Fundamental Properties of Biometric Systems

Eric Anderson
Student at Ontario Tech University
Oshawa, Canada
eric.anderson1@ontariotechu.net

Abstract – Throughout this paper there are multiple topics discussed. To start off the modes of a biometric system are mentioned. These modes include enrollment, authentication and identification. Then the structure of a biometric system is talked about. These systems can be broken down into the capture, signal processing, storage, matching and decision module. After this the biological factors that an organization must consider when picking a biometric system are talked about. These factors include universality, uniqueness, permanence, collectability, performance, acceptability, and circumvention. Finally, we will cover a few common types of biometric systems.

Index Terms – Biometrics

I. INTRODUCTION

In this world today biometrics has become and ever more common security technology. The average person though, probably does not have a great understanding of how these systems work. As such, throughout the upcoming sections you the reader will be enlightened on the innerworkings of this technology and how it can be applied to everyday life.

II. WHAT IS A BIOMETRIC SYSTEM

Biometrics systems are a way of determining who an individual is. With this information security systems can be put in place controlling access to places and devices. This in turn protects everything from information to physical hardware. Unlike most security systems, biometric systems use biological attributes to determine a person's identity. As a result, a person always has what they need to identify themselves. The entire structure of a biometric system allows the identity of a person to be ascertained in three logical parts. These parts are called enrollment, authentication and Identification.

A. Enrollment Mode

When your biometric device is in enrollment mode it is looking to add users. This means it is looking to collect a user's biological information so they can be identified at a later date. Through several phases of data acquisition, a robust biological model can be generated. With the individual's characteristics captured, their data signature can be stored in a database [4].

B. Authentication Mode

With the scanning device in authentication mode a person can be identified. During this process a person provides their biometric data to the system through the use of a username or smart card. Then the system goes looking in its database for the matching biological data. Once this one-to-one comparison is finished the individual will be allowed into the device or area they want to access [4].

C. Identification Mode

Identification mode shares a couple similarities with authentication mode. The main one being, once successful identification has occurred the person is allowed into the device or area. Also, the user is still required to provide their biometric data. From this point though things start to differ. Instead of the one-to-one comparison with authentication mode, identification mode is a one-to-n comparison. As a result of this when someone enters their biological data it is compared with all the user templates in the database. If a match is found then that person is let through. Of course, though, this method leaves the potential for the wrong person to be verified. This is called a false-positive, the severity of this varies between biometric technologies [4].

III. BIOMETRIC SYSTEM STRUCTURE

The actual hardware and software of a biometric device can be broken into five main parts. These consist of the capture, signal processing, storage, matching and decision modules [4].

A. Capture Module

When a user interacts with a scanner, they are interfacing with the capture module. Here the system extracts the user's biometric data and a digital representation is created [4].

B. Signal Processing Module

From the capture module the signal processing component optimizes the digital representation of the user's data. With this optimization process the processing time during an identification stage is much faster [4].

C. Storage Module

The storage module is pretty straight forward. All the module does is store biometric templates of users that have been enrolled into the system [4].

D. Matching Module

This element of the biometric system takes the optimized digital representation from the signal processing module and compares it for similarity with a template in the storage component. Then it outputs a similarity index [4].

E. Decision Module

Finally, the decision module actually determines whether the similarity index provided by the matching element is in its pre configured threshold. If it is, the user will be allowed past the security system, otherwise they will not be [4].

IV. BIOMETRIC CHARACTERISTICS

When an organization is in the process of deciding on the right type of biometric system to implement there are several factors they need to take into consideration. These include universality, uniqueness, permanence, collectability, performance, acceptability, and circumvention [3].

A. Universality

If a biometric system is universally viable, that means a majority of the people using the device have the feature being analyzed. For example, analyzing someone's preauricular pit as a method of identification would not be universally viable as such a low percentage of the population has one. A much more viable feature would be fingerprints as they are a very common trait. Even with this feature though some of the population does not have fingerprints. So that would need to be taken into account when picking a biometric system [3].

B. Uniqueness

After determining universality, it is important to look at uniqueness of the character trait. If a trait can be the same between multiple individuals there would be an increased chance of a false-negative occurring. If we were to look if a person has hair or not it would be a poor biometric system as it would group everyone into two groups instead of individually identifying them. A much better solution would be to use someone's iris pattern or their DNA. Both of these are very unique and happen to be very common in the human population [3].

C. Permanence

Now that we have a common and unique trait, we need to consider its permanence. When a feature has a high permanence, it does not change much overtime. That means a scan of the trait when someone is twenty years old, for example should still be identifiable when they are eighty. So, if we were looking a person's wrinkles this would have a low permanence because we get them as we get older. Fingerprints though, do not change over a life time so they would be an example of high permanence [3].

D. Collectability

A company or organization must also consider collectability. This takes under consideration how easy it is to extract a biological feature from a person. A fingerprint is a good example of easy extraction because it is quick for a person to access and they are easy to acquire [3].

E. Performance

When speaking about the performance of a biometric system an organization needs to consider speed, accuracy, and error rate for the device they will be implementing. Optimizing these areas will create an overall better user experience [3].

F. Acceptability

Acceptability is arguably one of the most important aspects when choosing a biometric system. If the user does not want to use the machine it would have adverse affects like a decrease in company moral. There are multiple reasons this lack of acceptability could occur. It could happen because the system is too hard to use, the user is uncomfortable with providing information like their DNA or the system is just simply to slow. Either way this must be taken into account during the biometric selection process [3].

G. Circumvention

Finally, a company must take into account how easy it is to trigger a false-negative, which would allow unauthorized individuals into a device or area. An example of an attack against these machines is gummy fingers. This attack basically involves replicating an individual's finger so that a scanner can be passed. Today though, scanners have become more advanced making attacks like this significantly more difficult [3].

V. TYPES OF BIOMETRIC SYSTEMS

There are many different types of biometric systems in the industry. A few of the common ones are facial, iris and fingerprint recognition.

A. Facial Recognition

A facial recognition system works to analyze both the shape and position of different elements on a human face. These systems can also take into account different skin features to further improve accuracy. An additional benefit of this technology is that it is capable of identifying people in crowds. It does have a few drawbacks. Due to the current nature of the technology, recognition from an angle is not possible. In addition, the security level of facial recognition is not as great as other biometric systems [1].

Universality (High), uniqueness (Low), permanence (Medium), collectability (High), performance (Low), acceptability (High), and circumvention (Low) [2].

B. Iris Recognition

An iris is the colored part of the eye. So, the job of an iris scanner is to read this part of the eye to determine the identity of a person. This device functions very well in the visible light spectrum and is very secure. Though it can perform even better when it uses infrared light. Like facial recognition, iris recognition has a few drawbacks. The biggest one is the acceptance of users. Many users find it unpleasant to get their eyes scanned, do not like standing in uncomfortable or weird positions, and find it to be unhygienic. The other drawback to note is, although an iris recognition system provides lots of security the speed of scanning comes at a cost [1].

Universality (High), uniqueness (High), permanence (High), collectability (Medium), performance (High), acceptability (Low), and circumvention (High) [2].

C. Fingerprint Recognition

A fingerprint based biometric system looks at the surface of a person's finger to determine certain characteristics. These fingerprints are made up of bifurcations, ridge endings and islands. Fingerprint recognition systems tend to have a fairly high acceptance rate and the technology is cheap and easy to implement. Though fingerprints can be easily replicated and different scanners can drastically vary from one another, which is a downside of this technology [1].

Universality (Medium), uniqueness (High), permanence (High), collectability (Medium), performance (High), acceptability (Medium), and circumvention (High) [2].

VI. CONCLUSION

The importance of biometric systems is becoming more, and more evident as time goes on. Which is why it is important that everyone becomes more knowledgeable about this field. With the use of biometric systems, we can have a more secure tomorrow.

REFERENCES

[1] "5 common biometric techniques compared," Recogtech. [Online]. Available: https://www.recogtech.com/en/knowledge-base/5-common-biometric-techniques-compared. [Accessed: 09-Oct-2021].

[2] A. Jain, R. Bolle, and S. Pankanti, Eds., Biometrics: Personal Identification in Networked Society, vol. 479. 2006.

[2] J. Nelson, "Biometric Characteristic," Biometric Characteristic - an overview | ScienceDirect Topics, 2013. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/biometric-characteristic. [Accessed: 08-Oct-2021].

[3] S. Guennouni, A. Mansouri, and A. Ahaitouf, "Biometric systems and their applications," IntechOpen, 01-Mar-2019. [Online]. Available: https://www.intechopen.com/chapters/65920. [Accessed: 08-Oct-2021].