Bulletin of Environment, Pharmacology and Life Sciences
Bull. Env. Pharmacol. Life Sci., Spl Issue [5] 2022 :28-35
©2022 Academy for Environment and Life Sciences, India
Online ISSN 2277-1808
Journal's URL:http://www.bepls.com
CODEN: BEPLAD

ORIGINAL ARTICLE **OPEN ACCESS**

3D Fingerprint Forgery and Biometric Security Threats: A Conceptual Study

Abdulrahman Mohammed Obaid Almheiri[1], Shanaihi Sanjay Patel[2], Bhoopesh Kumar Sharma[3]

[1]Lieutenant and Assistant Expert, General Department of Forensic Sciences and Criminology, Dubai Police General Head Quarters, Dubai, United Arab Emirates.
[2]Research Assistant, Houston Forensic Science Center, Houston, Texas (USA)
[3]Professor, Department of Forensic Science, Shree Guru Gobind Singh Tricentenary University, Gurugram (India)
[1]A.alsallaqi@hotmail.com, [2]bhoopesh_fosc@sgtuniversity.org,

ABSTRACT

Fingerprints are used for a variety of identity verification applications, including ID cards, access control, clocking in for attendance, at airports for immigration and security, banks for verification, to unlock phones and laptops, and many other applications as the use of biometric systems in daily work increases. Some of these applications include ID cards, access control, clocking in for attendance, etc. One of the forms of biometric identification that is utilised most frequently is the individual's fingerprint. The widespread use of fingerprints provides counterfeiters with a strong incentive to likewise fake biometric fingerprints. Dactyloscopy is significantly impacted by forgeries, despite the fact that it occurs less frequently under these conditions. In addition, the development of technologies such as 3D printing could potentially pose a threat to the safety of fingerprint biometric systems. This study's primary objective was to investigate the process of fingerprint counterfeiting by employing 3D-printed molds in conjunction with gelatin and glycerin casts of dummy fingers.The Automated Fingerprint Identification System was surprisingly able to correctly identify the fingerprints that were taken from these castings (AFIS). In addition to this, the fake finger created out of gelatin and glycerin has the ability to unlock phones and gain access to restricted areas. As a consequence of this, the conclusions of this study highlight the seriousness of the problem and its influence on the biometric security business. In addition, they offer suggestions regarding how law enforcement authorities might address issues of this nature. In order to differentiate between human skin (human finger) and other materials, the authors suggested that sensors may be made more sensitive by monitoring the heartbeat or body temperature (dummy finger).

Keywords: Fingerprints, Biometric systems, Fingerprints forgery, 3D printing, security, dummy finger, AFIS, sensitive sensors.

Received 22.10.2022 Revised 23.11.2022 Accepted 20.12.2022

INTRODUCTION

Since 300 B.C., friction ridge skin imprints have been used as proof of identity in China, Japan, the United States, and Dubai (United Arab Emirates) [1,2]. Since then, there have been breakthroughs in the many applications of fingerprint technologies.The creation of fingerprints as a method of individualization and an useful forensic and investigational tool was the result of a number of separate investigations, experiments, and research projects. Researchers have shown that fingerprints retain their unique characteristics over time. Over the course of time, people will keep studying whatever branch of science is being discussed, and that branch of research will keep developing and being more understood. [1, 3].The science of fingerprints has been used to identify criminals and solve crimes for more than a century, and it continues to be an extremely valuable tool for both the field of forensic science and law enforcement today. In addition to this, it assists the law enforcement in "tracking the criminal's past, previous arrests, and convictions to assist in sentencing, probation, parole, and pardoning decisions" [3, 4].In addition to their use in criminal identification, fingerprints have also been put to use in the identification of the deceased, in legal documents, in the conduct of background checks including applications for employment, defense security clearance, concealed weapon permits, in the provision of biometric security such as for accessing secured areas or systems, at airports for immigrations or banks for authentication, and as a form of password to unlock phones. In other words, fingerprints have been put to use in a wide variety of contexts.

The widespread use of fingerprints in biometrics makes it possible for impostors and fraudsters to forge fingerprints and frame someone or overcome security systems, as well as forgers to create fake biometric fingerprints [5].When an innocent person's latent fingerprints are planted at a crime scene, this is called forgery [6]. Forgery occurs when a fingerprint already exists on the surface but was deposited by someone else. The earliest known instance of a forged fingerprint was discovered in the 1920s [5,6].There are a number of methods for fingerprint forgery that have been described in the literature. These include making a cast of the fingerprint using a mould, transferring the fingerprint from one surface to another using wax paper or saran wrap-like materials, and etching the fingerprints onto metal plates so that the latent prints and the known prints are identical [7,8].

In a world where identity theft is rampant, fingerprint-based biometric security solutions are becoming vital for keeping people safe and granting them access to restricted places. Finger and fingerprint forgeries can be either cooperative or non-cooperative.The cooperative method creates a phoney fingerprint by having the subject put their finger into a Play-Doh-like material. Fingerprint forms are then transferred onto materials like gelatin or silicone, which have the ability to mimic the distinctive characteristics of real fingerprints [9].Dummy fingers that can trick biometric security systems can be made by casting real fingers in silicone and gelatin. The term "spoofing" describes this type of attack [9,10]. Casts of the fingers can also be made using 3D printing. Three-dimensional printing (3D printing) is the process of making physical objects from digital models using a printer that extrudes plastic filament. Designing something in 3D is as easy as sending a file to a 3D printer, and then you can have it printed out with 3D effects [10,11].As a result, the 3D printed finger that results from sending the scanned fingerprint file to a 3D printer can be used to make fake fingers, or if its texture is comparable to human skin, it can be used as a dummy finger to implant fingerprints.

The major goal of this research was to see if and how 3D-printed fingerprints will do in an AFIS search. The second goal was to learn how phoney fingerprints affect the security system and what kind of danger they pose to the security sector and 3D scanners.

MATERIAL AND METHODS

A. Substrate

Ceramic tiles were utilised as a non-porous surface and white paper was used as a porous surface to put down fingerprints in order to investigate the effects of counterfeiting.

B. Matrix

Oil and sebum from the face are used as a matrix to transfer fingerprints to paper. In addition, fingerprints were transferred to paper using blood and then developed with Amido black. The blood sample was collected with the help of the Dubai Police Clinic. The matrix for the false finger was already there, made of gelatin and glycerin.

C. Glassware and requirements

Using a blower and brush, latex was applied on the 3D-printed Fingerprint. The dummy finger's ingredients were mixed with a spatula in a microwave-safe basin. The "Professional shine-vanishing PRO powder" was employed to give the dummy finger the appearance of human skin.Baby talcum powder from Johnson & Johnson was used to keep the mold from breaking. The dummy finger was hung to dry using paper clamp clips (binder clips) after the solution was poured into the latex mold. A hair dryer was used to speed up the drying process for the latex.

D. Other ingredients and Techniques

Using the AFIS, a fingerprint was chosen from a fingerprint card containing ten fingerprints (AFIS). After deciding on a fingerprint, a 3D print was made. A fake finger was made out of the 3D-printed one.The molds were made using SIRCHIE's All-purpose evidence recovery kit (Accutrans), and the cast was made from the same substance. To transfer the prints to different materials, this mold was used.

A fake finger was created with MONSTER LIQUID LATEX (general purpose), FEVICOL MR (general purpose),Glycerin USP, BELL'S GLYCERIN B.P, and DAVIS GELATINE (Clear and Unflavored).

These counterfeit prints were made using "HI-FI" Latent print powder, Heavy Black (volcano), and "Lightning lifts" were used to take the prints off of ceramic tiles.On white paper, a "NinhydrinHT HFE-7100" pump spray was used to generate forgeries. The fake blood prints were made with Amido black. SIRCHIE manufactures all of these chemical supplies.

E. Preparation of Cast

Initially, Accutrans was spread over an area roughly the size of a person's first finger joint on a flat surface.The finger was then lifted after being put on the spread. Around thirty minutes were allowed for the preparation to dry. The mold was set up using this method. We reapply Accutrans and let it cure for another 20 minutes before using this mold again.This was done to prevent the print from being accidentally flipped. Once it had dried, the cast was removed from the styrofoam. For making fingerprint impressions on paper from bodily fluids including oil, sebum, and blood, this was the mold to use.

F. Fingerprint 3D printing from a scanned image

We started by obtaining a high-quality fingerprint card with ten fingerprints from the Dubai Police AFIS (AFIS).We picked one fingerprint from the card that was downloaded, and we scanned it very precisely. The fingerprint scan was sent to 3D SYSTEMS, who then created a 3D print of it.Since the 3D-printed fingerprint did not look like real skin, it was used as a pattern to create a prosthetic one.

G. Preparation of Dummy finger

After the 3D-printed fingerprint had been dusted with baby powder, latex was poured into the mold and allowed to dry for around 15 minutes. As the latex layers are removed from the mold, the baby powder helps keep them from cracking. With the use of a hair dryer, we were able to speed up the drying process. Three more applications of latex were made after the first set.The latex was consistent during all three uses, resulting in similar thickness. Baby powder was applied to the dried latex layers again before they were separated from the 3D finger, thus reusing the latex as a mold. The fingerprint must be inverted before being compared to a 3D-printed copy. A steady gelatin-to-glycerin ratio was maintained. One tablespoon of gelatin, one tablespoon of glycerin, and two tablespoons of water were mixed together with a spatula in a microwave-safe basin and heated for 15 seconds. This process is carried out to soften the gelatin.It was necessary to heat the mixture until the crystals disintegrated. Having melted the crystals, the Professional shine-vanishing PRO powder was added to give the combination its skin-toned appearance. The contents of the bowl were then microwaved for 10 seconds to facilitate homogeneity. The liquid was poured into the latex mould once it was properly mixed, and it was left to dry for around three hours in the air using paper clamp clips. In these cases, the longer something is let to dry, the better it will be. A latex mould was used to cast the liquid, and it was taken out once it had dried. This dried substance, shaped like a finger, is the dummy finger used to make the impressions. Consequently, the creation of the fake finger took around four hours. The dummy finger appeared as depicted in figure 1.

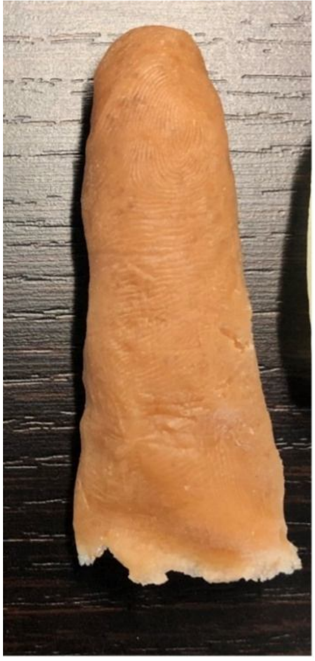

Fig 1: The final appearance of the dummy finger prepared with the aid of gelatin and glycerin.

H. Forgery using the cast made from Accutrans

Sebum and oil from the person's face were put to their fingerprint. Later, matrix was added to this cast, and it was touched twice on paper. In each case, the matrix was applied before the substrate was brought into contact. Once the prints had settled for an hour, they were developed using the Ninhydrin chemical procedure.The produced fingerprints were then scanned and searched using the Automated Fingerprint Identification System (AFIS) of the Dubai Police, and the results stated in the results section were acquired.

The second fake was cast in the same manner, but this time the matrix was blood. Blood was then used to cast the object onto paper. Blood was brushed onto the mold before each impression was made on the paper to guarantee consistency. These counterfeit prints dried for an hour before being processed using Amido Black dye. The aforementioned outcomes were obtained after scanning and analysing these fake fingerprints using the Dubai Police AFIS.

I. Forgery using the Dummy finger as the cast

There was no need to apply a matrix to the substrate before placing the prints on it because the gelatin and glycerin used to make the dummy finger already served that function. Two dozen prints were spread out on a ceramic tile and given anywhere from five minutes to an hour to cure.The fingerprints were taken, allowed to dry, then developed with black fingerprint powder and lifted with tape. The Dubai Police Automated Fingerprint Identification System was used to scan and examine these elevators. The findings are presented in the following section, appropriately named "Study results."

At the Dubai Police Fingerprint Department, this phantom digit served double duty as a cast for the biometric security system that controls entrance to the restricted area. The writer, who can read the secret material, used his own dummy finger to gain entry.It was tested by a lab assistant on the biometric scanner to see if a fake finger would be accepted. The phantom digit was also used to open the phone.The phone's unlock code was set to the author's fingerprint, and a copy of his finger was used to test the phone's ability to recognize fingerprints. Smartphones from Apple, Samsung, and Huawei were used for this. The section called "Results" talks about the results.

RESULTS

Accutrans made a casting that was free of air bubbles and other imperfections. However, the texture of 3D-printed fingerprints did not resemble that of human skin.It was used to make the dummy finger because it was strong. The only thing that needed to be thought about when making dummy fingers was how stable the parts would be. The parts don't last long, and the dummy fingers fall apart after three weeks.

The counterfeits that were put on paper with an Accutrans cast were made with a chemical process called Ninhydrin. However, the prints were spotted and dotted. The ridges that seemed to be there were broken. The AFIS looked up the prints in its database and gave a list of possible matches.Even though the prints were not very good, there was a hit, and the person was found. The fakes made from Accutrans casts with blood as the matrix and treated with amido black were better than the ones made from the other materials.These fingerprints were also put into the database and matched to the person whose finger was used to make the cast. Figure 2 shows what happened. Fingerprint powder was used to make fake prints on ceramic tiles that were made with a dummy finger and then developed with a dummy finger.When these fingerprints were looked up in the database, the AFIS again made a list of possible suspects. There was no doubt about who made these prints because they were of such high quality. Figure 3 shows the outcomes.

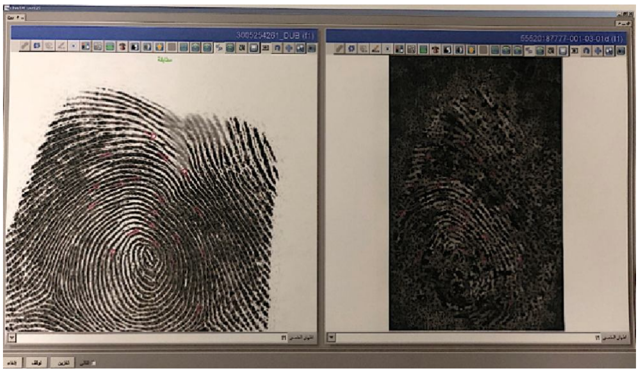

Fig 2: Forged fingerprint made with Accutrans and searched through the database (AFIS) resulted in a positive Identification.

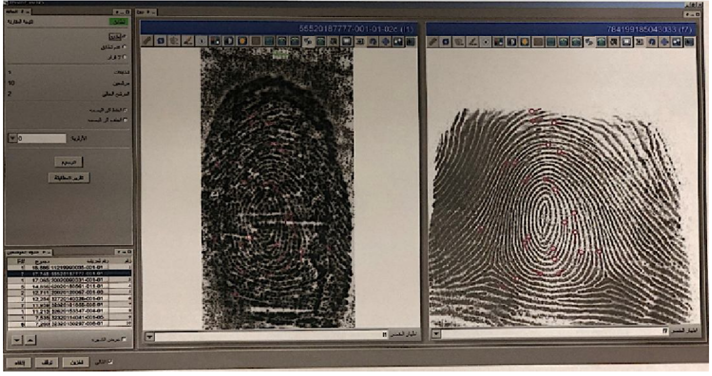

Fig 3: Forged fingerprint made with dummy finger and searched through the database (AFIS) resulted in a positive Identification.

Through the use of the dummy finger in the biometric security system, entrance was granted to the restricted area. The unlocking of a "Huawei Smartphone" was accomplished with some difficulty and was only successful on one occasion, however the unlocking of a "I-phone" and a Samsung smartphone was quite simple and straightforward.

DISCUSSIONS

In response to this new set of fingerprints, the AFIS once again compiled a list of potential suspects. Their authenticity was proved because to the high quality of these prints. These results are shown in Figure 3.Furthermore, we wanted to see how well it worked to fool biometric security systems. The authors employed several methods, some of which were discussed above in the discussion of methodology, to achieve these ends.

Passwords have traditionally been used as the gold standard for computer and network authentication. Passwords, however, are easily compromised, thus biometric authentication seems like the best option right now. Digital identification and authorization based on a person's unique physical or behavioural features is called biometrics. Facial recognition, retinal scanning, voice recognition, and fingerprint authentication are all examples of biometric authentication methods. These days, fingerprint verification is a common security measure. As technology has progressed, fingerprint authentication has been implemented on a wider number of devices such as laptops, telephones, padlocks, and encrypted USB drives. Each person has a distinct set of fingerprints [12–14, 21].

However, there is a security risk due to the increased use of fingerprint authentication and other technologies like 3D printing [15]. As Talos CEO Craig Williams puts it, "for the bulk of vendors, it does not need a large amount of money to overcome fingerprint-based authentication.""The fact that home 3D printing technology is capable of reaching a resolution that makes fingerprints less secure than they were ten years ago is concerning given that these printers are available to anyone who wants one. On the other hand, it is still challenging. It will still require some work on your part, as well as the capacity to capture the print "[15,16].Access to all of a person's fingerprints is not typically possible. It is possible to forge fingerprints by transferring them from one surface to another, but the process of transferring them to a surface that is suited for scanning and 3D printing is complicated and not always exact.

After gaining access to the Automated Fingerprint Identification System and receiving authorization from the Head of the Fingerprints branch of the Dubai Police, the authors downloaded a 10-digit fingerprint card and made use of it to make a 3D print of a particular fingerprint.Following that, the one-of-a-kind finger from the ten-digit fingerprint card was scanned and sent to 3D systems so that it could be 3D printed. The fingerprint that was 3D printed had a surface that was fairly rough and grainy. Because the firm did not have a material that could imitate human skin, the company used the 3D-printed fingerprint to make a dummy finger out of a variety of materials that were comparable to human flesh.In the not-too-distant future, the Dubai Police Department plans to build its own 3D forensics laboratory so that it can carry out additional experiments and study. The 3D-printed fingerprint faced challenges not just in terms of its surface texture, but also in terms of its dimensions and proportions. The mold that is used to create a fingerprint must have the same proportions and dimensions as a real fingerprint in order to make a fingerprint that is accurate in appearance. This could remove any doubt that the impression was formed by a dummy finger, which is important to know when searching the AFIS database because the distance between the ridges and the minute details is critical. When the measures of the created fingerprint match those required by the fingerprint recognition system, it is possible to conclude that the fingerprint is accurate or comparable to a real one. This is because the measurements match those required by the system. There were many different attempts made until the perfect 3D-printed fingerprint was created. The flaws encountered were reversed print, color reversal, and measurements that were significantly off. This obstacle was overcome by several 3D printing attempts.

Gelatin and glycerin were the key components that the author chose to use in the construction of the dummy finger. There are a number of parallels between gelatin and the protein keratin, which is found in human skin. One of the key reasons gelatins was employed as one of the primary ingredients [16,17] was because of this particular characteristic. Gelatin can be dissolved in aqueous solutions of polyhydric alcohols like glycerol without losing its solubility. Glycerin is the name that's used in the business world for glycerol.In addition, gelatin granules expand if cold water is added to them, and the resulting larger particles dissolve once the mixture is heated to produce a solution. One of the most useful properties that gelatin possesses is the ability to form thermo-reversible gels. If a gelatin solution is cooled to temperatures between 35 and 40 degrees Celsius, the viscosity of the solution will increase, and it will begin to gel.The gel strength of gelatin is absolutely necessary in order to accomplish the desired form and structure. Glycerin's extraordinary humectancy and flexibility [17,18] are the result of its hygroscopicity, which causes it to attract and retain water, and its low vapor pressure. Gelatin and glycerin were utilized by the author in the process of fabricating the artificial finger because of the properties described above. In addition, because glycerin has a tendency to soak up moisture from the surrounding air, we were unable to apply the matrix to the dummy finger in advance of the imprinting process.

Constructing the dummy finger presented a number of additional obstacles to be overcome. One of the primary problems was the length of time that was required for drying. If the gelatin was not allowed to dry out entirely, it would not reach its optimum gel strength, and the prosthetic finger would end up melting. This could be avoided by allowing the gelatin to dry out completely. Because of this, one of the most important steps in the process of making the desired form is to give the finger an adequate length of time so that it may dry completely. After a period of three weeks, the fake finger started to inflate and shed its skin, as was observed. It is recommended that the conditions of storage and temperature be investigated further as a possible reason. Gelatin is well preserved when kept at cool temperatures or in the refrigerator, however in this instance, it was allowed to settle at room temperature at all times. When stored in the refrigerator or at a cool temperature, gelatin maintains its consistency and texture the best. It's probable that this was the event that brought about the demise of dummy finger in the end. Caution is required when making the dummy finger because the 3D print appears to be the actual finger, and the latex mould that would be generated with the help of the 3D print would be an inverted impression of the finger if it were created. Caution is required because the 3D print appears to be the actual finger. Since this latex print does not faithfully mimic the first print, it cannot be used to make impressions and hence cannot be used at all.In order to fix this issue, inverted printouts were utilized to make the final cast with gelatin and glycerin. This cast behaved exactly the same way as the original finger in terms of the ridge characteristics and the skin-like texture it possessed.

The cast of the fingerprint was also produced with the help of Accutrans. When the imprint was placed in accutrans, it seemed exactly the same as the genuine fingerprint; however, when it was utilized as a cast to plant fingerprints, it functioned as an inverted impression. As a result, this first impression that was formed in Accutrans was utilized as a mold, and after it had been given sufficient time to dry, the mold was subsequently filled with additional Accutrans. This procedure was carried out on multiple occasions. The subsequent layer of Accutrans was allowed to dry and then peeled away from the layer beneath it. This allowed it to function as a mold for the deposition of prints on the surface that was chosen.An extra attempt was made to produce cast; however, because to the fact that it was unsuccessful, it was not included in the techniques part of the report. In order to create a mould, one method involves placing an imprint in an Accutrans, and another method involves using glue from a glue gun to create a cast once the mould has dried. Both of these methods are examples of how a mould can be formed. Putting an imprint in the Accutrans was still another approach that might be taken to create a mold.When the glue had finished curing, it peeled away from the Accutransmold.The cast was incredibly delicate and lacked the pliability of genuine skin in its place. Additionally, the cast was ruined when blood was used as a matrix to generate prints on paper. These prints were destroyed the cast. It was determined that the adhesive cast could not be used for the study since it had become mushy after absorbing the blood, which rendered it utterly unusable.

After all of the castings were made, the next step was to try to lay impressions with them, develop those impressions using the appropriate chemicals, photograph or scan the prints, and then run those prints through AFIS to see if the system can identify the fabricated prints.The AFIS was queried for any and all fabricated impressions, and each and every one of them was discovered in the list of possibilities that was returned. As a direct consequence of these findings, it became abundantly clear that it is not difficult to spot false fingerprints. In subsequent research endeavors, the differences between latent and manufactured impressions will be uncovered and characterized.

A biometric security system that depended entirely on fingerprints for unlocking was the focus of the second part of the inquiry, which aimed to ascertain whether or not a dummy finger could be used to bypass the system. Authentication presents a huge problem to the security sector [18], particularly in light of the growing prevalence of fingerprint authentication as well as technological breakthroughs like three-dimensional fingerprint printing.The attempt by one of the authors to unlock his own "iPhone" by using a dummy finger was successful on the very first try. In addition to this, with the permission of his other coworkers, he was able to access the "Samsung and Huawei phones" of those individuals. The establishment of these two brands was difficult in the beginning. Samsung was much simpler to unlock compared to Hawaii, which only allowed you one attempt before it was unlocked.To finally succeed in unlocking them required numerous attempts. The authors believe that this could have a positive impact on law enforcement while simultaneously having a negative impact on biometric security. For instance, it could make it possible for the police to unlock the phone of a deceased person or of any living person who refuses to cooperate in a criminal proceeding in which he is the lead suspect and is attempting to hide evidence that could assist the authorities. It could also make it possible for the police to unlock the phone of any person who is alive but who is the lead suspect in the case.For instance, if the criminal conduct had the potential to have significant repercussions on society as a whole, or if it constituted a threat to national security, such as an act of terrorism, then this method would be of tremendous use. However, if this strategy were to fall into the wrong hands, thieves might use fabricated fingerprints to obtain access to restricted areas, as well as the database and any secure information it contains. In order to successfully complete this task, he or she will need access to the fingerprints of the person whose prints are being fabricated. This presents a significant obstacle. However, it's not completely out of the question.

The authors concluded that the findings of this research study will be useful to fingerprint scanning companies in the development of strategies to improve the accuracy of their scanning systems. It will be helpful in the development of advanced technology and reading devices, as well as the design of algorithms that will protect the system from attacks using phoney fingerprints. It's possible that the sensors are more sensitive to human skin and have the ability to differentiate between human skin and other materials that are imitations or fakes. The authors hypothesised that sensors may be made more sensitive by distinguishing human skin from other substances by monitoring the human heartbeat or measuring the human body temperature.

CONCLUSION

The purpose of the study was to investigate whether or not 3D-printed fingerprint casts and fake fingers could be used to place fingerprints on different surfaces and have them be recognized, as well as whether or not the false fingers might offer access to biometric systems. The findings revealed that it is possible, despite the fact that it is challenging. The author believes that the development of technology that allows for 3D printing has an effect on the use of fingerprint authentication. Due to constraints such as the requirement that 3D-printed fingerprints have the same dimensions as actual fingerprints, it is necessary to have access to a variety of cutting-edge equipment, such as electronic microscopes, in order to measure the spacings prior to the process of 3D printing. This research effort would aid enterprises in the development of reliable fingerprint scanning technologies.

Once the resources are available, a future investigation will be done on the distinctions between counterfeit and authentic 3D-printed fingerprints.

ACKNOWLEDGMENT

The authors would like to express their gratitude to Lieutenant General Abdullah Khalifa Al Marri, who serves as the Chief of Police in Dubai, and Dr. General Ahmed Almansoori, who serves as the Head of the General Department of Forensic Science and Criminology, for their assistance in finishing this research project. The authors would like to express their appreciation to Amer Abu Aieta for his contribution to the successful completion of the research study at the Dubai Police Forensic Laboratory.In addition, the authors would like to express their gratitude to Dr. Major Hamad Mansoor Alawar, who serves as the chairman of the 3D printing task force, as well as the entire department of Forensic Science and Criminology, as well as the 3D printing task force, for their assistance in finishing the project. They would also like to express their gratitude to the administration of the Houston Forensic Science Center for the tremendous assistance they provided in finishing this study. In addition, the writers would like to convey their appreciation to Ron Smith and Associates for the help and encouragement they provided.

REFERENCES

1. Wentworth, Patricia. (2014). The Fingerprint. Pebook, pp. 7-21.
2. Dubai Police Museum. (2021). Documents the first fingerprint to reveal two crimes of the theft, Alittihad, 2017, https://www.alittihad.ae/article/20834/2017/.
3. Suwaidi, M.A.A.A.A et al. (2020). "Significance of Fingerprints in A Brutal Travel Bag Murder- A Case Report". Medico-Legal Update, vol 20, no. 1, Institute Of Medico-Legal Publications Private Limited, https://doi.org/10.37506/mlu.v20i1.390.
4. Forensicsciencesimplified.Org,2022,http://www.forensicsciencesimplified.org/prints/Fingerprints.pdf.
5. Abdel kareem, Ziad Alqadi. (2020). "Analysis Of Fingerprint Minutiae to Form Fingerprint Identifier". JOIV: International Journal on Informatics Visualization, vol 4, no. 1. Politeknik Negeri Padang, https://doi.org/10.30630/joiv.4.1.332.
6. Qinghai, Gao. (2014). "A Preliminary Study of Fake Fingerprints". International Journal of Computer Network and Information Security, vol 6, no. 12 pp. 1-8. MECS Publisher, https://doi.org/10.5815/ijcnis.2014.12.01.
7. Schwarz, Lothar, and Inga Klenke. "Improvement In Latent Fingerprint Detection on Thermal Paper Using a One-Step Ninhydrin Treatment with Polyvinylpyrrolidones (PVP)". Journal Of Forensic Sciences, vol 55, no. 4, 2010, pp. 1076-1079. Wiley, https://doi.org/10.1111/j.1556-4029.2010.01383.x.
8. Harper, William W. "Fingerprint "Forgery". Transferred Latent Fingerprints". Journal Of Criminal Law and

Criminology (1931-1951), vol 28, no. 4, 1937, p. 573. JSTOR, https://doi.org/10.2307/1136785.
9. Baek, Young-Hyun et al. "Fake Fingerprint Detection Biometric System Using Neural Network Algorithm". International Journal of Signal Processing Systems, vol 6, no. 4, 2018, pp. 27-30. Ejournal Publishing, https://doi.org/10.18178/ijsps.6.4.27-30.
10. Marcel, Sébastien et al. Handbook of Biometric Anti-Spoofing. Springer: London, 2014, pp. 13-34.
11. Uliyan, Diaa M. et al. "Anti-Spoofing Method for Fingerprint Recognition Using Patch Based Deep Learning Machine". Engineering Science and Technology, An International Journal, vol 23, no. 2, 2020, pp. 264-273. Elsevier BV, https://doi.org/10.1016/j.jestch.2019.06.005.
12. Gregg, Mike. (2019). Journal Of 3D Printing in Medicine, vol 3, no. 1, pp. 1-3. Future Medicine Ltd, https://doi.org/10.2217/3dp-2018-0029.
13. Bowyer, Adrian. (2014). "3D Printing and Humanity's First Imperfect Replicator". 3D Printing and Additive Manufacturing, vol 1, no. 1, pp. 4-5. Mary Ann Liebert Inc, https://doi.org/10.1089/3dp.2013.0003.
14. Dass, Sarat C. (2013). "Fingerprint-Based Recognition". International Statistical Review, vol 81, no. 2, pp. 175-187. Wiley, https://doi.org/10.1111/insr.12017.
15. Wayman, J.L. (2012). "Editorial: Spirit of IET Biometrics". IET Biometrics, vol 1, no. 2, p. 91. Institution Of Engineering and Technology (IET), https://doi.org/10.1049/iet-bmt.2012.0023.
16. Monson, Keith L. et al. (2019). "The Permanence of Friction Ridge Skin And Persistence Of Friction Ridge Skin And Impressions: A Comprehensive Review And New Results". Forensic Science International, vol 297, pp. 111-131. Elsevier BV, https://doi.org/10.1016/j.forsciint.2019.01.046.
17. Nast, Condé. (2022)."A Cheap 3D Printer Can Trick Smartphone Fingerprint Locks". Wired, 2022, https://www.wired.com/story/cheap-3d-printer-trick-smartphone-fingerprint-locks/.
18. "Artificial Gelatine-Based Skin Model That Simulates Human Skin Almost Perfectly". Medicalxpress.Com, 2022, https://medicalxpress.com/news/2017-04-artificial-gelatine-based-skin-simulates-human.html
19. Neville, Harvey A. et al. (1930). "A Study of Some Properties Of Gelatin I— Of Gelatin I—Hydration Of Gelatin And Its Relation To Swelling". Industrial & Engineering Chemistry, vol 22, no. 1, pp. 57-62. American Chemical Society (ACS), https://doi.org/10.1021/ie50241a017.
20. Aciscience.Org, 2022, https://aciscience.org/docs/Glycerine_-_an_overview.pdf.
21. Sharma, B.K et al. (2019). "Emerging Trends in Digital Forensic And Cyber Security- An Overview," 2019 Sixth HCT Information Technology Trends (ITT)". IEEE, pp. 309-313, Accessed 16 Jan 2022.

CITATION OF THIS ARTICLE

Abdulrahman Mohammed Obaid Almheiri, Shanaihi Sanjay Patel, Bhoopesh Kumar Sharma: 3D Fingerprint Forgery and Biometric Security Threats: A Conceptual Study. Bull. Env.Pharmacol. Life Sci., Spl Issue [5]: 2022: 28-35.