Bypassing Fingerprint Scanners Using Artificial Fingerprints

by

Kerry C. Ford

In Partial Fulfillment of the Requirements for the Degree of

MASTER OF SCIENCE

in

The Department of Electrical and Computer Engineering

State University of New York

New Paltz, New York 12561

Spring 2021

Bypassing Fingerprint Scanners Using Artificial Fingerprints

Kerry C. Ford

State University of New York at New Paltz

We, the thesis committee for the above candidate for the
Master of Science degree, hereby recommend
acceptance of this thesis.

Casimer DeCusatis, Thesis Committee Member
School of Computer Science and Mathematics, Marist College

Michael Otis, Thesis Committee Member
Department of Electrical and Computer Engineering, SUNY New Paltz

Submitted in partial fulfillment
of the requirements for the Master of Science degree
in Electrical and Computer Engineering
at the State University of New York at New Paltz

ABSTRACT

Although fingerprint scanning technology is a convenient and user-friendly method of securing many modern devices, it is not without its flaws. In this paper, a methodology for creating artificial fingerprints is presented, as well as the experimental results, in order to display several low-cost techniques that can be used to bypass modern fingerprint sensors. Three methods are employed: direct collection, indirect collection (mold), and indirect collection (copy). First, using direct collection, a mold and cast of a physical fingerprint is created using very low-cost materials. Second, a fingerprint is indirectly collected from a surface and is used to create a 3D printed mold. Finally, a fingerprint is gathered using the indirect collection method, but is then inverted to achieve a higher resolution 3D printed copy of the original finger. Experimental results are presented, showing the effectiveness of the three fingerprint fabrication techniques on optical and capacitive sensors. Experimental results reveal that it is possible to bypass most sensors 80-100% of the time. The artificial fingerprints produced this way are reusable for many months. This was accomplished using widely available tools, and at a lower cost than that which has been previously reported in other research.

Table of Contents

1. INTRODUCTION

One method of modern biometric authentication is through the use of fingerprint scanners. This paper seeks to identify the current landscape of modern fingerprint scanners, and identify their vulnerabilities. Upon achieving this, several experiments are conducted in order to attempt to bypass these scanners through use of several low-cost methods. This paper addresses methods of bypassing the two most widely used types of scanners (optical and capacitive), and provides three approaches to fabricating fake fingerprints (direct collection, indirect mold, and indirect copy). The experiments begin by replicating recent results as a baseline, before then further investigating novel areas including different types of sensors, different security thresholds, and long-term effectiveness of the artificial fingerprints. Experimental results are discussed, and potential areas of further research are identified.

2. CURRENT STATE OF FINGERPRINT SCANNING TECHNOLOGY

The use of biometric authentication is one of the most convenient methods of securing modern electronic devices. Recent surveys suggest that 87% of consumers feel comfortable using biometric security on their personal devices [1]. There are many forms of biometric authentication, including facial recognition, retinal scans, and voice recognition, but one of the most common types is fingerprint scanning. According to Apple, nearly 90% of users with compatible iPhones secure their devices with fingerprint scanning [1]. It is commonly accepted in society that fingerprints are a unique and secure method of identifying a person, and that they cannot be lost or stolen (unlike passwords). Fingerprints have unique ridge/valley patterns which

are durable over the course of an individual's lifetime (with the exceptions of natural distortions due to aging, scars, dirt, etc.). This, coupled with the ease by which fingerprints can be scanned using modern technology, has resulted in the wide adoption of fingerprint identification for many applications beyond its original use in forensics.

2.1 FINGERPRINT AUTHENTICATION RISKS

In recent years, the market for fingerprint readers has expanded to over two million units annually [2, 3]. Many modern devices use fingerprint scanning technology to secure sensitive data. Some of these devices include: smart phones, laptops, tablets, USB devices, padlocks, door access mechanisms, amongst others. These devices are often used to secure financial, medical, and government records, and thus the security provided by the fingerprint scanner is of great importance. These automated readers are also widely used to identify individuals at border control points, airports, police stations, and even to prevent ticket fraud for amusement park admissions [4].

One detriment of fingerprint authentication is that unlike passwords, fingerprints cannot be changed. If a cybercriminal could reliably spoof a fingerprint scanner by replicating a target's fingerprint, then a persistent security gap would be created that could never be resolved. Fingerprint reader accuracy continues to improve as the technology develops, but likewise methods of spoofing fingerprints is also becoming significantly less expensive and more widely accessible. Therefore there is a necessity to continually quantify the viability of modern fingerprint scanners in order to attempt to mitigate the risks from potential threat vectors.

Baseline statistics on the performance of fingerprint readers first became widely available following a NIST report in 2012 [5]. There have also been attempts to evaluate fingerprint readers and sensors conducted by the FBI Integrated Automated Fingerprint ID System (IAFIS) [6]. Additionally, various approaches to spoofing fingerprint scanners have been attempted, with varying degrees of success [7]. Previous studies have identified that the same physical fingerprints captured by different types of readers can result in significant differences in recognition accuracy [8]. In part, this can be attributed to differences in the orientation, pressure, and condition of the physical fingerprint. This can become an issue with the use of large distributed systems, since there is a strong probability that the fingerprint reader used to enroll a user's physical fingerprint will not be the same as the reader used to later identify or verify the same individual. The only available solution to such a problem would be to increase the margin of error when identifying the fingerprint, but this would result in an even greater potential for risk of spoofing. Efforts have been made to address this issue by developing universal fingerprint targets [9].

2.2 EVOLUTION OF FINGERPRINT SPOOFING

Fingerprint identification has been commonly available ever since the emergence of the Apple iPhone 5 in 2013 (whose scanner was bypassed shortly after its release) [3]. Ever since, there have been continued attacks to defeat fingerprint scanners. Such attacks require a copy of a valid fingerprint and physical access to the target device. Although most device manufacturers are aware of such attacks, their response is often limited by the current state of the art in fingerprint readers as well as the desire to strike a balance between security and ease-of use. For example, a

reader which strongly resists false positives is likely to also reject a portion of legitimate authentication attempts, which can easily frustrate users and cause them to abandon the technology completely.

Originally, such attacks were limited to highly motivated and well-funded attackers, who possessed specialized knowledge and equipment. Therefore, these attacks were limited to a small number of high value targets. However, in recent years the attack landscape has shifted, and has made it feasible for less skilled attackers to perform fingerprint spoofing against a wider range of potential targets. In April 2020, Cisco Talos researchers demonstrated an average success rate of 80% when spoofing different types of fingerprint scanners across a dozen different devices, with a budget of only a few thousand dollars [10]. With the evolution and availability of 3D printing services, it is no longer necessary to incur the cost of purchasing a 3D printer and materials. This also eliminates the time and knowledge it would normally require to learn how to operate and maintain a 3D printer. The Talos report notes that a significant amount of effort and ability was still required to obtain a good enough copy of a valid fingerprint [10]. It is important to obtain high quality prints due to the fact that devices often limit their fingerprint scanners to five attempts or less before locking the device and requiring a separate PIN code or password. This is currently effective in mitigating potential spoofing attacks, and the average user will recognize the net benefit of using fingerprint-based security or multi-factor authentication which includes fingerprints. Over time, the level of effort required to successfully spoof fingerprint scanners is expected to decrease, even as public usage and confidence in biometric authentication increases.

2.3 MODERN FINGERPRINT SCANNERS AND SPOOFING REQUIREMENTS

As of 2021, the most common types of fingerprint sensors in use include capacitive, optical, and ultrasonic sensors [3, 5-8]. Each sensor captures an image of a physical fingerprint using different techniques. The captured prints are then identified through use of a pattern recognition algorithm which will verify the fingerprint accuracy against an authentication database. Fingerprints are discerned by their valleys and ridges. The ridge of a fingerprint is the area of elevated epidermis on the finger, whereas the valley is the space which separates the ridges [3]. These ridges and valleys are generally about 500 microns wide, and valleys are between 40 and 60 microns deep [3]. Ultrasonic sensors are the most recent technology to emerge for fingerprint scanning. These scanners emit an ultrasound pulse whose echoes from the ridges and valleys of a physical fingerprint allow the construction of a three-dimensional fingerprint image. These devices are currently the most expensive to produce, are slow to scan, and (according to [10]) are the least reliable type of fingerprint sensor. As such, they are still not in widespread use, being deployed mainly as on-screen sensors. Since the technology is still in its infancy and has yet to prove itself as a viable method of authentication for the average user, it will not be considered in this current research. The remainder of this paper will focus on capacitive and optical sensors.

2.3.1 CAPACITIVE SENSORS

Capacitive sensors are the most commonly used type of fingerprint scanner, and are considered to be the most accurate. They consist of an array of capacitors connected to a conductive plate. When a fingerprint ridge touches the plate, the capacitors become charged via the natural conduction of the human body, and the sensor treats the pattern of charged capacitors as the region containing the ridges, and the pattern of uncharged capacitors as the region containing the

valleys. This forms a pseudo-image of a full or partial fingerprint in three dimensions. While many capacitive sensors are passive, some types of active fingerprint sensors additionally pass a small electrical signal through the fingertip to enhance accuracy. In order to spoof a capacitive sensor, an artificial fingerprint would need to possess electrically conductive properties similar to a physical fingerprint.

2.3.2 OPTICAL SENSORS

Optical sensors illuminate a fingertip in contact with the sensor using a light emitting diode; an image sensor or camera captures the contrast between valleys and ridges. Spoofing an optical sensor requires a fake fingerprint which has reflective, refractive, and absorption properties similar to a physical fingerprint. Since optical sensors cannot discern depth, they can be bypassed with a good quality two-dimensional fingerprint image. Spoofing both capacitive and optical sensors also require a fake fingerprint which has mechanical properties within the proper range, both to ensure a good quality reproduction of the ridges and valleys and to avoid distortion when the fake fingerprint contacts the sensor. For example, if the fake fingerprint is too elastic, when it is compressed against the sensor the ridges will collapse and minute details will be lost. On the other hand, if the elasticity is too small, the fake fingerprint will not flatten around the sensor properly, resulting in only partial print images.

.

3. EXPERIMENTAL PROCEDURE

3.1 FINGERPRINT SENSOR SELECTION

Before attempting to fabricate artificial fingerprints using advanced techniques, the scanners used for testing needed to be identified.

3.1.1 CAPACITIVE SENSOR

The capacitive sensor of a Samsung Galaxy S9 smartphone was selected, as it was (at the time of testing) amongst the most modern and widely used smart devices available, and provided a good baseline for the modern standards of fingerprint scanning. The target fingerprint is stored within its local authentication database, and is used to verify the identity of the current user. Many users set their smartphones to use fingerprint authentication to access their bank information, stored passwords, credit card numbers, social media accounts, amongst many other forms of private information that is stored within their smartphone. Therefore, a modern smartphone was an ideal selection for experimentation.

3.1.2 OPTICAL SENSOR

The optical scanner used was a ZFM-20 Series fingerprint scanner in conjunction with a GUI provided by Adafruit [11]. This scanner was selected due to its popular nature, being used frequently in custom embedded system design by users all across the globe, and providing access to several different security settings. The scanner stores fingerprint data locally, and verifies the identity of any fingerprint stored within its memory. It possesses five different security levels, each with varying levels of False Acceptance Rates (FAR). Level 1 possesses the highest FAR,

and Level 5 possessed the lowest. For example, according to Adafruit, Level 3 has a FAR of less than 0.001% [11].

3.2 EARLY EXPERIMENTATION

In order to identify a baseline for understanding the means in which scanners identify fingerprints, the optical scanner was used in conjunction with the provided Adafruit GUI in order to determine the means by which the scanner identified fingerprints.

3.2.1 INITIALIZING THE OPTICAL SENSOR

The optical sensor needed to be initialized before starting. Unlike the smartphone selected, the ZFM-20 did not already have the researcher's fingerprint stored within its memory. Therefore, using the GUI, the researcher (henceforth identified as "the target") had their right thumbprint logged into the module's memory. The thumb was then scanned on all five security levels, and the module recognized the thumb as being valid across all attempts. Likewise, the ZFM-20 rejected attempts made when the target tried to authenticate using different fingers, since only the thumbprint was logged into the module's memory.

3.2.2 EARLY OPTICAL SENSOR SPOOFING ATTEMPT

The GUI also allowed for a visual representation of the scanned fingerprints to be obtained as a 256x288 pixel bit map. Using a 2D image of a target's fingerprint is a commonly known way to bypass optical sensors. As such, this same methodology was attempted by printing out a scaled-down version of the captured bit map on a standard piece of printer paper. Ultimately, these attempts failed, and were abandoned due to the fact that a 2D image would be insufficient

against capacitive sensors. Since the goal of the experiment was to bypass both scanner types, it was not worthwhile to pursue this method much further, though it is suspected that altering the image contrasts could have resulted in a successful spoof of the sensor. For reference, the image of the raw scanned fingerprint can be seen side-by-side with the attempted spoof in Figure 1 (note that all fingerprint images in this paper have been slightly distorted to preserve the privacy of our researchers). This shows that the scanner detected portions of the image's pattern, but could not properly identify the full pattern due to the light reflection which caused the image quality to be diminished. Likewise, it is apparent that the scale of the attempted spoof was inconsistent with that of the original fingerprint.

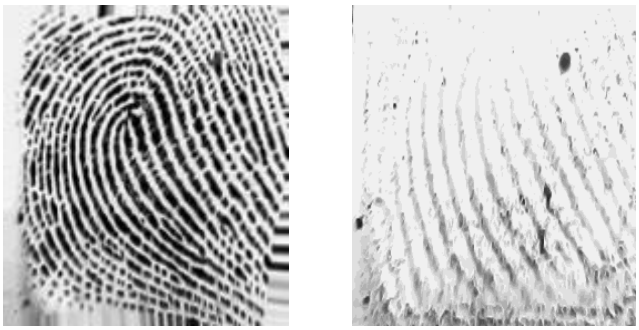

Figure 1 – the original scanned partial fingerprint (left) vs. the attempted 2D spoof (right)

3.2.3 DETERMINING FINGERPRINT COLLECTION METHODS

In order to produce an artificial fingerprint capable of bypassing a scanner, the original pattern of the target's physical fingerprint must be collected. Following the approach discussed in [10], two different methods of obtaining the initial fingerprint were identified: direct collection and indirect collection. Direct collection involves placing the target's fingertip in a molding material

to capture the fingerprint for later use. As noted in prior threat models [10], in this attack scenario, the target may be unconscious or incapacitated while the mold is taken. Indirect collection involves capturing a print from a surface via fingerprint powder. This attack scenario makes it much easier for the attacker to obtain a print, since fingerprint traces are left behind whenever a target touches a compatible surface, although the attacker cannot control the source or quality of the print collection as easily. Other indirect collection methods include acquiring prints using an ink stamp, or by photographing prints left on a reflective surface.

3.3 DIRECT COLLECTION

After initializing the optical scanner and identifying the methods of fingerprint collection, the experiment moved towards attempting to spoof optical and capacitive sensors using direct collection and casting techniques. This can be done with widely available, low cost materials; following the approach used in [10], fabric glue was selected as a casting material. This allows the results obtained to be properly measured against previously reported results.

In order to create the molds, a small amount of hot glue was poured onto a piece of aluminum foil. Once it cooled to the point where it would not hurt to touch, the target's finger was placed into the hot glue, and remained there for several seconds while the hot glue finished cooling. Once cooled, the finger was then removed, leaving behind a mold of the target's fingerprint. The hot glue material is capable of providing a suitably high-resolution image of the captured fingerprint. Other materials like the sculptor's clay (as used in [10]) are more prone to smudging, especially when the finger is removed from the material, and thus has greater potential for altering the integrity of the molded fingerprint. Hot glue, on the other hand,

resulted in a quick and reusable mold that maintained a high resolution of the base fingerprint.

After cooling, the hot glue mold was then filled with fabric glue, which can be poured and dried in a thin layer before being peeled out of the mold. Care must be taken to remove the fabric glue cast slowly so as to avoid stretching and distorting the resulting artificial fingerprint. The detriment of using hot glue in conjunction with a cast of fabric glue is the need for temperature control. During experimentation it was discovered that the two types of glue would bond to one another if kept in a hot or humid environment, thus making it impossible to remove the fabric glue cast without ruining the integrity of the cast. As such, the experiment was conducted in a controlled environment, maintained at 70°F, in order to prevent the casts from bonding to the mold.

Casts made with fabric glue are thin enough to propagate the conductivity of a person's finger placed behind the cast while scanning. This small residual level of conductivity allows the artificial fingerprint to bypass capacitive scanners. While other materials such as silicone are capable of producing accurate casts, they are nonconductive, and therefore would prove useless against capacitive scanners. As such, fabric glue proved to be one of the most efficient low-cost casting materials available. An image of the hot glue mold and resulting cast can be seen in Figure 2. As can be seen, another detriment of using the fabric glue as a casting material is the presence of air bubbles which lessens the resolution of the cast. However, in testing, these imperfections proved to be insignificant.

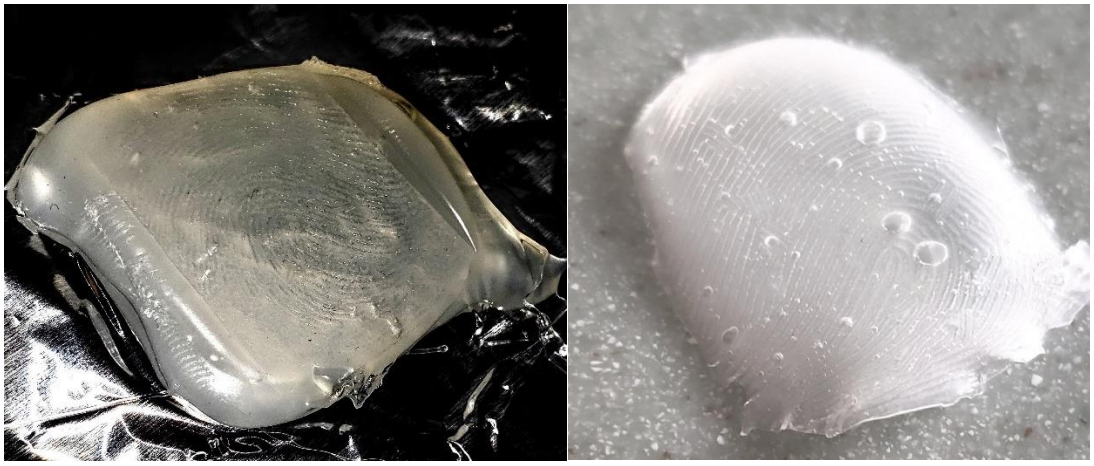

Figure 2 – Direct Collection Mold/Cast – the hot glue mold (left) and the resulting fabric glue cast (right)

3.4 INDIRECT COLLECTION

Next, two different types of indirect collection were attempted – namely fingerprint dusting and stamping. Dusting with fingerprint powder (such as graphene) provided a more authentic capture of the fingerprint, but stamping provided a cleaner and more usable pattern. Figure 3 shows the resulting captured prints using both methods.

Figure 3 – Indirect Collection – fingerprint dusted image (left) and fingerprint stamped (right)

3.4.1 INDIRECT MOLD

After obtaining these prints, the next step was to develop a 3D model that could be used as a base mold. Two different methodologies were employed to develop a 3D model: manual modeling and automatic modeling.

3.4.1.1 MANUAL MODELING METHOD

Manual modeling required importing a scanned image of the obtained fingerprint into 3D modeling software (Autodesk Fusion 360), outlining the valleys of the fingerprint, and then extruding them by 50 microns so as to generate an artificial mold of the fingerprint. The model for this original design can be seen in Figure 4.

Figure 4 – The manually modeled fingerprint mold

After completing the model design, the 3D printer being used needed to be optimized in order to achieve maximum quality. The most readily available printer was a Tevo Tornado, which is a Fused Deposition Modeling (FDM) printer, and has a z-axis resolution of 40 microns, and variable x-axis and y-axis resolutions (based upon available nozzle sizes). The selected nozzle

was 0.2mm in diameter, and the 3D printer settings were optimized for this particular detail-oriented design.

After calibrating the printer, the model was imported into the Cura slicing software [12], which generates the G-Code that ultimately controls the movement of the 3D printer. When slicing the model, it was identified that the 3D printer would be unable to print all desired ridges (as some were smaller than 0.2mm thick - which is the smallest size the nozzle selected can handle). The attempted slicing at the standard scaling can be seen in Figure 5. Notice that many of the ridges towards the bottom of the model are not present in this 3D rendering.

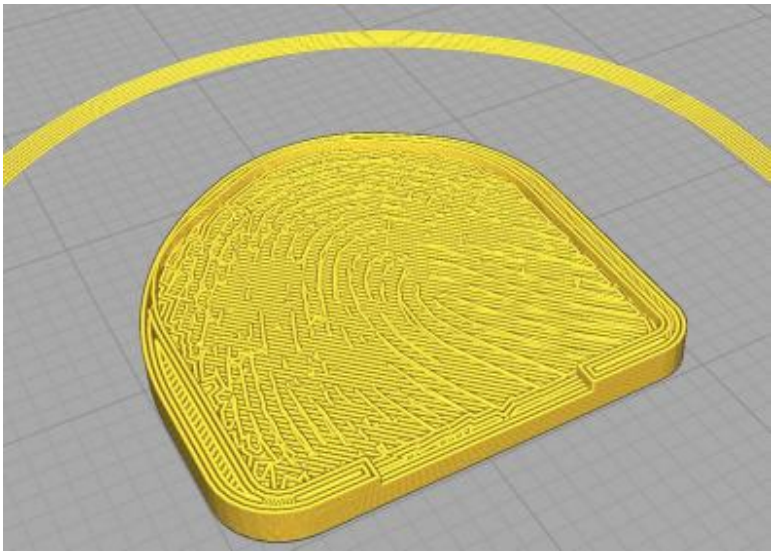

Figure 5 – The fingerprint model after being sliced in Cura using standard settings at 100% scaling (50 micron ridge spacing)

To compensate for this, the x-axis and y-axis of the design was gradually scaled up until the majority of ridges became visible. It is important to note that the z-axis did not need to be scaled, as the 60 micron depth of the mold fell within the printer's capabilities. The x-axis and y-axis were both scaled by 160%, thus resulting in a much larger mold than anticipated. However, the main priority of this initial mold was to test the quality of the model (regardless of scale), as well as the potential results of a cast made out of such a mold. The slice model can be seen in Figure 6.

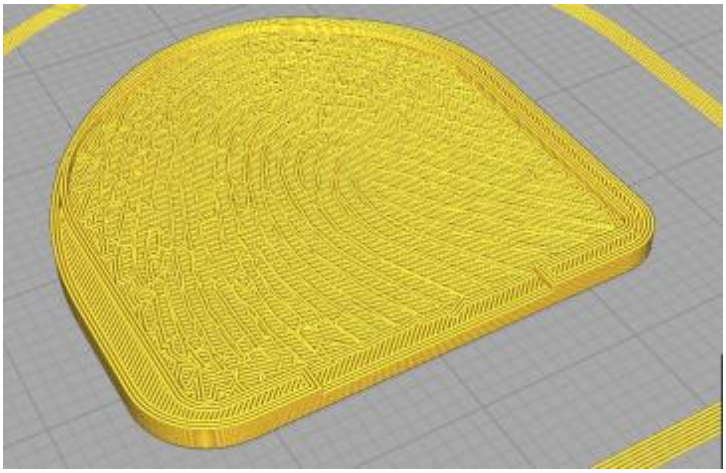

Figure 6 – The fingerprint model after being sliced in Cura after scaling the x-axis and y-axis to 160% (80 micron ridge spacing)

This scaled up model was then printed on the Tevo Tornado using PLA for the material, and took nearly four hours to complete. After printing, it was observed that there were some minor imperfections, particularly one notable ooze in the top-right corner of the print, some over-extrusion towards the bottom, and a slight amount of over-extrusion around the edges. However, the part of the mold which possessed the fingerprint itself was of acceptable quality, and can be

seen in Figure 7. Note that in the ridges, 45 degree angle lines can be seen - this is a result of the FDM printer, and is a standard occurrence in all FDM PLA prints. Even though this is unwanted, it is largely unavoidable using this printing method.

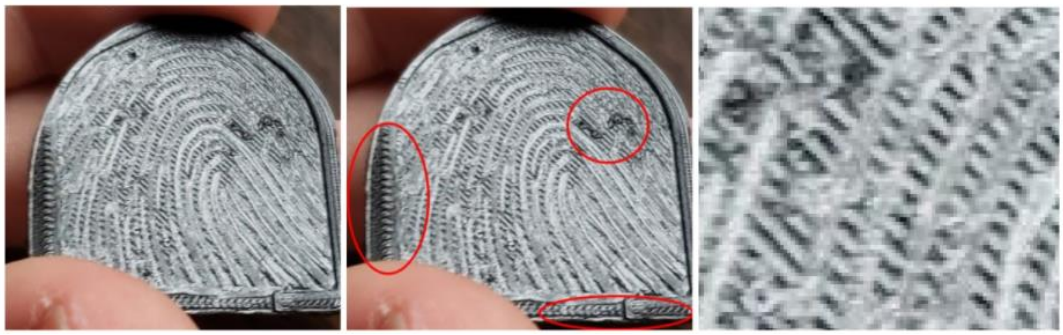

Figure 7 – The 160% scaled 3D printed fingerprint mold (left), imperfections encircled in red (middle), and top-layer ridge-lines amplified (right)

The mold was then filled with fabric glue and was allowed to dry for 24 hours. Compared to the direct collection molds (which were fabric glue on hot glue), this cast was removed from the mold with extreme ease. The quality of the cast was of high quality as well, even considering the imperfections identified above. This cast can be seen in Figure 8.

Figure 8 – The fabric glue cast of the fingerprint (as taken from the 3D printed mold)

This cast was then used on both the optical scanner (programmed via Arduino) as well as the capacitive sensor (native to a Samsung Galaxy S9). On both scanners, the cast failed to be recognized as the right thumb, however it is important to note that on both sensors the cast was still recognized as a fingerprint in general (albeit an invalid one). This is likely due to two things: the 60% increase in scale, and the 45 degree lines left behind by the printer. For reference, a few of the optical scanner results from this cast are displayed below in Figure 9, and can be compared to the original fingerprint used.

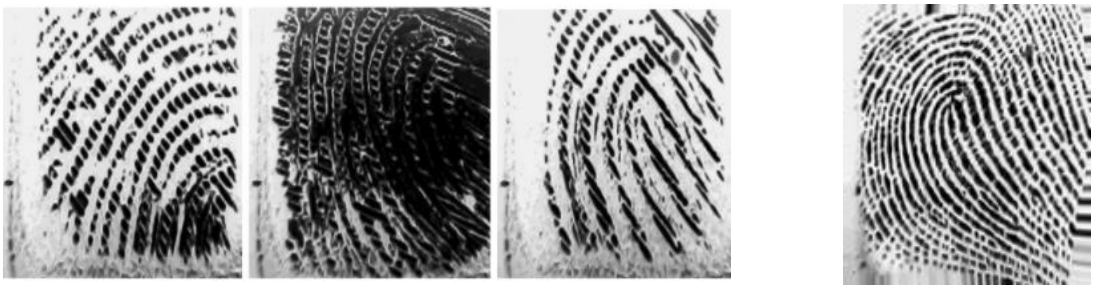

Figure 9 – The optical scanner results of the cast (pressed against the scanner at moderate, strong, and light pressure levels, respectively) vs. the original fingerprint (on the far-right)

Figure 9 further confirms the scale of the fingerprint mold relative to the original, showing that the mold is much larger than the original scale. The ridges are much thicker, and the ridge-to-ridge distance is much increased when compared to the original fingerprint. Due to these issues, an alternative 3D printing method was pursued. An online 3D printing service [13] was selected in order to have the models produced using high-resolution stereolithography (SLA) printing. These services typically offer about 20-30 microns resolution, which allows us to achieve the necessary precision required to mimic the minimal depth and ridge-to-ridge distance of a

properly sized fingerprint. The model was slightly adjusted and then printed (without needing to be scaled up) using this 3D printing service. The resulting mold can be seen in Figure 10.

Figure 10 – The manually constructed mold printed on an SLA printer with 100% scaling (50 micron ridge spacing)

3.4.1.2 AUTOMATIC MODELING METHOD

Ultimately, the manual modeling method, although functional, proved to be time-consuming and inaccurate due to human errors when manually outlining the model. For these reasons, the automatic modeling approach was preferred. Using the online service Selva3D [14], a black and white fingerprint image was uploaded and converted into a 3D model, with variable extrusion percentages. After uploading the fingerprint images onto this service and generating a model, that model could then be imported into the 3D printer slicer software Cura [12], where it could be manually resized to meet the required dimensions of the original fingerprint. This method gives less direct control over the features of the resulting model, but does provide a quick and accurate means of generating the desired mold. The resizing helps compensate for errors in the

mold sizing; as reported previously [10], if the size of the mold varies by more than half a millimeter from what the reader is expecting, the mold will not work (as noted with the 160% scaled FDM mold). Since there is no direct mapping from the size of a real-world object to a digitized object, scaling the 3D models is required in order to obtain a useful mold.

For comparison, the results of the manual and automatic molds, after being 3D printed on an SLA printer, can be seen in Figure 11. The molds were then filled with fabric glue in order to produce the type of artificial fingerprints discussed earlier.

Figure 11 – Indirect Collection Mold – the manually constructed model (left) and the automatic Selva3D model (right), both with 50 micron ridge spacing

3.4.2 INDIRECT COPY

The resolution of the 3D models produced by indirect collection (i.e. the indirect mold fingerprints) were significantly lower than the direct collection results. To address this, instead of extruding the valleys of the fingerprint in the 3D model (which are very fine features) to create an artificial mold, the indirectly collected fingerprint image was inverted and the ridges were extruded instead (which are thicker, and require less precision). Selva3D was used once again in this process, which resulted in a much higher precision SLA print, as shown in Figure 12. This result shall be referred to as the indirect copy method, since the resulting 3D print is virtually a replica of the original fingerprint (this is in contrast to a mold, which produces an imprint of the original fingerprint).

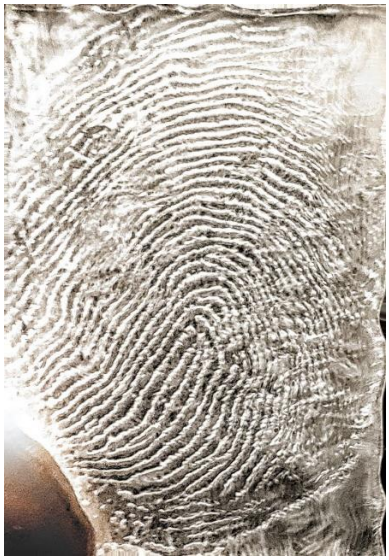

Figure 12 – Indirect Collection Copy – result of using Selva3D to create a direct copy of the original fingerprint based on the indirectly collected base (with 50 micron ridge spacing)

The same approach was used with this artificial fingerprint copy as was done with the indirect collection method, in order to maintain consistent results. The 3D model print was pressed into hot glue in order to form a mold of the artificial print, and the mold was then filled with fabric glue. Thus, the procedure for direct and indirect collection is similar, but indirect collection requires additional steps. Further, the indirect collection method was applied in two different ways, namely the indirect mold and indirect copy.

3.5 EXPERIMENTAL COSTS

The cost to produce a direct mold fingerprint was under $50 for all prints produced, and many more direct mold fingerprints could have easily been produced with this amount of material. The cost for indirect methods using 3D printing was limited by the cost of the 3D printing service ($50 per print). The experiment conducted by Talos, which involved purchasing a 3D printer and resin materials, cost them approximately $2,000 [10]. The net costs for all experimentation described in this research paper resulted in a cost of approximately $590, which is significantly less than that required by the researchers at Talos [10].

4. EXPERIMENTAL RESULTS

In order to test the quality of the artificial fingerprints created in the direct mold, indirect mold, and indirect copy methods previously discussed, each artificial fingerprint was tested on both an optical scanner (the ZFM-20) and a capacitive scanner (the Samsung Galaxy S9). For reference, the FAR value for Level 3 of the optical scanner (0.001%) also seems to be typical for many commonly available smart phones [15]. The testing was conducted by first using the scanners to

capture and record the target's fingerprint. Next, each type of artificial fingerprint was tested on the two scanners.

4.1 OPTICAL SENSOR RESULTS

First, the optical scanner was tested. Figure 13 shows an example of the direct collection fingerprint spoofing the ZFM-20 on its highest security setting (Level 5).

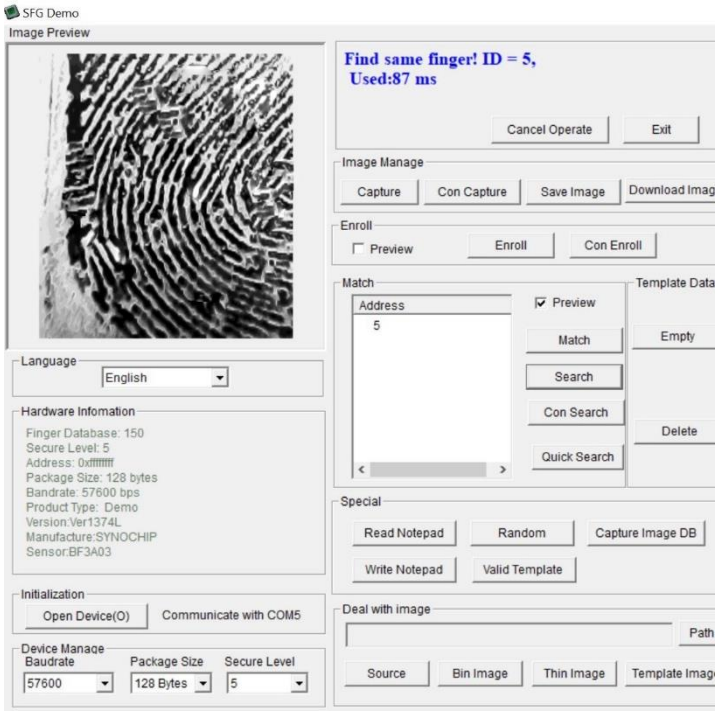

Figure 13 – Example of an artificial fingerprint spoofing Level 5 of the optical scanner within the provided Adafruit GUI

The success rates of the tests done on the optical scanner can be seen in Figure 14, in the form of a running-average, taken across a one-week span of 100 trials. These tests were all run at a security setting of Level 3, so as to maintain consistency across a known FAR value.

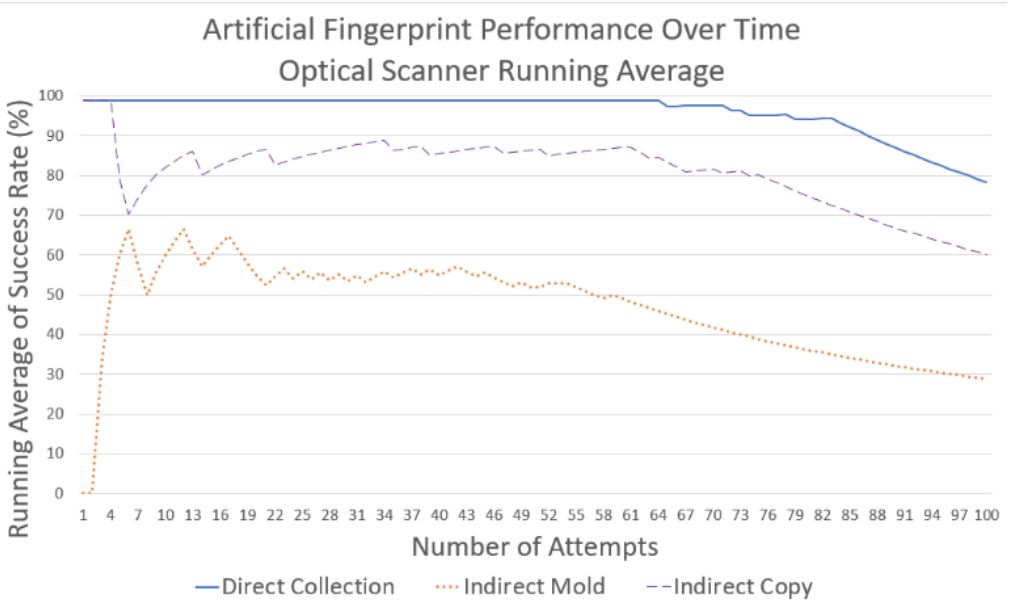

Figure 14 – Running Average of each of the three tested artificial fingerprints across 100 trials

It can be observed that the directly collected mold successfully fooled the scanner every time for the first 64 attempts, across various orientations and pressures. After this point, enough time had elapsed that the fabric glue material was beginning to dry out and harden. This resulted in worse optical results since the artificial print could not be properly pressed against the glass plate of the scanner. This trend proved true for all three of the artificial fingerprint types being used. Still, after 100 trials and one week after fabrication, the directly collected mold successfully bypassed the optical scanner close to 80% of the time, on average. This benchmark test is consistent with previously reported results [10]. The indirectly collected mold was more dependent on ideal positioning and an appropriate amount of pressure during testing. The scanner was successfully

bypassed 65-70% of the time, on average, for the first 10 attempts. As the material began to harden, this fell to around 40% for up to 70 trials, eventually dropping to around 30% for the final rounds of testing. Finally, the indirect copy performed significantly better than the molded version, probably due to the increased resolution achieved with this approach. Early trials successfully bypassed the scanner 90-100% of the time, on average, and for up to 70 trials this remained greater than 80%. For later trials, it remained able to successfully bypass the scanner 50-60% of the time. The optical scanner performance at different security levels was also investigated. Both the direct collection and indirect copy were able to bypass all five security levels, with performance similar to that reported in Figure 13. By contrast, the indirect mold was only able to bypass security levels 1-3. Even with the reduced performance of the indirect mold, it is still suggestive that each of the three methods are capable of bypassing the FAR set by most modern consumer products (which is typically set at 0.001%, the same FAR percentage as can be found on Level 3 of the ZFM-20).

4.2 CAPACITIVE SENSOR RESULTS

The same tests described above were conducted using the capacitive scanner from a Samsung Galaxy S9 smart phone (note that this model of smartphone was not previously tested by previous researchers [10]). Like most smart phone manufacturers, Samsung does not develop their own fingerprint sensors; they integrate components from third-party vendors such as Synaptics. The direct collection artificial fingerprint bypassed this scanner 100% of the time. This is an improvement on prior research, which demonstrated 80-90% success rates on capacitive sensors used in Samsung and Hitachi devices, although the result is not unprecedented; prior efforts with direct collection methods were able to achieve close to 100%

success rates on capacitive sensors used by Samsung Note 9 and Honor 7A smart phones [10]. Prior research did not consider long-term usability of fake fingerprints, therefore the experiment outlined in this paper also investigated the usefulness of these prints even after the fabric glue began to dry and harden. It was discovered in this research that even 8 months after casting, when the materials had fully dried and their mechanical properties had stabilized, the directly collected artificial fingerprint still bypassed the Samsung Galaxy S9's scanner 100% of the time (although slightly more pressure needed to be applied in order to get the dried fabric glue to form about the capacitive plate). There are two theories for why this was able to occur. First, the capacitive plate is much smaller than the optical plate, thus requiring less of the fingerprint pattern for authentication. Second, the capacitive nature of the scanner means that it will not capture a fingerprint until enough pressure is applied; therefore, the scanner would either trigger and accept the artificial print, or fail to trigger due to inadequate pressure. Therefore, this resulted in a continued 100% success rate even after the artificial fingerprint had fully hardened.

The same positive results cannot be attributed for the two indirectly collected artificial fingerprints. In the case of both the indirectly collected mold and the indirectly collected copy, neither fingerprint was capable of bypassing the capacitive scanner under any conditions. It is suspected that the failure of the indirectly collected fingerprints is largely due to a difference in the level of extrusion. Recall that an optical scanner can be spoofed with a 2D image, while a capacitive scanner requires a 3D image. Since the optical scanner could be bypassed using both types of indirectly collected artificial fingerprints, this implies that depth variations were responsible for the capacitive scanner failures. Depth plays more of a role in capacitive scanning since the distance between the valley and the conductive plate dictates the level of capacitance

recorded by the sensor. Three additional molds with various extrusion depths were developed in an attempt to counteract this negative impact, but all failed to spoof the capacitive scanner. This is consistent with results from [10], which required over 50 fabrication attempts on indirectly collected prints before producing an artificial fingerprint that worked consistently with capacitive scanners. This difficulty was attributed to the ultraviolet curing process required after SLA printing, which results in minor contraction of the produced molds and creates invalid ridge depths.

5. FUTURE RESEARCH

There are several different ways in which this research can be continued. The most directly-related experimentation would be regarding the means by which indirectly collected molds can be properly scaled so that the negative effects of ultraviolet curing can be countered. One consideration may be to identify a 3D printing material which can maintain fine resolutions without the negative impact of post-molding contraction. Another consideration would be to identify the rate at which the material contracts, and enhance the scale of the initial model in order to preemptively compensate for the contraction in the curing process. Additionally, testing could be performed on ultrasonic sensors, as they become more widely available.

Another area for research would be through the use of artificial intelligence to create generic fingerprint images which could be indirectly printed and cast. Some research exists that suggests that, despite all fingerprints being unique, many fingerprints have some common features [16]. This same research claims to have identified an algorithm to develop generic segments of

fingerprints which are capable of spoofing many forms of fingerprint pattern recognition. Since most modern fingerprint scanners only scan a small portion of the target's fingerprint, it could be possible to combine the research of [16] with the 3D molding process of this paper in order to develop a generic artificial fingerprint capable of bypassing the biometric security of an array of different targets instead of just being limited to one single target. Likewise, it would eliminate the need to indirectly collect the target's fingerprint, thus increasing the ease by which their device security could be bypassed.

6. CONCLUSION

Fingerprint scanning technology is a popular and convenient way of adding an extra layer of security to modern electronic devices. Despite the uniqueness of every person's fingerprints, it has been demonstrated that both optical and capacitive fingerprint scanners are vulnerable to artificially created fingerprints. Fake fingerprints were generated using direct collection, indirect collection (mold), and indirect collection (copy) techniques. Experimental results from prior work were successfully replicated in this research, noting that these fake prints were produced quickly, using publicly available tools (including 3D modeling, slicing, and printing services), and at a cost point significantly lower than previously reported. Directly collected molds were able to bypass optical scanners 100% of the time for the first 64 attempts, after which they declined to around 80% effectiveness. Directly collected molds were also able to bypass all five optical scanner security levels, and bypassed a capacitive scanner 100% of the time, even 8 months after casting. Indirect molds bypassed an optical scanner 65-70% of the time for a small number of trials, eventually declining to 35-40% effectiveness. Indirect molds were only able to

bypass security levels 1-3 on a five-level optical scanner, and were unable to bypass a capacitive scanner. Indirect copy fingerprints were also unable to bypass a capacitive scanner, but did successfully bypass optical scanners 90-100% of the time for a small number of trials and over 80% for later trials; they also bypassed all five optical scanner security levels. As the declining cost and complexity of fingerprint spoofing (under $50 per print using 3D printing services) makes these attacks more accessible to a wider range of threat actors, ongoing research is required to continuously quantify fingerprint reader threats. Future research directions include investigating more advanced 3D printing techniques, testing on new types of ultrasonic sensors, and evaluating new methods of indirectly producing fake prints employing artificial intelligence systems.

7. REFERENCES

[1] H. Kelly, “Fingerprints and face scans are the future of smartphones. These holdouts refuse to use them.”,
The Washington Post, November 13, 2019
https://www.washingtonpost.com/technology/2019/11/15/fingerprints-face-scans-are-future-smartphones-these-holdouts-refuse-use-them/ (last accessed December 20, 2020)

[2] Acuity market intelligence report, “Biometrics market evolution: towards identifiable anonymity”, 2019 https://www.acuitymi.com/whitepapers (last accessed December 10, 2020)

[3] D. Maltoni, D. Maio A.K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer, NY (2009)

[4] K. Harmel and L. Spadanula, “Disney World scans fingerprint details of park visitors”, Boston Globe, September 3, 2006
http://archive.boston.com/news/nation/articles/2006/09/03/disney_world_scans_details_of_park_visitors/ (last accessed December 10, 2020)

[5] “NIST fingerprint testing and standards”, https://www.nist.gov/programs-projects/fingerprint (created January 2012, last accessed December 10, 2020)

[6] “Privacy impact assessment integrated automated fingerprint identification system (IAFIS)”, https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/iafis-ngi-biometric-interoperability (created January 2012, last accessed December 10, 2020)

[7] J. Englesma, S. S. Arora, A.K. Jain, and N.G. Palter Jr., “Universal wearable 3D fingerprint targets: advancing fingerprint reader evaluations”, May 2017, https://arxiv.org/abs/1705.07972 (last accessed December 10, 2020)

[8] K.K. Sadasivuni, M.T. Houkan, S. Mohammad, and J-J Cabibihan, *"Anti-spoofing device for biometric fingerprint scanners"*. 2017 IEEE International Conference on Mechatronics and Automation (ICMA). (Aug.2017). IEEE. *doi*:*10.1109/icma.2017.8015898*. *ISBN* *978-1-5090-6758-9*.

[9] S.S. Arora, K. Cao, A.K. Jain, and N.G. Paulter Jr., “Design and fabrication of 3D fingerprint targets”, IEEE Trans. On Information Forensics and Security vol 11, pp. 2284-2297 (October 2016)

[10] P. Rascagneres and V. Ventura, “Fingerprint cloning: myth or reality?” Cisco Talos technical report, April 8, 2020 https://blog.talosintelligence.com/2020/04/fingerprint-research.html?m=1 (last accessed December 5, 2020)

[11] https://www.adafruit.com (last accessed December 10, 2020)

[12] https://ultimaker.com/software/ultimaker-cura (last accessed December 10, 2020)

[13] https://www.xometry.com (last accessed December 20, 2020)

[14] http://Selva3D.com (last accessed December 10, 2020)

[15] "Biometric Technologies", https://www.fingerprints.com/uploads/2019/10/fpc_white_paper_digital.pdf [White Paper] (created October 2019, last accessed May 2, 2021)

[16] J. Vanian, "Artificial Intelligence Is Giving Rise to Fake Fingerprints. Here's Why You Should Be Worried", November 2018, https://fortune.com/2018/11/28/artificial-intelligence-fingerprints-security/#:~:text=Julian%20Togelius%2C%20one%20of%20the,by%20storm%20for%20the%20last (last accessed April 18, 2021)