SOCIETY’S NEED FOR BIOMETRICS: THE IMPORTANCE OF FACIAL RECOGNITION

Kayla Banks, klb231@pitt.edu, Sanchez 3:00, Jordan Bradley, jeb342@pitt.edu, Balawejder 5:00

Abstract— All the latest models of phones, laptops, and other similar gadgets have implemented biometrics into their security systems. Biometrics systems analyze biological data to identify an individual based on its unique characteristics, making it a better option than simply entering a password or signing one’s name. Whether it be for security purposes or for the convenience of global consumers, facial recognition has gained credibility as one of the higher-quality biometric technologies available to our society today. It has become increasingly relevant in the lives of consumers all around the world, from entrepreneurs, to teenagers, and to engineers.

Facial recognition software uses a series of scanners designed to detect and store data for 80 different nodal points on an individual’s face, while ideally being able recognize said individual through changes that may occur such as putting on glasses or weight gain. In order to know if facial recognition is a good investment of one’s money and interest, the workings of facial recognition must be analyzed. Modern day examples can offer insight into the strengths and weaknesses of the software, such as accuracy levels and concerning privacy issues, ultimately allowing for a conclusion on whether facial recognition is worth the investment.

Key Words— Biometrics, Facial Recognition, Mechanism, Modern Technology, Technological Innovation

BIOMETRICS: WHAT ARE THEY AND HOW DO WE USE THEM?

The turn of the 21st century was a pivotal time for many different aspects of our society, and technology arguably became one of our most important innovations. Technology has provided unlimited access to information about ourselves, each other, and the world as a whole, which consequently calls for higher levels of security in order to prevent fraudulence. Biometric technology is one of the most reliable security systems being used in today’s society. Commonly utilized in a plethora of ways for modern technology, biometric software is considered to be efficient and accurate, which aids in making it one of the most appealing options for companies and consumers.

Biometrics are, according to Biometrics Research Group Inc., “…the processes by which a person’s unique physical and other traits are detected and recorded by an electronic device or system as a means of confirming identity. The term ‘biometrics’ is a derivative of the word ‘biometry,’ which refers to the statistical analysis of biological observations and phenomena.” [1]. Biometric software consists of a series of scanners designed to detect and store data from specific nodal points on a user’s face or body. The stored data is then compared with the features of the user, whose identity is confirmed if the data matches closely enough. Biometric identification, when implemented correctly, is unique to each individual human being, making it more reliable than using only an identification card or a password that could potentially be stolen.

Early Biometric Technology

Although the use of biometrics in technology spiked around the late 20th century, the practice of using biometric identification has been dated as far back as 500 B.C. Ancient societies have always used the face as a way to identify one from another; it’s simple human nature. However, archaeologists have found handprints marked next to paintings in caves estimated to be around 31,000 years old and have surmised that it was their way of signing their work with an “unforgettable signature.” Additionally, Chinese merchants and Egyptian traders are also known to have used fingerprints to document their transactions and exchanges. [2].

By the 1800’s, the industrial revolution called for a need to formally identify people, as the world population was growing too rapidly to continue using faces, memory, and paper-documented-fingerprints for identity...
confirmation. As a result, William Herschel developed the first system for recording handprints in 1858. The use of systemic identification gained popularity quite rapidly. Upon seeing the system in use, people began working towards making it as efficient as possible, creating fingerprint classification systems for easier management [2].

The method of fingerprint identification inspired others to search for different and more advanced methods that would maintain reliability and accuracy. In 1938 the first example of this was brought to light by an ophthalmologist who proposed the idea of using the iris for identification. From there, scientists worked to innovate biometric software and automate the methods they were using; the results were automated fingerprint identification and signature systems, speaker recognition, and eventually iris and facial recognition as well [2].

These new branches of biometrics have each been uniquely implemented and improved upon over the last 30+ years, especially since the terrorist attack on the United States on September 11th, 2001. The innovations have reached a point where each branch has its comparative strengths and weaknesses that may make one seem more appealing than another, depending on the situation. Facial recognition, especially, has become increasingly popular over the past year and a half, as it has been more thoroughly exposed to the public population. Major corporations, such as Apple, have been incorporating the software in their modern devices as a primary selling feature.

Nevertheless, with any increase in popularity comes constant criticism; some people who have used facial recognition have reported back with serious glitches, and others have been unable to find a single flaw. The contradiction among the reviews brings a level of uncertainty to the table, leaving consumers hesitant to incorporate the technology into their lives. For specific, complex career fields such as engineering, the integrated technologies have to be of very high quality and strength ensure that important processes and projects are done correctly. Understanding facial recognition is the key to knowing whether or not this biometric is reliable or not. People rely on biometric security to protect everything from their text messages to their bank account and homes; if we, as a society, are going to put all of our trust into this method of protection, it is important that there is firm evidence that the software will do exactly what it is designed to do.

**WHAT IS FACIAL RECOGNITION?**

The main function carried out by facial recognition software uses the miniscule differences in an individual’s face to connect a device or account to its user with a series of scanners. Ideally, the software is able to recognize and scan faces in less practical situations as well, such as if an individual decides to put on glasses or if the lighting is against your face. As time has passed, facial recognition has slowly gained its credibility, being considered reliable and safe by the majority. But every great invention has had their trial and error; because of a limited access to the technology and resources needed to carry out the desired functions, the software was not always as efficient as it proves to be now.

**Origins of Facial Recognition**

In the 1960’s, Woodrow Bledsoe, Helen Chan Wolf, and Charles Bisson developed the first automated facial recognition program [3]. According to an article published by FaceFirst, they managed to develop a system that could use photos of faces and categorize and compare them to the images of human individuals. The article states:

> “Bledsoe developed a system that could classify photos of faces by hand using what’s known as a RAND tablet, a device that people could use to input horizontal and vertical coordinates on a grid using a stylus that emitted electromagnetic pulses. The system could be used to manually record the coordinate locations of various facial features including the eyes, nose, hairline and mouth,” [4].

The information gathered was then run through a database and stored, so when the system retrieved a new image, they could match it to the stored data that most closely resembled the new image. Even though facial recognition still had to be completed manually at the time, this was a very important step in the software’s development. This was as far as one could go with such limited knowledge of and access to technology, and in spite of their restrictions, Bledsoe and his team were able to use machinery to do what the human mind was incapable of doing.

**LIMITATIONS AND ADVANCES**

From this point, scientists and technologists worked to improve what Bledsoe had developed, trying to find ways to increase the accuracy and efficiency of the system. The next version of facial recognition went from only using images to using facial markers, implemented to help the system detect specific features and nodal points on said images. From there, scientists tried to figure out how facial recognition could be carried out without any manual input. A few were able to bring their ideas to life, but the majority of prototypes tested unsuccessfully. The path towards perfecting facial recognition has been a long one, and much to our
society’s dismay, we still have not found the perfect system. However, each setback that technologists faced throughout the process allowed for them to improve, bringing us closer to a flawless algorithm with each failure.

The first set of limitations were found in Bledsoe’s original facial recognition system. Not only did the system require a great deal of manual input for its operation, but it was not specific enough to be considered efficient or reliable. While Bledsoe and his team created a strong foundation for the technology, their system could not differentiate one face from another. The scanners could only detect the general features of a face, such as eyes, a nose, and ears; it was not capable of analyzing smaller details that make individual faces unique from one another.

Throughout the 1970’s, in order to improve Bledsoe’s innovations, new algorithms were being modified to fill in the gap between facial recognition and facial differentiation that Bledsoe’s version failed to do. Software developers Goldstein, Harmond, and Lesk were able to incorporate different markers into the software that differentiated between hair color, lip thickness, and other minute details of the sort. Although they made significant advances, the measurements and color differences still had to be manually computed. [4]

In 1988, the Lakewood Division of the Los Angeles County Sheriff’s Department attempted to make use of the new software as well. They created a system that could take mugshot images and categorize them, which would have made it easier to track and identify their inmates. Their system, however, was too complex for its purposes, as it attempted to record too many different nodal points that were not necessary for identification. To combat this, coders M. Kirby and L. Sirovich, managed to add a linear algebraic system that allowed for a smaller quantity of measurement values to be able to carry out the same functions and differentiate one face from another.

In the early 1990’s, Matthew Turk and Alex Pentland worked towards creating a physiologically and informationally theoretical method for tracking an actual human face instead of an image, still using the two-dimensional aspects of the face as it is usually upright and facing forward. Their theory proposed that a system could calculate eigenvectors (defined as a vector that when operated on by a given operator gives a scalar multiple of itself) found on both stored images and live human faces. The eigenvectors would then be compared to each other projected onto a face space. The distance between the vectors determined whether or not an individual would be identified, as shown in Figure 1 [5].

In the figure, the two eigenvectors (u) were close enough to potentially match with three different individuals in their system:

![FIGURE 1 [5] Projection of eigenvectors onto face space](image)

Although their eigenvector theory was too expensive and technologically advanced to be physically implemented, Turk and Pentland opened the door to the possibility of completely automated facial recognition. This possibility quickly became a project that the government took great interest in. In 1993, the Face Recognition Technology (FERET) program, sponsored by the Defense Advanced Research Products Agency (DARPA), was initiated by government officials. The program hoped to promote the development of algorithms and processes that would embody this theory. [4]

The modification and simplification of facial recognition algorithms paved the way for extensive testing by the U.S. Government, mostly unbeknownst to the public. One example of this took place in 2002 during Super Bowl XXXV. Government officials used cameras in the Tampa Bay Stadium to scan the faces in the audience, hoping they could find wanted criminals using facial recognition to match them to their mugshots [4]. This attempt in particular was a failure, along with many others tests of similar nature. The Facial Recognition Vendor Tests are another example of the government tests on the software. Such tests were created and ran throughout the 2000’s as a result of desperation. Since there was no progress towards improving the software, the government started running these tests to evaluate the workings of the software and create different prototypes, hopeful that they could pinpoint the problems and devise a solution. They also hoped that upon seeing so many proposals and prototypes, other technologists and scientists would be inspired to work on the project as well, ultimately speeding up the process.

With the new information these tests provided, by 2008, the U.S. government was able to begin working on a new database that could apply biometrics differently. This database utilized facial scanners as well as other biometric systems as a means to categorize and identify people. The database proved to be of quality and eventually aided the government in terrorist identification. In fact, according to FaceFirst, it was able
to "identify the remains of Osama bin Laden with 95% certainty." [4]

The use of facial recognition software evolved from its place in government affairs to widespread commercial use when social media spiked in 2010. This brought the software usage to the light of the public, causing more and more companies such as Samsung and Windows to attempt to integrate the software into their devices, including the Google Smartphone in 2011 or the XBOX Live [6]. The software has been significantly improved since then, as it has gone through many tests for continuous debugging and reconfiguration.

Unfortunately, throughout the entire process, there were overarching problems that remained unsolved. For example, there was a very strong racial bias that did not consider the diversity of the human population. The images and prototypes used to formulate the facial recognition software were all based around the facial structure of Caucasian males; scientists did not account for the fact that although Caucasians were the majority, their facial features can differ incredibly from those of people with different, more complex racial backgrounds. The calculations used to build the software only included the similar measurements of one specific group, thus the systems’ scanners did not have the range to detect faces of different shades and structures. This unfortunately has prevented the growth and usefulness of facial recognition in different societies.

Additionally, technology in the 20th century was a very limited resource that not many had the privilege or financial means to access. The lack of knowledge on the topic, let alone the low-quality cameras available at the time, stopped the advancement of the project and left many proposed ideas to become nothing more than theoretical concepts. But even so, the progress that has been made is enough for the public to trust its accuracy and dependency. Today, the software is very commonly implemented in our everyday lives, in many ways that most people do not even recognize.

**FACIAL RECOGNITION TODAY**

The latest algorithm for facial recognition software has proven to be quite versatile and efficient. Although each software used by a different company is not identical to the next, each version functions in generally the same manner. The software combats almost all of the issues that technologists were previously faced with, which has consequently opened the door for a greater number of uses and created a much wider attraction to this method of security. Today there are two different versions available and in use, although one is proven to be much stronger than the other.

According to an article written by *Time Inc.*, the first-generation version of the software relies solely on the distances between the features on one’s face, similar to taking a quick snapshot and recording the measurements. The article explains this minimally, saying, "The other method used by this first-generation software looks at points of interest on the face and tracks how the pixels in a photograph cluster to form a nose...matching a face is similar to matching a fingerprint,” [7]. They explain that the goal of the software is to find how closely certain characteristics line up to match with the stored data. Nevertheless, a full-frontal picture of a face and good lighting is necessary to compare your “faceprint” and effectively use this version of the software. [7]. Another article on *Ex-Sight* explains the first-version as well, stating that an individual face is analyzed in real time by using a digital video camera to take measurements between the landmarks on the face. Figure 2 provides a visual representation of the process, showing vectors that are measured to find between nodal points:

![FIGURE 2 [8]
Distance between nodal points measured by facial recognition software](image)

Although the human face has 80 different nodal points that could each be used for measurement, the software does not require data from each one. Instead, it only measures a few, such as the distance between the eyes, the width of the nose, the depth of the eye sockets, the shape of the cheekbones, and the length of the jawline. These measurements are then compared to the average measurements obtained from the initial scans used to set up the software—if the measurements are close enough, the face is confirmed as a match [9].

While this method of the software successfully compares human faces to the stored images in its database, there are still many factors that could affect its accuracy. Many believe that there are too many factors; the 21st century is focused on immediate access to everything, and this version of the software unfortunately does not accommodate to users who may be in a less-than-favorable setting.

Technologists therefore wanted to create a stronger version of facial recognition—one that could find and match your face even in partial lighting or without being
completely faced forward. Their innovation resulted in a second, stronger algorithm for the software. This version of facial recognition takes four components—a camera, a facial template, a database, and an algorithm to compare images—and uses them to carry out the functions with much more flexibility than the first-generation software. Figure 3 breaks the process down into a step-by-step explanation:

**FIGURE 3 [10]**
Step by step description of a basic facial recognition software’s process

As stated in a report published by the United States Government Accountability Office, this version of the software is able to perform more functions than the first-generation version with greater accuracy. The process does take similar steps to the first-generation software to complete these functions, but nevertheless, the newer software is still more flexible and more accurate in overall comparison. First, the facial recognition system analyzes the patterns found in an image or video and compares it to a generic face model to determine whether or not a face is even present. Once a face has been detected, the system proceeds to create a faceprint in one of three ways.

One option is a geometric approach; the system quickly calculates the location, area, and spatial relationship between the features found on the face, very similar to the first-generation software previously mentioned. The second approach uses a photometric effect that employs ultrasound technology to detect or identify a face as a combination of different facial structures and features. Thirdly, the software may complete a skin-texture analysis, capturing specific yet unique placement of the fine lines, pores, and spots that may appear on an individual’s face. The software will often incorporate more than one of these methods to create a faceprint, as accuracy improves when each method is used concurrently [11].

Following the creation of the faceprint, the software could carry out many different functions. The report published by the U.S. Government Accountability Office further explains what these functions are, stating that it can, "1. detecting a face in an image; 2. estimating personal characteristics, such as an individual’s age, race, or gender; 3. verifying identity by accepting or denying the identity claimed by a person; and 4. identifying an individual by matching an image of an unknown person to a gallery of known people." [11]. These functions proceeding the creation of the faceprint are illustrated through the flow chart in Figure 4:

**FIGURE 4 [12]**
Flow chart describing the creation of the faceprint

Since the second software does not rely solely on distances measured along the face, it can still be used in less ideal situations, even without the entire face being present in a scan. The versatility partnered with the accuracy of the software makes it the most appealing option to fulfill our society’s wishes. In fact, this version of the software has gained a lot of positive attention from companies such as Facebook, Microsoft, and Google, as they are looking to adapt the software to help collect data on their users. This allows these companies to provide services such as image-matching and enhanced login security.

**Different Models**

Because the newest version of the facial recognition algorithm can be used for so many different analyses, it has been adapted in many ways beyond its original security/identification purposes. In today’s modern society, facial recognition is used so often that one can barely even recognize that they are using it. The first instance that brought the use of facial recognition to the
public light took place in 2010; notably, Facebook was one of the first companies to demonstrate a successful example of its usage. They began implementing the software to tag people in photos with one another, and in some instances, the social media site was automatically able to match an image to a user's profile. Likewise, in 2016, Snapchat adopted the facial recognition software, which quickly became and remained as an essential part of the application’s popularity. Snapchat released an update that allowed for its users to scan their face and apply different filters, using a facial template to line up the features on the user's face with the designated areas on the filters. The filters used distortive properties to change the appearance of the user on camera, allowing users to enhance their pictures and selfies for comical and/or aesthetical purposes [13]. This Snapchat update resulted in an astounding increase in their user numbers and market values, and most users do not even realize that the filters are a form of facial recognition software.

Apart from social media, many companies have started using facial recognition software as well, whether it be for the use of the company or the convenience of the consumers. For instance, casinos use the biometric technology to track their traffic and see who comes in and out. They also use it to catch card counters and identify the faces involved in other illegal activity. Eyeglass companies such as Glasses USA and Warby Parker have adopted facial recognition too, using it to allow their customers to "try on" glasses from the comfort of their own home. This works similarly to the way Snapchat uses its filters; they use a template to locate the features on the user's face and line it up with the glasses the user selects, then places the glasses over the eyes as if the user had them on.

Today's most popular implementation of facial recognition by far is Apple's latest release, the luxurious iPhone X. With this phone, Apple has completely abandoned its previous use of fingerprint identification and now uses facial recognition to allow users access to their devices and accounts. According to IDG Communications Inc., the iPhone X has a series of sensors that form Apple’s True Depth camera system. An infrared camera, a flood illuminator, a regular camera and a dot projector all work together to do what any strong facial recognition software will do [14]. The flood illuminator shines the infrared light to scan one’s face through whatever accessories he/she may have on and/or in different lighting conditions. The dot projector then shines over 30,000 small points of light onto the user’s face to help scanners detect the different points of depth and dimension; Figure 5 shows an example of a faceprint that was created from the iPhone X scanning process, clearly illustrating depth and dimension.

![Figure 5](image.png)

**FIGURE 5 [15]**

*iPhone X facial recognition perceives depth and dimension for faceprint*

After the initial steps, the software proceeds to carry out the functions that any facial recognition software would; a facial template is created, stored, and matched to users with the cell phone’s camera. Although facial recognition has been seen in Samsung devices such as their Galaxy cell phones, Apple claimed to have made groundbreaking improvements to the software, giving their version its own patented name, Face-ID. But even so, these improvements are only accredited to the more detailed scanning process in the beginning. The steps that follow the initial Face-ID scan are completed in the same manner as any other standard facial recognition software.

**Accessibility**

Facial recognition software does not only provide extreme convenience for its users and the companies that implement it, but most cases have proven that the software is a good investment. For example, according to Gizmodo, the FBI has just recently completed their Next Generation Identification (NGI) system, which will not only incorporate facial recognition software, but will be able to scan tattoos, birthmarks, and other seemingly minor details as well. The system was designed to more efficiently and effortlessly convict criminals that are caught on NGI cameras. It took close to six years and cost over $1 billion to complete. Nevertheless, the government is expected to make at least three times as much in revenue once the system is installed, as it will minimize the costly efforts needed to identify a criminal on camera [16]. Other companies have also made much higher profit after the adoption of facial recognition software, with Snapchat posing as an example. The quantity of daily users has spiked tremendously since the creation of Snapchat Filters, allowing them to increase the price of advertisements and thereby making Snapchat more money per user.
Another prevalent example of modern day facial recognition is the iPhone X. Retailing for $1000 (before the additional costs of storage and data), it is the only Apple product that uses facial recognition for security so far. The iPhone X is without a doubt considered a luxury; it is the most expensive iPhone that Apple has released. Nevertheless, the public was very excited to get their hands the product; Apple sold 11.2 million iPhone X’s in the first two weeks.

Although these prices may be reasonable for big-name companies and upper-middle class civilians, the majority of the human population does not fall in these categories. Additionally, as of December 2017, only 54.4% of the world’s population has facial recognition access in some form, with the majority of these users residing in first world countries [17]. This draws the conclusion that facial recognition is only moderately accessible, just as other forms of technology are. For large companies and corporations, the software is affordable and usually proves to be a smart investment. Facial recognition is accessible to anyone with access to laptops or smartphones through apps such as Snapchat or companies’ websites like Warby Parker’s. However, having your own facial recognition system for your home security or within the expensive iPhone X for example is not feasible, especially if you are part of the near 80% of people below the upper class [17].

Persisting Concerns

With every new technological innovation, there is controversy regarding its pros and cons. And while the pros of facial recognition tend to outweigh the cons, there is still a large number of consumers that are weary of the innovation. The question of privacy has been up in the air since biometric technology first surfaced, as users are concerned that their fingerprints and faces are being stored by the companies that scan them for secretive uses. Also, according to the U.S. Government Accountability Office (GAO), a number of federal agencies, privacy and consumer groups, and industry representatives have managed to identify different privacy issues that come with facial recognition. An article published by the GAO mentions this while referencing the topics of the accuracy of the software and the large quantities of tagged images on social media. Their article states:

“The convergence of these two trends may make it technically feasible one day to identify almost any individual in a wide range of public spaces, according to some privacy advocacy organizations and others. Key privacy concerns related to the commercial application of facial recognition technology have generally centered around (1) its effect on the ability of individuals to remain relatively anonymous in public; (2) the capacity to track individuals across locations; and (3) use of facial recognition without individuals’ knowledge or consent.” [11].

The ability for companies to use facial recognition to record their traffic and take statistics on their customers has been considered a benefit of the software’s existence. However, for the majority of the time that companies are taking collecting the biometric data, consumers have not given their consent for them to do so and are often not aware that it is happening [11]. This is especially so with the common use of security cameras; the wide-spread usage of both closed-circuit television based (CCTV) and network-based (IP) security camera systems can leave the public in the dark about whether their visage is being stored for future analysis. As of May 2017, there are only three companies that have laws preventing companies from collecting biometric data without consent: Illinois, Texas, and Washington [18].

To our society’s relief, companies such as Apple have claimed that they do not store biometric data in their company-wide database. Apple contends that a unique facial template is stored in each individual device and is used for comparison and identification, but this template is never relayed back to Apple and does not have the ability to recreate the image of your face.

MOVING FORWARD

While some of the limits of facial recognition are still unknown, technologists have been making predictions on what society can expect from the technology in the next few years. According to The Technology Review, provided by Massachusetts Institute of Technology, many different companies have already started building off of the modified facial recognition software that Apple produced, in hopes to eliminate any apparent lagging or inconsistency reported by customers. Their article on the future of facial recognition talks about this briefly, saying, “It could also lead more companies to add similar three-dimensional facial-recognition technology into their phones, either by trying to cram all the hardware for it into their own phones, or by using software-based facial recognition from a company…” [19].

Additionally, while there have still been reports on racial bias and accuracy for the latest versions of facial recognition software, technologists are working hard to find ways to take measurements and determine how often these errors take place and why. Furthermore, as the facial recognition software continues to be modified and improved upon, technologists are using the same methods to produce and/or modify the existing software for other biometrics such as iris recognition [19]. The future for any technology is always focused on
advancement, whether it is by means of accuracy, efficiency, or availability, and facial recognition is no different.

IS FACIAL RECOGNITION WORTH IT?

The future of facial recognition is not well defined as it seems that there are future innovations that can complement current biometric capacities. But, one thing is for sure, with the speed of technology innovation and increased frequency and use of features for the purposes of convenience, security, and data collection, it can be expected that there is a solid future for facial recognition. Consumers and companies will continue to evaluate the benefits and disadvantages of facial recognition for its desired purposes from an individual’s perspective. From this point, it is safe to assume that there will be improvements and new uses for the software coming soon, such as more privacy for the consumer or less expensive versions of the software. The specific details and possibilities depend on society’s feedback to the current models in use today, but nonetheless, the collective benefits such as ease of access and versatility firmly suggests that facial recognition technology may be worth the future efforts.

SOURCES


Banks, Bradley


ADDITIONAL SOURCES


ACKNOWLEDGEMENTS

We would like to thank Professor Prymus and our co-chair Kevin Schaeffer for providing such helpful feedback throughout the process of writing our paper. We would also like to acknowledge our parents, specifically Mrs. Bradley, for taking the time to review and comment on our paper as well.