computers

MDPI

Review

A Review of Facial Biometrics Security for Smart Devices

Mary Grace Galterio, Simi Angelic Shavit and Thaier Hayajneh *

Fordham Center for Cybersecurity, Fordham University, New York, NY 10458, USA; mgalterio1@gordham.edu (M.G.G.); sshavit@fordham.edu (S.A.S.)

* Correspondence: thayajneh@fordham.edu

Received: 29 April 2018; Accepted: 22 June 2018; Published: 27 June 2018

Abstract: Biometrics play an avid role in today's mobile security realm. Security experts have attempted to implement different forms of biometrics, from finger, hand, and signature to voice, retina, and iris. Recently, facial biometrics has been added to this list and has introduced another method for a more secure form of authentication. Various organizations believe that by using something you are, like biometrics, their system would be strongly secured. As this may be true, applications used for facial biometrics have lost their credibility when easily defeated. This may be through printed photographs, electronic images, and even look alike. This paper explores the scientific background as to why facial biometrics have become a trusted form of authentication, a user-friendly method, and explores the security of mobile device applications available for Android and iOS systems. We test several applications with our developed methods and discuss the results.

Keywords: facial biometrics; smart devices; biometric authentication

1. Introduction

A biometric system is a recognition system that establishes the authenticity of a specific physiological or behavioral characteristic of a user. The biometric system is divided into two stages: the enrollment module and the identification module. The enrollment module is accountable for training the system to identify a specific person by scanning the person's physiognomy to create a digital representation. This digital representation becomes a template to be compared. The identification module is accountable for recognizing a given person by capturing the characteristics of the person to be identified and converting this into the same digital format as the template [1]. The identification module is divided into two stages, the identification stage and the verification stage. The identification stage prompts the system to ask, "Who is X?" and attempts to compare "X" to every template in the database. In contrast, the verification stage forces the system to ensure that a user, who claims he is "X," answers and solves, "Is this X?" [2].

This technology has had a growing popularity for decades and still continues to grow. In the 1970s, in Osaka, Japan, many were attracted to the "Computer Physiognomy" exhibit presented by the Nippon Electric Company (NEC) at the World's Fair. When guests sat down, their picture would be taken and fed to a computer. The computer would then show them lines from an image and could locate feature points on their faces. It would classify each face into one of seven categories, corresponding to a famous person's face. This event, like many others similar ones, amazed many observers and made people think of what the future had to offer. Computers were now able to look at a picture of someone and make sense of them in a technologically advanced way. As computer networking began to play a large role in the business and government sectors, biometric technologies were envisioned to meet the demand for a more secure computer network, as well as a more intensified, automated form of surveillance, access control, and identification [3].

In the 1960s, the U.S. Department of Defense and intelligence agencies began to invest in research labs that attempted to program computers to identify human faces. By the 1990s, there was a growing interest for this technology in places such as passport agencies, State Department of Motor Vehicle offices, law enforcement companies, and penal systems. Facial identification systems were meant to operate automatically, in real time and at a distance. In addition, they were meant to create a more effective institutional and administrative form of identification, social classification, and overall, give back control [3].

In January 2001, MIT's *Technology Review* proclaimed biometrics as one of the top ten technologies that would change the world. There is no doubt that facial biometrics have come a long way, just as there is no doubt the technology still has far to go [3]. The demand for facial biometrics has proved to be necessary from our research. Banks, militaries, government, and various organizations have continued to rely on photo IDs and face-to-face interactions as opposed to fingerprints or other forms of verification. We attempt to analyze various mobile applications using facial biometrics technologies in order to understand which, if any, is the best form.

This paper will explore facial biometrics in great detail, starting with its background. We discuss the past and present advancements, as well as the hopeful future of facial biometrics and the security features it handles. Next, we report on the different applications that facial biometrics are, and potentially can be, used for. Then we briefly discuss and test a sample of available mobile applications that use facial biometrics. Lastly, we examine security, exploring why the current verification and authentication methods are not sturdy enough as well as supplying new methods that we believe are more soundly secure.

The remaining parts of this paper are organized as follows. Section 2 discusses some background on biometric authentication technologies. Section 3 focuses on facial recognition technologies and their applications. Issues of facial recognition and common applications are discussed in Section 4. Section 5 presents our testing and results, and Section 6 concludes the paper.

2. Biometric Authentication Technologies

Facial expressions and patterns have been studied since 1872, when Darwin investigated the expression of emotions. Facial profile-based biometrics were introduced by Galton in 1888. Psychophysicists, neuroscientists, and engineers have conducted widespread research on facial recognition by humans and machines for the past 42 years. Principal component analysis (PCA) tracks a subject's head and then attempts to recognize them by comparing the characteristics to those of the known individuals. Bledsoe was the first to cultivate a semiautomated face recognition system with a hybrid human-computer arrangement that is able to classify faces by fiducial marks entered on photographs by hands. Goldstein established a system with up to 21 features and recognized faces using standard pattern classification. Fisher and Elschlager had a similar approach in which they measured shades of hair, length of ears, lip thickness, and other features. Zhujie and Yu focused on the properties used to characterize the human face under various environmental conditions [4].

This extensive research had many practical implications for performing identification. The need to institutionalize identification can be dated back to the early nineteenth century. By the 1880s, photographs of a person's face on identification documents had been implemented. World War I brought about photographic portraits to be included on or with passports. In 1914, the United States Secretary of State stipulated the inclusion of photographs on all new passports issued. While biometric facial recognition was necessary and proved to be advancing, it was complex and required necessary resources that were not completely obtainable [3].

As technology advanced, new attempts at using biometrics were made. Optical fingerprinting, hand geometry, retinal identification, voice, and signature recognition all took shape during the 1980s. When banks noticed how efficient it could be for their business, they began to invest in the industry as well. However, for the banking industry, it was difficult to get their customers to agree to this technology. Nothing felt as safe for customers as dealing face to face with a banker [3].

While the bulk of funding for research in the United States came from military agencies, the civilian sector still played a prominent role in the development of this technology. Civilian agencies have sponsored tests of vendor systems, negotiated technology standards, and established a policy environment conducive for biometric system implementation. In addition, the United States' driver's license administration has been a special site of experimentation with facial recognition technology [3].

Biometric technologies assured the binding of identities to bodies over networks and facilitated the security of identity in various markets. For some systems, fingerprinting, hand geometry, iris, or voice recognition may be more applicable [3].

Despite these advancements, introducing biometric authentication into everyday systems still faced challenges. Fingerprinting was a technology that was believed to be present for hundreds of years. However, the connection it had with criminality made it less appealing and user acceptable. Hand geometry was problematic, as hand measurements were not an individual characteristic. An attempt at using blood vessels in the eye was also tested by a company called EyeDentify, whose process required careful attention to the alignment of the eye to capture a usable image. However, there was an additional fear that it would harm the eyes. The notion of eye (both retina and iris) recognition is often assumed to be intrusive and uncomfortable by users. Voice recognition was problematic, as a person's voice could sound different depending on the recording device and prosody, or the tone, tempo, and stress at which words were said. What facial recognition has maintained above all of these other recognition technologies is that billions of photographed faces already exist and circulate on documents, making the biometric identification seem self-evident. Everyone in the modern world is accustomed to carrying a photo identification and presenting it, or constantly taking and posting pictures of themselves [3].

3. Facial Recognition Technologies

There are two main technologies used for facial recognition, face metric and eigenface. Face metric uses the normal face picture, or the canonical image, to inspect special features of the face [5]. These features include the distance between the eyes, distances of eyes to nose, mouth to nose, and many others. These metrics are used and stored as a template to be compared to for future recognition.

The eigenface technology works differently, as it changes the presented face's lighting by using different scales of light and dark in a specific pattern. The different light and dark areas computed on the face cause the picture displayed to not actually look like a face anymore. The pattern created from the shaded areas is very important, however, as it is a way to portray and calculate how the different features of the face are singled out and to evaluate the symmetry of the face. The pattern is calculated to a degree of eigenfaces, or eigenvectors, that is determined by including facial hair or the size of facial features. Using different numbers of eigenvectors to calculate a face can allow for easy reconstruction. The standard technology uses around 150 eigenfaces, but with only 40 eigenfaces used it is possible to accurately reconstruct the face [5].

Facial recognition allows for quick and stealthy verification of humans due to the fact that it can be performed without any physical contact with the system. The software is able to capture faces of people in public areas and compare them to linked databases. Therefore, the technology can benefit a wide range of businesses and agencies. This section identifies different potential application uses for facial recognition technology. The use cases investigated here are specifically for the government/criminal sector, the commercial sector, and most importantly, the security sector.

3.1. Government/Criminal Sector

Using facial recognition software for surveillance purposes would assist government authorities in locating certain criminals, extremists, and missing children. This would make it harder for fugitives to get away and for children to go unnoticed. However, for the system to recognize a given person, it needs to already have records in the system to match and verify to. So, although there are high quality

mug shots of criminals, potential, and future convicts are likely to not be in the system, which raises an issue for this application.

This use case works by a simple surveillance camera capturing a scene, space, or event. The video streams are sent over a network to a central control facility, where the computer finds faces in the video. Lastly, it will attempt to find a match to the found faces in the connected database. The system alerts an officer if there is a match, presenting him with both images, and he decides if this is accurate.

The system is beneficial over human verification because human beings have difficulties with facial recognition. This is because they have a hard time recognizing unfamiliar faces, have a short attention span, and it is difficult for humans to connect new faces to those they have seen in the past.

3.2. Commercial Sector

In a British study, supermarket cashiers were tested on their ability to screen shoppers using credit cards that included the card owner's photo. Every shopper received four credit cards, one with a recent picture of them, one with a minor change to their hair, facial hair, or accessories, one with a photo similar in appearance to them, and one with a person who was only of the same sex. More than half of the fraudulent cards was accepted by the trained supermarket cashiers [2].

In addition to payment authorization, facial recognition can also be used in stores to alert the sales associates of a customer who just walked in. If a person has been in the store before, they would have been previously recorded from the store's surveillance camera. It is possible that now upon entering the store, the same person is recognized and judged and treated based on their past purchases and habits. For example, they did not buy anything the last couple of visits, so they are ignored and the associates do not waste their time persuading them to buy, especially if someone else in the store has been recognized as being a big spender. People can also be profiled as impulse shoppers, or even marked by their attitudes. This applies not just to stores but can be useful for banks as well, linking high bank accounts with faces [6].

3.3. Security Sector

The most relevant, popular, and realistic use case is security. Buildings, border checkpoints, airports, and seaports all require authentication for access. ATM machines, banking applications, computer and network security, and email logins are some examples where authentication is also absolutely necessary for access. However, unlike the former examples, where there may be police or physical security present, the latter examples have to rely on other security measures. This is important because it makes it uncomplicated to fake one's identity and be easily verified as someone else. When people withdraw money from an ATM, they fear someone may see them entering their PIN number; this is something facial recognition can solve. If facial recognition was installed on ATMs and banking applications, having the credit card (account) number and pin, or login information, would not be enough to get access to the account. Facial recognition could also be beneficial even where physical security was in place. At border checkpoints, it would be more efficient, fast, and accurate for people to be verified through a machine rather than just by a person comparing pictures and names. This could also avoid biases, misjudgments, and unlawful profiling.

Facial recognition software is also applicable for access and entry into data centers or secured office buildings. This would limit the availability of sensitive data to only the necessary group of predetermined faces. Similar access to encrypted data could be enforced by using faces as private keys to decrypt data. Lastly, as phones and mobile devices have become omnipresent, the ability to access all of the owner's accounts and the vast amounts of information stored on the devices has become almost effortless. Android is one of the major operating systems that has been trying to perfect facial recognition technology to lock their devices. By using facial recognition to unlock a device or a specific application on the device, it not only ensures that the correct person is opening the device/application, but also allows for quick access without the need to remember anything, like a password and username [7–11].

4. Issues with Facial Recognition

Although proven to be quite helpful in systems like criminal justice, for mug-shot verification, post-event analysis, and forensics expertise, as well as securing devices and accounts, there are several issues with how facial recognition is being used today.

We have tested five different mobile applications for Android and iOS operating systems. Based on our web search we selected the most commonly used facial recognition applications. In particular, we tested True Key, FaceLock for Apps, AppLock, and Luxand Face Recognition on Android Lollipop (version 5.1), as well as BioID Facial Recognition, Luxand Face Recognition, and True Key on iOS 10.2.

Four out of the five tested applications are used to secure a phone, settings, and applications from being opened or changed by anyone other than the owner of the device. This creates access rights for an otherwise open device, so installing and implementing these applications creates read and write privileges granted to only the recognized faces. Luxand Face Recognition, however, is different because it builds a face recognition database. This section details the tested mobile applications thoroughly, and the following section outlines our tests and results.

4.1. FaceLock (Android)

FaceLock is available in a free and paid version. The free version will lock settings, Google Play store, task manager, and one application of your choice. The reason Wise Orchard, or the application developer, chose to lock settings, Google Play, and task manager is to ensure that no one can go and uninstall the application to bypass the facial recognition authentication. The "pro" version, or the paid version, allows the user to lock any and all of the applications of their choosing, with the mandatory locking of settings, Google Play store, and task manager. FaceLock Pro also allows the user to unlock the screen using their face. If the face is not recognized, a pin code or password is required to unlock the screen and all applications in both versions. However, it is not necessary to supply both the face and pin, just one or the other.

FaceLock mandates that the user takes pictures of him or herself through the app, Figure 1. These are used for "training images", and they suggest taking 10–15 different pictures in different settings and lighting. It is also suggested that one adds a training image whenever they are not recognized right away. This application uses eigenface technology to calculate and compare the training images.

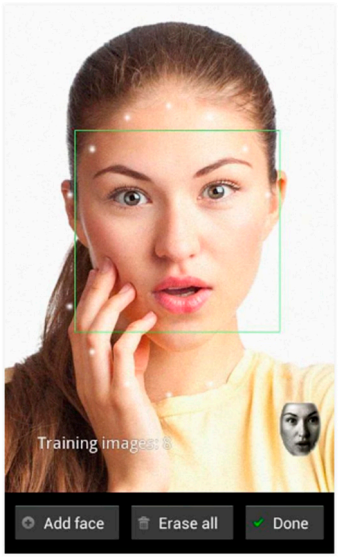

Figure 1. Taking a training image, FaceLock application download page, Google Play [12].

To take a training image, the camera opens with an oval of dots to center the face. When the face is centered properly, a green box will appear. If it is acceptably centered, the box will appear yellow, and if the face is not centered efficiently there will be a red box. If the camera does not detect a face, there will be no box. The training images are compiled and used for a template to be compared to. Once the training images are set and the user attempts to unlock an application, the screen becomes black except for where the face is to be captured, and it is the same size as the dots from the training images were calculated to be.

4.2. AppLock (Android)

AppLock is similar to FaceLock, as it allows a user to lock down applications and uses facial recognition software to unlock them. Figure 2 shows AppLock authentication page. However, unlike FaceLock, the owner of the Android device can choose the security level in which the application is locked down. There are two different levels: convenience mode and truly secure mode. These modes are based on enrollments saved to the application. After installing AppLock, it is necessary to configure the initial enrollment. In doing so, the application captures a picture of the face and the user picks one of three phrases, or a custom phrase of their own, which is recorded. For convenience mode either voice authentication or facial authentication is accepted, and for truly secure mode it is necessary to supply both the spoken phrase and face.

Similar to FaceLock, if facial recognition is not sufficient or the voice is not being recognized, a pre-setup pin can be used instead to get into the applications. Also similar to FaceLock, a square appears on the screen to guide where to place and center the face to be recognized. This application uses the normal face for face metric recognition.

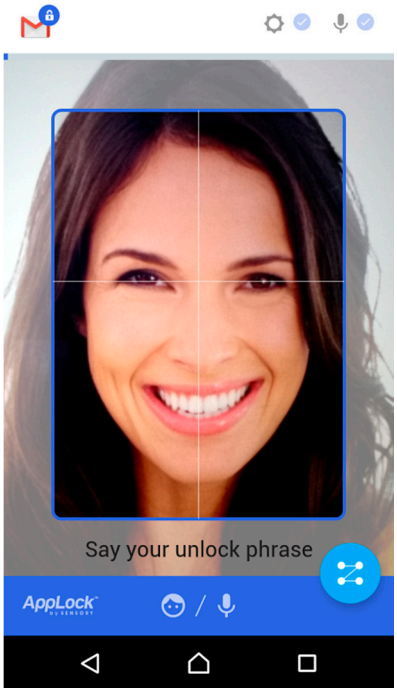

Figure 2. AppLock authentication page [13].

4.3. Luxand Face Recognition (Android and IOS)

Luxand Face Recognition is different from the other applications tested. This is a recognition application, but not an authenticator so much as a verifier. To identify and introduce the person to the application, it is necessary to click "tap to name" and type in the name you want the person to be identified as [5], Figure 3. One presents a face, and gives it a name. When the application sees this face

again, it will display the name that you originally gave. In a way, it is creating a facial recognition library. This library is created by using the camera function enabled through the application. The application notices a face and will show a box around the face using the normal face metric technology. If the face is recognized and matches a pre named face, it will name the face. Otherwise, the user clicks on the face and can type in the name it belongs to. If the application matches the face with the wrong name, modification is possible by clicking again on the box and typing in the correct name.

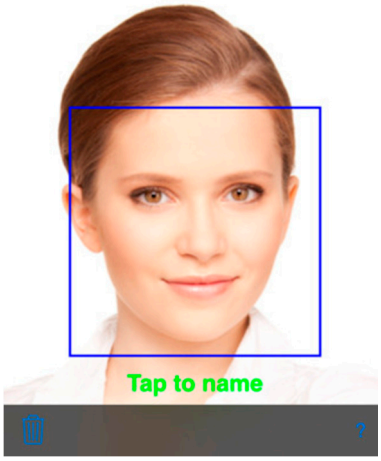

Figure 3. To identify and introduce the person in Luxand [14].

The Android application allows for the front and back cameras to be used to detect faces. The iOS version only allows for the front facing camera to be used.

4.4. True Key (Android and IOS)

True Key, created by Intel Security, uses eigenface technology to authenticate a user. It is available on mobile devices, laptops, and desktops. This application stores passwords and usernames to popular websites and applications, like Facebook, Gmail, Netflix, Starbucks, and many more. Android systems allow for the application to be present on all login pages of previously installed applications. If there is a username and password stored in True Key for the application, it will push it to the app. IOS systems allow for True Key to be easily accessed from web browsers to copy and paste the username and password into the correct fields [15].

The application can also create safe passwords, store passports, driver's licenses, credit cards, membership cards, and social security numbers. It encrypts this information and scrambles the provided passwords using the AES-256 algorithm. The data is decrypted once the user is authenticated by a recognition method using the face, fingerprint (depending on the device), or master password. The "basic security" level would be access into the application (and therefore to the applications that have stored usernames and passwords on True Key, and sensitive personal information) using only one of the recognition methods, whereas "advanced security" is a combination of two of the three methods. All information stored in the application is stored locally on the device. However, it is possible to set up more than one trust device, and the information is encrypted when being transferred during the sync process [15].

4.5. BioID Facial Recognition (IOS)

BioID is available on all iOS versions for iPhones and iPads, but only some Android versions and devices. The application is similar to True Key, where it uses facial biometric authentication to log into other applications and services. BioID, Figure 4, uses normal face metric technology, but needs a "liveness factor" to authenticate. The nodding or moving of the head is necessary to authenticate a person. They developers did this to prevent the entry of an adversary by displaying a picture or video.

Figure 4. Taken from the BioID facial recognition application download page from the iTunes App Store [16].

4.6. Galaxy S8

The Samsung Galaxy S8 offers a set of different features for authentication. In addition to the traditional PIN, the new device includes fingerprint recognition, facial biometrics, and iris scanning, which previously debuted on the Galaxy Note 7. Face scanning is used by taking a photo of your face when attempting to unlock the device, matching the known details of your face to the photo. Iris scanning, on the other hand, is considered to be more secure and supposedly impossible to recreate. This iris scanning uses an infrared sensor and front facing camera.

These additions to the Galaxy S8 makes users feel more safe and avoids the complication of deciding on the most secure facial biometric application to use [17].

5. Testing and Results

The testing methodology that we developed is shown in Figure 5.

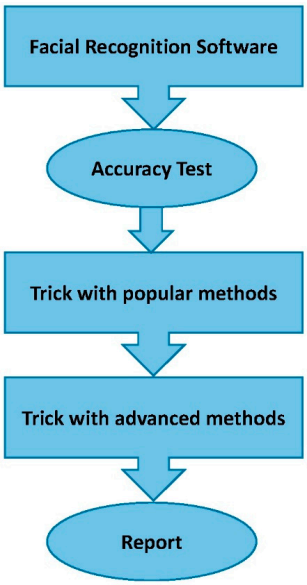

Figure 5. Testing methodology.

We tested the above applications by installing and setting up the applications as specified in the developer's instructions. We tested them all for accuracy before trying to trick the system. All of the applications were able to correctly identify Subject 1 and Subject 2 as themselves. However, Luxand Face Recognition would identify Subject 1 as themself half of the time and depended greatly on the lighting.

Next, we tried to trick each of the applications with seven different strategies. At first, we used: printed picture, electronic picture, and a video of Subject 1, these are the most popular techniques to trick facial recognition software [18]. Secondly, we used advanced techniques to trick the applications including: a printed picture of Subject 1 with contacts, having someone who looked like Subject 1 use the app, and displaying a printed and electronic picture of someone who looked like Subject 1 were all tested against the applications. These strategies are methods that have not been fully tested or explored often in the past.

Each of the five applications tested were tricked at least once by one of the test methods. Each application is marked with a "yes" or "no". The "yes", colored with green in the tables, signifies that the application verified the method and gave access to the application and information locked. A "no", colored with red in the tables, is marked if the application did not verify or grant access in ten attempts. The Yes/No, colored with orange in the tables, indicates that the application verified the method few times and gave access to the application. The results of these tests are illustrated in Tables 1 and 2 for Android and iOS, respectively.

The Galaxy S8 was tested by Subject 2. It recognized Subject 2's printed and electronic images for both the facial recognition lock and the iris recognition. However, the device was not tricked by using a picture of someone with similar features. The results of this test are as illustrated in Table 3.

Table 1. Results on Android Lollipop, version 5.1.

Android	True Key	Luxand Face Recognition	Face Lock	App Lock
Subject 1	Yes	Yes/No	Yes	Yes
Printed Photo Of Subject 1	Yes	Yes	Yes	Yes
Electronic Photo Of Subject 1	No	No	Yes	Yes
Printed Photo Of Subject 1 with Contacts	Yes	Yes	Yes	Yes
Video Of Subject 1	No	No	Yes	Yes
Someone Else	No	No	No	Yes
Printed Photo Of Someone Else	No	No	Yes	Yes
Electronic Photo Of Someone Else	No	No	Yes	Yes

Table 2. Results on IOS 10.2.

IOS	True Key	Luxand Face Recognition	Bio ID
Subject 1	Yes	Yes/No	Yes
Printed Photo Of Subject 1	No	No	No
Electronic Photo Of Subject 1	Yes	No	No
Printed Photo Of Subject 1 with Contacts	No	No	No
Video Of Subject 1	Yes	No	Yes
Someone Else	No	No	Yes
Printed Photo Of Someone Else	No	No	No
Electronic Photo Of Someone Else	No	No	No

Although not the most reliable application, as it had trouble identifying Subject 1 as herself 100% of the time, Luxand Face Recognition is the most secure of the tested applications. The second most trusted application is True Key, by Intel Security, a recognized and respected security company. The application was tested on both Android and iOS systems. The results from testing vary in regards to system even though each device was shown the same printed picture, electronic picture, and video. Most importantly however, True Key did falsely authenticate on both systems.

Table 3. Results on Galaxy S8.

Galaxy S8	Face Recognition	Iris
Printed Photo of Subject 2	Yes	Yes
Electronic Photo of Subject 2	Yes	Yes
Printed Photo of Subject 2 with Contacts	Yes	Yes
Video of Subject 2	Yes	Yes
Someone Else	No	No
Printed Photo of Someone Else	No	No
Electronic Photo of Someone Else	No	No

It is evident from our testing that IOS facial recognition applications are more secure than the applications offered in the Google Play store for Android devices. We conclude this because all of the applications tested on Android fell for the printed picture, both with and without contacts, whereas none of the IOS applications authenticated a printed picture. Additionally, half of the Android applications falsely authenticated an electronic picture versus only one-third of the iOS applications validating this method. Pictures are found very easily through Google searches and social media, and printing can be done by anyone for a fee or shown electronically through another device, like a cell phone, tablet, or computer. All of the applications tested, for both Android and iOS, claim to be secure and unable to be cracked using video or pictures, which as one can conclude from the results, is simply not true [12–16].

6. Conclusions

Governments have put in a significant amount of resources in order to develop facial biometrics and have begun to implement them for day-to-day use. Biometrics have had a positive impact on border crossing at airports, identifying fugitives and criminals, and with the right development, can also be implemented in banks, shops, and many other offices. Facial biometrics can easily save those in danger if used in the right way, leading us to believe that the development of facial biometrics is critical and will continue. However, the growth of this technology is completely dependent on the security measures in place to ensure that privacy is protected and accuracy is exact. In order to do so, authentication needs to be precise.

Authentication can be divided into three methodologies: something you have, know, or are. Something you have is a card, token, or key, which can easily be stolen. Something you know is a PIN or password, which in today's world can easily be hacked, and something you are is a biometric. Requiring all three would give the highest level of security [2]. It is evident from our results after testing several applications that using a password and biometric recognition alone is not enough. By utilizing all three authentication methodologies, people using applications that secure personal information, settings and preferences, bank information, account information, and so much more can be fully confident that their data is safe and private.

Author Contributions: M.G.G. and S.A.S. contributed equally to this paper, they conducted the experiments, reported the results, and wrote the paper. T.H. supervised the project and provided guidance on the work and throughout the paper.

Funding: Fordham University, Faculty Research Program.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Pankati, S.; Bolle, R.M.; Jain, A. Biometrics: The Future of Identification. *Computer* **2000**, *33*, 46–49. [CrossRef]
2. Woodward, J.D., Jr.; Horn, C.; Gatune, J.; Thomas, A. *Biometrics: A Look at Facial Recognition*; RAND Corporation: Santa Monica, CA, USA, 2003.
3. Gates, K.A. *Our Biometric Future. Facial Recognition Technology and the Culture of Surveillance*; NYU Press: New York, NY, USA, 23 January 2011.

4. Joshi, J.C.; Gupta, K.K. Face Recognition Technology: A Review. *IUP J. Telecommun.* **2016**, *VIII*, 53–63.
5. Bhattacharyya, D.; Ranjan, R.; Alisherov, F.; Choi, M. Biometric Authentication: A review. *Int. J. u- e-Serv. Sci. Technol.* **2009**, *2*, 13–27.
6. Chabrow, E. Facial Biometrics Pose Privacy Woes: Lack of Consent Bothers Privacy Advocate Beth Givens. Available online: http://www.bankinfosecurity.com/interviews/facial-biometrics-pose-privacy-woes-i-1231 (accessed on 20 June 2018).
7. Snelick, R.; Uludag, U.; Mink, A.; Indovina, M.; Jain, A. Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems. *IEEE Trans. Pattern Anal. Mach. Intell.* **2005**, *27*, 450–455. [CrossRef] [PubMed]
8. Ohana, M.; Dunkelman, O.; Gibson, S.; Osadchy, M. HoneyFaces: Increasing the Security and Privacy of Authentication Using Synthetic Facial Images. Cornell University. Available online: https://arxiv.org/abs/1611.03811 (accessed on 20 June 2018).
9. Mardikar, U. Systems and Methods for Authenticating Facial Biometric Data against Secondary Sources. U.S. Patent 20170091533 A1, 30 March 2017.
10. Traoré, I.; Nakkabi, Y.; Saad, S.; Sayed, B.; Ardigo, J.D.; de Faria Quinan, P.M. Ensuring Online Exam Integrity through Continuous Biometric Authentication. In *Information Security Practices*; Springer: Cham, Switzerland, 2017; pp. 73–81.
11. Chowdhury, M.; Gao, J.; Islam, R. Fuzzy rule based approach for face and facial feature extraction in biometric authentication. In Proceedings of the 2016 International Conference on Image and Vision Computing New Zealand (IVCNZ), Palmerston North, New Zealand, 5 January 2017.
12. Google Play. FaceLock. Available online: https://play.google.com/store/apps/details?id=com.facelock4apps&hl=en (accessed on 20 June 2018).
13. Google Play. AppLock. Available online: https://play.google.com/store/apps/details?id=com.domobile.applock&hl=en (accessed on 20 June 2018).
14. Luxand. Luxand Face Recognition. Available online: https://www.luxand.com/apps/facerecognition/ (accessed on 20 June 2018).
15. Intel Security. True Key. Available online: https://www.truekey.com/ (accessed on 20 June 2018).
16. Apple Itunes Application Store. Bio ID. Available online: https://itunes.apple.com/us/app/bioid-facial-recognition-authenticator/id1054317153?mt=8 (accessed on 20 June 2018).
17. Bader, D. The Galaxy S8 Has Face Recognition and Iris Scanning, and You Have to Choose One. 3 April 2017. Available online: https://www.androidcentral.com/galaxy-s8-face-recognition-iris-scanning (accessed on 20 June 2018).
18. Xu, Y.; Price, T.; Frahm, J.-M.; Monrose, F. Virtual U: Defeating Face Liveness Detection by Building Virtual Models from Your Public Photos. In Proceedings of the 25th USENIX Security Symposium (USENIX Security 16), Austin, TX, USA, 10–12 August 2016; pp. 497–512.