISLAB, and we will be using my own fingerprint, or fingerprints from a public database, there are very few ethical considerations to make. In addition we will operate a borrowed 3D printer, which no one else has access to. This means that I have as much control as we can over the physical objects involved in my experiments.

In terms of legal considerations, there is not much to speak of. The thesis will not involve experiments where permission is needed, as far as I am aware.

In terms of ethics, there are very few considerations to take because I control most of the materials involved with it, and no data collection will be done other than statistics.

2 Related work(s)

2.1 Background: Standing on the shoulders of giants

In terms of information security, keeping confidentiality is an important aspect. Passwords have been the norm for keeping our information and accounts safer for decades. A password is defined as something that the user knows, which is secret. Generally, people choose weak passwords because complex passwords are hard to remember. Additionally, passwords are often mixed with personal data such as special events, relations, date of birth or even pets, which make them even weaker, because this is easily obtained information. Passwords are easily broken, either statistically or by brute force approaches since the entropy of a "best-practice" password of length 8 using all 94 characters is 94^8. In cryptography, Shannons entropy is used to assess the level of unpredictability of a cryptographic key[27]. Applying Shannon's entropy to the above example we get 52 bits of entropy[28]. In comparison, alternatives such as biometric fingerprint might yield as much as 82 bits of entropy [29], depending on the level of minutiae required by the sensor.

Biometrics is the field of automated recognition of individuals(humans) based on their behavioral and biological characteristics [30]. There are many different modalities of which is used for authentication and verification in biometric systems. Recently, fingerprinting technology is becoming readily available in most of our devices and it is not hard to see why. There are several reasons as to why this is, the key argument is most likely simplicity; while remembering passwords is cumbersome, very few people forget their finger or eye. The biometric functionalities such as universality, uniqueness, permanence, collectability, performance as well as gradually increasing acceptability are all reasons why someone would use biometrics as a security measure. Recently, as in the last 5-10 years, biometric sensors are being added to most of our electronic devices for authentication.

A fingerprint is a biometric characteristic which can be used for identification largely based on two factors which has long historical ties. Its individuality, even for twins[31], has been recorded by looking at early archaeological findings which suggest that people have been aware of its individuality since 2000 B.C[4]. It was not until Galton did a extensive study on fingerprints and minutiae in 1888[4] that it became scientifically recognized. Its permanence or persistence, was established as William J. Herschel found proof of its persistence in epidermal ridges in 1888. Herschel used the fingerprints for paying allowances to pensioned soldiers. This establishes the fingerprint as one of the oldest and one of the most used biometric features used by law enforcement agencies all over the world[4].

Purinkje, in 1823 proposed the very first classification schemes for the fingerprints, divided them into nine different categories(transverse curve, central longitudinal stria, oblique stripe, oblique loop, almond whorl, spiral whorl, ellipse, circle, and double whorl) according to global ridge configurations[4]. Galton then divided fingers into classifications, and then into major classes such as the arch, loop, and whorl and then further divided each category into subcategories[4]. This classification was then extended again by Henry, and this classification is now adopted by most countries, with some variations. In fingerprint recognition, minutiae, or more colloquially Galton details, after its inventor, is used for feature comparison of fingerprints. Minutia actually means small detail, but in terms of fingerprinting it refers to ways the ridges can be discontinuous[4]. In figure 6 we can see how the different details make up different patterns. For example, a ridge can suddenly divide into two ridges(bifurcation), or come to an abrupt end(ridge ending). These details, or minutiae are used to a large degree in automatic fingerprint matching[4].

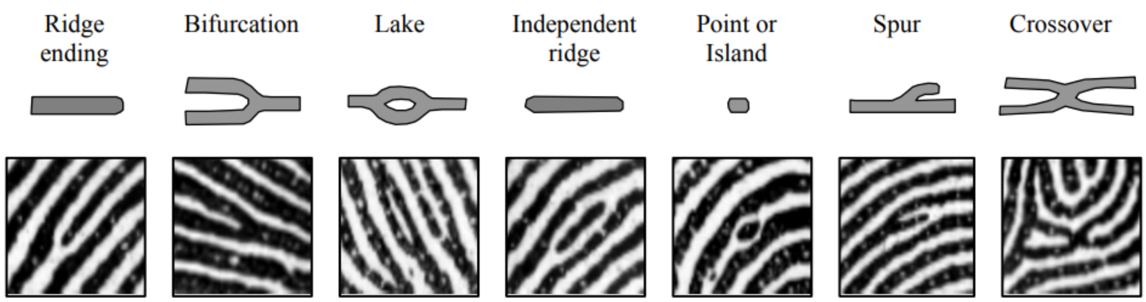

Figure 6: The seven most common minutiae details, picture curtsey of [4]

This grows more important as smart devices equipped with fingerprint sensors are becomming standard equipment, and is gradually protecting more and increasingly diverse information. Attacks on devices such as these are then becomming more and more valuable, since it now unlocks increasingly bigger values. It is not difficult to see the allure of biometric devices such as the fingerprint scanner, it requires limited effort as a by literally a touch of a button your phone is unlocked, your digital paper signed.

In order to measure the performance of a biometric system, several indicators are used. Most commonly[32] these are False-match-rate(FMR or FAR(false accept rate)), the probability that a system incorrectly matches the input pattern to a non-matching template in the database. Or, in other words, the number of invalid inputs which are incorrectly accepted. On the other hand, we have *False-non-match rate*(FNMR), in which a user which should have been recognized is not recognized. To describe events such as failure to enrol or capture we use *failure to enrol(FTE)* or *failure to capture(FTC)*.

Attacks to the biometric sensor, *presentation attacks*, are attacks which interfere with the sensor so that the sensor cannot operate properly[33]. A spoofing attack is an attack in which the attacker tries to mimic the capabilities of the finger and match it with a signature[33]. Spoofing, depending on whether or not the genuine finger is enrolled, has many subsequent different sub definitions. If the genuinely enrolled finger is available during the fabrication of the fabrication process, the method is called *cooperative* or *direct casts*. If the original finger is not directly available, the methods are what are called *non-cooperative*, or *indirect casts* [23]. In terms of spoofing attempts which are *direct casts*, there are many different types of attacks using cheap everyday materials, such as thermoplastic, silicone, plasticine and candle wax[23]. These types of spoofs require that mould material be soft enough to make an imprint, this has to be done in a fashion in which conserves the details of the fingerprints. When this is done the mould needs to be harden. When this is done, the actual fake finger is made by means of silicone, latex or gelatin[23].

When using *direct casts*, you usually have the advantage of having the actual fingerprint, but when using *indrect casting*, it requires that you have a latent fingerprint in which you have made visible, as it is not visible in most cases. After making it visible, by e.g. using a finely grained powder to highlight the structure of the fingerprint. The fingerprint is then either digitised by either taking a photo or by means of scanning. After scanning, these pictures are converted to black and white mask, which is used for the next steps. This mould could potentially be used directly, because the toner deposit creates elevations on the surface of the film[23]. If wanted, the finger could be created by any machine in which can potentially be created with any device in which give sufficient detail and built with various different materials such as latex, silicone, plasticine, wood cement or glue[23]. This is however not the only type of methods that can be used to make fingerprints, such as 3d printing or making a rubber stamp[23]. The examples of spoofed fingerprint capture devices are many. The Brazilian doctor who signed absent colleagues into the system with the use of a silicone finger [34] or the fact that by the help of dental mold, a Apple phone would easily be unlocked[35]. Biometric scanners are prone to many different types of attacks, and presentation attacks on biometric devices is a hot research topic. Successful spoofing attacks on even the most state of the art presentation systems have been carried out[23].

In terms of presentation attack detection, there are many different factors which needs to considered. In a survey about presentation attack detection [23], the authors have identified two requirements which is needed for PAD(Presentation attack detection), these are liveness detection[36] and fingerprint alteration detection[37]. The PAD should ideally be able to detect fake or altered biometric characteristics, but also be able to detect coercion, non conformity and obscuration of the print. Liveness detection can be further divided into two; hardware and software groups[23]. The Hardware based method tries to apply liveness detection methods by adding extra hardware modules or it tries to create new technology which is hard to deceive because of the nature of the fingerprinting acquisition process[23]. The software based approach, offers a cheaper solution to the problem, but cannot offer the universality that a hardware approach will. The software based approach looks at how the image is processed by the fingerprinting sensor, and tries to apply a dedicated attack detection algorithm which is able to distinguish between the live patterns between living fingers as well as fake, dead or cut off fingers[23].

According to Sousedik and Busch[23], presentation attack detection still requires knowledge about the fabrics used to make the artefacts. Most of the liveness detection methods mentioned in [23] are reporting universal rates for all the fakes their method has been checked against, but Sousedik and Busch conclude that depending on the specific fake being used, the type of materials used, liveness detection performance varies. Sousedik and Busch conclude that the state-of-the-art cannot be considered reliable in environments which demands high security. However, OCT(Optical coherence tomography) is a medical device used for retina scanning which exploits the interference of beams in order to measure the reflectance of the scanned material at different positions and depths; this allows for a volumetric scan of the material to be acquired; and the skin can be penetrated[23]. OCT seems to be promising because it can give us a bigger amount of information to determine if the subject is alive or not and thus make the manufacturing of fake artefacts harder than it is today[23].

As technology continues to progress, 3d printing(or additive manufacturing), a process to produce 3D parts with complex and free-form geometries layer by layer from computer-aided-design (CAD) models[38], is seeing more use in the field of biomedicine and is a hot research topic, and its uses have proven to be many. Additive manufacturing allows for rapid prototyping biofunctionalization and allows for precise placement of cells and extracellular matrix with a high resolution[39] and allows for printing tissue which can recapitulate the physical and cellular properties of the tissue micro environment for investigating mechanisms of disease progression and for screening drugs[39]. Given that printers now are capable of making organic tissue[40], chances are that it can also create a realistic fingerprint artefact.

2.2 Related Works

Current research in the field of presentation attacks using 3D modelled artefacts is diverse, but remains a active research-field. Most research in the field has historically been 2D or 3D targets for testing the imaging capabilities of a sensor. But 2d artefacts are inadequate for operational testing due to environmental factors such as finger placement, pressure and distortion of the fingerprint plate[19]. In earlier works, such as Arora et al. [21], a design and fabrication of 3D fingerprint targets is described.

The focus of Arora et al. [21] was to make evaluation of fingerprint sensors consistent in a operational setting by making repeatable behavioural evaluation of fingerprint readers. The conventional way of testing sensors, is to make a 2D/3D calibration targets to ascertain if the images meet the specifications. If needed, the configuration is changed to meet the desired specifications, and a reader will be compliant of a specific standard. This is what the current research is hoping to change by making dummy artefacts which imitates properties similar to the human skin. This allows for repeatable evaluation of sensors. Arora et al. [21] has made a mould which fits on the fingertip, which allows it to be used for repeatable evaluation. This makes it both easier to make moulds, and easier to do testing, because it is not a complete mould of a finger. These moulds could then be available to use for evaluating feature extraction and matching algorithms, and thereby testing the life cycle of sensors. To make the model for their experiment, Arora et al. [21] used a Artec EVA[41] 3D scanner to make a physical 3D target and then make a 3D model of the finger surface. After capturing, the finger surface is aligned such that the finger length is along the Y-axis and the width is in the X-axis, and Z-axis contains depth. The finger is then engraved onto the frontal electronic 3D finger surface and the artefact is manufactured using a 3D printer. Arora et al. established that the conversion from 2D to 3D still allowed for features to be preserved and intra-class variability between multiple impressions of the same 3D target is sufficiently small for matching at a False-accept-rate(FAR) of 0.01%.

In other works, such as [24], Arora et al. investigates the possibility to make whole hand artefacts for evaluation of contact-less and slap fingerprint readers, where the aforementioned method of generating a 3D target is used to generate a whole hand artefact. The authors claim that the replication from 2D to 3D is still viable and the model retains details in the original 2D picture, which enables 3D-hand generation. The resulting 3D-artefact was manufactured with a opaque material called RGD8520-DM[42] which was used to generate a thumb and four finger targets. Whereas TangoPlus FLX930[43] was used to make the fingerless glove, making it easy to wear. These artefacts where then tested with a PIV certified contact-less slap fingerprint reader, with a resolution of 500 PPI. Arora et al.[24] found that the model generated had little deviation(0.25%) from the original 2d pictures ridge spacing, and further found that the physical features of the fingerprinting process was the limiting factor, such as finger alignment and pressure to the sensor platen. Arora et al.'s findings where that even though they had materials which were able to conduct electricity, their findings are not yet concluded, and still needs to be worked on in order to find the best materials to spoof liveness detection.

Thus, in [19] Arora et al. looks into 3d targets which can be used to evaluate capacitive fingerprint readers. Furthermore, the conductivity of materials for use in spoofing liveness detection on capacitive sensors are investigated. Since capacitive fingerprint readers are gaining prominence in particular in smart phones, its security is essential. Arora et al.'s goal, in cohort with NIST, is to make 3D artefacts which can be used for repeatable evaluation of capacitive readers. Generally, sensors like these are in fact often an array of sensors which measures the difference between ridges and valleys[4]. This array of sensors acts as a single plate of a parallel-plate capacitor. The conductivity, is achieved by having the finger act as the other plate and the non-conductive epidermal layer acts as a isolator. Most capacitive readers use active sensing, this means that a small voltage is applied to the skin to induce a electric field between the finger and the sensor array. This electric current follows the pattern of the ridges in the dermal layer, where the difference in the voltage is used to sense the fingerprint[19]. Arora et al. were able to show that they could make 3d targets with materials similar in hardness and elasticity to the human skin. The authors then utilize a sputter deposition technique to coat the surface of the 3d target with a thin layer of conductive materials. The research showed that at $300\ nm$ the features were not altered, and the artefact retained accuracy in its features. To make the sputtering viable, the decision regarding choice of material is important, and more specifically, its durability. During testing of the sputtering technique, several different materials were tested, such as silver(Ag), copper(Cu) and Chromium(Cr) over a titanium(Ti) coating because of its good adhesion/binding properties[19]. Regardless of being able to impart the conductivity needed, the metal coatings reacted with environmental variables such as atmospheric gases and water vapours over time and thus became tarnished. Other attempts included tin(Sn), Zinc(Zn) as well as Al doped indium oxide (IZAO) using DC sputtering. These coatings have a significant advantage over metal, due to their high transparency which do not impact the underlying optical properties of 3d targets, according to Bishop et al. [44]. However, due to wear and tear, the conductive oxide coatings were inadequate for repeat evaluation of capacitive readers over time. Since the coatings were found to wear out after taking about five to ten impressions of the coated targets with capacitive readers.

After trying different materials, Arora et al. [19] tried gold(Au) which was chosen because it is a stable metal which do not react with atmospheric gases and is very resistant to wear and tear. These artefacts showed to work well on capacitive readers, but due to high reflectivity after coating, the artefact was ineffective against optical sensors.

The research questions referred to in section 1.5, are still somewhat unanswered. The current state of the art in making 3d models is to either span 2d calibration patterns for fingerprints to fit on a generic model, or a 3D scanner to get a model of a direct physical object. In regards to the different types of materials chosen for the artefact, the state-of-the-art in the field tells us that a range of materials can be used, but ultimately comes down wear and tear[19]. Furthermore, the current state-of-the-art is inconclusive in terms of what would best work in optical sensors.

There are some preliminary research on optical sensors, and how to manufacture artefacts for it. However, conductivity, and material choice for making viable models is still not something that is answered in the literature. Gold(Au) can be used, but due to high reflectivity, it cannot be used for optical sensors. In their work on optical sensors, [21] Arora et al. found that they were able to do behavioural evaluation of 3 (500/1000PPI) PIV certified sensors. But still the main problem seem to revolve around choice of materials and finding materials which both leads enough current as well as has the feel and elasticity of the real human skin.

As a continuation of the works presented in [24, 21, 19], Engelsema et al. [6] explored how many different types of artefacts could be created for different types of sensors. This however, is impractical for testing a fingerprinting sensor of unknown type and requires that a plethora of different artefacts are generated to test, which is impractical. To further their research Engelsma et al. [6] explored how they could achieve interoperability between different sensors with different capabilities by making a single artefact. This problem is best exemplified through India's Adhaar biometric system. With 1.14 billion enrolled users in may 2017[6], Adhaar is a large distributed system. This requires interoperability due to the fact that the sensor used for enrolment and the sensor used for identification / verification might differ between locations. Furthermore, the sensor might be upgraded due to advanced made in the field. Interoperability is thus essential, as the cost of re-enrolling the whole database would be astronomical.

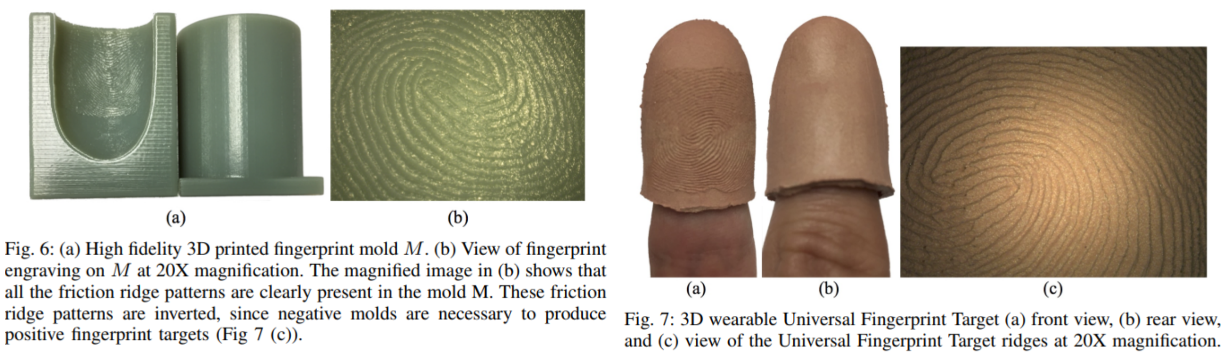

Figure 7: Fingerprint mould for negative as well as artefacts presented in [6]

To make robust standardized fingerprint for interoperability evaluations, a digital mould is created, then 3d printed and subsequently chemically cleaned using $2M$ $naOH$ to dissolve support materials from the printed mould in order to not hurt the fingerprint ridges. Since its important to remove variables such as individual pressure on the fingerprint platen, the mould is made as a negative so it will fit on a robotic arm which is able to apply pressure in the same manner every time. This means that a scaffolding will be required. To create this, a hollow shape is created based on the shape of the mould visible in figure 7 so that the robotic arm or human finger can be placed inside during evaluation. The dimensions of M are used to create scaffolding, F, whcih is used to insert a fingerprint surface $S\prime$ which has a diameter which is slightly smaller than that of M, allowing for repetitive casting of fingerprints, and a casting material is injected into the mould, allowing the space between S and $S\prime$ to be filled to a form a wearable fingerprint T. A picture of the process can be seen in figure 8. After this process is done, F is cleaned using 2M NaOH, to further remove residual printing support material.

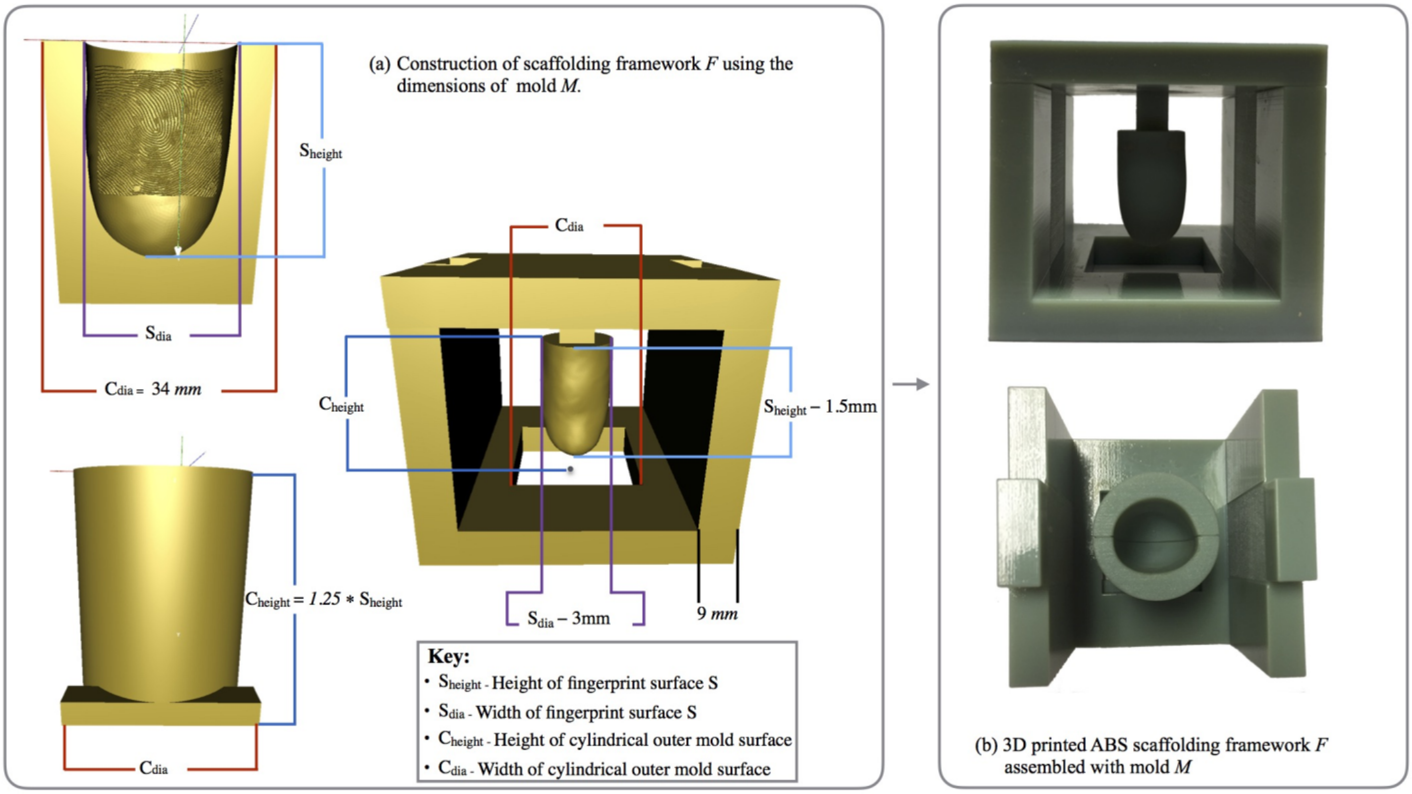

Fig. 8: Fabricating scaffolding F using the dimensions of the mold, M. (a) scaffolding framework F is electronically modeled; (b) the electronic scaffolding system is physically generated in acrylonitrile butadiene styrene (ABS) using a high resolution 3D printer. Using F in conjunction with M, 3D wearable fingerprint targets T are repeatably produced.

Figure 8: Fingerprint scaffolding for repetitive manufacturing of artefacts [6]

Since a method of manufacturing is made, Engelsema et al.[6] discuss different material requirements which ensure that the artefact will work on optical readers, touch less optical readers as well as capacitive sensory readers. Since Optical readers rely on proper reflectance and refraction of light rays, the optical properties must be similar to that of human skin in order to be correctly read by optical readers. Materials which are black will improperly absorb light rays and materials of high reflectivity will improperly scatter all light rays, essentially preventing the artefact from being recognized by a optical reader. In addition to this, an artefact will need to be conductive in order to create capacitive differences between ridges and valleys within the cells in the semiconductor chips on a capacitive sensory array. Lastly, the mechanical properties of the target material must be similar to that of the human epidermis to allow for high quality fingerprint target acquisition. Materials which deviate a lot from materials which match the human epidermis could negatively impact the artefact, such as having too much elasticity, which leads to loss of minutiae details. Too little elasticity will make sure the fingerprint will not flatten around the sensor platen and might only give a partial print of the surface.

In order to achieve all these goals, Engelsema et al. [6]. used electrically conductive silicone(SS-272S) sheer mixed with silicone thinner as well as a flesh-toned pigment. This casting material is transferred using a disposable pipette. Prior to this, the mould and scaffolding is sprayed with silicone release agent. After this, the material is vacuum degassed to remove air bubbles. After 72 hours, a high fidelity 3d wearable universal fingerprint target, T, can be carefully extracted from the fingerprint mould and scaffolding system.

To verify their claims, a spectrogram of the fingerprint target material is compared to human skin spectrograms obtained by NIST from 51 human subjects. By doing this, the Engelsema et al. [6]. were able to find that the spectral reflectance of the universal fingerprint target material lies within the range of human skin for almost all of the visible spectrum (400-700nm). Based on the NIST report, spectral reflectance varies significantly even across multiple readings of the same subject, meaning that this spectre could be even higher. The electric conductivity is verified by obtaining a resistivity reading from 4 square samples of the material.

After verifying the properties, the artefacts are tested against multiple PIV/appendix F certified fingerprint readers. The images captured by the contact less optical fingerprint reader had smaller ridge-to-ridge distances than the impressions captured by contact based readers, probably due to absence of fingerprint distortions in a contact less sensory device. Additionally, errors in the contact less reader may be introduced when a three dimensional picture is projected into a two dimensional picture(because the ridge height of a universal fingerprint target is greater than the ridge height of human fingers). In most target impressions, capacitive fingerprint readers captured the ridge to ridge distances more closely to the ground truth than contact optical readers did. Engelsema et al. [6] were able to establish that their artefacts could be used for both individual fingerprint reader assessments and fingerprint reader interoperability studies, with good result.

Thus, as is presented in this section, most of the work already exists, allowing the focus to be on reproducibility on cheaper and less accurate machines, which are more affordable. This translates into cheaper and more available benchmarking for system implementers. Additionally, in [19] the conductivity is given by means of a gold sputtering technique in which many small pieces of gold is sputtered onto the artefact. This will not be the case in our case, where we will try to solve the problem with traditional 3d printing methods such as standard filaments.

3 Creating 3d artefacts with a low cost 3d printer

Figure 9: Prusa I3 MKII used in production. [7]

Since we are not in possession of a expensive 3d printer, we are instead opting to use a filament fed thread based Prusa I3 MK II, using various models generated using many different methods, these will be highlighted in the sections beneath. Most prints will be using 10mm layering if nothing else is emphasized. In other related research, a printer capable of printing at 16 microns[6] has been used. Prusa I3s MK IIs are not nearly as delicate as these printers, producing best results over its threshold of 50 microns[1].

3.1 An overview of the proposed approach

The proposed approach contains three steps, which is presented in figure 10. In general the preprocessing is done using these preprocessing steps[45]. After the model is made, it is loaded into a program which transforms the 2d images to a 3d plane. This step also involves changes made in the slicer such as scaling or size of nozzle. Manufacturing involves making the artefact on the printer, using the filament we have tested. This also includes a visual inspection of the final artefact.

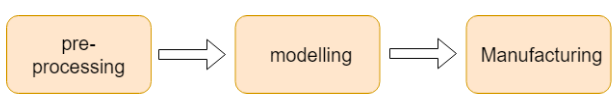

Figure 10: The proposed approach

3.2 Modelling

This section will focus on the feasibility of making a printed fingerprint. The most essential part of an artefact is the model. The model needs to match the raw as much as possible, or atleast need to match the minutiae points, since most sensors today only match minutiae points. After a sufficient model is made, the performance of said model needs to be examined, if the model is not sufficient enough, a new model needs to be developed or the current model needs to be reworked.

After making a sufficient model, a artefact needs to be made which accurately represents the fingerprint. The initial goal is to enable the artefact to be made of a material that enables it to fool liveness detection. As conductivity is generally used in liveness detection in capacitive sensors, the artefact will need to be conductive. Since the conductivity of the different fabrics available are unknown, they will need to be investigated to find the best available material which mimics the capabilities of the human skin.

When considering making the model, having a good image capture is essential. For this purpose, we have chosen to use FVC2002 DB2 samples. 40_1.tif was chosen. Normally, when doing fingerprint recognition, pictures are cleaned to make minutiae easier to recognize, and to remove factions which were not intended to be there. This has not been done in this case.The pictures were then loaded into two different programs(Magics Materialize and Windows 3d Builder) to make different models using different methods. These programs allows for importing pictures and making 3d models out of bitmap files. This has been the method chosen for making models. Using either software, a model is generated as file with .STL extension. Since we are using Prusa I3s, Slic3r Prusa is used as as a slicer. A slicer makes 3d models into printing instructions for 3d printers, generating tool paths as well as calculates the amount of materials to be extruded.

Once a file has been introduced to Slic3r, we change the X-axis by 90 degrees so that the model is printed upright. This allows us to keep more detail in the final model due to how layers are layered. If this is not done, layers might not be produced correctly, thus potentially losing details. In addition to this, a plastic brim is added to ensure that the final 3d model has a base which allows for cohesion of the initial layer.

Figure 11: A left B middle C right - First attempts making model from [4], with error propogation seen in image C).

Before printing, an appropriate nozzle size is chosen, and the model is re sliced so the latest changes are kept. A nozzle size of 0.25 was chosen. The model chosen was based on a picture in Maltoni et.al's [4] work on fingerprinting. As we can see in figure 11B and consequently in figure 11C we see that the model was not accurate enough to reproduce the fingerprint, ignoring minutiae details in the left corner, highlighted in figure 11B.

In addition to this, making a final artefact needs to be out of something which is elastic and mimics the capabilities of the skin as well as something which is conducts a small current. Furthermore, as is visible in 11C we can see that this model comes with a frame. This is due to how pictures are imported into the 3d modelling program Materialize Magics.

In initial testing, a model chosen from a FVC2002 db2 database was made as well. In this case, 80_1 was chosen because of the clear details in the initial photo. This picture was subsequently

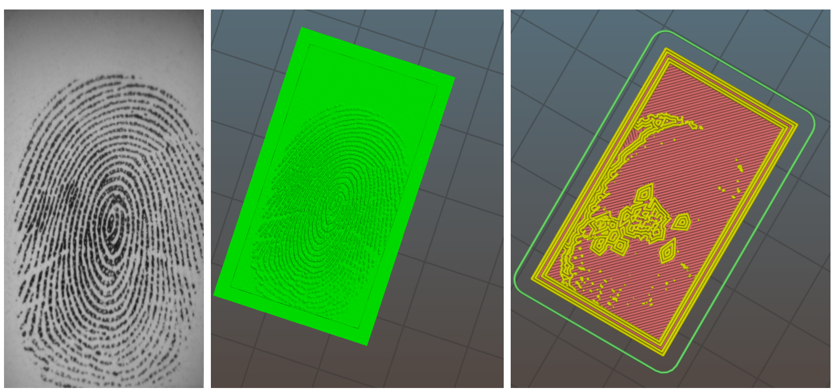

Figure 12: A left B middle C right - Initial picture(80_1) chosen for visual clarity, but discarded due to issues with layering as can be seen in the third picture

determined not to be good enough due to layering problems. In Prusa slic3r, the colour red means highest layer of plate. As we can see in figure 12 C, there is not much detail which is transferred from raw into the model. Therefore, the model was quickly discarded.

Another attempt was done with the model 40_1 which also was determined as a visually good image to use for this purpose. This attempt was somewhat successful. As can be seen in figure 13

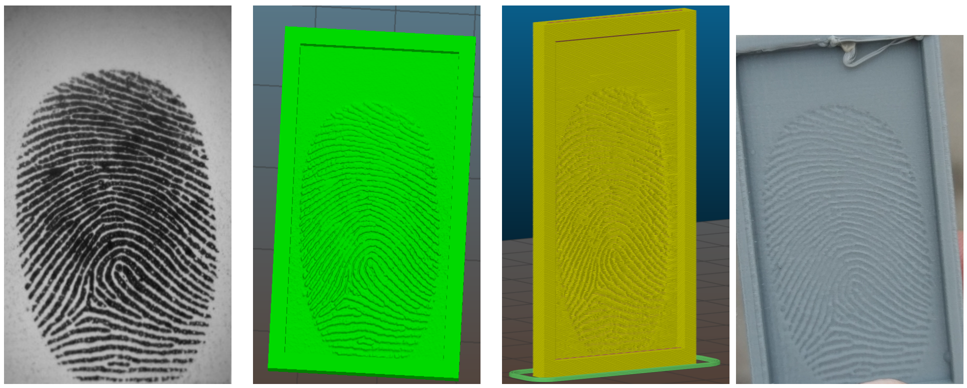

Figure 13: A left B middle C right - Workflow when generating models from image to finished artefact

image D, much of the features present in figure 13 A, are clearly visible. The problem, however, is scale. While being close to the correct size, it is somewhat too big, and the frame mentioned in figure 11 is still a prevalent problem. The choice of hard plastics is also not viable, but since this was done as preliminary testing to see the actual feasibility, this was the best initial results available.

There is a reason the frame is used. The frame works in some of the same way as a brim would. To print a brim / frame, allows us to ensure the correct production of the model. However, using a brim, some initial models printed for testing gave various results.

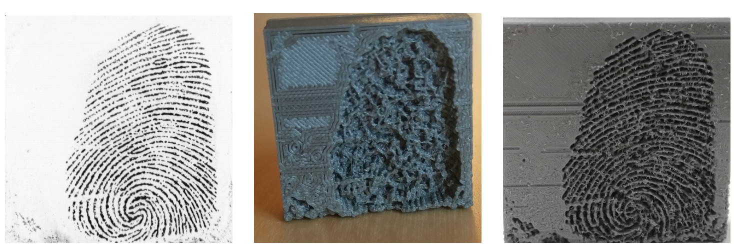

Figure 14: models generated of own fingerprint

To test the results of making fingerprints without the frame, models created in Windows 3d builder was used. To test these, pictures of my own thumb was chosen. As seen in the end result in figure 14 is not usable, due to the simple fact that it lacks essential textures. On a visual inspection of artefact presented in figure 14, the model looks to be containing most of the essential details, and does not contain the frame. There also seems to be some plastic shavings which is degrading the quality. This model is also not made in materials which are viable for testing conductivity, due to plastics rigidity and its isolation capabilities. Given the many problems encountered with initial testing, it leaves a lot of room for improvement. First of all, models generated for this experiment, are strictly just processed from image files directly to 3d models by means of a program. To correct for this, image enhancing of the initial model can be done.

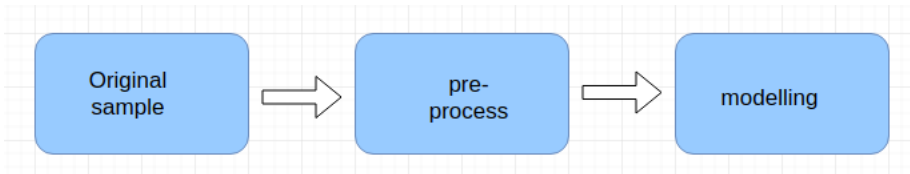

Figure 15: Pipeline for picture enhancement

In Figure 15 we can see the workflow of how this would work in practice. This is done by handling the initial image. The scripts used for this is freely available [45]. The scripts enhance fingerprint images. The image is first ran through ridgesegment.m, which identifies ridge-like regions of the given image. The intensity values of the image is also normalised. Next, ridgeorient.m segment determines the local orientation of ridges in the fingerprint. Next, the ridges orientation is plotted by plotridgeorient.m and ridgefreq.m estimates the ridge frequency across a given image. Freqest.m estimates the ridge frequency within a small block of an image, which is then used by ridgefreq. Finally a ridgefilter(ridgefilter.m) enhances the fingerprint using oriented filters made in previous steps. In figure 16 the pipeline is presented.
In terms of modelling there are a few considerations which needs to be made. The current method is to handle the picture as a height map, and then increase the smoothness of the perceived heights generated from the image. This allows us to adjust distances of minutiae points if need be and also makes the surface appear much as a fingerprint, with curves and ridges. After being modelled in 3d builder, the model itself is scaled down to match the actual size of an fingerprint, and the model is visually inspected to make sure the quality of the model is a good fit in terms of 3d modelling. Additionally a brim is attached to the model, to make sure that the artefact do not break because of lack of adhesion. If and when this is done, manufacturing is next.

Creating a valid model is a big part of this research. As the traditional way of creating a 3d model is to model this in either Solid works/CAD, and tracing the fingerprint would be time consuming. I have opted to try to automate the process by using freely available tools to generate models such as Windows 3d builder, `http://3dp.rocks/lithophane/` as well as Materialize Magics, which does the tracing and generates a model based on the picture input. The most important step of manufacturing, is to choose the correct material and the correct composition of material(s), in order to get the most accurate resemblance and conductivity. This will most likely require compromise, as

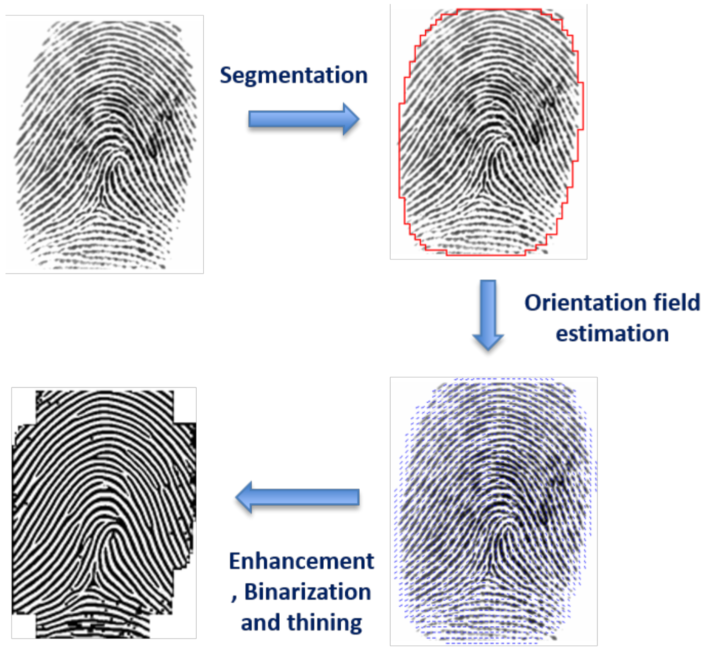

Figure 16: Image enhancement pipeline [46]

making a artefact of pure copper or gold, would most likely not be very flexible, and on the other side, an artefact made solely of rubber would not be conductive. Additionally, given that the process of printing is an iterative and time consuming process as well as have a tendency to break, getting consistent results might be an issue. If an artefact of sufficient quality is produced, it will be tested using Neuro Technology Verifinger Comparator, to measure its performance.

The advance of 3D-printers is exciting in terms of exploring the safety of our biometric devices and in particular liveness detection, and spoofing of such an element. The technology of 3D printing is getting mature. Meanwhile the cost of 3d printing is getting low, issues a motivation to use a low cost way to attack a high security biometric system. As a recent video [22] by Jain at Michigan State University shows, he was able to fool liveness detection using a conductive ink to open a dead man's phone. This video serves as a motivation for the research. By exploring different types of presentation attacks for fingerprinting, it might be possible to look at how feasible it is to make such a fingerprint or even a finger replica, how viable it is in use and performance and how well it would hold up against other forms of scrutiny.

3.3 Manufacturing

Before manufacturing can start, the model is loaded into a slicer. The slicer is used to change variables which affect the printer, such as size of nozzle, type material and if the model should include a brim. In addition, adjustments such as cutting can be performed here. When these settings are made, the final product is loaded onto a SD card, and put into the printer. The printer is preheated according to the material you are using. For PLA this is 215 degrees.

As manufacturing has started, several problems have presented itself. In terms of manufacturing, there are several issues which needs to be handled differently. The model might or might not be a problem in terms of quality. A visual inspection of the model and its layering might tell us it is of sufficient quality to be printed, but after printing, one can clearly see that details which should have been clearer in the model, are just not printed as finely grained as promised by the model. The manufacturing process is a complex process due to the many variables which can change the outcome. Initial trials indicate that small changes in both model and printing process has a big impact on final result, such as material, placement and scaling. Further, due to the way 3d printers work, models are more likely to be better if printed standing. This is due how layers are built, allowing more details to be layered on.

Experiments show that there is a likelihood that you cannot have your cake and eat it too; since making a model which is standing requires thickness of the model for it to have the right rigidity to be successful, while laying, the model can be very thin but might lack details in terms of layering. Since the size of the nozzle is small, debris gets stuck and has a tendency to fall off or disturb the manufacturing process.

3.4 Other knowledge we discovered

Initially, 3d printing is a very iterative process. There are many pitfalls which only become apparent only after a print has been made. Initial tests using own 3d models, have not been as successful as one would want them to be. 3D printing is iterative, so the first step would be to manufacture an artefact which has the necessary level of detail. Before assessing other properties such as flexibility and conductivity, the scale is an issue which needs to be investigated. Due to access to materials which are used in the state of the art research, like TangoFlex used in [24, 21, 19] is very limited and the materials themselves are expensive (500USD for 1.44Kg), other materials must be considered.

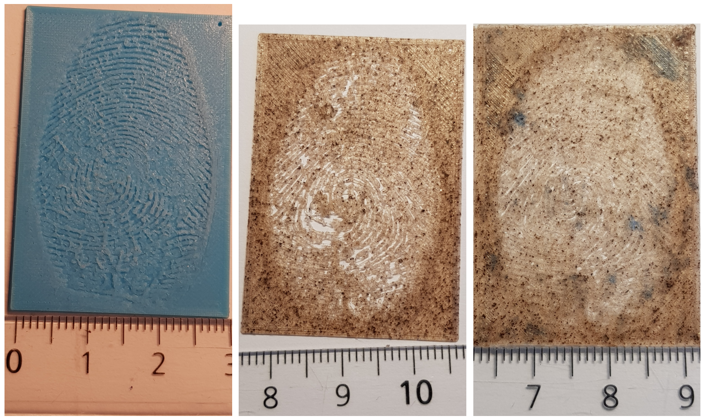

Figure 17: A) PLA B) Proto-pasta HTPLA C) Proto-pasta HTPLA

In figure 17 two different filaments are used. in A, a 1.75 PLA standard filament is used, while in B and C a more reliable Proto-pasta HTPLA is used. While 17A) is pretty close to the original, it is printed using a standard PLA filament which is not flexible. In the top of figure 17A) we can see that some of the ridges in the model is not reproduced accurately enough. Figure 17B) retains most details, but lacks detail in ridges, very visible in the top of the picture. 17C) is not viable in terms of level of detail. This is probably due to manufacturing, as is visible in e.g. the top corner. It is important to note that both 17B) and C) is cut to be as thin as possible, with the idea that by making something thin you also get some degree of flexibility and thus allowing for conductivity using a single material. Both B and C are printed on top of tape, to give the printer a better bonding surface for printing.

Figure 18: PLA 1.755 filling, ignoring thickness

While all artefacts in figure 17 were printed to be as thin as possible, a separate model which ignores thickness was also made, using a PLA 1.75 filament. In figure 17, some of the focus was to make the artefact as thin as possible, while in figure 18 the original dimensions generated by Microsoft 3d builder were kept. As we can see, this is a print of the model generated using the method described in the image enhancement pipeline in figure 16. In earlier attempts an artefact made from a fingerprint which was not cleaned was used, which was good in terms of quality, but due to the way the model was generated, it had an additional frame which made the print look like a framed photo. Furthermore, the scale was a bit off, and the material used was a hard PLA, which did not give much in terms of elasticity, also the artefact was too thick.

The model has now been reworked, so that the model does not have a solid frame, is thinner and a significant portion has been removed so the lower artefact does not contain any spare unnecessary details, such as the previous flat surface. Results indicate that we are reliably generating the same output at any given time. To achieve higher cohesion, a brim is used, visible in figure 19.

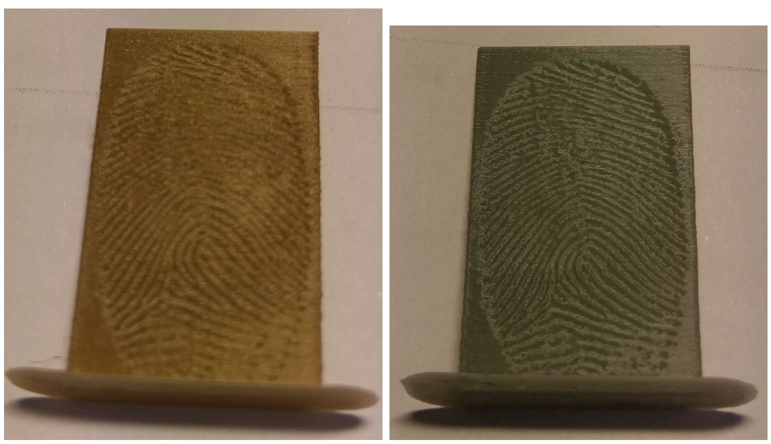

Figure 19: PLA 1.755 filling, no frame, very thin.

In general, the goal of this process has been to reduce the thickness of the model by as much as possible, and I believe that this has been achieved by having a model which is 0.98mm thick. Simply because if we cut it any more, there are visible holes through the model, which means that it won't print successfully due to lack of cohesion, and the print will most likely fail altogether.

3.4.1 Materials for achieving flexibility

Addressing flexibility aspects depends on having a model which gives good results and is easily printed using the previously mentioned method. However, given the nature of fingerprints minutiae, being very small, printing using flexible materials might prove difficult and give artefacts which do not have sufficient minutiae-details, especially when scaling down in accordance to a normal fingerprint. After decreasing thickness, two different flexible materials have been tried, such as Ninjatek Armadillo and NinjaTek Cheetah. These filaments were chosen because the Cheetah give good flexibility, while the Armadillo gives good flexibility but offers some more rigidity which makes it potentially ideal for printing minute details such as minutiae details. Unfortunately this is not the case for manufacturing artefacts.

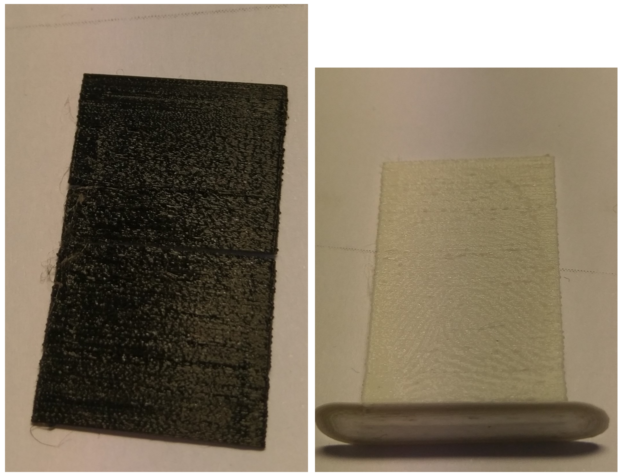

Figure 20: ABS 1.75 filaments

As we can see in figure 20, not many details are visible, supporting the claims which have been made earlier, that there is a certain loss of detail due to layering(which can clearly be seen in 20 left picture). Additionally, printing with flexible filaments leads to loss of details.

3.4.2 Materials for achieving conductivity

Conductivity is crucial in order to make a valid artefact, its conductive resistance would need to match that of human skin. In [6] Engelsma et.al note that the resistance of human skin is $\Omega\ 2.5*10^2$ - $8*10^6$ or between 2.5 Ω and $8M\Omega$. In [6] Engelsema et.al showed that they created artefacts which had a electric resistivity of $2.4*10^{-5}$ using gold, and a resistance of $9.8*10^{-1}$ for their PDMS, silicone thinner and Pantone 488C pigment artefact. Thus the span between upper and lower bounds of the conductivity of each artefact is big, and allows for flexible material choices to get a conductive surface.

Methods of imparting conductivity to an object is not confined to only conductive filaments. There have been examples in which a conductive pen and some tape have been used to fool capacitive sensory devices by applying some amount of conductivity to a tape and applying pressure, thus using the latent fingerprint available to us. If this idea is transferable to printing using traditional filaments, it could ease the manufacturing process and allow for use of other materials which can be more effective against issues such as reflectance in optical sensors.

As to the feasibility of using a normal conductive filament to impart electricity to an artefact, in preliminary works it has shown good promise. Using 1.75 PLA with conductive capabilities, we are able to print with the same accuracy as with regular PLA without an conductive element. Furthermore, initial trials have shown good promise in terms of leading a current. However, what we have found testing on a Huawei mate 9, is that using a simple plastic bag with a artefact generated using a conductive filament allows us to enrol a "subject" and use a phone as if this was a finger. This leaves us to believe that this is attributed to active sensing[19] in which the sensor applies a small current between the finger and the sensory array.

4 3D printing experiments and evaluation

In order to evaluate many of the variables which are crucial in the 3d printing process, small scale experiments are needed. In this thesis work several small scale experiments have been carried out to see the impact of the changing variables. The motivation behind these small scale experiments are to explore as many areas of the 3d artefact generation process as possible. This allows us to isolate each variable and make changes according to the specific variable. This also allows us to change sensing method, such as including mobile phone sensors or look into materials.

4.1 Experimental design and experimental methodology

The following experiments have been carried out:

- From FVC sample to 3D artefact
- From real finger to 3D artefact
- Checking conductivity and cohesion of materials
- Flexibility of materials
- Impact of scaling and artefact interoperability
- Mobile sensory technology

Experimental designs to explore these variables are largely based on the same pipeline of production, as seen in figure 21:

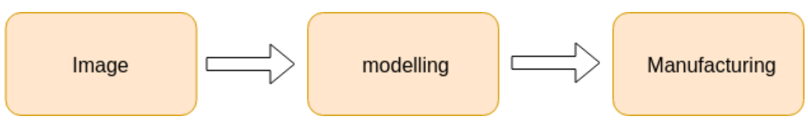

Figure 21: Engineering pipe line used for experimental designs

As most of the work is done using this work flow, changes are applied to each module where it is necessary(i.e in image we can either add an extra step with pre-processing. In modelling, we can change the model generation method, and in manufacturing we change the filament). This allows for flexibility and isolation of each module, which allows us to only change the variable we are interested in investigating.

The first experiment is to check the feasibility of making an artefact out of a good sample from a renown database such as FVC fingerprint data. This experiment will follow the general pipeline explored in figure 21 directly, as no enhancement will be done to the initial original image. This allows us to see if a model transferred from a 2d plane to a 3d plane will retain enough quality to

use it for biometric verification with its original image.
After we have verified this gives a sufficient result, we will try to carry out the same process using a real finger, of a real life person. This means that an additional step to the process. Image acquisition is added, as can be seen in figure 22. Image acquisition in this case is done by using a capacitive sensory device, the Precise 25M0C sensor, to get a picture which we transfer from 2d to 3d.

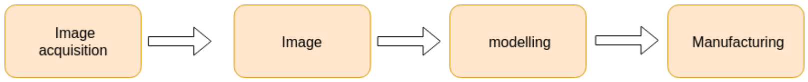

Figure 22: Engineering pipe line used for experimental designs including image acquisition

To test a model for conductivity and cohesion requires us to change our approach. Instead of doing image acquisition or otherwise making a translation of an image or a model, the design is more like a loop. The manufacturing process changes since it requires at least two different filaments.

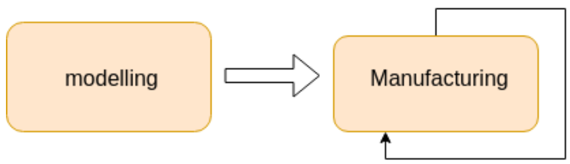

Figure 23: Engineering pipe for testing cohesion and conductivity

In order to investigate the impact of proper scaling and interoperability, the pipeline in figure 24 is used. First, a sample is chosen from the FVC2002 database. In this case, the 1_1 was chosen as an initial model. The model is then cleaned using the methods elaborated in section 3.2. This process returns an image which is handed to Magics Materialize and turned into a model which is cut to be as thin as possible(while still retaining essential details). The measurements of the model was 22.62x1.60x29.42, which is a 160% increase of the original image. This is done to make the model retain quality through manufacturing. The model is manufactured in gray 1.75MM PLA filament which has shown to be a good material for optical touchless sensory devices since it is not reflective. After the model has been manufactured and is confirmed to retain enough details, the model is tested for interoperability.

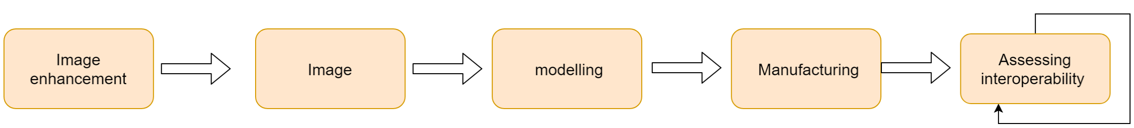

Figure 24: Engineering pipe for testing impact of scaling and interoperability between FVC data samples

To test artefacts for mobile phone sensory devices, we use the work flow described in figure 25. For the image and modelling phase, both the 1_1 and Guoqiang's sample was chosen. For manufacturing, we used conductive PLA to engage with the mobile sensor. For the enrolment phase of the pipeline, the artefacts were enrolled to the system. If we were able to enrol the artefact, we tried to authenticate using the artefact. For Guoqiangs fingerprint we tried to first enrol the artefact and unlock using the artefact. Then we tried to unlock the phone with the original finger with the artefact serving as a template.

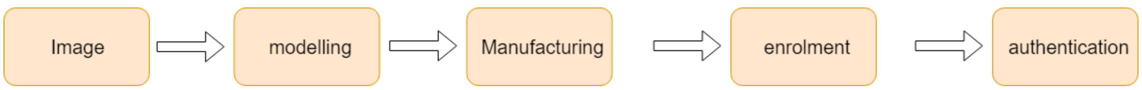

Figure 25: Engineering pipe for testing mobile sensing devices

4.2 From FVC sample to 3D artefact

While models using PLA 1.755 hard plastic was originally created to investigate if fingerprints retain quality. Upon a visual inspection it can be said that they retain most details using the model of picture 40_1, which has been used for most experiments regarding printing. A plethora of different artefacts have been printed using this model with small variances such as those mentioned in section 3.4 such as thickness, frame vs no frame, and materials chosen as well as colour of filament. As these mostly have been made with the intention of getting minutiae details, the properties of elasticity and conductivity has been addressed in other ways by e.g. making the model as thin as possible(0.98mm) thick, and thus gain some elasticity.

Figure 26: Source picture from FVC2002(40_1), and artefact generated using PLA 1.75mm thread

As we can see in figure 26, the artefact retains most minutiae points, potentially making it viable for biometric recognition. This artefact as well as "siblings" were created using the same filament, but with different types of colours, just because of efficiency in printing and due to the fact that most 3d printing have a tendency to break.

Since this artefact is made of plastic, an natural insulator, assessing its performance in regards to conductivity would be meaningless. Thus a optical sensors was chosen for testing, more precisely a optical contact less sensor, TST BiRD 3[47]. The TST BiRD 3 has a resolution of 500 DPI[8], which is a common resolution for fingerprint sensors. Gafurov et al. [8] note the difference between the TST BiRD 3 and other sensors. The nature of the picture is clearly different from other scanners, as we can see in figure 27.

(a) TST (b) IDT (c) CMT (d) PBA (e) LUM (f) SAG

Figure 27: Images of the same finger in one session on all scanners used in [8] data collection

Initial trials revealed that we were able to take two concurrent pictures of the same artefact, one as reference and one as probe to get a similarity score of 112 using Neurotechnology's Verifinger SDK[48]. The next step was to load the original 40_1 picture as the reference, and use the artefact as the probe. This initially revealed a design flaw with the model, which until now was not apparent. The image was not matching due to being mirrored the wrong way. This was quickly fixed by mirroring the probe image and then comparing with the original picture.

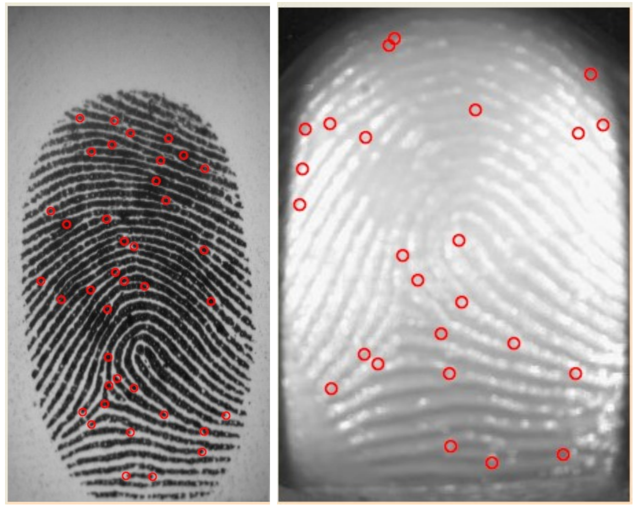

Figure 28: Successfully comparing original reference with artefact probe, giving a similarity score of 92

As we can see in figure 28, many of the same minutiae points are found. A similarity score of 92 is achieved with Verifinger SDK. Since scores above 50 is considered a match, this is deemed a successful attempt. It is very likely that the results are due to the fact that the sensor is a contact less sensor, and is just taking a picture using a CMOS chip. This is backed up when trying it on other sensors, such as the Sagem MorphoSmart MSO300[49]. Since our artefact was not visible using it, it is likely because it could not reach the sensors in the platen, and could then not be read.

Figure 29: Due to the material being reflective, the model cannot be read and is instead blank

Given that our artefacts were generally printed using different colours, we were able to accidentally confirm what [19] experienced when testing their gold finger on a optical sensor. In figure 29 we used a blue PLA artefact as the probe on the TST. Thus, using optical sensors on artefacts which do not give sufficient levels of darkness or is very reflective makes it hard to produce a probe, meaning that if additional light is present, a optical sensor will not work as well.

4.3 From real finger to 3d artefact

In order to make the research more realistic, my supervisor, Guoqiang Li, volunteered his print to test "real-life" artefact generation. This was done by extracting his right thumb(finger index 6) using the Precise 250 MC capacitive sensor[16] using Verifinger SDK[48]. The software saves BMP files of the captured finger which can then be extracted from the computer. The file is then imported into a proprietary program called Materialise Magics, a data preparation software package and STL editor. The BMP file previously extracted is then imported in the program and a model is automatically generated adding a frame. The frame is then subsequently removed, and two models are generated, one a bit thicker(1.29mm) and one a bit slimmer(0.96mm). After the model is generated and saved, the model is loaded in the slic3r, described in section 3.3, and the model is rotated 90 ° so that the model is standing as well horizontally flipped so that it presents correctly to a sensory device. An essential support structure(brim of 5mm) is added to improve odds of having fewer manufacturing issues such as tearing and layering of the artefact.

Figure 30: Initial capture of Guoqiang right fingerprint(index 6)

The initial model was printed using gray 1.75mm PLA filament, to highlight the different minutiae of the fingerprint and then subsequently using the 1.75mm conductive PLA filament for both models. A picture of is then taken using a touch less optical device(TS3 BiRD), and compared using Verifinger comparator. In this case, the Verifinger comparator did not recognize the probe. While it could not be recognized as a match, the comparator was able to extract minutiae points from the probe, and some of these minutiae points line up.

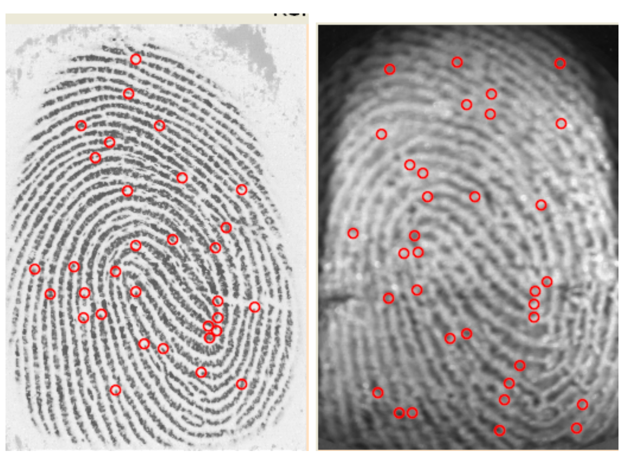

Figure 31: Showing minutiae points for source image and artefact, with a similarity score of 0

There are likely many different reasons as to why this is won't give a positive comparison decision. First of all, the capture of the initial finger was done on a capacitive sensor and tested on a optical touch less sensor. This might cause a scaling issue because of sensory interoperability. Second, our initial capture in which the model is based on, could potentially not be of a sufficient quality which makes the artefact generated, void. Additionally, this image has not been enhanced like mentioned in section 3.2, which could potentially improve similarity scores. Scaling could also be a problem. In order to verify some of these claims, a new model was made. This model was cleaned using previously mentioned methods, and scaled up in order to ease the printers work. In 32 we can see how the image is affected by cleaning.

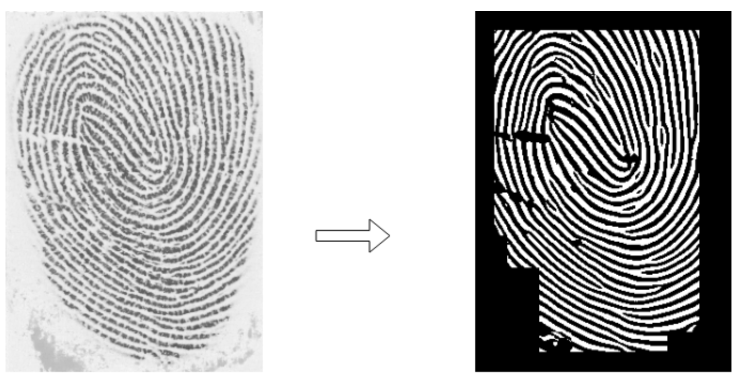

Figure 32: Right shows original image, left shows new and enhanced version

First scaling up the artefact to a bigger size, and then scaling it down when doing actual scanning, allowed us to get a positive score of 129. Adding to the positive score, another aspect for this artefact generation is also time. Generating the model took 10 minutes(with enhancement), while printing the model took approximately 1 hour. This means that "amateurs" would be able to generate a working prototype of a fingerprint(e.g. from a capture) without much preparation nor time available.

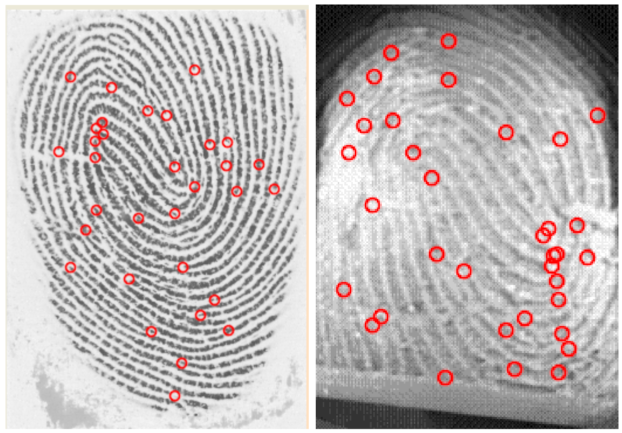

Figure 33: right image original with minutiae points, left image artefact with minutiae points

4.4 Checking conductivity and cohesion of materials

Since many filaments behave differently in printing despite being the same type(PLA), they might have different capabilities which make them harder to print with. For example, using flexible filaments(such as Ninjaflex Cheetah or others) we have seen that we are not able to get the same level of detail which enables us to make an valid artefact. The artefact generated using 40_1 with a thickness of 0.98mm, retains most details, it is only in the upper most part of the artefact in which the artefact do not retain the ridges and valleys. This is a problem shared with the reference model as seen in figure 34. While being conductive, conductive proto plastic, which is the filament used to achieve conductivity, comes in black. This is not ideal for interoperability in terms of sensor choice. As previously mentioned, using a black artefact for fooling a optical sensor will not work due to its very reflective surface.
The artefact generated using conductive Proto is flexible to an extent, but not enough to mimic the capabilities to that of the human skin, which is much more flexible. We have found that using artefacts generated with this filament, we are able to get sufficient conductivity of 1K Ω(measured using a voltmeter corner to corner), but due to the missing element of flexibility, which ensures that the whole artefact is read, we are getting incomplete readings.

To explore the conductivity of our filament, two different models were made in order to let us try it on a capacitive sensory device. This was done by using Solidworks and generating a single plane including five horizontal lines which mimic the similarities of ridges we find in a fingerprint. This was done to see whether we could produce a less advanced print which could give good results on a conductive reader allowing us to see the ridges clearly. Of the three artefacts generated, one

Figure 34: 40_1 original source image

was made with conductive filament, while one was made by being fused together with another flexible material in the hope that it would give both desired properties. After making three artefacts which vary with size from 0,3mm height to 0,5mm height and another with the aforementioned fusing, they were tried on a conductive sensor, the Precise 250MC.

Figure 35: a) model used for generating artefact. b) artefact on sensor with a depth of 0.5mm c) flexible filament fused with conductive filament with a thickness of 0.3mm

In figure 35 we can see that we are able to gain some conductive capabilities, and we can read all five lines from the artefact. However the probe in this case, seems to be weak in the sense that it seems more like a latent print than an actual print. It must be stressed that to even get this result, an unnatural amount of pressure on the artefact was exerted to make it register with the sensory device in both cases for figure 35b/c. Extending on this experiment, we expanded to a real fingerprint to see its effects.

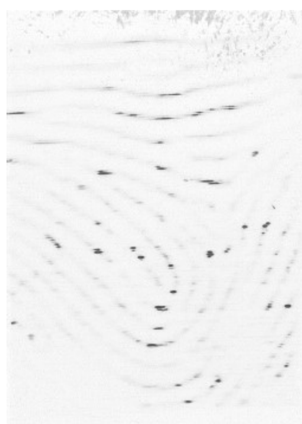

Figure 36: A conductive print generated using a conductive filament

As we can see in figure 36, we are clearly able to see discernible minutiae points of a fingerprint, while being a bit weak it is clearly conductive and able to give a current which is high enough for the sensory array.

The reason as to why the results are not better, probably lies in what is documented in related works, is that these conductive artefacts are not flexible enough and thus when pressure is applied, the pressure is applied unevenly and only parts of the artefact is touching the sensory platen to a sufficient degree. If pressure is exerted on a human finger, the finger will, due to its flexibility, flatten, and pressure will be somewhat evenly distributed. This will not happen on a this type of artefact because its rigidity. Possible solutions to this problem, could be to make a mould of a finger using a 3d scanner which properly reflects the curvatures of the finger, or try to generate a artefact which uses several extruders which allows for mixing of filaments such as conductive Proto pasta, and a flexible filament such as Ninjaflex. However, there are several issues with this idea, such as the degree to which flexible filaments are not able to replicate the level of details. Similarly getting enough conductivity might prove a problem.

4.5 Impact of image enhancement and interoperability between artefact and samples

A claim can be made that using image enhancement cleans up the image and makes it easier to model. In figure 37 we can se an example of raw image capture and the enhanced image. In the enhanced version(right) we can see that the ridge points are easier to see, and the delta and core are easily identified. These small changes to the model can ease the modelling process since there are less small layers which will have to be applied to the artefact. This allows the ridges to "breathe" in terms of modelling, so that they are easier to generate for the printer.

Figure 37: raw image capture(left) and processed image(right)

But how much does this affect the final result? To find out we made two models. One model was made with the preprocessing step, the other made by copying the measurements of the enhanced one, using the raw image as its base. After generating sufficiently good models, each model were tested to get their individual score. Initial results when testing the enhanced artefact were negative in that they gave us a similarity score of 0, but positive in that many of the same minutiae points were recognized. The score of 0 was most likely because the scale of the artefact was off. This means that even though many of the minutiae points line up, because the comparator would find additional points, they would give it a score of 0. This led us to cut the reference image so that we were able to isolate the area in which contains the delta and the core, as seen in figure 38.

Figure 38: Isolated image with core and delta points

The results were immediate, achieving an positive score of 76 as seen in figure 39. In the probe image(right) we can see that the image is showing much more detail than that of the reference image. In this image we can clearly see that there are many points which are found in the probe which is not in reference.

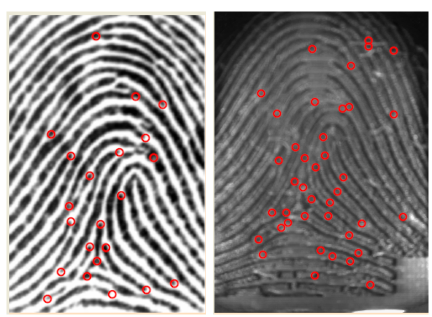

Figure 39: Minutiae points marked for artefact and resized image, getting a 76 similarity score

In order to assess the effect of scaling, we also scaled down the artefact picture to 75% of its original size and compared it to the resized image. This further increased the similarity score to 96.

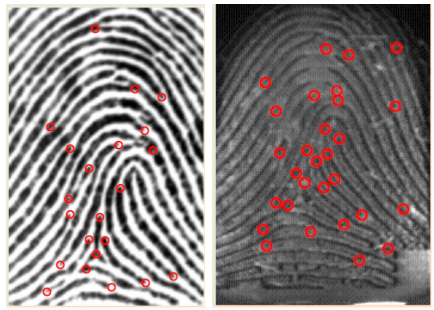

Figure 40: Minutiae points marked for resized probe and resized original image, getting a 96 similarity score

Since the scaling worked well on this image, we decided to try the original 1_1 raw image comparing it to the scaled artefact. This further increased the similarity score to 189. In figure 41 we can see that many of the artefact points are coinciding.

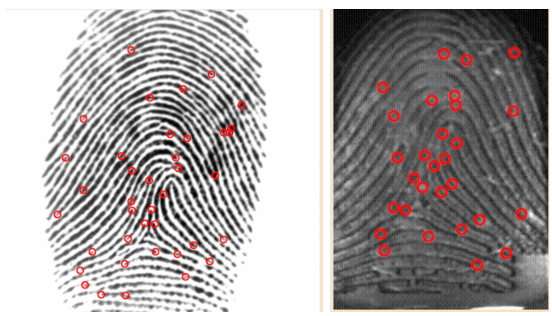

Figure 41: Minutiae points marked for resized probe and original image, getting a 189 similarity score

As for the raw image, the model images shows a different story than that of the enhanced one.

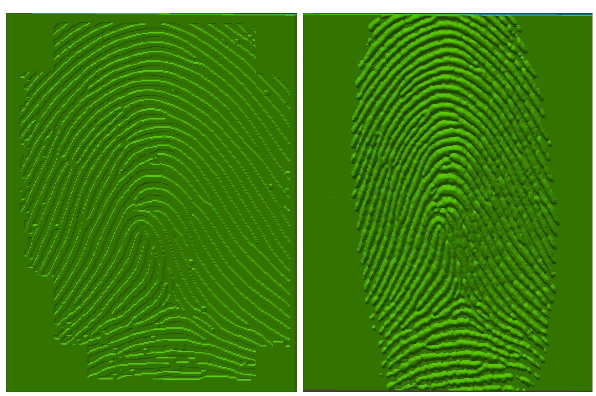

Figure 42: left: enhanced image, right: raw image capture of 1_1

As we can see in figure 42 we can see that the level of detail needed to be replicated in the left image is far greater than the one in the right, making it harder to to build. This becomes more apparent when we compare this artefact to the focused version of the raw image for a comparison. In terms of the enhanced sample, we can see that the score has dropped from a 96 similarity score to a 93 similarity score.

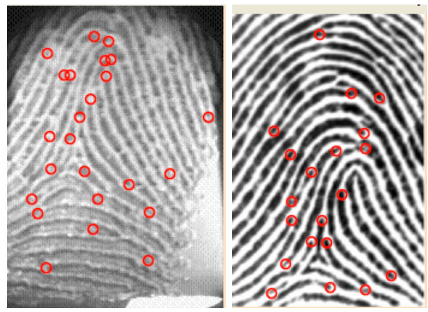

Figure 43: Minutiae points marked for resized probe and focused original image, getting a 93 similarity score

There is a slight drop in scores, as we can see in 43, which becomes further highlighted when we compare the scaled artefact to the original source image in 44 and achieve a score of 102 similarity score. When compared to the other model, we can see that there is a significant drop in score from the enhanced version to the raw version.

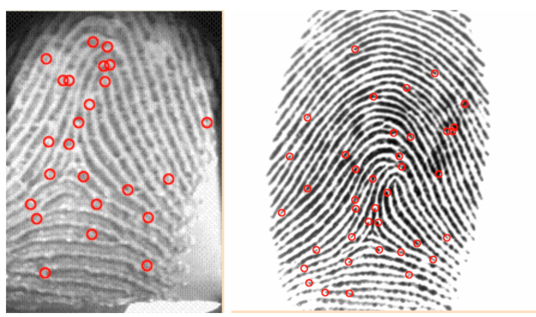

Figure 44: Minutiae points marked for resized probe and original image, getting a 102 similarity score

This can be an indicator that enhancing the model has an effect. By using enhancement, we are able to alleviate some for the printer, removing unnecessary detail from the model.

4.5.1 Checking interoperability

We can use the term interoperability to determine how good our model is, and how easy it is recognized over more than just direct 1:1 comparisons of the same raw image vs the artefact. The next natural step was to check for interoperability between the different original raw pictures in the FVC2002 database. In the FVC2002, all samples are gathered 8 times with varying degree of quality. To assess the interoperability of our two artefacts we compared them with other images of the same finger, we compared both of our scaled artefacts with all the remaining 7 raw images.

Interoperability for enhanced artefact

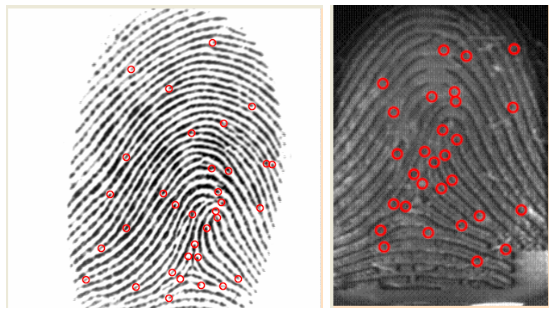

Figure 45: Minutiae points marked for resized probe and original image(1_2), getting a 161 similarity score

In terms of performance, the performance of the enhanced artefact dips a bit, but it is still very viable in terms of similarity scores. Since there is only a small deviation between the two images, the scores remain high, still achieving a 161 similarity score, as seen in figure 45.

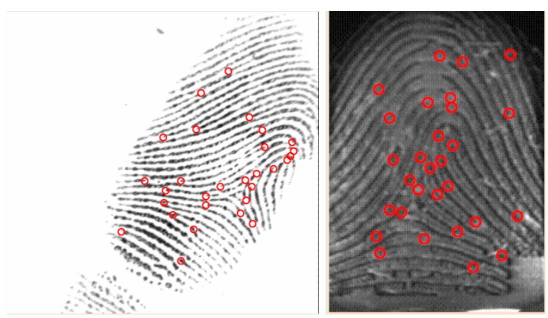

Figure 46: Minutiae points marked for resized probe and original image(1_3), getting a 63 similarity score

In further exploration of our next sample, 1_3(figure 46), the similarity score drops significantly. Here we are only able to get a similarity score of 63. Looking at figure 46 we can make assumptions about why this is happening. One idea could be that since the image capture has the finger tilted right, the minutiae points are further apart. This essentially would have the same effect as our pre scaled sample would achieve, scattering the minutiae points. This leads to worse recognition as the comparator assumes its either noise or bad placement. Adding to the last assumption about comparators, one could argue that 1_3 shows more of the whole finger than what is captured in 1_1 and would therefore cause the score to go down.

One can argue that the scores of 1_4 validates this theory. In figure 47 we can see that the left image is only a partial, but this partial has the the deltas and the core visible. This allows our scaled enhanced artefact to match better with this specific sample and have many of the similarities to our original attempts at scaling the raw image.

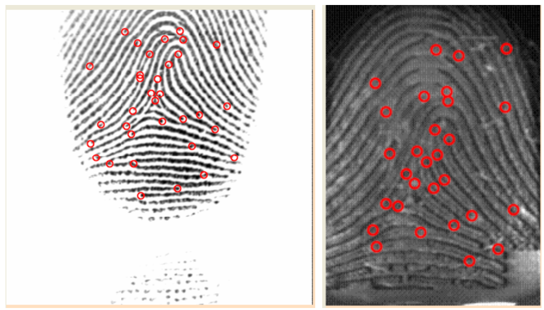

Figure 47: Minutiae points marked for resized probe and original image(1_4), getting a 168 similarity score

In 1_5 we can see that this is a partial print which has none of the defining characteristics of this print, the core and the delta, which is further down on the finger. We also see a dip in performance when comparing the 1_1 raw to the 1_5 raw, achieving only a 269 similarity score, whereas the raw 1_1 to raw 1_2 has a similarity score of above 1100. However, we can argue that if we based our model for generating the artefact on the 1_5 image, we would be able to get a positive score, since we would be able to get that specific sample's characteristics.

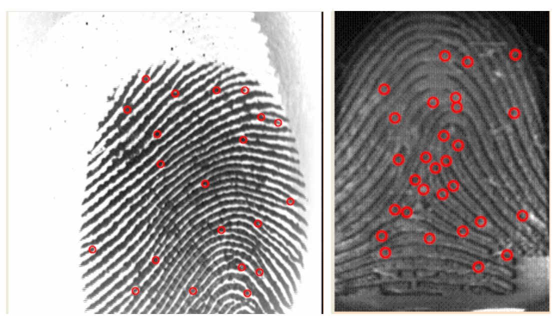

Figure 48: Minutiae points marked for resized probe and original image(1_5), getting a 0 similarity score

The scores of 1_6 increases, most likely due to the fact that the core and delta is visible. This has many similarities to the 1_1 raw image, but some of the top capture is different from the 1_1 and 1_2 samples. Combined with the fact that core and delta is clearly visible, probably explains the rise in score.

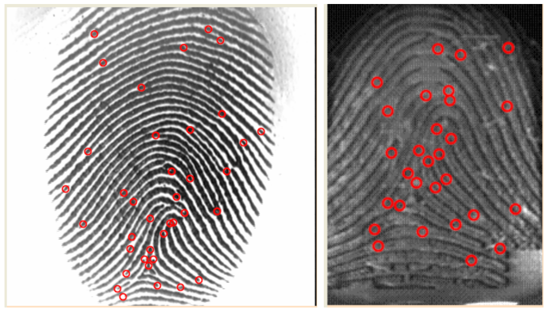

Figure 49: Minutiae points marked for resized probe and original image(1_6), getting a 92 similarity score

We see it increase further in figure 50, where most of the raw images ridge lines are much more visible than the ones in figure 49, which are somewhat smudged down. In addition to this, the core and delta is clearly visible which gives a good foundation for comparing the two samples. The low score compared to the other samples can be most likely be attributed to a bad capture, where the subject has pushed the sensory platen to hard.

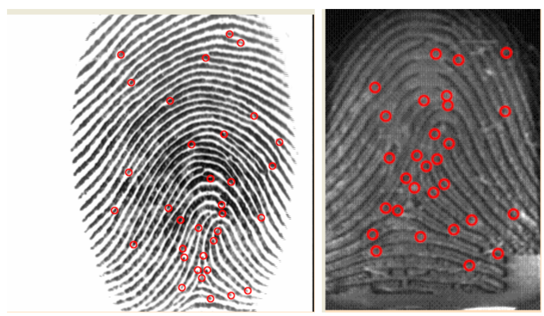

Figure 50: Minutiae points marked for resized probe and original image(1_7), getting a 140 similarity score

It increases further in the last sample(visible in figure 51), probably due to ridges being easier to read. This is probably a result of the pressure of the sensory platen this capture was done on, and not something which is controlled by the artefact.

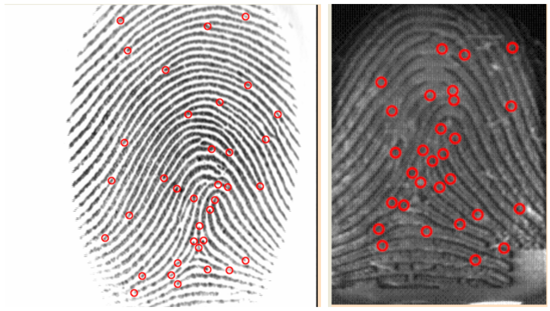

Figure 51: Minutiae points marked for resized probe and original image(1_8), getting a 150 similarity score

Based on these 8 samples, we are able to determine that there is a high level of interoperability where the raw images cover the same region of interest. This means making two artefacts for this set of fingerprints would allow us to authenticate as subject 1.

Interoperability between model generated from raw artefact and other samples

In order to assess the impact of enhancement of the model in artefact generation we made two models and compared them with the same raw samples. This allows us to assess the performance of the two artefacts in the subset of subject 1 from the FVC2002 database. Additionally, we are able to assess the interoperability of the model and by extension the artefact. The interoperability gives us an indicator of how good the artefact is.

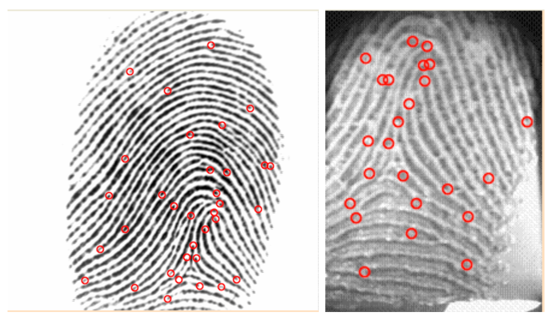

Figure 52: Minutiae points marked for resized raw probe and original image(1_2), getting a 80 similarity score

We can note that the score achieved in figure 52 compared to the enhanced version is significantly lower than score when comparing to 45 which has a similarity score of 160. One can argue the significance of this, but already we see that enhanced models are more interoperable. In 1_3, which has already been established as a bad capture, scores keep decreasing. In figure 53 this is highlighted, as the score has decreased to 63.

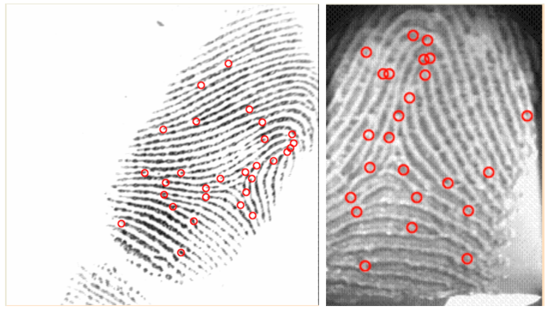

Figure 53: Minutiae points marked for resized raw probe and original image(1_3), getting a 57 similarity score

When assessing 1_4 we can see the score increase again, which is probably due to the same reasons which were highlighted earlier, that the source image contains cores and deltas which enables us to recognize it.

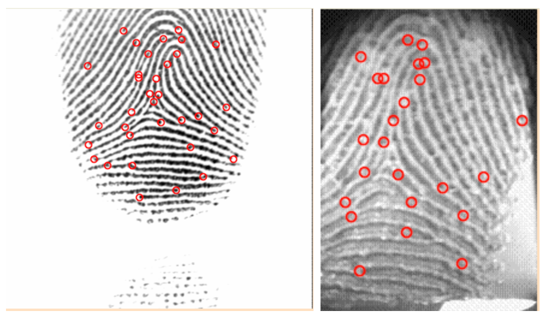

Figure 54: Minutiae points marked for resized raw probe and original image(1_4), getting a 113 similarity score

Like before, figure 55 shows the bad sample getting a 0 similarity score. This is most likely due to a combination of both the bad model and the bad initial capture.

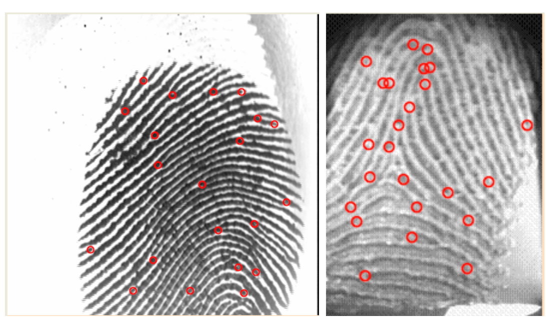

Figure 55: Minutiae points marked for resized raw probe and original image(1_5), getting a 0 similarity score

Compared to 1_6 vs enhanced, we see a significant drop in quality score. Since 50 is the similarity threshold which defines that the probe and the reference is from the same subject, we can only blame the model. This means that the artefact shows signs of bad interoperability, most likely due to its complexity in terms of modelling and printing.

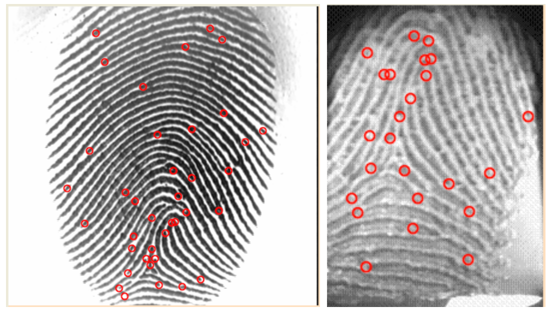

Figure 56: Minutiae points marked for resized raw probe and original image(1_6), getting a 54 similarity score

As 1_7 was one of the highest scoring probes with our artefact, it is significant that in figure 57 gets a 0 significance score. This might be because the enhanced probe has clearer minutiae details in the top probe capture. A combination of manufacturing imperfections as well as modelling complexity causes this.

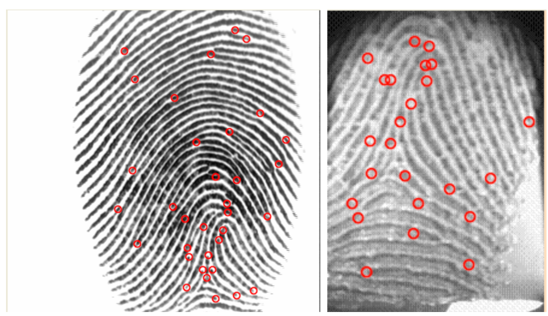

Figure 57: Minutiae points marked for resized raw probe and original image(1_7), getting a 0 similarity score

One of the highest scoring samples comparing to our enhanced capture, 1_8(figure 51) receives a score of 0 when comparing to our raw capture. This is probably due to the complexitity of the modelling. When comparing the models in figure 42, we can see that the upper levels of the model is significantly more detailed. This causes some of the ridges to "collapse" in manufacturing most likely due to its complex and its proximity to other ridges.

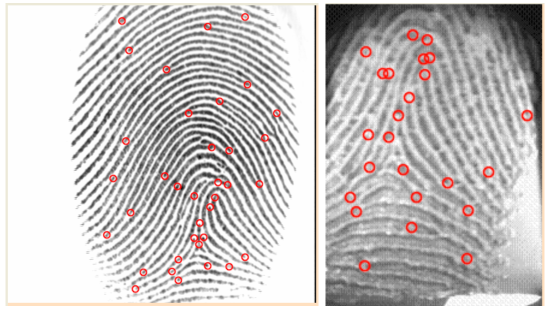

Figure 58: Minutiae points marked for resized raw probe and original image(1_8), getting a 0 similarity score

Using the two artefacts and comparing its interoperability allows for comparison of the quality of the artefact, and make a decision about a preferred method of modelling. In table 1 the scores of the two artefacts are compared. As we can see, the enhanced artefacts provides interoperability between all samples, only missing 1_5, but if we would have made an artefact of the 1_5 model, chances are that we might have gotten a positive score for this as well.

Image	enhanced artefact	raw artefact	difference
1_1	189	102	87
1_2	161	80	81
1_3	63	57	6
1_4	168	113	55
1_5	0	0	$\emptyset$
1_6	92	54	38
1_7	140	0	140
1_8	150	0	150

Table 1: Similarity scores for comparison of interoperability between enhanced artefact and raw artefact

As to why several scores were missing from the raw artefact comparison, we can assume that this can be attributed to a bad or too complex model or complications to the manufacturing process e.g. making the ridges collapse. This would mean that layers would melt together, and the ridge wall would be double its intended parameters. This would cause worse similarity scores since ridges would be missing or its location skewed. We could also say that the raw artefact has limited interoperability. The average scores of the two, shows the enhanced artefact averaging 120.1 in similarity score across the board, while the raw artefact only has a score of 50.7. According to imposter scores generated from the 2d plane, we are able to assess that the similarity scores indicate that the artefact is good enough to be recognized as a genuine user by the commercial comparator. To expand on this, according to the Neurotechnology biometric SDK[50] a FAR threshold of 0.01%(or 48 similarity score) would indicate that similarity scores above 48 would give us a 0.01% chance that a finger is incorrectly recognized by Neurotechnology biometric SDK.

Similarity score threshold	FNMR enhanced artefact	FNMR raw artefact
48	$1/8 = 12.5\%$	$3/8 = 37.5\%$

Table 2: FNMR for enhanced artefact and FNMR for raw artefact with a similarity threshold score of 48

In accordance to the Neurotechnology biometric SDK[50], if we set a FAR threshold of 0.01%, we would achieve the following FNMRs(matches which should have been matched, but are not) presented in table 2. These thresholds are chosen because we use Neurotechnology verifinger SDK as a comparator, and in accordance to the SDK documentation[50]. If we set a stricter false acceptance rate of 0.000001%, with a corresponding threshold of 96 similarity score we would achieve the results presented in 3. This would indicate that if we set the threshold at 0.000001%, the FNMRs[32] indicate we would be falsely declined 25% of the time, while using the raw artefact we would be falsely declined 75% of the time.

Similarity score threshold	FNMR enhanced artefact	FNMR raw artefact
96	$2/8 = 25\%$	$6/8 = 75\%$

Table 3: FNMR for enhanced artefact and FNMR for raw artefact with a similarity threshold score of 96

4.6 Mobile phone sensory device

While conventional conductive readers just use one or more full capture(s) for the enrolment phase, smart phones due to their small size, have to take several partials [51] to form a full fingerprint. This means that it might be possible to utilize our artefact on a phone to enrol a subject, even though the artefact is not flexible enough to be fully recognized by a conventional capacitive reader. To explore mobile phone sensory devices, we use the Huawei Mate 9. This is a fairly recent phone, with an advanced sensor. To make viable artefacts for a mobile sensory device consists largely of trying to make conductive artefacts, since most phone readers are conductive readers[52]. This means that we use Proto-pasta Conductive Graphite-PLA 1.75 as previously explored in section 4.4 for its conductive capabilities. To explore mobile phone sensory devices, we use the Huawei Mate 9[53]. This is a fairly recent phone, with a capacitive sensor.

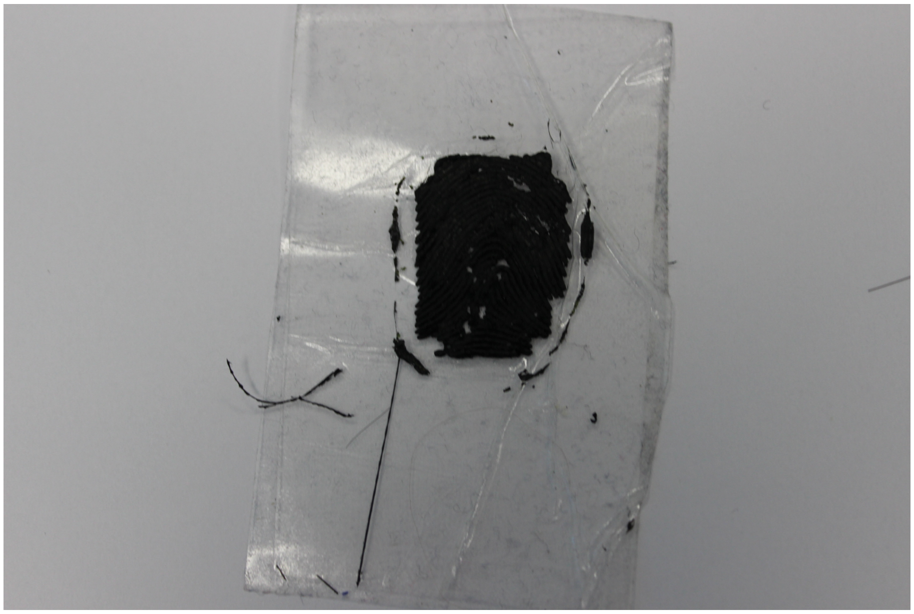

Figure 59: Thin artefact printed on two way cello tape

To test if we are able to impart flexibility using a inflexible conductive filament, the thinner model will be made and printed on a piece of tape. When printing the thin model, we apply a rectangle of tape around the print surface to make sure the print would lay still. Without the tape, we found that the extruder would slip and we would get an inaccurate or malformed print. When the print is finished, the tape on the sides were dragged of the sides, and we were able to remove the thin artefact which is sticking to the middle using a two way tape. The artefact is visible in figure 59. Using the artefact presented in figure 59 we were able to enrol as a user and unlock the phone using our generated artefact.

Figure 60: Artefact of Guoqiangs finger

However, Since subject 1_1 was picked out of a database, and could not be available for personal testing, We decided to use Guoqiangs model of his right thumb(index 6) to test interoperability with a real finger. In figure 60 we can see the artefact. Using this artefact, we were able to both enrol and authenticate as seen in figure 61.

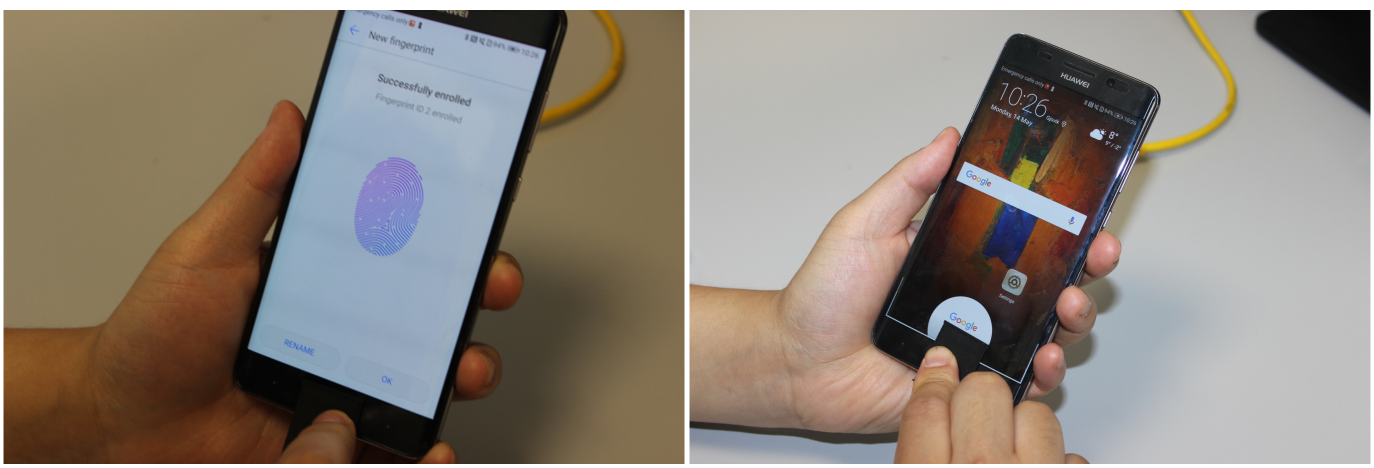

Figure 61: Showing authentication and subsequent unlocking of phone using artefact

Since having multiple of the same finger enrolled into a phones database would make no practical sense, the phone refuses to enrol the same finger twice. This makes it a good interoperability test. This meant that if we were able to enrol Guoqiangs finger, the artefact would not match the finger. Since we were able to enrol Guoqiangs finger, we can conclude that they do not match. This is likely due to scaling, meaning that while the necessary minutiae points are replicated in the model, they are probably too big. Reducing the artefact to 70% of its current size could potentially make it match since this has been the case in e.g. section 4.5. In addition to scaling, due to layering in heights, we would lose significant detail because the details would be too small to replicate. This leaves room for further improvement using e.g. fluid 3d printers, which would alleviate this issue.

5 Discussion

5.1 The process of making an artefact

In terms of what has been produced in this thesis, one can argue that on the offset the idea of reproducing the artefact(s) which others have produced, was flawed. In hindsight trying to achieving the same level of accuracy which has been done in other relevant research using a machine which is about 200 times more expensive than the ones that we have used, is clearly not a good idea. However, throughout our experiments, we can see that the level of details to replicate some of the artefacts have been more than sufficient in terms of similarity scores in Verifinger SDK. Like those presented in section 4.2 which on a visual inspection has retained most of the details of the original sample, allowing it to be used for recognition in touch less optical sensors with good result. In order to discuss the results, it is important to also see the process as an iterative process, which moves fairly quickly. In order to first be critical of the process, one needs to start where the iterative process begins, by defining the model. In order to discuss the model, it is important to understand how the process is done.

The process starts by making the model. The model is crucial in order to make a valid artefact, because it is the deciding factor in terms of many questions related to scale, accuracy and level of detail. Thus, a critical view of how images for artefact generation is required. The artefacts created for the thesis work have all been created with the basis in FVC2002 or using a capacitive sensory device for the capture. These images have not been enhanced using the software mentioned in section 3.2, due to the success of the work presented in section 4.2 and the failure of making a valid artefact in figure 18, which made auto generating models using software harder. One could argue that given the success achieved in section 4.5, it would make sense that every image is enhanced, but alas it was not. This is probably the biggest critique to the process; that this really rudimentary technique was tested at such a late stage in the process.

This leads directly into another critical aspect of making the model; the fact that I am not by any means a industrial engineer nor graphical designer which means that I have been limited to "autogenerate"-functions of programs like Materialize Magics and Windows 3D builder. Using no tools other than visual inspections, the model is then determined by visual inspection both in the Slic3r if the model is good enough both in terms of layering and if minutiae points are visible. Here, related research have used microscopes to verify the quality, but this has not been done either due to early discussions in which we determined that this would not have been beneficial. In hindsight, one can argue that it *might* give us an indicator of the artefacts quality.So instead of doing it more scientific, this means that my personal bias could have an influence on what is deemed good and not before checking it with Verifinger SDK.

Another essential critique could be that the artefact generated is a positive rather than a negative mould, which would allow for more choice in terms of materials, but at the same time, one can argue that this is then not a 3d printed artefact but a moulding technique. This could of course be very positive as it would lead to better material choice. This could be explored further in related research.

In terms of modelling, one can ask if whether a wide spread sample of images would be better suited for the purpose of doing this research. This would have allowed us to explore the meaning of NFIQ 2.0 scores in model making decisions. This could also be suiting for future work.

Regarding material choice, one can argue that there was not a sufficient sample size to pick from. Using PLA 1.75MM filaments, I was able to find four materials which potentially could be used. The fillaments used were flexible filaments such as Ninjaflex Cheetah and Ninjatek Armadillo, which are not conductive, but also filaments such as Proto-pasta Conductive PLA. While on paper being able to make flexible materials which were both conductive and flexible, a mix between the two was not possible due to lack of cohesion between the two materials. This means that achieving "best of both worlds" has not been possible with the materials chosen for the experiments. In addition to this, PLA is the only filament type which has been considered for this experiment, still leaving it possible to make valid artefacts using materials in e.g. PLS, which has been documented as successful in section 2.2.

In terms of additional ways of imparting conductivity extending beyond filament choice, Chinese news sites reported the use of transparent tape and a conductive pen was able to provide enough conductivity to fool a fingerprint sensor. We were not able to verify this technique due to international flights not allowing conductive pens on-board. However, artefacts printed using a filament have been made which give sufficient conductivity(1K Ω(measured using a voltmeter corner to corner). According to section 2.2 the human skin has a electrical resistance of between Ω $2.5 * 10^2$ - $8 * 10^6$ or between 2.5 Ω and 8MΩ, which implies that additional measures are not not needed, but rather than lacking conductivity lacks flexibility. After discussing filaments and methods for imparting additional conductivity, another essential step to look at is the manufacturing itself.

The manufacturing of the artefacts were all done on two Prusa MK II filament based printers, so manufacturing could have been tested on other available machines such as Ultimakers. However due to discussions with staff at ADDLAB, they were decided against because the belief that they would not be able to produce better results than what was already being produced by the PRUSA MK II.

5.2 Methods

As previously mentioned, the process has been iterative and highly modular which allows for many subsequent (re)tries in terms of experiments, allowing the same experiment to be done several times only differing in materials used. This allows for consequent testing of different variables such as length, width and depth. What can be critiqued is the work flow of printing in the lab, which some times have lead to confusion as to what type of model which is printing where, and has in some cases lead me to print two of the same model, while at the same time believing they were different.

Since I am not an expert on additive manufacturing, I have been relying on ADDLABs expertise, which means that their expertise extends mine. This means that if they are unaware of a additive technique or material, this will not get pursued. This means that there is a risk of missing something fairly obvious, which others might not have missed.

5.3 Final results

While we have been able to enrol and unlock a Huawei mate 9 using a artefact created using conductive materials(section 3.4.2) and have been able to get a similarity score of 92(figure 28) on a optical touch less sensory device with the original image as the reference and the artefact as the probe, it can still be discussed how significant this is. While we are able to make artefacts which could easily match the reference purely on the basis of direct picture comparison, the more advanced scanners such as capacitive sensors should not be as easily fooled. The possibility of fooling devices such as these, are based on the availability of flexible AND conductive filaments, since as we have shown, the conductivity alone is not enough. The biggest threat to making valid artefacts for capacitive sensory devices it seems, is not the level of conductivity, but rather the combination of the two. The problem with the conductive filament used in this thesis, is that it requires a lot of pressure and adjusting to even get some recognizable input from the sensor. When pressed hard on the sensory platen, the artefact will at some parts of the sensor look like a normal fingerprint but will lack essential minutiae in other parts, or it will appear as very weak. This means that as soon as making both conductive and flexible filament for e.g. filament based printers are available, authentication of humans using fingerprinting potentially needs rethinking.

Such a claim is bold, but I believe it is justified because of results seen in related works, and also shown in my thesis. The fact that we are able to accurately replicate minutiae using the "off-the-shelf" printers, means that only materials for achieving properties are missing. In related research, the researchers are claiming their artefacts are cheap to produce(approximately 10 USD), this does not take into account that the machine they are using to produce these artefacts costs upwards of 200 000 USD. So the risk of attacks like that are, should we say, for those extra motivated individuals. As far as being able to replicate their results, one could argue that I have been able to in some degree. I have been able to create an artefact which is recognized when comparing to a reference image, as the real one. This was printed on normal PLA roll of 700 grams, which is available retail at 350 Norwegian kroner. If you add the price of the printer, you would still be able to print viable optical touch less artefacts for less than 10000 Norwegian kroner, including the full price of the printer! An estimate based on the 1_1 artefact would put the per unit cost at 2 NOK using 1.67grams of filament, allowing a total of 449 artefacts to be printed of one spool of filaments weighing 0.75kg.

What is puzzling is that we have been able to use several phones' sensors using a finger and a thin plastic bag under the finger to authenticate. The plastic bag should in theory act as a insulator, but authentication has been successful on many different phones' sensors using this approach. The reasoning behind this is unclear. It could be a retention of static electricity, which in touch with the sensor is unleashed, giving enough electricity for the sensory device. Another theory, is that this works because of interoperability like different weather conditions, allows it to read patterns which are slightly obfuscated for different reasons. This is probably done for interoperability reasons, which makes it potentially more durable in everyday use. While that being said, trying to apply it to using a non-conductive artefact on the sensor by way of thin plastic bag was not successful. A third reason might be active sensing, in which the sensors send a small current through the touching surface to enable it to sense.

That this is possible, might also be the reason we were able to enrol the artefact on the Huawei Mate 9. We were successful in enrolling an artefact on a phone, and using the same artefact for authentication. When trying to repeat our efforts, by enrolling Guoqiangs finger, we were successful in enrolling the artefact, but when trying Guoqiangs right thumb index 6 to unlock, this was unsuccessful. The theory as to why this was possible is that since phone capacitive sensory devices needs to be highly versatile, they also need to accept degraded pieces of fingerprints in enrolment to ensure high availability and universality.

We have been able to prove that pre enhancement of pictures has a positive effect for modelling, and that the interoperability between artefacts are generally higher for the artefact which has had enhancement, compared to that of the raw artefact. This means that the potential for alleviating some of the complexity in the manufacturing process. If one had to be critical to the process for exploring interoperability between artefacts, we partially hit upon one of the essential problems with biometric comparing. This is the fact that we can never ensure that we get the *exact* same capture of the probe. Which means that some of the negative interoperability scores achieved might be either due to bad placement or manufacturing issues. Adding critique to this we can argue that the sample size is too small to make this claim and that by increasing it would give us more data about how much it affects model generation.

5.4 Research questions

The research questions allow us to discuss our findings. While the the current state of the art is able to make "global" artefacts which can be used on all devices for performance measuring, they would need to be ordered, and not self made, since the initial cost of a the printer used is very high. The feasibility of an artefact created using cheap materials and using less accurate printers have shown to have great promise. Using a auto generated modelling approach we have been able to make several models which are good enough to be considered genuine by a commercial comparator. Using various PLA samples of different colours, we have found that what other research indicate, that the colour of the filament can obstruct the artefact generation process for optical sensors. We have also found that gray 1.75mm PLA gives us a very good results for artefact generation for touch less optical sensors. While we have not found a good solution for conductive sensory devices, we have found that our filament is conductive enough. However, the fusing of two or more filaments could alternatively give us better results, but requires filament which gives good cohesion with the conductive material. This was not achieved in this thesis, most likely due to bad cohesion. We have tried introducing conductivity into the artefact generally by making an artefact which in fact is conductive. We also saw the use of conductive pens being able to unlock phones[54], meaning we could potentially find other ways than filament to use for giving conductivity.

The quality of our fingerprints have been of a high enough quality to fool commercial comparators, with the exception of conductive comparators, which most likely due to flexibility could not fool the sensors. It is important to note the fact that our conductive artefact retained the quality which it should. We saw that given enough pressure on the finger platen allowed us to get a partial fingerprint. This fingerprint resembled what the raw image showed, so this means that if additional flexibility would be introduced by a filament, it would most likely give significantly better results.

Further we have found that our artefact has been able to match that of the original sample of the same subject. Not only have we been able to do this, we have also been able to prove better interoperability for artefacts which uses pre-enhancement of the raw image than artefacts generated from a raw model. This is probably due to the decrease in model complexity, meaning fewer details for the 3d printer to replicate. In terms of similarity scores, they have all been mostly positive. This means that reliable artefacts can be made using this method.

While we have been able to make sufficient artefacts, it is important to note that they are not printed in their original size, but rather the artefact is enlarged. This allows us to get a richer level of detail. This means that we had to scale it down to match it with the print on the capture device. This is not however something which would have been possible when testing on a commercial system which is in production but would have required us to make a smaller artefact. We tried making the artefact life-size, but due to e.g. layering, essential minutiae points were lost. Using a liquid based printer, would potentially make better artefacts for this purpose as we would lose the layering effect.

If we were to not scale them, we would not achieve a positive score, meaning that we would not be able to generate sufficient artefacts. This is however something which could be further explored using other printers in future works.

6 Conclusion

In this thesis we assess the different challenges of making 3d printed artefacts with 1.75mm PLA filaments. In this thesis we have been able to verify knowledge already in the body of knowledge such as the impact of colour of artefacts in artefacts for touch less optical sensors. We have been able to highlight the need for both conductivity and flexibility in artefacts generated for conductive sensing arrays. This is highlighted by the force that is required to get a reasonable imprint on a conductive sensory device. Where force is not applied, the fingerprint looks weak or not visible. From the state-of-the-art we know that flexibility would most likely help with this, since this allows for "yield" in the finger which spreads the pressure.

Besides being able to confirm findings which the state-of-the-art also reports, we have been able to get a positive similarity score in a direct comparison of a source image versus an produced artefact using a touch less optical sensor. This means achieving the appropriate levels of details in the artefact. This allows us to claim that achieving a satisfactory level of detail can easily be done on more affordable and less accurate 3d printing machines than that of the ones used in the current state-of-the-art. This has also been one of the main motivational points for this research. We were also able to generate similarity scores which show that our generated artefacts are showed as genuine by a commercial comparator. We have also been able to enrol an artefact on a mobile phone sensor, unlocking it with the same device afterwards. While being able to unlock phones with an artefact, we are not able to generate a conductive artefact which has interoperability with a real finger.

Our preliminary research show enhancement significantly improves similarity scores and allows for interoperability within the same subject. To further confirm such a claim it will most likely need to be further explored using a larger sample size. We are able to investigate interoperability between artefacts and other sample captures finding that the artefacts which has had enhancement has a higher average score within the sample size(120) than that of the raw source image artefact(50).

6.1 Future Work

As for future work, there are many possible avenues to pursue.An additional exploration of other low cost printers and filaments would be interesting in order to see their potential. Other materials than PLA would be interesting, as they might have qualities which PLA does not have, such as flexibility. In terms of layering, it would be interesting to see what filaments could offer which decrease the visibility of the layer. If another filament is available which decrease the layer size, this could potentially mean more detailed artefacts. Since off-the-shelf filaments which provide both sufficient conductive capabilities as well as flexibility are lacking, it would be interesting to further investigate alternate ways of achieving this. Another interesting idea in terms of manufacturing with affordable 3d printers, is the idea of the Masterprint[51]. The basis of the masterprint is that since modern mobile phones are small, the fingerprint sensor also has to be small. Since the sensor is small, when enrolling, the phone takes several partials of the fingerprint to ensure that at least one of them will be successfully authenticated. In [51] the masterprint looks at the possibility of generating a "Masterprint", a synthetic or real fingerprint which matches one or more of the stored templates for a significant number of users. The idea of generating such a fingerprint is interesting and would be a good way forward.

When generating the similarity score between 3D artefact and the fingerprint samples captured from the capacitive / optical sensors in section 4.5.1, the scores showed that even though our scores are good enough to be recognized by a commercial comparator, the genuine scores were significantly higher. This leaves room for improvement. If other printers are more accurate, but still affordable, they could potentially be viable for further exploration. It would also be interesting to look at comparative liquid based printers, which have fewer issues with layering. To add to the number of filaments would also be interesting, such as filaments as [55] using TPU which according to [56] is both flexible and conductive.

Bibliography

[1] Technical specifications (november 2017 edition). https://shop.prusa3d.com/en/3d-printers/53-original-prusa-i3-mk2s-3d-printer.html.

[2] Objet350 and objet500 connex3. http://global72.stratasys.com/~/media/Main/Files/Machine_Spec_Sheets/PSS_PJ_Connex3.ashx.

[3] Commons, W. 2014. File:fingerprintonfinger.jpg — wikimedia commons, the free media repository. [Online; accessed 18-May-2018]. URL: https://commons.wikimedia.org/w/index.php?title=File:Fingerprintonfinger.JPG&oldid=141656889.

[4] Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. 2009. *Handbook of Fingerprint Recognition*. Springer. URL: https://www.amazon.com/Handbook-Fingerprint-Recognition-Davide-Maltoni/dp/1848822537?SubscriptionId=0JYN1NVW651KCA56C102&tag=techkie-20&linkCode=xm2&camp=2025&creative=165953&creativeASIN=1848822537.

[5] Labati, R. D., Piuri, V., & Scotti, F. 2015. *Touchless Fingerprint Biometrics (Series in Security, Privacy and Trust)*. CRC Press. URL: https://www.taylorfrancis.com/books/9781498707626.

[6] Engelsma, J. J., Arora, S. S., Jain, A. K., & Paulter, N. G. June 2018. Universal 3d wearable fingerprint targets: Advancing fingerprint reader evaluations. *IEEE Transactions on Information Forensics and Security*, 13(6), 1564–1578. doi:10.1109/TIFS.2018.2797000.

[7] Prusa i3mkii). https://shop.prusa3d.com/317-thickbox_default/original-prusa-i3-mk2s-3d-printer.jpg.

[8] Gafurov, D., Bours, P., Yang, B., & Busch, C. March 2010. Guc100 multi-scanner fingerprint database for in-house (semi-public) performance and interoperability evaluation. In *2010 International Conference on Computational Science and Its Applications*, 303–306. doi:10.1109/ICCSA.2010.71.

[9] U.S customs and borders. 2018. Border patrol - fingerprint recognition system. https://www.cbp.gov/newsroom/photo-gallery/photo-library/border-patrol-fingerprint-recognition-system. Online; accessed 14.05.2018.

[10] E.U immigration Portal. 2018. The schengen entry/exit system: biometrics to facilitate smart borders. https://www.gemalto.com/govt/coesys/eborder/entry-exit-system. Online; accessed 14.05.2018.

[11] uidal.gov. 2018. Aadhaar enrolment. https://www.uidai.gov.in/enrolment-update/aadhaar-enrolment.html. Online; accessed 14.05.2018.

[12] A year when the conditions changed. https://corporate.fingerprints.com/en/about-fpc/interview-with-the-ceo/.

[13] Apple Inc. 2018. Iphone x. https://www.apple.com/iphone-x/. Online; accessed 14.05.2018.

[14] Anil K. Jain, R. B. P. 1999. Biometrics: Personal identification in networked society (the springer international series in engineering and computer science). URL: https://www.amazon.com/Biometrics-Identification-Networked-International-Engineering/dp/0792383451?SubscriptionId=0JYN1NVW651KCA56C102&tag=techkie-20&linkCode=xm2&camp=2025&creative=165953&creativeASIN=0792383451.

[15] Tartagni, M. & Guerrieri, R. Jan 1998. A fingerprint sensor based on the feedback capacitive sensing scheme. *IEEE Journal of Solid-State Circuits*, 33(1), 133–142. doi:10.1109/4.654945.

[16] Precise 250 mc: Fingerprint and smart card reader with fips 201 compliance. https://precisebiometrics.com/wp-content/uploads/2014/11/ProductSheetPrecise250MC.pdf.

[17] Brandom, R. Your phone's biggest vulnerability is your fingerprint. https://www.theverge.com/2016/5/2/11540962/iphone-samsung-fingerprint-duplicate-hack-security.

[18] Hern, A. Hacker fakes german minister's fingerprints using photos of her hands. https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands.

[19] Arora, S. S., Jain, A. K., & Paulter, N. G. Sept 2017. Gold fingers: 3d targets for evaluating capacitive readers. *IEEE Transactions on Information Forensics and Security*, 12(9), 2067–2077. doi:10.1109/TIFS.2017.2695166.

[20] Raja, K. B., Wasnik, P., Raghavendra, R., & Busch, C. Oct 2017. Robust face presentation attack detection on smartphones : An approach based on variable focus. In *2017 IEEE International Joint Conference on Biometrics (IJCB)*, 651–658. doi:10.1109/BTAS.2017.8272753.

[21] Arora, S. S., Cao, K., Jain, A. K., & Paulter, N. G. Oct 2016. Design and fabrication of 3d fingerprint targets. *IEEE Transactions on Information Forensics and Security*, 11(10), 2284–2297. doi:10.1109/TIFS.2016.2581306.

[22] Ruptly. Usa: Murder victim's phone unlocked using 3d printed fingerprint replica. https://ruptly.tv/vod/20160802-042.

[23] Sousedik, C. & Busch, C. 2014. Presentation attack detection methods for fingerprint recognition systems: a survey. *IET Biometrics*, 3(4), 219–233. doi:10.1049/iet-bmt.2013.0020.

[24] Arora, S. S., Jain, A. K., & Paulter, N. G. Sept 2016. 3d whole hand targets: Evaluating slap and contactless fingerprint readers. In *2016 International Conference of the Biometrics Special Interest Group (BIOSIG)*, 1–8. doi:10.1109/BIOSIG.2016.7736900.

[25] Supply, B. Fingerprint scanners. http://www.biometricsupply.com/cgi-bin/fingerprint-scanners-list.cgi?group=single_finger#.

[26] 3d printer price. https://www.cati.com/3d-printing/3d-printer-price/.

[27] Wikipedia. Entropy (information theory). https://en.wikipedia.org/wiki/Entropy_(information_theory)#Limitations_of_entropy_in_cryptography.

[28] Babu, C. N. K., Rajendiran, M., & Ibrahim, B. S. Nov 2014. Random password entropy and crack time calculation for south asian languages. In *2014 International Conference on Science Engineering and Management Research (ICSEMR)*, 1–4. doi:10.1109/ICSEMR.2014.7043593.

[29] Ratha, N. K., Connell, J. H., & Bolle, R. M. 2001. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3), 614–634. doi:10.1147/sj.403.0614.

[30] Christoph Busch. 2016. Harmonized biometric vocabulary. https://christoph-busch.de/standards.html#370103. Online; accessed 08.03.2018.

[31] Han, Y., Ryu, C., Moon, J., Kim, H., & Choi, H. *A Study on Evaluating the Uniqueness of Fingerprints Using Statistical Analysis*, 467–477. Springer Berlin Heidelberg, Berlin, Heidelberg, 2005. URL: https://doi.org/10.1007/11496618_34, doi:10.1007/11496618_34.

[32] Information technology — vocabulary — part 37: Biometrics. Standard, International Organization for Standardization, Geneva, CH, February 2017.

[33] Schuckers, S. 2016. Presentations and attacks, and spoofs, oh my. *Image and Vision Computing*, 55, Part 1, 26 – 30. Recognizing future hot topics and hard problems in biometrics research. URL: http://www.sciencedirect.com/science/article/pii/S026288561630052X, doi:https://doi.org/10.1016/j.imavis.2016.03.016.

[34] BBC NEWS Latin America. 2016. Doctor 'used silicone fingers' to sign in for colleagues. http://www.bbc.com/news/world-latin-america-21756709. Online; accessed 23.09.2017.

[35] Fortune,Kia Kokalitcheva . 2016. Fingerprint spoofing is much easier than you think. http://fortune.com/2016/02/24/fingerprint-spoofing-easy/. Online; accessed 23.09.2017.

[36] Coli, P., Marcialis, G. L., & Roli, F. 2007. Vitality detection from fingerprint images: A critical survey. In *Advances in Biometrics*, Lee, S.-W. & Li, S. Z., eds, 722–731, Berlin, Heidelberg. Springer Berlin Heidelberg.

[37] Feng, J., Jain, A. K., & Ross, A. Aug 2010. Detecting altered fingerprints. In *2010 20th International Conference on Pattern Recognition*, 1622–1625. doi:10.1109/ICPR.2010.401.

[38] Yao, B., Imani, F., & Yang, H. 2018. Markov decision process for image-guided additive manufacturing. *IEEE Robotics and Automation Letters*, 1–1. doi:10.1109/LRA.2018.2839973.

[39] Vanderburgh, J., Sterling, J. A., & Guelcher, S. A. Jan 2017. 3d printing of tissue engineered constructs for in vitro modeling of disease progression and drug screening. *Annals of Biomedical Engineering*, 45(1), 164–179. URL: https://doi.org/10.1007/s10439-016-1640-4, doi:10.1007/s10439-016-1640-4.

[40] Schutte, J., Yuan, X., Dirven, S., & Potgieter, J. Nov 2017. The opportunity of electrospinning as a form of additive manufacturing in biotechnology. In *2017 24th International Conference on Mechatronics and Machine Vision in Practice (M2VIP)*, 1–6. doi:10.1109/M2VIP.2017.8211511.

[41] Artec. Artec eva 3d scanner. https://www.artec3d.com/portable-3d-scanners/artec-eva.

[42] Stratasys. Stratasys rgd8520-dm. http://www.stratasys.com/-/media/files/material-spec-sheets/mss_pj_digitalmaterialsdatasheet_0617a.pdf.

[43] Stratasys. Stratasys tangoplus. https://www.stratasysdirect.com/wp-content/themes/stratasysdirect/files/material-datasheets/polyjet/PJ_TangoPlus_FLX980_FLX930_Material_Datasheet_201602.pdf.

[44] Bishop, C. A. *Transparent Conducting Coatings on Polymer Substrates for Touchscreens and Displays*, 975–988. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012. URL: https://doi.org/10.1007/978-3-540-79567-4_64, doi:10.1007/978-3-540-79567-4_64.

[45] Kovesi, P. Fingerprint enhancement. http://www.peterkovesi.com/matlabfns/#fingerprints.

[46] Li, G. *Innovative methods for large-scale fingerprint identification systems - Facilitating searching in a large-scale database*. PhD thesis, Norwegian University of Science and Technology, Trondheim, Norway, 2016. URL: http://hdl.handle.net/11250/2424904.

[47] neurotechnology. Tst biometrics bird 3. http://www.neurotechnology.com/fingerprint-scanner-tst-biometrics-bird-3.html.

[48] neurotechnology. Verifinger sdk. http://download.neurotechnology.com/VeriFinger_SDK_Brochure_2017-12-27.pdf.

[49] Morpho. Morhpo 300 series. https://www.morpho.com/sites/morpho/files/morphosmart_300_series_en-8_0.pdf.

[50] Documentation: Megamatcher 10.0, verifinger 10.0, verilook 10.0, verieye 10.0 and verispeak 10.0 sdk. http://download.neurotechnology.com/Neurotec_Biometric_SDK_Documentation.pdf.

[51] Roy, A., Memon, N., & Ross, A. Sept 2017. Masterprint: Exploring the vulnerability of partial fingerprint-based authentication systems. *IEEE Transactions on Information Forensics and Security*, 12(9), 2013–2025. doi:10.1109/TIFS.2017.2691658.

[52] Gao, M., Hu, X., Cao, B., & Li, D. June 2014. Fingerprint sensors in mobile devices. In *2014 9th IEEE Conference on Industrial Electronics and Applications*, 1437–1440. doi:10.1109/ICIEA.2014.6931394.

[53] Huawei inc. 2018. Huawei mate 9. https://consumer.huawei.com/en/phones/mate9/. Online; accessed 14.05.2018.

[54] waonews. 2018. Is fingerprint identification safe? touch key break free to unlock orange peel. [Online; accessed 18-May-2018]. URL: https://www.waonews.com/news/5910-Is_fingerprint_identification_safe_Touch_key_break_free_to_unlock_orange_peel.html.

[55] Conductive graphene pla filament 100g. http://graphenelab.com/blackmagic3d/Filaments/Conductive_Graphene_Filament_216x279.pdf.

[56] Conductive flexible tpu filament 1.75mm. https://filament2print.com/gb/graphene/785-filamento-conductivo-flexible-tpu-175mm.html.