World Journal of Engineering Research and Technology

WJERT

www.wjert.org

SJIF Impact Factor: 5.924

HUMAN ORGANS AS INFORMATION SECURITY TOOLS: A BRIEF REVIEW ON BIOMETRICS

Khalid Mohammed Osman Saeed*[1] and Abdelhamed Mhmod Ali Elhassan[2]

[1]Faculty of Computer Science and Information Technology, Omdurman Islamic University, Khartoum, Sudan.

[2]Faculty of Applied Science and Computer, Omdurman Ahlia University, Khartoum, Sudan.

Article Received on 05/07/2022 **Article Revised on 26/07/2022** **Article Accepted on 15/08/2022**

***Corresponding Author**
Khalid Mohammed Osman Saeed
Faculty of Computer Science and Information Technology, Omdurman Islamic University, Khartoum, Sudan.

ABSTRACT

The fact that the majority of human activities and data are now computerized and that most of them—if not all—of them take place over an unsecure public network, as well as the fact that these digitalized forms of data could be attacked by network breakers, disclosed by strangers, or even forgotten or lost, only serves to increase the need for security precautions and measures. Additionally, it demonstrates the critical necessity for strong, trustworthy identity and verification mechanisms. In light of this, the idea of using human organs as security tools has emerged. However, due to their uniqueness and sensitivity, human organs play a huge role in identifying and confirming persons. However, despite everything mentioned and the delicate nature of the procedure, the success of biometrics techniques depends on a variety of factors, including workforce acceptance, the level of security required, the budget, and how easily these distinctive features can be converted into digital form for evaluation. In this article, the researcher tries to provide a summary of several biometric traits and how they work.

KEYWORDS: Face & Iris Recognition, Retina scan, Finger Print, FRR, FAR, CER.

1. INTRODUCTION

Biometric systems, which relate to how computer systems are capable of extracting, analyzing, and evaluating physiological or behavioral unique attributes of individuals from specific human body organs, are currently one of the main branches that constructed and supported information security science. The words bio, which means life, and metric, which means to measure, are both Greek words, and they are the origins of the phrase "biometrics" (A. k. Jain, P. Flynn, A. A. Ross, 2008). However, it is now generally accepted that any identity or verification processes may include a biometric system, according to Rudd M. Bolle and Jonathan H. Connell and et al. (2003).

Despite the many benefits that come from using biometric technologies to secure organizational assets and control employee's they can also be utilized as a more official method of recognizing civilization history (Brad wing, jim zok, david young and et al., 2006).

2. Paper Questions

When it became clear that accurately confident identification could only be based on the distinctive characteristics of the human organs, two problems had to be raised:

- What bodily component might be employed?
- How could authorization be completed quickly and accurately?

3. Characteristics of Biometric Systems

Organizations struggle to determine which biometric system is the most effective and efficient due to the vast array of biometric systems that are currently available in the information security market, including Fingerprint Systems, Hand Geometry Systems, Voice Pattern Systems, Retina Pattern Systems, Iris Pattern Systems, and Signature Dynamics Systems (Harold F. Tipton and Micki Krause, 2007). Particularly when all of the aforementioned biometric systems might be thought to share similar features and traits. Therefore, from the perspective of the researchers, learning the important aspects of the accessible biometric systems is valuable and vital for any company looking for such a matter:

- Accuracy and uniqueness: Are crucial components of any authentication system or device used to distinguish between authorized and unauthorized personnel.
- Speed and Throughput Rate: One of the most important aspects of any biometric system is the speed at which the data from the human body is gathered, and as a result the throughput or how quickly the decision on whether to recognize or reject the employee.
- Acceptability to employees: This factor should be taken into consideration when management decides to suggest any biometric system, as employees must believe that there is a need for such a protection mechanism and that it is safe to use, doesn't slow down employees' movement and hasn't slowed down production, and that the system

doesn't make it easier for organizations' management to gather information about employees' health.

- A biometric system is regarded as trustworthy when it performs precisely, vehemently, and without the need for ongoing maintenance. Additionally, it has the capacity to detect any effort to enter false data.

4. Some Types of Biometrics

The researcher attempts to explain popular biometric systems now in use, including the characterized have to measure, the devices used to collect the biometric, how it operates, the features retrieved, the algorithms employed, and the regions of applicability.

4.1 Fingerprint

Because fingerprint systems are regarded to be the earliest biometric systems currently in use and the easiest to gather and manipulate as input through computerized systems, they are widely used. The presence of hills, arches or curves, and sweat holes can all be seen in a fingerprint. However, because these scars are neither inherited nor genetic, they vary greatly between people and between the fingers on a single hand. However, there are other techniques to employ in order to collect fingerprint features, such as.

- The hills, arches, curves, and sweat pores on a person's finger are focused by an optical fingerprint scanner, which converts the light into ones and zeros to create a digital image. Therefore, complementary metal oxide semiconductor cameras (CMOSC) or charge coupled devices (CCD), both of which are dependable and affordable, are typically used in the capture procedures of fingerprint scanners (Miguel Gudino, 2021).
- Capacitive fingerprint scanners use the conductivity of the human body to create an electrostatic field from a finger and create a digital image. They then utilize dielectric measurements to differentiate between hills and gaps; hills yield greater values than cracks. To put it another way, capacitive scanners employ the finger hills that are placed above the conductive surface to convert the static charge stored there, while the empty crevices between curves maintained the charge unchanged. These modifications, however, are documented and turned into digital files that can subsequently be examined. Finally, the image that is produced is good, but capacitive scanners are expensive and quickly consume power (Robert Triggs, 2021).
- In comparison to optical scanners, ultrasonic scanners offer higher security and dependability while also being able to be used in dusty environments and with moist

fingers. Additionally, by simply touching the panel, they can create an accurate, digital 3D image of a person's finger using sound waves. In comparison to capacitive scanners, the created image is therefore more secure due to its 3D nature. However, the hardware of ultrasonic scanners includes a transmitter and a receiver. However, to capture the fingerprint's details based on the hills, curves, perspiration holes, and other details that are particular to each one, the transmitter generates an ultrasonic pulse that hits the gaps and hills on the fingerprint. While some of the pulses are absorbed, some are reflected back to the sensor. Although I do say so myself, the issue with ultrasonic scanners is that they are not quick enough, and screen protectors, especially thicker ones, can affect their ability to correctly read the print (Margaret Rouse, 2021).

- The temperature variations between fingerprint hills and gaps are detected using temperature fingerprint scanners. Additionally, it determines the lowest temperature differences between fingerprint components to create a thermal image that is then transformed to an optical image. For example, because of sweat holes, hills are colder while gaps are hotter. Despite the heat, fingerprint scanners are inexpensive, but they consume power quickly and perform poorly (ALMAS TEAM, 2021) and (Kishor Kumar Sadasivuni, Mohammad Talal Houkan and et al., 2017).

So, all fingerprint scanner technology may be fooled by taking a photo of a fingerprint and altering it to look like the real thing (Davey Winder, 2019).

4.2 Face Recognition

Face recognition technology attempts to identify a human by their facial features, much like it does with humans (Rudd M. Bolle and Jonathan H. Connell and et al., 2003). The capacity to compare a human face from a digital image or a video frame to a recorded face is known as face recognition, and it is typically used to confirm and verify people by analyzing their facial features (S.K. Cheng, Y. H. Chang, 2014). It's vital to note that, depending on the features employed, facial recognition technology now employs either of two methods.

- Appearance-based features describe the texture of the face caused by expression; as a result, they are produced after a human face has been successfully photographed numerous times in the same lighting conditions to create Eigen-faces, which are then normalized so they can be modeled at the same pixel resolution (Pablo Navarrete and Javier Ruiz-Del-Solar, 2002).

- Geometry-based features: characterize the shape of the subject's mouth, eyebrow, nose edge, and cheeks, and their symmetrical features are employed for face detection and identification (Deepak Ghimire and Joonwhoan Lee, 2013).

4.3 Iris Recognition

It uses a computerized method to identify people based on characteristics found in the area of the eye that surrounds the pupil. Alternately, the iris may be the colored portion of the eye, which may be brown, blue, gray, or greenish in hue. In either case, iris features are distinctive, stable, and may be observed at a distance. The number of features that biometric systems can encode and use in comparison gives them their distinctive power (Stan Z. Li, Anil k. Jain, 2015).

4.4 Retina scan

Both the retina and the iris, which are both components of the eye, have distinctive qualities and are extremely sensitive. However, they employ several methods to gather information about human biometrics for authentication. While a retina scan requires one to concentrate on a specific point in order to gather data. Again, this will be tiresome for those who wear glasses and are concerned about touching the scanning plate with their eyes, which is why people believe it to be more bothersome and unsettling than other biometric methods. Even though the researcher claimed that retina scans are crucial for usage in identification, verification, and authentication, they can become unreliable over extended periods of time due to conditions like diabetes or glaucoma (John Gustav Daugman, 1993).

4.5 Hand Geometry

Three different hand photographs are taken to register the features such breadth, length, gaps between joints, thickness, and bone structure of the hand and fingers in order to capture the distinctive aspects of hand geometry. The gathered information is then kept in a database for hand geometry. Additionally, just like with fingerprints, someone must place their hands to determine whether they are legitimate (Jesus Suarez, Robin R. Murphy, 2012).

5. Performance Metrics

Unquestionably, a biometric system is used for one of two things—or both—in any facility, regardless of the level of security required. However, systems used to identify humans, in this case a one to many decision should be made, or systems used to verify humans, in this case a one to one decision should be made, while identification (matching against all records in the database), verification (matching against a single record), and the matching process itself are relevant (Darran Rolls, Gerry Gebel and et al., 2015).

Even while biometric systems are highly sensitive and accurate, they frequently result in false matches because biometric samples can differ from capture to capture and because time and other factors can modify a person's characteristics. In light of this, the researcher decided to quickly address this topic in the following section.

5.1. Verification Performance Metrics

Therefore, if X and Y were real-world subjects, Xb, Yb would be their biometrics, and Dx and Dy would be the digits produced from Xb, Yb, their corresponding biometrics by the function F, where:

$$Dx = F(Xb)$$

$$Dy = F(Yb)$$

However, because gathering biometric information from a subject and matching processes take place at various times or in various environments, let T be the time.

$$Dx = Dx(T) = F_T(Xb)_T$$

$$Dy = Dy(T) = F_T(Yb)_T$$

Although the matching process for the two input subjects took place at different times, biometric systems work by determining whether there is a chance that they are the same. Assume that this matching procedure uses the samples Xb and Xb', where Xb is the registered sample from time T and Xb' is the live sample current at the present. Designate T as the past and T' as the present. The evaluation procedure then calculates the sum of the two biometric models in accordance with the function let's call S as follows.

$$S\,(Xb', Xb) = S\left[(Xb')_{T'}, (Xb)_T\right] = S\left[F_{T'}(Dx'(T')), F_T\,(Dx(T))\right]$$

The likelihood that Xb' and Xb belong to the same person at various times is higher if S is large. This results in false match rate and false non-match rate, which is why (Darran Rolls, Gerry Gebel and et al., 2015):

- False non-match: This occurs when a registered biometric does not appear to match the one that was previously gathered, leading to a false rejection. Or, the likelihood that every single lawful endeavor will fall short. When Xb'=Xb, Dx' does not match Dx.

- False match: This occurs when a recorded biometric appears to match the features of another person, leading to a false acceptance. In other words, the possibility that one impostor may be mistakenly recognized as a suitable match. When Xb' ≠ Xb, then Dx' match Dx.

5.2. Identification Performance Systems

The Threshold Based Identification system checks each database entry with the biometric DX'; to achieve this, it computes the sum for each record in accordance with the function S as follows:

$S\,(DX', (Dx)_i)\; where\; i = 1, 2, 3, \dots \dots \dots . . Z$

Once more, the process was carried out for all of the entries that were recorded, accounting for all of those that met the criteria by exceeding zero. The complete list of matching entries is then returned, and one of the following states is possible:

a) In the event that the sample DX' is not registered, the ideal system responds "NO MATCH."

b) A particular "YES MATCH" if the database contains the sample DX's.

c) Multiple "YES MATCH" results indicate a hazy outcome and an uncertain identification.

d) The sample DX is not registered, despite the fact that a specific "FALSE ACCEPT" response is given, indicating misidentification.

e) The sample DX' is recorded, despite the result of "FALSE REJECT."

The latter two points are particularly essential since they demonstrate the efficiency of any biometric technology in terms of resistance to counterfeiting and highlight two significant mistakes.[4]

- False Reject Rate: This rate is typically expressed as a percentage or proportion. The false reject rate is the percentage of genuine registered subjects that a biometric system rejects as being unidentifiable or unverified. False rejection is also referred to as a Type I error. False rejection is considered the least major error in access control when the need for security is not very important. It might be the most significant mistake in other biometric systems, though.
- False Accept Rate: This is the percentage of non-registered or imposter subjects that a biometric system accepts as genuine subjects. False accept rates are sometimes referred to

as Type II errors. It is often measured as a biometric system's maximum significant inaccuracy.

- Crossover Error Rate (CER), which can alternatively be expressed as a percentage or ratio. This is also known as the equal error rate, and it denotes the percentage or point at which the false rejection rate and false acceptance rate are identical. Occasionally, it is referred to as the equal error. This is now considered to be the key indicator of how accurate a biometric system is.

6. CONCLUSION

When necessary, an effective information security system may ensure that the organization performs as planned. Unauthorized operations, however, pose a threat to the assets, people, data, and occasionally even the very life of organizations. Because of this, guards, fences, passwords, doors, personal identification numbers, badges, locks, and keys may all be broken or faked with little effort; carrying them also makes them vulnerable to loss, theft, or revelation, especially in high security zones. However, relying on the distinctive characteristics of the people themselves, or in other words, their organs, for identification and verification purposes is the only method that can be relied upon to accurately and confidently authenticate the identity of individuals before providing access. As a result, restricting access to and protecting precious resources requires the identification and verification of persons as a crucial step.

As a result, biometrics are introduced as a security measure because their distinctive characteristics cannot be imitated. Additionally, carrying them is not cumbersome, and there is no need to remember or conceal them.

ACKNOWLEDGEMENT

The author would like to thank *Mohammed Ali Mohammed Shaeldin* for his assistance and encouragement.

REFERENCES

1. A. k. Jain, P. Flynn, A. A. Ross, (2008), “The Handbook of Biometrics”, Springer.
2. Rudd M. Bolle, Jonathan H. Connell, Sharath Pankanti, Nalini K .Ratha, Andrew W. Senior (2003), “Guide to biometrics”, Springer.
3. Brad wing, jim zok, david young and et al. (2006), Biometrics History, national science and technology council.

4. Harold F. Tipton and Micki Krause (2007), Information Security Management Handbook, 6th Edition, CRC Press.
5. Miguel Gudino (2021), “How Do Fingerprint Scanners Work? Optical vs Capacitive”, https://www.arrow.com/en/research-and-events/articles/how-fingerprint-sensors-work.
6. Robert Triggs (2021), “How Fingerprint Scanners Work”, https://www.androidauthority.com/how-fingerprint-scanners-work-670934/.
7. Margaret Rouse (2021), “Experts Agree: Face ID Is Not the Answer, In-Display Fingerprint Sensors Are”, https://www.e3displays.com/experts-agree-face-id-is-not-the-answer-in-display-fingerprint/.
8. ALMAS TEAM (2021), Fingerprint Scanners: What are the Different Types?, https://almas-industries.com/blog/fingerprint-scanners-types/.
9. Kishor Kumar Sadasivuni, Mohammad Talal Houkan, Mohammad Saleh Taha, John-John Cabibihan (2017), “Anti-spoofing Device for Biometric Fingerprint Scanners”, IEEE International Conference on Mechatronics and Automation (ICMA).
10. Davey Winder (2019), “Hackers Claim 'Any' Smartphone Fingerprint Lock Can Be Broken In 20 Minutes”, Forbes.
11. S.K. Cheng, Y. H. Chang (2014), International Conference on Artificial Intelligence and Software Engineering (AISE2014), DEStech Publications Inc.
12. Pablo Navarrete and Javier Ruiz-Del-Solar (2002),” Analysis and Comparison of Eigenspace-Based Face Recognition Approaches”, International Journal of Pattern Recognition and Artificial Intelligence, Volume 16, Issue No. 07.
13. Deepak Ghimire and Joonwhoan Lee (2013), “Geometric Feature-Based Facial Expression Recognition in Image Sequences Using Multi-Class AdaBoost and Support Vector Machines”, PubMed Central, Volume 13, Issue 6.
14. Stan Z. Li, Anil k. Jain (2015), Entropy, Biometric, Encyclopedia of Biometrics, 2nd Edition, Springer, 2015.
15. John Gustav Daugman (1993), “High Confidence Visual Recognition of Persons by a test of Statistical Impedance”, IEEE Transactions on pattern analysis and machine intelligence.
16. Jesus Suarez, Robin R. Murphy (2012), “Hand gesture recognition with depth images: A review”, 2012 IEEE RO-MAN: The 21st IEEE International Symposium on Robot and Human Interactive Communication.
17. Darran Rolls, Gerry Gebel, Robin Wilton, Ryan Disraeli (2015), Biometric Authentication Introduction, NIST.