e-ISSN 2320 –7876 www.ijfans.org
Vol.11, Iss.11, 2022
 **UGC CARE Listed (Group -I) Journal**

# An Overview on the Technology of Biometric

DR.KULDEEP PANWAR[1], MR. ANKIT KUMAR[2], DR. VIKAS SENGAR[3]

1Department of Mechanical Engineering, Shivalik College of Engineering, Dehradun
2College of Pharmacy, Shivalik, Dehradun
3Shivalik Institute of Professional Studies, Dehradun

Drkuldeep.panwar@sce.org.in

***ABSTRACT:*** ***As one of the most effective methods for identifying people by collecting and evaluating the unique feature or trait that each person has, including their physical and behavioural features, biometric technology has emerged as a major field of computer vision research. The biometric system is in charge of validating and authenticating each person. Initially used to identify fingerprints, biometric technology has now undergone improvements to become more secure, such as face and iris recognition. Nearly both of them are available, and they are largely regarded as the most reliable and accurate biometric validation method. Face recognition methods in biometric locking systems and Iris recognition technique of identification are discussed in this review article, as well as approaches to make locking systems more efficient, user-friendly, safe, and much better than previously in order to improve locking or security. It goes over face recognition, how it works, and how it's used in many fields, as well as iris recognition, how it works, and how it's used.***

***KEYWORDS:*** ***Biometric, Physiological Biometric, Machine, Security System.***

## 1. INTRODUCTION

Body measurements and calculations are referred to as biometrics. It alludes to the dimensions related to how people seem. In computer science, biometric authentication is employed as a form of access control and verification. Both behavioural and physical traits may be included in biometrics. Examples of physical biometrics that fall under the category of quantification and fact that are produced directly from quantification and make use of human traits are finger scans, facial recognition, iris scans, retina scans, and hand scans. The measurement and data produced by an activity, such as voice-scanning and signature-scanning, are referred to as behavioural biometrics. A biometric system is the combined hardware and software used to carry out biometric validation and authentication [1]–[3].

Biometrics are measurements of the body and computations of human traits. In computer science, access control and identity are accomplished by biometric authentication, also known as realistic authentication. It is also used to locate people in groups that are being watched. The unique, quantifiable traits that are used to identify and categorise people are called biometric identifiers. Physiological traits that are connected to a person's physical attributes, such as body form, are sometimes classified as biometric identifiers. Examples include fingerprint, palm vein, facial recognition, DNA, palm print, hand geometry, iris recognition, retina, odor/scent, and palm veins, among others. Behavioral traits, such as behavioural profile, stride, keystroke, typing rhythm, signature, and voice, are connected to a person's pattern of behaviour. The latter category of biometrics is referred to as "behaviometrics" by some researchers.

Token-based identity systems, like a passport or driver's licence, and knowledge-based identification systems, like a password or personal identifying number, are more conventional methods of access control. Since biometric identifiers are unique to each person, they are more trustworthy than token- and knowledge-based approaches for confirming identification. However, collecting biometric identifiers raises privacy issues regarding how this data may be used in the future.

All biometric identifiers will be categorized into two categories:

- Physical or Physiological.
- Personality.

Physical or behavioural traits: The measurement of distinctive physical and behavioural traits is the main goal of biometrics. Physical biometrics, which uses measurements of human body parts including fingerprints, facial recognition, retina scans, and iris scans, is based on data. The quantification of data generated from achievement is required for the development of behavioral biometrics. Voice and signature scans, for example. The categorization of biometric characteristics is shown in Figure 1.

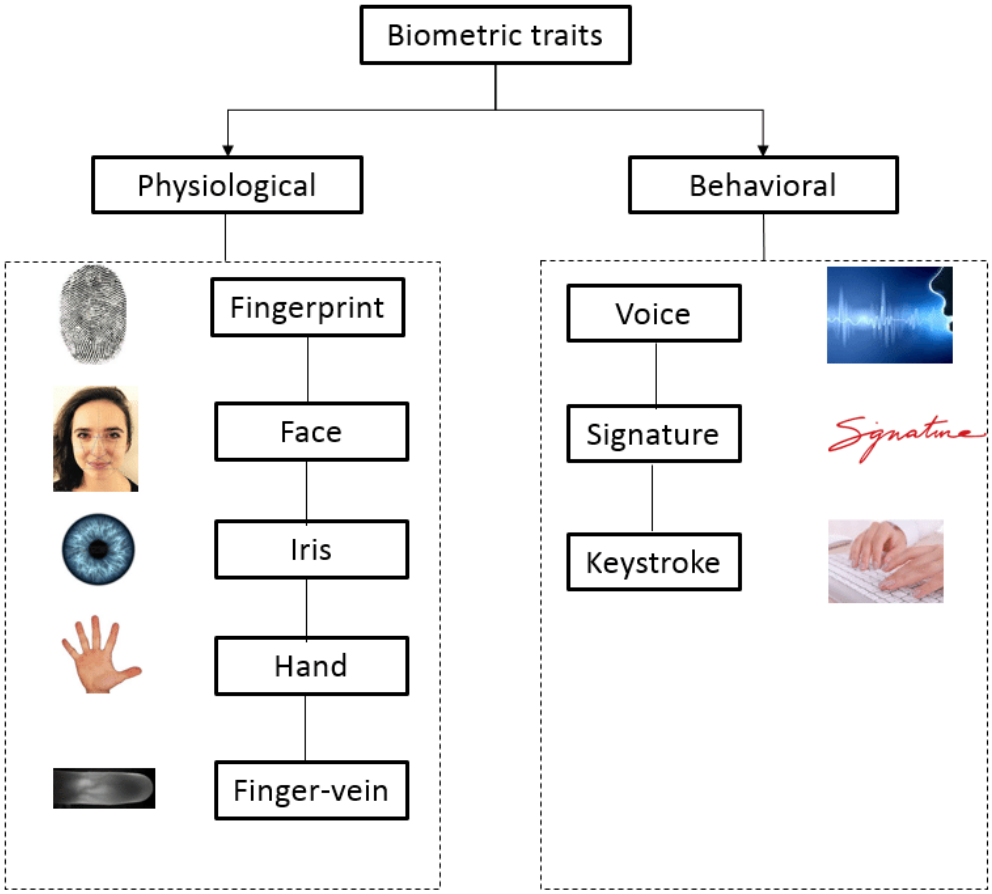


**Figure 1: Illustrates the classification of Biometric traits**[4]**.**

*Physiological Biometric Authentication System:*

*Fingerprints Scanning:*

Fingerprinting is one of the oldest and most widely used biometric technologies today. The technique of likening two instances of friction ridge skin impressions from the human fingers, palms, or toes is known as fingerprint identification, sometimes known as dactyloskopy or hand identification.

*Face Detection:*

A face recognition system has a talent for classifying or verifying a person based on a digital spitting picture or a video source. Facial recognition systems operate in a variety of ways, but in general, they work by matching chosen facial characteristics from a spitting picture with

faces in a database. Originally a computer science application, it has recently found wider applications on mobile platforms and in other fields of expertise, like as robotics. It is naturally used in security measures and may be compared to the following biometrics, which include an individual's physical characteristics that vary from one another. It has recently also become the most widely used business paperwork and a method of marketing in the industrial market among individuals[5]–[8].

For biometric identification, a variety of facets of human physiology, chemistry, or behaviour may be employed. A number of criteria are weighted when choosing a biometric to employ in a certain application. When evaluating the viability of any attribute for use in biometric identification, there are seven such criteria to consider.

- Universality refers to the idea that each user of a system should have the characteristic.
- Uniqueness refers to the need that the feature should differentiate people within the relevant population from one another.
- How a quality changes through time is referred to as permanence. A characteristic with "excellent" persistence will, more particularly, be relatively invariant over time with regard to the particular matching technique.
- Measurability (collectability) refers to how simple it is to measure or acquire the feature. Additionally, the gathered data must be in a format that enables later processing and feature set extraction from the relevant feature sets.
- Technology robustness, precision, and speed are all factors that affect performance (see performance section for more details).
- Acceptability refers to how well members of the target group embrace technology to the point that they are ready to have their biometric characteristic recorded and evaluated.
- The ease with which a characteristic may be mimicked via an item or replacement is referred to as circumvention.

Face recognition is broken down into phases:

- Capture: The system takes a sample of physical or behavioral type upon acceptance, as well as during validation or authentication.
- Extraction: The sample's individual data are extracted to form a template.
- Equivalence: A new sample is next compared to the template.
- Match/nonmatch: The system decides whether the characteristics obtained from the new sample are a match or a nonmatch.

*Working:*

It simply looks for all nodal points on the face that serve as comparison points with the template; these nodal points include the distance between a person's eyes, the width of their nose, the depth of their socket, their cheekbones, jaw lines, chin, and so on. Using nodal points that stand in for a face in the database, a string of integers and a numeric code are formed. It's referred to as a face print. Software like "face it" only needs 14 to 22 face prints to identify a face, whereas validation uses up to 80 nodal points on the human face.

*Benefits:*

- Face recognition has a lot of advantages since it is easy and socially acceptable.
- It's simple to use and recognize.

- Its market value is too low, and it may be called low-cost biometrics.

*Disadvantages:*

- When it comes to recognizing twins, it fails miserably.
- Image quality is important.

*Recognition of the Iris:*

Iris remembrance is a biometric identification and authentication technique that classifies and authenticates an individual's iris pattern using pattern recognition algorithms. In order to be able to verify a person, it requires taking a high-resolution photo of their iris, which is distinctive and differs from person to person. It is now acknowledged as the most accurate and secure biometric technology on the market. Iris recognition is the biometric technique that is most often utilised. A shielded and internally protected organ, the iris has a distinct texture that is constant throughout the course of a person's lifetime.

*Working:*

Rings, furrows, and freckles are among the more than 200 spots on the iris that may be utilized for contrast. The scan is carried out using a conventional camera that uses both visible and infrared light. John Daugman provides one of the iris recognition algorithms used by the industry. A picture of the iris is recorded and transformed into an iris code, which is a bit stream similar to a bar code. The information from a collection of Gabor wavelets is used to create the Iris code.

*Applications:*

- Banking: To prevent ATM and INTERNET BANKING scams, banks are using it as an authentication criterion.
- Social Welfare: Could be used to track down someone who has applied for social welfare several times under various names.

- *DNA:*

Not long ago, rumors circulated in Russian show industry that one of the country's most famous singers had two dads, each of whom attempted to exert influence on his son. Special programs were produced, and the issue was addressed, but the audience was only interested in one thing: who was the singer's actual father. The vocalist was perplexed as well. The musician and both of his father’s decide to undergo a DNA test in one of the shows.

- *Geometry of the Hand:*

The utilization of the geometric form of the hand for recognition is known as hand geometry. This technique was popular ten years ago, but it is now seldom utilized. The technique is based on the notion that one person's hand shape varies from another person's hand shape and does not change beyond a certain age. It is, however, not unique.

- *Stroke Pattern:*

The keystroke is a human behavior, which means that various people have distinct methods for pressing keys, which allows for identification.

- *Scanning Signatures:*

Another behavioral biometric is signature, which allows data to be extracted from a person's signature.

- *Recognition of speech:*

The voice, like many other features utilized in biometric techniques, is one-of-a-kind. Analyzing the voice and identifying the individual takes very little time, similar to gait style. In biometrics, a numerical representation of the sound is given as a "voice print."

## 2. LITERATRUEREVIEW

E. Al Solami et al. discussed a review on analysis of Biometric Technology[9].This research looked at the use and acceptability of biometric technologies in Canada. The paper's introduction shows that biometrics technology has been around for decades, despite just becoming prominent in the past two decades. In terms of information technology, Canada is well ahead of the pack. Financial services, immigration, and law enforcement are the three areas where biometric technology are being used and accepted. For sampling, the research relies on judgment, and questionnaires are used to gather data. The study finds that biometric technology adoption is at the adaption stage in Canada, based on the high rate of uptake and acceptance of these technologies. Individuals' acceptance of biometric technology is also influenced by their age and experience, with the most experienced participants exhibiting the greatest percentage of acceptance.

John Effah et al. discussed about Biometric technology for voter identification[10]. Our research investigates how and why Ghana's first effort to utilize biometric technology for voter identification and verification in national elections in 2012 failed. The analytical lens is activity theory, and the technique is interpretative case study. Our results indicate that biometric technology's ability to offer accurate identification is dependent not just on its technological capabilities, but also on real-time connection between registration centers and an electronic national register. Furthermore, election officials must be thoroughly taught to operate the devices and given instructions on how to deal with malfunctions. While biometric technology provides useful capabilities, it is just one component of a larger human activity system.

T. Kazimov et al. discussed a review on the role of Biometric Technology[1]. The importance of biometric technologies in information security is discussed in this article. The increasing terrorist danger in the globe has prompted the development of biometric identification systems in order to enhance security systems. The benefits of biometric technology are shown to solve problems confronting law enforcement, state security, and national defense assurance agencies. This is where the suggestions are made.

## 3. DISCUSSION

Individuals may be identified using biometrics, which are biological measures or physical traits. It is utilized in systems that employ fingerprints for identification, such as national identity cards and health insurance schemes. Airport security is a must. Biometrics, such as iris recognition, are sometimes used in this area. Biometric technology, such as fingerprint scanners and facial recognition, are widely utilized on contemporary devices and are often regarded the safest way of protecting accounts and devices. Biometric technology has a number of drawbacks, including costs, data breaches, tracking, and data. The author covers biometric technologies, kinds, and biometric characteristics in this article. Biometric technology has a promising future since it can be used for verification and authentication.

## 4. CONCLUSION

Individuals may be identified using biometrics, which are biological measures or physical traits. Fingerprint mapping, face recognition, and retina scanning, for example, are all examples of biometric technology, although these are just the most well-known. So far, we've grasped the definition of biometrics and the many kinds of biometrics. We've also looked at the many kinds of biometrics technologies. We will be able to get a solid understanding of the superior one technology by the conclusion of this article. Iris recognition is more accurate here, but it's also more expensive, and it can't locate the iris on the fly. So, in order to improve, we must strive to make this method less expensive, and to enhance iris locating talent, we can combine it with facial recognition technology, which doubles security. This would improve the security of data in a nation like the UAE, as well as the simplicity with which a person may be authenticated.

**REFERENCES:**

[1] T. Kazimov and S. Mahmudova, "The Role of Biometric Technology in Information Security," *Int. Res. J. Eng. Technol.*, 2015.

[2] H. F. Neo, D. Rasiah, D. Y. K. Tong, and C. C. Teo, "Biometric technology and privacy: a perspective from tourist satisfaction," *Inf. Technol. Tour.*, 2014.

[3] K. Karkazis and J. R. Fishman, "Tracking U.S. Professional Athletes: The Ethics of Biometric Technologies," *Am. J. Bioeth.*, 2017.

[4] "Classification-of-biometric-traits-adapted-from-15." .

[5] C.-H. Ko and C.-C. Yu, "Exploring Employees' Perception of Biometric Technology Adoption in Hotels," *Int. J. Organ. Innov.*, 2015.

[6] L. Hamid, "Biometric technology: not a password replacement, but a complement," *Biometric Technol. Today*, 2015.

[7] J. Lindquist, "Reassembling Indonesian Migration: Biometric Technology and the Licensing of Informal Labour Brokers," *Ethnos*, 2018.

[8] R. Clodfelter, "Biometric technology in retailing: Will consumers accept fingerprint authentication?," *J. Retail. Consum. Serv.*, 2010.

[9] E. Al Solami, "Analysis of biometric technology adaption and acceptance in Canada," *Int. J. Adv. Comput. Sci. Appl.*, 2018.

[10] J. Effah and E. Debrah, "Biometric technology for voter identification: The experience in Ghana," *Inf. Soc.*, 2018.