The Mobile Biometric Testing Project

Sidney Sykes
Department of Computer
and Information Science
University of Mississippi
University, Mississippi 38677
Email: *swsykes@go.olemiss.edu*

Abstract

In today's world, technology gives us an upper advantage of the access that are in the tip of our fingers, It brings us instant satisfaction that we do not have to worry about making as many long road trips to grocery stores, libraries, and even financial institutions. It ranges from iris verification, voice recognition, facial authentication, and fingerprint verification. When biometric features came to the mix in mobile devices and mobile application, it expanded our dependencies on technologies. However, someone is benefitting from our complacencies. Therefore, I investigated the possible methods that can cause those problems, and I found an accurate way that hijackers can access our personal technology, and there are proposed but continuous solutions to this issue.

1. Introduction

Technology is a tool that we use to an advantage daily. It is a part of our lives academically, athletically, financially, gymnastically (describing fitness), medically, socially, etc. Almost every industry uses technology to innovate its businesses. In recent years, Android, Apple, Dell, LG, and Samsung have implemented biometric features on laptops, mobile phones, etc. The biometric finger scanner allows users to log in with their fingerprints conveniently. Cardio machines in fitness centers, and smartwatches such as CORX devices, have hand sensors to log in quantity data such as burned calories, body weight, and timer; and it would help attendees' fitness goals. Everyday citizens take advantage of fitness programs, fingerprint logins, and pin-code while storing their information in these devices. Doctors gain access to patients' health records with conscious consent, and they usually store them in mobile health devices. Devices such as laptops, mobile phones, and smartphones store passwords; email addresses; financial information such as bank account(s), debit and/or credit card numbers; health records. This information becomes vulnerable when users become unconscious.

Mobile and wearable devices have weak security due to lack of testing, the size of the device, and the lack of value. Most recently, those devices use some form of biometric screening such as finger scanning, voice recognition, face recognition, etc. These features would make devices more vulnerable for hackers to hijack those devices. The best way to prevent and lower attacks are to disconnect any devices' linkages through Bluetooth, remove any saved financial information from the devices or any accounts with saved financial information from devices, and wipe out any biometric features.

For my project, I plan to test the biometric fingerprint and facial authentications of mobile devices with my cell phone called the LG Stylo 4 Phone. For the biometric fingerprint, I will test different household and office materials to test the fingerprint scanner feature on my phone. I will place my index fingerprint on a piece of paper and attempt to scan them. I will also use my phone to use an application called the Luxand Face Recognition for the vulnerability of facial authentication. Afterward, I will print the color ink with the Canon printer to print my photos. Then, I will scan the paper against the app to test whether they are recognizable and vulnerable.

After evaluating the safety and vulnerability of the authentications, I will propose solutions to make biometric features safer and secure.

2. Background

The [1] pointed to using a biometric fingerprint scanner in mobile devices. They rephrased the benefits of smartphones such as communications, convenient banking, entertainment, and internet browsing without ignoring the possible victimization of the PIN system and the biometric fingerprint scanner. Users did their best to ensure that their devices and the applications, accounts, data, files, etc. were secure. The author

pointed out the three-layer security structure: the collection of the user fingerprint, the continuous user verification via trusted zone, and the verification certificate. They found this structure to be more secure than a single-stage verification. A team of lab engineers and advisors used direct and indirect methods for data collection. For the direct method, the user imprinted his finger on play dough for an inverse sample of finger imprint. For the indirect method, four participants and victims had their fingerprints applied on the following brands of mobile phones: Samsung, Infinix, Apple (iPhone), Vivo, and Huawei. Sensor locations were in the rear or front end of those devices. The team performed 11 experiments with combinations of different mold materials for direct and inverse impression molds. They found the following combination to be the best strategy to unlock the devices: Hot Glue + PX-70 Coating, White Cement + PX-70 Coating, Silicon + Silicon, Soft Silicon + Soft Silicon, and Play Dough + Hot Glue. They successfully united different materials together, using different devices and individuals, and displaying the results to help understand the experiment. Understanding the experiment even better from the beginning would be easier if they could go in-depth about the direct and indirect data collection methods.

In [2], this work touched on multiple examples of biometric authentication, such as fingerprint scanning, eyes recognition, and face recognition. Devices such as iPhone 5's Motorola Atrix, and Fujitsu F505i contain a touch sensor that automatically unlocks the phone with a fingerprint. Asus and Toshiba laptops have built-in biometric face recognition. According to a survey, about 3.4 billion users would have biometric features on mobile devices by 2018. However, users are at higher risk of spoofing attacks such as face spoofing, iris spoofing, and fingerprint spoofing. Hackers would take an individual's photo and alter it to hijack devices as if it belonged to them, which is an example of face spoofing. They would alter it as 3D face model, photo spoofing, or video spoofing. Hackers would use an iris photo, iris video, or printed contact lens in iris spoofing. The authors proposed the MoBio System, also known as the Mobile Biometric Liveness Detection System. They presented three security levels: low, medium, and high. While the lowest security system represents the success rate of fooling the system, the highest system would heighten the chance of compromising with a spoof attack. The system's low level uses only the LUCID descriptor to analyze and detect the local representation of the face, fingerprint, and iris input images. It would detect it against other images and the Support Vector Machine classifier. The LUCID and CENTRIST features would collaborate to analyze and detect the global representation of the face, fingerprint, and iris input images at a medium level. At the high level, POEM, LUCID, and CENTRIST would combine to analyze and detect the local and global representation of the face, fingerprint, and iris input images. After the experiment, the CENTRIST performed better with fingerprint and iris input images. The LUCID has hit and misses with the fingerprint. Overall, this proposal has ways to go and other factors to account for to ensure a successful spoof-proof method.

In [3], the authors pointed out that Personal Identification Number, also known as PIN, is the subsequent most accessible access to laptops and mobile devices. They stated that biometrics could not be stolen, which is contradictory to real-life examples. There are two stages of biometric-based authentication: enrollment and authentication. Direct attacks, also known as Sensor attacks, consist of presenting Synthetic or Fake Biometric Traits to the Sensor. Indirect attacks can launch on the interface Between Modules or on the Software Modules. They used the following categories of alterations: luminosity, noise, blur, past of a user's image, mosaic image, and negative image. After evaluations, the levels of alteration affect the matching score in fingerprint authentication systems and the number of matched associations in facial authentication systems. Poor quality fingerprints and facial images can lead to incorrect or spurious biometric features and remove actual biometric features, which can deceive the effectiveness of the biometric system. The authors thoroughly explained the different alterations, displayed the visualizations of the altered images, and differentiated biometric fingerprint and facial authentications. They should not state that biometrics cannot be stolen.

Scientists in India are investigating strategies to improve Biometric Security by reducing the false acceptance rate, false rejection rate, and the failure to enroll rate. There are five categories in the Multibiometric System: Multi-Sensor Systems, Multi-Algorithm Systems, Multi-Instance Systems, Multi-Sample Systems, and Multimodal Systems. The fusion levels in the system are sensor level fusion, feature extraction level fusion, matching level fusion, and decision level fusion. They proposed a model with liveness detection to determine whether the input user is real and live or fake. The enrollment and authentication stages will help with the verification and identification of the user. They proposed an algorithm that will take extra steps to verify the users. The algorithm helped reduce the false acceptance and rejection rates with a single device. The caveat is that the process is tedious, and it costs the

device more storage spaces. The authors successfully describe the algorithm and its logic; however, they should have further data to prove this proposal [4].
Computer scientists collaborated to propose an XML-database to support biometric templates to protect the data in mobile devices. Those devices contained at least one biometric feature, especially fingerprint and facial recognition. Sensor, feature extractor, template database, matcher, and decision component are significant components of the biometric systems' architecture. Enrollment and authentication were the two stages of the biometric systems. The biometric template database is part of the proposal as the authors were looking to fulfill privacy and security requirements. The privacy requirements are identity privacy, irreversibility, and unlikability; and the security requirements are confidentiality, integrity, and renewability and revocability. They plan the database to be a non-traditional XML database to support the extra layer that supports the APIs: XML:DB API (XAPI) and XQuery API for Java specification (XQJ). It plans to support the Android devices with Java programming language (primary for Android), and XCBF specification should allow the database to do its job to protect the mobile devices with biometric devices. This can help the whole technology world to have a trustworthy security system without worry about hackers picking up our biometric identities and use them to their advantage. The author made a unique proposal; however, the action should come into play [5].

3. The Work of This Project

For the facial and fingerprint authentication, I tested the vulnerability by attempting to use fake biometric identification with the LG Stylo 4, 4th Generation.
First, I installed the Luxand Face Recognition Application from the Google Play store. When I opened and tested the application for the first time, I used the front-face camera and named my identity Person1. For the facial authentication, I used the following materials: printed photos with different effects (normal, negative, grey, negative grey once, and gradient). I snapped photos using the front-face camera with the LG Stylo 4, and it went to the Gallery app. I accessed the photos through my photo gallery and downloaded them to my laptop machine. I place those photos in the appropriate folders.

Afterward, I used the Anaconda project application called the Jupyter Machine to create edited photos in the following effects: negative, grey, negative grey once, and gradient (with three images). I used the

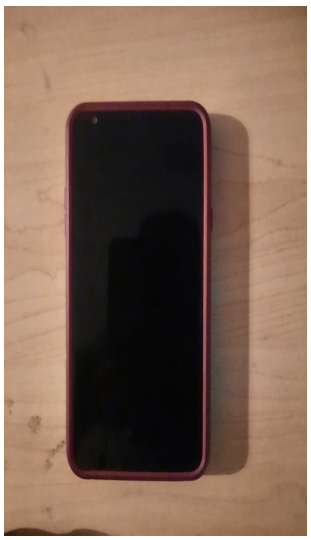

Figure 1. The LG Stylo 4 Phone Used In This Project

Figure 2. Back The LG Stylo 4 Phone with the Biometric Fingerprint Scanner

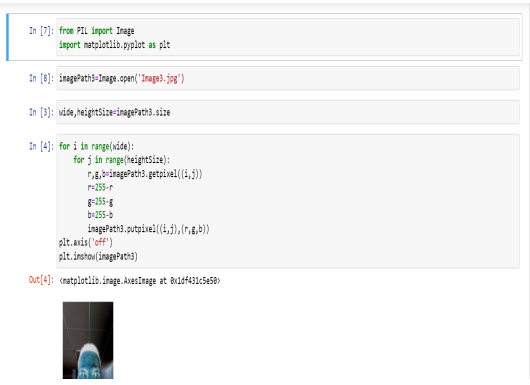

Figure 3. Altering Images in Anaconda

Figure 4. Second Part of Altering Images in Anaconda

Figure 5. Altering Images with Gradient in Anaconda

Python programming language to edit those photos in the notebook. After the editing was complete, I used my Canon TS3520 with the Canon PG-275 Black Ink and the Canon CL-276 Color Ink to print those photos. To conserve typing papers and ink, I printed the photos with the Print Application on my laptop using the following commands to select multiple photos: control + select the photos with the mouse. Then, I right-clicked on one of the selected photos and clicked on Print. When the Print Pictures window popped up, I selected the ”4 x 6 in.” or mostly the ”5 x 7 in.” option. I would leave the ”Fit Picture to Frame” option checked. Then the photos print.

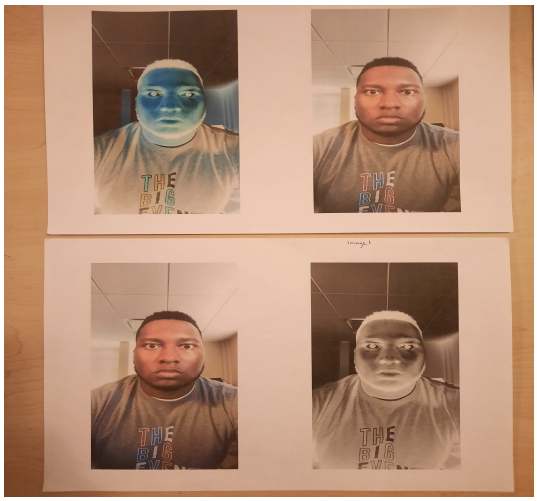

Figure 6. First Image of The Facial Authentication

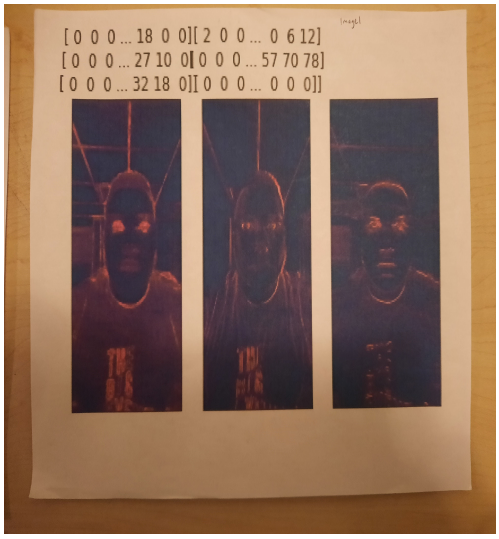

Figure 7. First Image of The Facial Authentication with Gradient

When the printing was complete, I assessed each set of photos with the Luxand application on the LG Stylo 4 using the back camera. If the photos are recognizable, then the app will identify the face.

For the fingerprint authentication, I attempted to test whether the fake fingerprints would make the LG Stylo Fingerprint-Spoof. Therefore, I used the following materials on my index finger: Crayola Playdoh, Elmer's Glue Stick, A Combination of Emler's Glue Stick and the Brown Shoe Polish, and the Brown Shoe Polish alone. I placed the fingerprints on a sheet of typing paper for each material or material combination. I took the LG Stylo 4 phone and scanned the biometric feature against the fingerprint to see whether those fingerprints could access the phone screen.

Figure 8. Second Image of The Facial Authentication

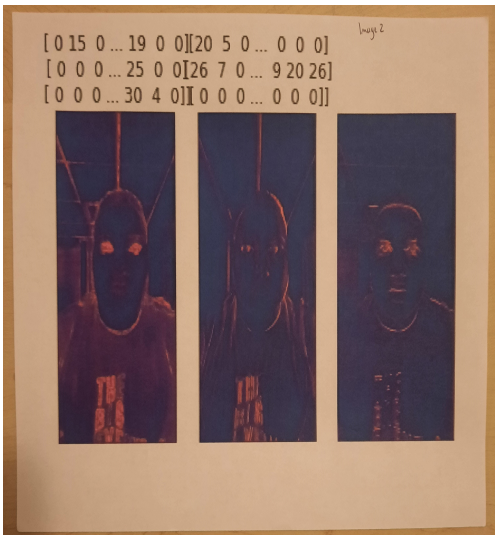

Figure 9. Second Image of The Facial Authentication with Gradient

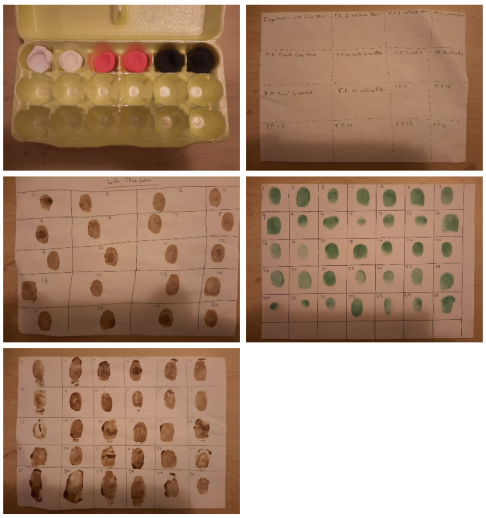

Figure 10. The Artificial Fingerprints With The Playdoh, The Glue-Stick Fingerprints, the Shoe Polish Fingerprints, The Ink Pad Fingerprints, and the Glue-Stick and Shoe Polish Combined Fingerprints. (From top left to bottom left)

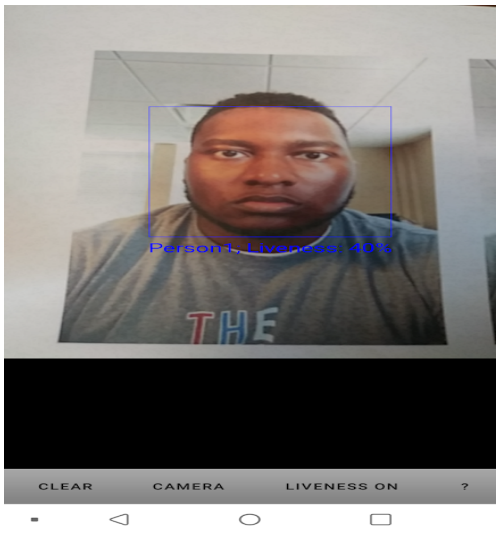

Figure 11. Using the Luxand App Against a Printed Photo

4. Evaluation

For evaluation, I calculated the following for facial authentication [6]:
False Acceptance Rate For Facial Authentication =

$$\frac{Number of Photos Are Being Detected}{Number of Overall Photos}$$

False Rejection Rate For Facial Authentication =

$$\frac{Number of Photos Are Not Being Detected}{Number of Overall Photos}$$

The False Acceptance rate for the facial authentication is 31.67 percent. Out of this percentage, all the regular grey and the normal printed photo have a perfect false acceptance rate. The rest of them have a 100 percent false rejection rate. Therefore, we have an 68.33 percent overall False Rejection Rate. There is a type of direct attack called presentation attack that is happening. A presentation attack means that an alternative version of an identity such as online photos, a face masks, etc. has been used to attack an individual device security and privacy. With a clearer face, recognizable iris, and familiar detection, the Luxand application successfully detected the grey and normal printed photos of "Person1". To strengthen the security of the camera on the phone, the operating system should be able to recognize the difference between a real individual and a photo. Let alone an impersonator of an individual. Creating algorithms that would target the difference and the similarity between a liveness detection circumstance and a non-liveness detection event to prevent and reduce any false acceptance from attacking a user's data and mobile device.

For evaluation, I calculated the following for fingerprint authentication [6]:

False Acceptance Rate For Fingerprint Authentication =

$$\frac{Number of Fingerprints Are Being Detected}{Number of Overall Fingerprints}$$

False Rejection Rate For Fingerprint Authentication =

$$\frac{Number of Fingerprints Are Not Being Detected}{Number of Overall Fingerprints}$$

Image 1				
Effects	Success	Failures	FAR Percentage	FRR Percentage
Normal Printed Photo	1	0	100%	0%
Negative Photo	0	1	0%	100%
Negative Grey Photo	0	1	0%	100%
All Three Gradient Photos	0	3	0%	100%

Figure 12. The Data of Image 1 To 10 For Facial Authentication

Image 2 through Image 10				
Effects	Success	Failures	FAR Percentage	FRR Percentage
Normal Printed Photos	9	0	100%	0%
Negative Photos	0	9	0%	100%
Grey Photos	9	0	0%	100%
All Three Gradient Photos	0	27 (9 * 3)	0%	100%

Figure 13. The Data of Image 1 To 10 For Facial Authentication

Detected Fingerprints				
Materials	Success	Failures	FAR Percentage	FRR Percentage
Elmer Glue Stick	0	20	0%	100%
Shoe Polish	0	26	0%	100%
Elmer Glue Stick + Shoe Polish	0	30	0%	100%
Ink Pad	0	35	0%	100%
PlayDoh	0	6	0%	100%

Figure 14. The Data of the Detected Fingerprint Scanning

We attempted a direct attack on the biometric fingerprint scanner. It is found that neither material is effective enough to hijack the biometric fingerprint scanner on the LG Stylo 4. Therefore, this experiment encountered an overall 100 percent false rejection rate. Despite using materials such as shoe polish, Crayola Playdoh, and Ink Pad, which obtained huge amounts of fingerprint trace, the Android 8.1 operating system was too much for those artificial fingerprints to overcome. The fingerprint spoof attempt is also a direct attack. The reason why this presentation attack did not work because the user of this phone, which is me, recorded the actual fingerprint closely when setting up this device, and the biometric fingerprint scanner designed to recognize the actual fingerprint from an actual human being. That does not mean that it should not be any further improvement in the biometric arena with mobile devices. Creating a non-traditional XML-Database in phones such as Android can help track any biometric attack attempts, and it should send the attempt information to Google automatically under consent. The Apple corporation must find something similar to the iPhone.

5. Conclusion and Future Work

In this project, I tested the security and vulnerability of facial and fingerprint authentications. I used an older mobile phone with a biometric feature and two cameras to test both authentications, and I found that the most accurate photos, similar to an actual face, can successfully perform a presentation attack, a direct attack. On the other hand, a successful biometric fingerprint scanner can overcome artificial fingerprint, especially with the latest security features. However, these issues cannot be overlooked.

I would like to continue to work on this project by using a Patient Health Monitoring System on ESP32 Web Server, and this time, I would like to have all the fingerprints involved instead of one finger to test all vulnerabilities with different materials. I would like to continue to pursue more ways to detect fake images. Also, I desire to research how to strengthen security on mobile and wearable devices.

References

[1] Z. Zahid, A. Haider, N. Sabahat, and A. Tanwir, "Vulnerabilities in biometric authentication of smartphones," in *2020 IEEE 23rd International Multitopic Conference (INMIC)*, pp. 1–5, IEEE, 2020.

[2] Z. Akhtar, C. Micheloni, C. Piciarelli, and G. L. Foresti, "Mobio_livdet: Mobile biometric liveness detection," in *2014 11th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, pp. 187–192, IEEE, 2014.

[3] S. Ghouzali, M. Lafkih, W. Abdul, M. Mikram, M. El Haziti, and D. Aboutajdine, "Trace attack against biometric mobile applications," *Mobile Information Systems*, vol. 2016, 2016.

[4] M. Devi, C. Kant, *et al.*, "A novel approach to improve the biometric security using liveness detection.," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, 2017.

[5] R. Thirumathyam and M. O. Derawi, "Biometric template data protection in mobile device environment using xml-database," in *2010 2nd International Workshop on Security and Communication Networks (IWSCN)*, pp. 1–7, IEEE, 2010.

[6] K. K. A. Ghany, A. E. Hassanien, and G. Schaefer, "Similarity measures for fingerprint matching," in *Proceedings of the International conference on image processing, computer vision, and pattern recognition (IPCV)*, p. 1, The Steering Committee of The World Congress in Computer Science, Computer . . . , 2014.