IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 1, Jan 2022

A Primer on Biometric Technologies with Associated Challenges and Barriers

Amit Kumar Bishnoi, Assistant Professor
College Of Computing Sciences And Information Technolog, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email id- amit.vishnoi08@gmail.com

ABSTRACT: Biometrics is attracting more and more attention as businesses look for more secure authentication techniques for e-commerce, user access, and other security applications. With the primary goal of serving as an introduction to this topic, this paper provides an outline of major biometric technologies. Compared to conventional ways of recognizing persons, biometrics can provide more security and ease. Therefore, this paper aims to provide a fundamental behind the topic and further challenges associated with the use of biometrics. It has been revealed that biometric security is a rapidly expanding area of study that deals with using the body's unique identifiers for access management and control. As Biometric technologies are gaining traction, more and more security, ethical and privacy concerns are emerging that need to be addressed for harnessing the full potential of biometric technologies.

KEYWORDS: Authentication, Biometrics, Fingerprint, Identification, Security.

1. INTRODUCTION

The term biometrics is derived from the Greek words "bios" (life) and "metrikos" (measurement or measure). It strictly refers to a science that entails the statistical study of biological properties. Therefore, biometric recognition of individuals should be defined as security systems that examine human traits for proof of identity or authentication. Yet, the word biometric will be used to refer to the biometric identification of individuals. Biometric recognition is a potential solution for security applications that has several advantages over traditional approaches that rely on something that you have such as cards, keys, etc., or something you remember or you know such as passwords, PINs, etc.). A wonderful feature of biometric characteristics is that they are not dependent on anything you are or do, thus you are not required to memorize anything or do any tasks[1].

1.1.The Key Concept of Biometrics

An authentication method known as biometrics depends on the automatic recognition or validation of a person based on distinctive physiological or behavioral traits. Inherent qualities that originate in the earliest phases of human development are referred to as physiological characteristics. The face, retina, fingerprints, iris, and hand of a person are some common physiological traits that are analyzed. Not inherited, but learned, are behavioral traits. Keystroke dynamics, handwriting, voice patterns are examples of common behavioral traits that could be measured [2], [3].

The idea of biometrics has existed for thousands of years. According to history, potters from East Asia used to sign their work by imprinting their fingerprints into the drying clay. Additionally, physical characteristics including weight, hair colour, height, eye colour, and other physical characteristics were used to identify Egyptian traders. Criminologists employed fingerprints to identify repeat offenders during the 19th century. Biometric technology as an automated technique

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 1, Jan 2022

did not first arise until the 1970s. Controlling physical access to buildings was one of early industrial uses of biometrics [4].

This pattern has persisted as the necessity to lessen fraud and restrict physical and logical security flaws has grown.

1.2. Technologies of Face Recognition

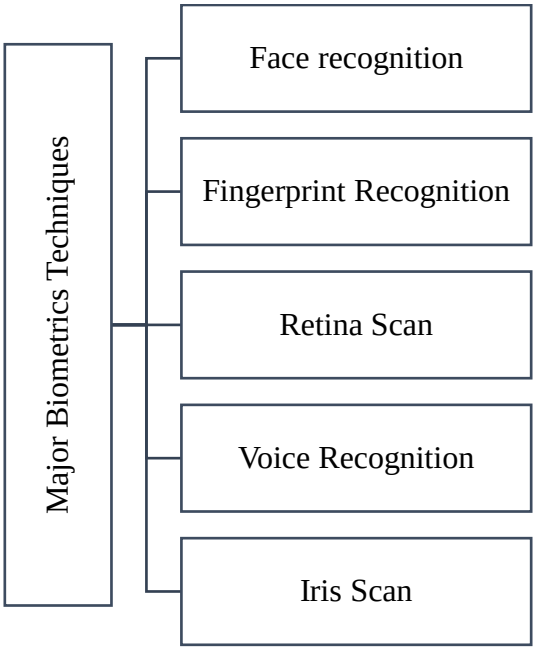

Figure 1: Illustrating the major techniques of Biometrics.

1.2.1. Face Recognition

A facial recognition system evaluates the placement and structure of several facial features to find a match. Sometimes consideration is given to exterior characteristics like the skin. Face detection technology is used to recognise faces in complicated photos where several faces may also be present. Facial recognition for security reasons is a spinoff of this technology. If a system is required for distant recognition, this technology is a great choice because it has advanced rapidly in the last decade. Another benefit of the technology is that faces can be excluded or used in "negative identification," which makes it much simpler to search a crowd for suspicious people[5] (Figure 1).

1.2.2. Fingerprint Recognition

A fingerprint-based identification system scans the surface area of the finger for certain features in the pattern of lines. The ridge ends, bifurcations, and islands of the line patterns are represented by an image that is stored[6].

1.2.3. Iris scan

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 1, Jan 2022

An iris scan involves reading out a person's iris' distinctive features, which are subsequently turned into an encrypted barcode. Iris scanning is renowned as a highly effective security method, particularly when carried out using infrared light.

1.2.4. Retina Scan

Retinal scans are used to map the distinctive patterns of the retina of an individual. Due to its effectiveness as a security precaution, retina scanners are used in nuclear reactors, several military bases, and other high-security areas. Retinal scans are very difficult to fake. Additionally, a scan can only be retrieved from a living individual since the retina destroys so fast after death[7].

1.2.5. Voice Recognition

The process of turning a speech into digital data is referred to as voice recognition. Voice recognition, often known as voiceprint, provides a software-based solution that is contactless, that is widely recognized as among the most efficient biometric authentications. The authentication and identification of an individual depending on the sounds they make while they talk are known as voice recognition. Voice recognition software can detect the biological elements that distinguish each voiceprint [8].

2. DISCUSSION

A well-implemented biometrics solution can assist organizations in dealing with difficult authentication challenges. While it may appear that biometrics should be thriving, in reality, just a few enterprises and government organizations are testing or have adopted biometrics. Skeptics argue that the technology is still too costly, not reliable, difficult to combine with some other systems, and demands people to modify their working habits [9] (Figure 2).

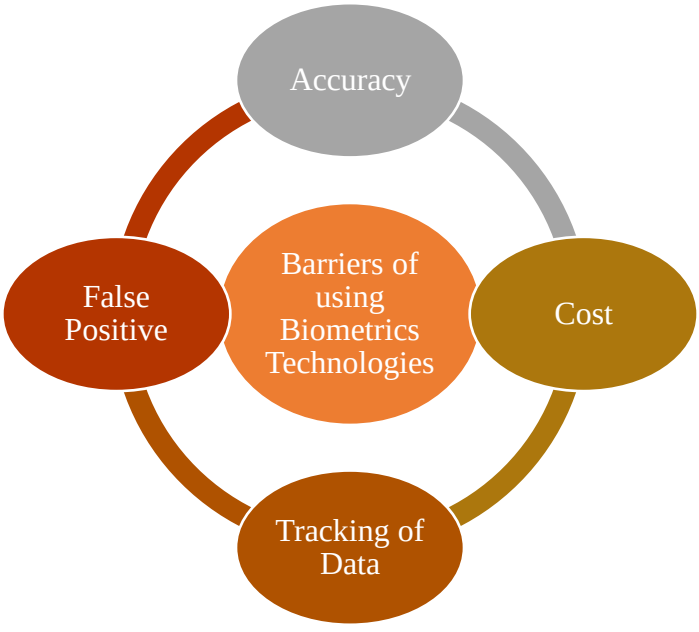

Figure 2: Illustrating the Major Barriers of Using Biometric Technologies.

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 1, Jan 2022

The following are some of the issues that firms encounter when attempting to integrate biometrics into their business processes:

2.1.1. Accuracy

Incorrect matches in validation and affirmative identification systems can allow unauthorized persons to gain access to services or resources. A false match in a negative identification system could result in access denial [10].

2.1.2. False Positives

The majority of popular biometric authentication techniques rely on insufficient data to confirm a user's identity. For instance, during the registration step, a mobile biometric device will scan a whole fingerprint and turn it into data. Future fingerprint biometric verification, however, will only require a portion of the print to confirm identification, making the process speedier overall. By comparing similarities of partial prints to the whole biometric information, a research group from New York University was able to fraudulently hack fingerprint verification in 2018 with a 20% rate of success.

2.1.3. Cost

It should come as no surprise that installing a more sophisticated security system would involve large financial outlays. According to a Spiceworks poll from 2018, "the top reason for not using biometric authentication" is cost, which is cited by 67% of IT experts. A corporation would not only have to pay for the move to biometric identification; according to 47% of those polled, their present systems will also have to be upgraded to enable the switch to biometric security on their gadgets.

2.1.4. Tracking of Data

The privacy of users must be taken into account as the usage of biometric identification systems, such as face recognition technology and other biometric security measures, rises across the world. A user stands the danger of leaving a permanent digital trace that might be followed by malicious actors when biometrics are transformed into data and kept, especially in locations or nations with extensive surveillance measures. Governments and corporations have frequently utilised face recognition technologies to follow and identify people with unnerving precision, severely compromising privacy. Biometric information can become a permanent digital tag that can be used to monitor someone, both knowingly and unknowingly, as surveillance levels rise.

3. CONCLUSION

Biometric technology has been there for centuries, but it has mostly been used in extremely secretive locations with strict security precautions. Biometric systems are all still in their early stages. This study gives an overview of different biometric techniques. In addition to that it also discusses on the barriers that are preventing businesses and authorities to use biometric technique for identification and authentication.

REFERENCES:

[1] M. L. Gavrilova, "Emerging directions in virtual worlds and biometric security research," 2017. doi: 10.1007/978-3-662-56006-8_1.

[2] A. Lumini and L. Nanni, "Overview of the combination of biometric matchers," *Inf. Fusion*, 2017, doi: 10.1016/j.inffus.2016.05.003.

[3] "Biometric sector to generate $13.8bn revenues in 2015," *Biometric Technol. Today*, 2015, doi: 10.1016/s0969-4765(15)30044-8.

[4] J. V. di Nardo, "Biometric technologies: Functionality, emerging trends, and vulnerabilities," *J. Appl. Secur. Res.*, 2009, doi: 10.1080/19361610802210327.

[5] R. Bhatia, "Biometrics and Face Recognition Techniques," *winteknologi.com*, 2013.

[6] V. Conti, "Biometric Authentication Overview: a Fingerprint Recognition Sensor Description," *Int. J. Biosens. Bioelectron.*, 2017, doi: 10.15406/ijbsbe.2017.02.00011.

[7] M. Z. C. Azemin, D. K. Kumar, L. Sugavaneswaran, and S. Krishnan, "Supervised retinal biometrics in different lighting conditions," 2011. doi: 10.1109/IEMBS.2011.6090986.

[8] M. Saini and A. Kumar Kapoor, "Biometrics in Forensic Identification: Applications and Challenges," *J. Forensic Med.*, 2016, doi: 10.4172/2472-1026.1000108.

[9] R. Das, *Adopting biometric technology: Challenges and solutions*. 2017. doi: 10.1201/9781315369945.

[10] R. V. Yampolskiy and V. Govindaraju, "Direct and indirect human computer interaction based biometrics," *J. Comput.*, 2007, doi: 10.4304/jcp.2.10.76-88.