Biometrics: A Security Perspective

West Chester University of Pennsylvania: Department of Computer Science
Sean Berlin, Holly Bostwick, Alexander Burns, Emily Maneri

Introduction

Biometrics is a form of one's physical identification. It has existed for many years. Biometrics, without technology, began by using paintings, which helped to identify an individual. Today, we use identification cards with a picture of the individual. However, other forms of biometrics are used daily. In law enforcement, fingerprints are commonly used to identify an individual, as well as photos of an individual, also known as a mugshot. Today, biometric technology reformed the world. It is used as a replacement for a password, where one can log into their smartphone or laptop using facial recognition or a fingerprint scan.

Biometric data is the future of passwords. Its use is skyrocketing; according to an Imageware survey, over 75% of Americans used biometric technology, which includes facial recognition or fingerprint scans (2021). Most modern cell phones include a fingerprint scanner or a facial recognition scanner to conveniently unlock the cell phone. Tablets, laptops, and desktops are also built with biometric hardware. As biometrics' use is increasing, it raises some questions in terms of security. Biometrics is user-friendly, but is it security friendly?

As the security component of biometrics may or may not raise some concerns, it also raises some questions about what exactly is biometrics, and what it does. Biometrics, according to Liu et al, is:

> "a general term used alternatively to describe a characteristic or a process. As a characteristic: the measure of a biological (anatomical and physiological) and/or behavioral biometric characteristic that can be used for automated recognition. As a process: automated methods of recognizing an individual based on the measure of biological (anatomical and physiological) and/or behavioral biometric characteristics" (2015).

Elaborating on Liu et al, biometrics measures one's physical or behavioral characteristics, such as fingerprint scans, facial recognition, iris recognition, gait (how one walks), or speech recognition (2015). For example, two of the most promising biometric modalities are iris and retina recognition. Iris recognition has the capability of taking images of the eye from a distance. As a result, iris scanning can occur in physical and digital scenarios. On the other hand, retina scanning works best for physical identification. Retina scanning works by simply bringing a person's eye near an eyepiece. In comparison, both primarily use the function of nonionizing radiation in the infrared region. However, these biometric modalities are not without concern. There is a growing concern in regard to light-emitting diodes being capable of causing direct eye damage. Furthermore, exposing the eye to near-infrared radiation may cause biological effects after prolonged use (Tzaphlidou, M. & Pavlidou, F.-N., 2011). Because of this potential issue, iris and retina scans are not used as much as other forms of biometrics, such as fingerprint scans and facial recognition.

Human fingerprints consist of an enormous range of details. As a result, fingerprint options cannot be simply duplicated which suggests a high level of security. To be specific, fingerprint recognition systems use area unit distinctive patterns. Furthermore, the area is created by furrows (recessed) and friction ridges (raised) that reside on the pads of fingers and thumbs. The minutiae of the process are best described by the International Journal of Innovative Technology and Exploring Engineering (IJITEE): "Minutiae of the fingerprint provides accurate results compared to the ridge shape features since the ridge shape features contains only the loop (∩), arch (Δ) and whorl(o) information which may lead to false recognition. Minutiae details are precise and it consists of two types of minutiae features namely ridge ending and bifurcation"

(Sagayam et al, 2019). As a result of fingerprint recognition's uniqueness, permeance, and collectibility, it is in various sectors such as government, organizations, libraries, universities, banks, etc.

Face recognition is the most established form of biometrics used by humans today. In addition, it is the most natural biometric identification. Yet, face recognition is less reliable over time due to facial changes with aging. Specifically, humans can age as little as five years before face-recognition algorithms begin to struggle to identify us as the same person. Consequently, face recognition generally requires periodic re-enrollment. Lastly, to preview ethics, it can range from one of the least intrusive biometrics to one of the most. When combined with extensive surveillance systems, the more intrusive face recognition becomes (Liu, C.-H. et al, 2015).

Since biometric scanners measure the characteristics of an individual, it is user-friendly. Humans do not have to memorize passwords to unlock their phone, their tablet, or their laptop. Instead, they can conveniently use a scan of their face or fingerprint to unlock their devices. While the use of biometrics is exponentially increasing, cybersecurity professionals focus on how to use biometrics and maintain password security.

While discussing biometrics and what it means for society, this paper will discuss the benefits or biometrics, the vulnerabilities of biometrics, and the ethical concerns the use of biometrics may cause.

Benefits

The biggest advantage of a biometric system is an increase in security. With biometrics, an individual does not have to worry about their password being guessed, shared, or stolen. This not only saves time but creates a safer environment for businesses that use this. These systems tend to be extremely accurate, and the use of eye scans and fingerprints cannot be duplicated very easily. This can be utilized heavily at large businesses to increase the workflow of employees by speeding up the authentication process for getting into the building, logging into the computer, and even purchasing items at the cafeteria.

Security is the first benefit biometrics presents. In previous years, the security of biometrics has been improved through biometric template protection. An example of biometric template protection is cancellable templates. Cancellable templates address the common issue of biometric non-revocability which arises when victims of identity theft cannot obtain a "new" set of clearance. The importance of revocability is that individuals have control over their biometrics if they are compromised. The addition of biometric template protection allows for biometrics to act like a key to a lock that has the capability to be shut down if stolen (Liu, C.-H. et al, 2015). This feature adds a level of security, therefore making the use of biometrics in everyday life benefical.

Furthermore, another way biometrics implements a strong sense of security is by forcing users to partake in enrollment instruction and training. Enrollment generates the template used for all subsequent comparisons and user recognitions. For further details, the system will either average readings or select the highest quality sample given. Next, an enrollment template or reference is produced to be stored for later comparison (Liu, C.-H. et al, 2015). The most common and relatable example of an enrollment process is setting up a new smartphone. Whether the smartphone uses facial recognition or fingerprint recognition, the enrollment process can be tedious as the phone requires a multitude of scans.

The second benefit of biometrics is its accessibility. Accessibility being the reliability and ease of use of a biometric security system. The reliability of biometrics is expressed by providing quick authentication without the need to memorize a password. As a result, biometrics are rapidly replacing traditional authentication methods such as a PIN or graphical 'pattern' passwords (Blanco-Gonzalo, R. et al, 2018). Additionally, it must be accessible to as wide a cross-section of the population as possible. This includes groups such as the elderly, people with disabilities, or those with little knowledge of technology. The appeal biometrics has to the technologically illiterate is through its presentation.

The presentation of biometrics is generally straightforward and even described as "transparent". An example as simple as looking at a screen and face authentication occurring is transparent because the process is performed without the user even noticing. Appropriately, European Biometric analyst Dr. Ramón Blanco Gonzalo et al. writes:

> "Given that mobile authentication methods are at a stage of entering implementational maturity, there is a great opportunity to inspire the deployment of new systems that have the desirable characteristics of universality, ease of use and high performance, with the potential to make daily tasks much easier for a wide population" (2018).

With the continued development of biometrics all around the world, we are starting to see a huge improvement in its reliability and availability. The biggest contributor to biometric development and use in China. China is collecting DNA, facial scans, and voice biometric data as a form of analytics/tracking. Within 13 years (2006-2019) the Chinese government has bought over 1,400 cameras and 300 of those have biometric support. In regions of China, they are starting to detect identity fraud with facial recognition. The technology detects disguises such as hats, glasses, wigs, and fake mustaches. China file, China's surveillance government agency aims to have biometric-capable cameras installed in every aspect of societal life by 2025. With the growing number of biometric sensors, China leads the development and availability of the market. Seeing the rise of biometrics in everyday lives, technology is now more available and implemented than ever before.

Vulnerabilities/Disadvantages

With the growing use of biometrics comes the concerns of privacy and security of stored biometric data. The biometric data collected from a user needed for both authentication and authorization is unique and personal, which, unlike the traditional password or pin, cannot be re-established. One of the biggest privacy concerns pertaining to biometric data collection is the threat of data being used to identify a user in other systems without their knowledge or consent. An article investigating the security and privacy risks of biometric authentication poses the scenario where "a user providing a fingerprint for the purpose of authenticating an e-vote will want to be assured that an impostor cannot masquerade as him/her and that the data is not being supplied to a 3rd party (e.g. the police) for checking against a criminal database" (Ogbuabor, 2015). It is important to protect biometric data when it is collected, which results in strong cybersecurity procedures. Another major privacy concern is the threat of identity-based attacks. The breach of a user's personal biometric data can result in permanent damage as physical assignments such as a fingerprint, iris, or face cannot be replaced. The permanent linkage users have to their biometrics, brings about the fear of stolen data being used to access other important information on that user. There is also the fear of being identified, stalked, or tracked if a

malicious user is able to obtain that data as it is much easier to build a personal profile given that intimate information.

Biometrics are not immune to fallibility. Since biometrics are the unique physical characteristics that can be used to identify an individual, “a vulnerability in biometric security results in incorrect recognition or failure to correctly recognize individuals” (Adler, 2004). A biometrics authentication system can make two types of errors. A false acceptance, in which two samples of biometric data from different individuals are correctly identified as a match, and a false rejection, in which two samples of biometric data from the same individual are not recognized as a match. The False Acceptance Rate (FAR), “is the percentage of imposters that are incorrectly granted access to a biometrics system rendering them as supposed genuine individuals” and the False Rejection Rate (FRR), “is the probability that the system incorrectly rejects access to an authorized person” (Harun et al, 2017). Both the false rejection rate and false acceptance rate depend on the operating threshold. A threshold value is a minimum value that a given entity must possess in order to be considered eligible for a certain action or to qualify for certain privileges. In biometric systems, a “reference threshold is defined as a value that can decide the authenticity of a person” (Dahiya et al, 2014). The larger the threshold, the smaller the false acceptance rate and thus the more secure the system. The reduction of the false acceptance rate and enhanced security comes with the tradeoff of a higher false rejection rate affecting convenience and usability. In turn, the reduction of the false rejection rate comes with the tradeoff of a higher false acceptance rate creating a user-friendly system at the expense of security. As it is not possible to simultaneously have both a low false acceptance rate as well as a low false rejection rate, a big challenge biometric identification systems face is finding a balance of the two (Adler, 2004). A balance where users can trust that their data is secure and safe from unauthorized access without having to sacrifice usability and convenience.

Another challenge to the security of biometric systems is the practice of ‘fooling’ a biometric security system. This is known as a presentation attack or spoofing, an attack that occurs when a person tries to masquerade as someone else by falsifying data and thereby attempting to gain illegitimate access and advantages (Correia et al, 2017). In contrast to an indirect attack which is performed inside the system, spoofing falls into the category of a direct attack. Direct attacks are dangerous because they are performed at the sensor level, outside the digital limits of the system, and thus no digital protection methods can be used (Correia et al, 2017). One of the easiest direct attacks on a system is fingerprint spoofing which uses artificial fingerprints created from inexpensive and easily accessible materials. One notable experiment carried out was done with “gummy fingers” or fake artificial fingers made of cheap gelatin products to be used on 11 different fingerprint detection devices. In the case of pressing a participant's finger directly into the gelatin mold to make the gummy finger, successful recognition rates ranging from 68 to 100% were reported for the fake fingerprints in all of the 11 systems tested. In the case in which a latent fingerprint was lifted from a surface and then used to make the gummy finger, the acceptance rate was always above 60% (Alfonso-Fernandez et al, 2011). A facial recognition system was also tested for spoofing in which an image of a user on a laptop was successful in verification. A video clip of a user’s face was successful in the verification of a system that had a liveness detection algorithm (Schuckers, 2002). Spoofing attacks on facial recognition systems pose a risk due to how easy it is to find photos of people online as well as technology that allows the creation of increasingly accurate AI-generated images and facial morphing software.

Ethics

While biometrics has its benefits and vulnerabilities, using biometrics also involves ethical concerns. A large ethical argument regarding biometrics is gathering biometric data without consent. For example, most of the population has access to a camera, whether that be on a smartphone, a tablet, a laptop, or a digital camera. Because of this, anyone is able to take pictures of one's face at any given time without their consent. The case of this particular event violates one's free will. Perhaps they did not want their picture taken.

Now one may argue that if one is in a public place, their consent is implied. In the modern age, public places are overloaded with multiple forms of security, such as security cameras equipped with facial recognition. For example, Walmart uses facial recognition to spot shoplifters. In a Fortune article, Walmart admitted to using facial recognition as a part of its anti-theft program (Roberts, 2021). Although this technique may be helpful to spot and identify thieves, using facial recognition software in a store is not entirely ethical. According to Gray, "a foundational ethical issue of facial recognition is that these technologies are often employed without consent or notification. Having access to surveillance cameras or video feeds of employees, customers or the general public doesn't mean it's a good idea to use that data without informing the affected parties" (2022). Shoppers are not asked verbally or asked in writing to consent to the use of cameras and facial recognition software, therefore, making the use of facial recognition software unethical to the shopper. However, is the use of facial recognition in Walmart ethical to the public? According to the utilitarian framework:

> "Utilitarianism holds that we should give equal moral consideration to the well-being of all individuals, regardless of characteristics such as their gender, race, nationality, or even species" (MacAskill, 2022).

Facial recognition software is installed in Walmart for safety and security purposes for Walmart, and other shoppers present in the store. While utilitarianism focuses on the well-being of individuals, facial recognition in Walmart can help to identify individuals accused of stealing. Perhaps the individual used a violent attack to steal. With facial recognition, it can help to identify the violent thief, therefore, maintaining the safety and security of other shoppers in Walmart.

Walmart's use of facial recognition raises some ethical concerns, and so does Snapchat's use of facial recognition. Snapchat uses facial recognition technology to apply filters, such as filters that place a dog nose and dog ears on one's face or place a mask filter over one's face. When Snapchat first introduced face filters, many users were excited to use them. However, for some, it raised concern. Some believed that Snapchat was saving the scanned faces into a database, and sending the database to the FBI. However, this statement is not exactly true. From multiple sources, Snapchat has claimed that they have not saved facial recognition (Dekyvere, 2017). Although Snapchat has facial recognition which recognizes one's face, it recognizes a nose or an eye, not a particular eye/nose which would pinpoint to an individual (Dekyvere, 2017). Therefore, Snapchat is not saving biometric data and selling it to the FBI.

In the case that the Snapchat conspiracy would be true, it would have to be listed in their privacy policy. However, it was not clearly stated. Instead, Snapchat states how they collect information one provides: such as name, date of birth, username, password, email address, or phone number (Snap Inc., 2022). Snapchat clearly does not state that they use facial recognition to sell to third parties, or in this case, the FBI. Instead of concerning the general public, one may

simply read the privacy policy of select software, to alleviate the concerns of selling or misusing biometric or personal information.

Including a privacy policy with the release of the software is ethical because it clearly lists the privacy rights of the user. Before the user creates an account on a specific software, they are asked to read the privacy policy and accept it. Although many may not read the privacy policy thoroughly, it is important to read it because some software may clearly state that they will sell one's information to third parties. In the event that information is sold, it would be ethically allowed, as it was clearly stated in writing, and one has given consent to share information with third parties.

Expanding into the topic of privacy policies, they are a key component to creating and maintaining software. Privacy policies are an important document that describes the company's data processing practices (Laird, 2022). It includes policies on the type of information the company collects and what the company uses the information for. It is important to have strict policies that users can agree or disagree with. In the event of a disagreement of policies, the user can withdraw or delete their account from the software.

Providing a privacy policy is mandatory for all types of collected data, not just specifically biometric data. However, biometric data is very personal information, therefore, making a privacy policy very beneficial and ethical to users. It is important to know where and how one's personal biometric data is being used.

Conclusion

The rapidly evolving technology known as biometrics has become a part of most people's everyday life and continues to be implemented across many fields. Biometric recognition systems are the future of both user-friendly and secure authentication using our physical traits to gain access to devices such as smartphones and computers. In today's world, facial recognition and fingerprint scanning is the most common method of biometric identification used by the general public but as biometrics continue to replace passwords, the use of retina scanning, voice recognition, and behavioral biometrics will soon be implemented across many identification systems. Security and usability have become the biggest draw to using biometrics for authentication and identification. As biometric traits are unique signatures linked to a specific individual, the fear of a stolen or forgotten password is no longer.

The future of biometrics is bright as it becomes more normalized in society. Their use is growing specifically in relation to cars, housing, and payment methods. Biometrics are already being used to eliminate vehicle theft through the ability to use biometric authentication to turn on the ignition of a car. Furthermore, biometrics are currently being used to open the front doors of homes. Soon, newer-built homes will not need traditional locks and keys. Lastly, biometrics are predicted to become the future method of payment eliminating the need to carry any form of payment such as cash, card, or smartphone. As a result, the global biometric technology market is expected to reach $55.42 billion by 2027 (Admin, 2021). In all, the possibilities are endless and only time will tell how much society elects to depend on it as a whole.

Bibliography

Adler, A. (2004), Biometric System Security Security, *Systems and Computer Engineering, Carleton University, Ottawa, Canada. DOI: 10.1007/978-0-387-71041-9_19* *https://link.springer.com/chapter/10.1007/978-0-387-71041-9_19*

Admin. (2021, October 27). Biometric trends and statistics to keep an eye on in 2022. Imageware. Retrieved November 15, 2022, from https://imageware.io/biometric-trends-and-statistics/

Alfonso-Fernandez, F., Fierrez, J., Galbally, J., Martinez-Diaz, M. (2011, August). Evaluation of direct attacks to fingerprint verification systems. DOI:10.1007/s11235-010-9316-0 https://www.researchgate.net/publication/226041690_Evaluation_of_direct_attacks_to_fingerprint_verification_systems

Biometric Trends and Statistics to Keep an Eye on in 2022. (2021, October 27). Imageware. https://imageware.io/biometric-trends-and-statistics/.

Blanco-Gonzalo R, Lunerti C, Sanchez-Reillo R, Guest R (2018) Biometrics: Accessibility challenge or opportunity? PLoS ONE 13(3): e0194111.

Correia, L. P., Hadid, A., Li, L. (2017, November 16). Face recognition under spoofing attacks: countermeasures and research directions. *The Institute of Engineering and Technology.* DOI: https://doi.org/10.1049/iet-bmt.2017.0089

Dahiya, R., Girdhar, D., Malik, J., Sainarayanan, G. (2014), Reference Threshold Calculation for Biometric Authentication, *International Journal of Image, Graphics and Signal Processing 6(2):46-53, DOI: 10.5815/ijigsp.2014.02.06*

Dekyvere, E. (2017, April 6). *Face/off: Is Snapchat stealing your face one cute dog filter at a time?* Ku Leuven. https://www.law.kuleuven.be/citip/blog/faceoff-is-snapchat-stealing-your-face-one-cute-dog-filter-at-a-time/

Gray, P. (2022, August 31). *Ethical issues of facial recognition technology*. TechRepublic. https://www.techrepublic.com/article/ethical-issues-facial-recognition/

Harun, A., Mazlan, F., Suliman, S. (2017), Facial Recognition in Multimodal Biometrics System for Finger Disabled Applicants. *Indonesian Journal of Electrical Engineering and Computer Science.* 6. 638-645. 10.11591/ijeecs.v6.i3.pp638-645.

Laird, J. (2022, July 1). *What is a Privacy Policy?* Privacy Policies. https://www.privacypolicies.com/blog/what-is-privacy-policy/

Liu, C.-H., Wang, J.-S., Peng, C.-C., and Shyu, J. Z. (2015), Evaluating and selecting the biometrics in network security, *Security Comm. Networks*, 8, 727– 739, doi: 10.1002/sec.1020

MacAskill, W. (2022). What is Utilitarianism? *Utilitarianism.net*. Utilitarianism. https://www.utilitarianism.net/

Ogbuabor, O. G., Ani, J. O. (2015), Investigation of the Security and Privacy of Biometric Data, *Quest Journals*, *Journal of Electronics and Communication Engineering Research.* https://www.questjournals.org/jecer/papers/vol2-issue11/B2110407.pdf.

Roberts, J. J. (2021, April 24). *Walmart's Use of Sci-fi Tech To Spot Shoplifters Raises Privacy Questions*. Fortune. https://fortune.com/2015/11/09/wal-mart-facial-recognition/

Sagayam, K. M., Ponraj, D. N., Winston, J., Yaspy, J. C., Jeba, D. E., & Clara, A. (2019). Authentication of biometric system using fingerprint recognition with euclidean distance and neural network classifier. Int. J. Innov. Technol. Explor. Eng, 8(4), 766-771

Schuckers, A. C. S. (2002). Spoofing and Anti-Spoofing Measures. *Information Security Technical Report, Vol 7, No. 4 (2002) 56-62. doi:10.1016/S1363-4127(02)00407-7.* http://php.iai.heig-vd.ch/~lzo/biomed/refs/Spoofing%20and%20Anti-Spoofing%20Measures%20-%202002_Schuckers.pdf

Snap Inc. (2022, June 29). *Privacy Policy - Snap Inc.* https://snap.com/en-US/privacy/privacy-policy

Tzaphlidou, M., & Pavlidou, F.-N. (2011, January 19). Biometrics applications: Technology, ethics, and Health Hazards - Hindawi. The Scientific World. Retrieved October 5, 2022, from https://downloads.hindawi.com/journals/tswj/2011/350924.pdf