A Comparative Review of Biometric Security Systems

Ryan Ercel O. Paderes

College of Computer Studies
University of Antique
Sibalom, Antique, Philippines
xe0nixus@gmail.com

Abstract **-Security is a way to protect files or property. Evolution on security has been a consistent way on improving the methods and ways on having an effective security system. Biometric system is one of the effective methods when it comes to security. In this paper, fingerprint biometric system and iris recognition will be discussed. Also, some other forms of biometric system will be mentioned as well. Comparing such will differentiate each system for their vulnerabilities and effectiveness.**
Keywords*: security, biometric, iris recognition, fingerprint*

I. Introduction

Security has been an essential part of our everyday life. We are dependent on data storage, it maybe online or offline. Massive amount of important information are being uploaded, copied or stored online.

Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals [1]. Biometric identifiers are often categorized as physiological versus behavioral characteristics[2]. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odor/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice.[3] Some researchers have coined the term "behaviometrics" to describe the latter class of biometrics.[4]

II. Types of Biometric Recognitions

A. Fingerprint Biometric Systems

Biometrics is an automated method of recognizing a person based on a physiological or behavioral characteristic. Among the features measured are face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. Biometric data are separate and distinct from personal information. Biometric templates cannot be reverse-engineered to recreate personal information and they cannot be stolen and used to access personal information. [5]

Unique characteristics or unique identification of a person is used. Physical attributes of your body such as fingerprint, palm print, iris pattern, and other unique physical features that your body has contributes to an effortless identification of you.

As shown in *Figure 1*, an example on how a fingerprint biometric is being read and its unique markings that a person has. There are two ways on how it's stored; first, the scanner takes several images of your fingerprint. Then, these images are read for its unique patterns. After that, the unique patterns were determined; these patterns are converted into binary numbers that represent those unique patterns.

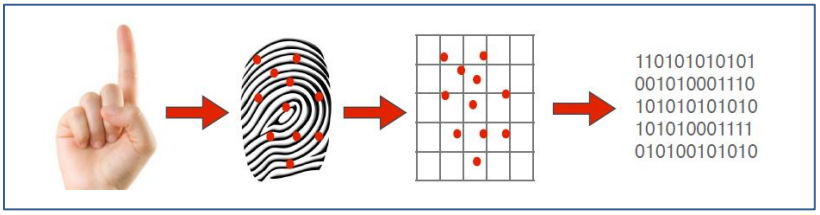

Figure 1.
An example on how a fingerprint biometric is being read

Fingerprint biometrics is hard to fake out. Unlike cards that can be easily copied or duplicated, fingerprint biometric, because of the prints' unique patterns, you just cannot guess the fingerprint pattern of a

978-1-4673-9843-5/15 $31.00 © 2015 IEEE
DOI 10.1109/BSBT.2015.12

person. Unlike passwords, or cards which are easy to guess, fingerprint patterns are unique and each person has a unique pattern. Therefore, only the person who has the print can log in or access a system.

Although, like any other system fingerprint biometric system flaws. There are two basic types of recognition errors: the *false accept rate (FAR)* and the *false reject rate (FRR)*. A False Accept is when a nonmatching pair of biometric data is wrongly accepted as a match by the system. A False Reject is when a matching pair of biometric data is wrongly rejected by the system. The two errors are complementary: When you try to lower one of the errors by varying the threshold, the other error rate automatically increases. There is therefore a balance to be found, with a decision threshold that can be specified to either reduce the risk of FAR, or to reduce the risk of FRR [6].

According to www.biometricnewsportal.com [6], these are the areas that a biometric system attack occurs:

- Presenting fake biometrics or a copy at the sensor, for instance a fake finger or a face mask. It is also possible to try and resubmitting previously stored digitized biometrics signals such as a copy of a fingerprint image or a voice recording.
- Producing feature sets preselected by the intruder by overriding the feature extraction process.
- Tampering with the biometric feature representation: The features extracted from the input signal are replaced with a fraudulent feature set.
- Attacking the channel between the stored templates and the matcher: The stored templates are sent to the matcher through a communication channel. The data traveling through this channel could be intercepted and modified - There is a real danger if the biometric feature set is transmitted over the Internet.
- Corrupting the matcher: The matcher is attacked and corrupted so that it produces pre-selected match scores.
- Tampering with stored templates, either locally or remotely.
- Overriding the match result.

B. Iris Biometric Systems

Iris recognition is a method of identifying people based on unique patterns within the ring-shaped region surrounding the pupil of the eye. The iris usually has a brown, blue, gray, or greenish color, with complex patterns that are visible upon close inspection. Because it makes use of a biological characteristic, iris recognition is considered a form of biometric verification

Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of one or both of the irises of an individual's eyes, whose complex random patterns are unique, stable, and can be seen from some distance.

What makes iris scanning a unique form of biometric recognition, is that the iris is the colored ring of muscle that opens and shuts the pupil of the eye like a camera shutter. The colored pattern of our irises is determined genetically when we are in the womb but not fully formed until we are aged about two. It comes from a pigment called melanin—more melanin gives you browner eyes and less produces bluer eyes. Although we talk about people having "blue eyes," "green eyes," "brown eyes," or whatever, in reality the color and pattern of people's eyes is extremely complex and completely unique: the patterns of one person's two eyes are quite different from each other and even genetically identical twins have different iris patterns.[7] Figure 2, shows how machines scans our eyes for our iris recognition using Infrared light. Infrared helps to show up the unique features of darkly colored eyes that do not stand out clearly in ordinary light.

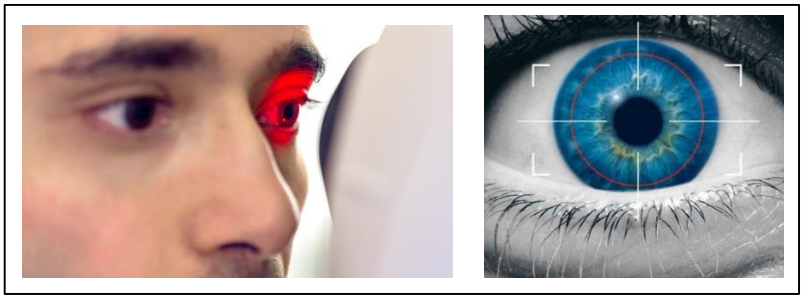

Figure 2 :
Shows how machines scan our eyes for our iris recognition using infrared light

A camera scans our eyes and takes a digital image of it. Unique characteristics that are present in our iris are being mapped out and make a unique recognition. System software attempts to isolate the iris by drawing two circles, one at its inner boundary (between the pupil and the iris) and the other at its outer boundary. The inner boundary is relatively easy to detect, because it is generally a circle with a sudden change in brightness where the pupil gives way to the iris. A broadly similar process is used to find the outer boundary, though it has to allow for the likelihood of the eyelids blocking part of the iris. Then, Polar coordinates are then added to the image to define separate "zones of analysis," so that key features of the iris can be accurately located and compared in two-dimensional space. This system cleverly allows for the way the iris changes as the pupil grows (dilates) and shrinks (constricts) in different light conditions. Finally, the pattern of light and dark areas in the iris is then converted into digital form using bandpass filters and, with the help of mathematical equations, this generates the unique, digital code. A particular eye will generate roughly the same code whether its pupil is dilated or not.

Accuracy and reliability are the main advantage of the iris scanning identification for biometric systems. It's more accurate than the fingerprint biometric system. Due to fingerprints are constantly exposed to damage and possibly ruin the unique pattern that is present on our fingers. Also the iris patterns remain intact or unchanged for a longer period since our eyes are more likely not exposed that much than our hands. Constant care of our eyes is also a factor that we always consider.

On the other hand, iris scanning technology has its own drawbacks as well. One is the great initial cost that this technology needs to start. This technology has yet to be tested thoroughly, even though some research have tests done but the success rate was not that promising. Also, having this kind of biometric system for security, persons private life will not be that private anymore. Privacy is always an issue when it comes to this kind of biometric system. Constant monitoring of persons' whereabouts can be done without the knowing of such individual that they are being stalked or monitored.

C. Other Biometric Recognitions

C. 1. Speaker or Voice Authentication

Speaker or voice authentication is the analysis of vocal behavior by matching it to a voice model template (an already recorded voice). Since every voice is unique, the physical characteristics of the speaker's voice can be measured through its tone, pitch and unique modulation. This is an effective biometric system to protect sensitive information, fraudulent acts, even the protection of sensitive and critical information. *Figure 3* shows how the voice is being used as a system using the voice recognition authentication

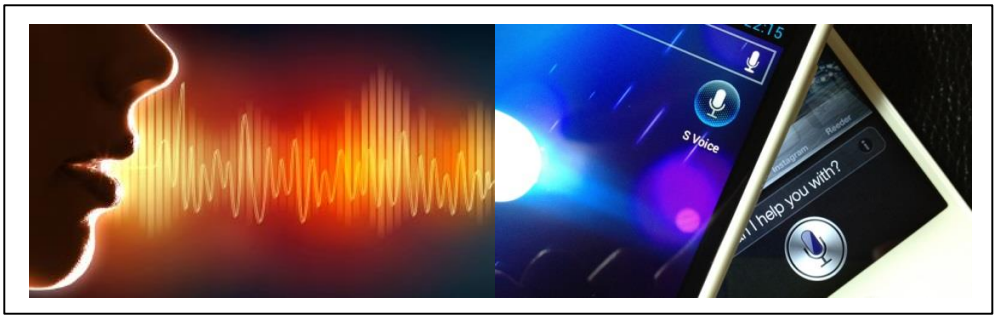

Figure 3 .
Sample image on how voice recognition system works.

C. 2. Speaker or Voice Authentication

Facial recognition uses algorithms to analyze features. These include the position/size/shape of the eyes, nose, cheekbones and jaw line. Initially, this process was known as 2D facial recognition. The 2D images were typically taken from security cameras that have integrated facial recognition technology. For the best results, face images needed to be looking directly at the camera with enough lighting. After analysis, they could be compared to other face images for identification purposes. As shown in Figure 4.

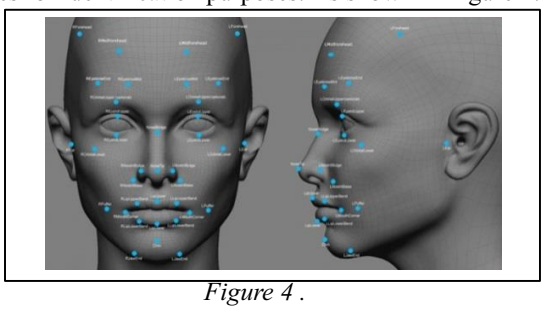

Figure 4 .
Sample on how facial recognition mapping is done to identify areas of the face.

3D biometric facial recognition is the updated version of this identification process. Images are captured with a real-time 3D camera or by digitally scanning a 2D photo. Detailed information like the contour of the eye sockets, nose and cheekbones help make identification easier. The 3D method is also not affected by lighting issues. This improvement has benefited law enforcement and biometric forensics investigations. [8]

III. Discussions

Biometric security system is an effective way when it comes to uniqueness and integrity. Different kinds of biometrics differ from each other. Fingerprint biometric is the most economical biometric system and also the most developed nowadays. Also, the accuracy is high since the system gets several images from the source (fingerprint) to compare and authenticate its uniqueness in pattern. However, Iris biometric security, a camera scans our eyes using an infrared light and takes a digital image of the eye Unique characteristics that are present in our iris are being mapped out and make a unique recognition. Iris biometric however, has a high level of accuracy but could last longer once enrolled in the system. It's more accurate than the fingerprint biometric system. Due to fingerprints are constantly exposed to damage and possibly ruin the unique pattern that is present on our fingers. Also the iris patterns remain intact or unchanged for a longer period since our eyes are more likely not exposed that much than the fingerprints.

IV. Conclusion

Security plays an important role in everyday life. The above mentioned biometric security systems prove the evolution and need for a stronger and more secured way of security. Fingerprint and Iris biometric recognition and other biometric systems, possessesintegrity, accuracy, uniqueness and strong way of security. The comparing fingerprint and iris biometrics, both possesses strong security; however, drawbacks from both systems must be considered and financial capabilities as well. Depending on the level of security needed, these biometric systems play an essential role as far as security is concerned.

References

[1] Jain, A.; Hong, L. and Pankanti, S. (2000). "Biometric Identification".*Communications of the ACM*, 43(2), p. 91–98. DOI 10.1145/328236.328110

[2] *Jain, Anil K.; Ross, Arun (2008). "Introduction to Biometrics".In Jain, AK; Flynn; Ross, A. Handbook of Biometrics.Springer. pp. 1–22. ISBN 978-0-387-71040-2.*

[3] *Sahidullah, Md (2015). "Enhancement of Speaker Recognition Performance Using Block Level, Relative and Temporal Information of Subband Energies". PhD Thesis (Indian Institute of Technology Kharagpur).*

[4] "Biometrics for Secure Authentication" *(PDF)*.Retrieved 2012-07-29.

[5] http://www.bioelectronix.com/what_is_biometrics.html

[6] http://www.biometricnewsportal.com/biometrics_issues.asp

[7] http://www.explainthatstuff.com/how-iris-scans-work.html

[8] http://www.brighthub.com/computing/smb-security/articles/63325.aspx