ISSN 2278-3091
Volume 12, No.3, May - June 2023
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse061232023.pdf
https://doi.org/10.30534/ijatcse/2023/061232023

Opportunities and Challenges in Biometric Technology

Aakash Pravinbhai Vamja[1], Jatin Satishbhai Shirsath[2], Prof Jigar Bhawsar[3]
[1]Student of MCA,Parul University,India, skyvamja206@gmail.com
[2]Student of MCA,Parul University,India, jatinshirsath212@gmail.com
[3]Prof of MCA and MSc IT, FITCS , Parul University, India, jigar.bhawsar24744@paruluniversity.ac.in

Received Date April 19, 2023 Accepted Date: May 22, 2023 Published Date: June 06, 2023

ABSTRACT

Biometric advancements have the potential to provide more robust security and authentication approaches compared to conventional password-based security measures. When compared to knowledge-based security, biometrics relies on what makes you unique rather than what you know. Biometrics offers promising opportunities to enhance security but also comes with its own set of challenges. Successful implementation requires attention to these possible flaws and a rise in user approval. This article explores the potential benefits of biometric security in an effort to ascertain how broadly adopted it is. It analyses the correlation between user approval and their opinion of the feature's usefulness and accessibility. It also examines crucial acceptability elements like social, organizational, and cost considerations.
Biometric systems are a type of pattern recognition technology that may identify a person by vetting their claimed physiological and/or behavioural traits. The following concept of a biometric system can be very broad, which is problematic when thinking about the specifics of contemporary biometric applications. The use of biometrics has the potential to greatly improve upon the security of current methods of authentication and identification. The broad use of biometrics solutions, in fact, has significant ramifications for the way we think about the individual's place in society. However, certain factors and limits are taken into account in the context of the application area, as is the case with any technology. Further progress will be made as scientists investigate multiple, interconnected topics. This paper addresses technical and engineering concerns while highlighting potential applications of contemporary biometric technologies.

Key words : Biometrics, Face, Finger print, Iris, Information Security, Authentication.

1.INTRODUCTION

The term "biometrics" was coined by combining the Latin terms for "life" (bio) and "measurement" (matron). Thus, it is the process of establishing the user's identity by verifying their possession of specific, measurable characteristics. Biometric identification, then, is the process of verifying an individual's identity—for example, in order to log in to a service or gain access to private information—using some aspect of that person's biometrics, such as a fingerprint scan, face image, signature, or voice recognition. If the user has already been added to the system database or if the user's information has already been entered into the database, then the user's identity has been verified. When a person signs in, their input data is compared to their previously fed input data to ensure a match between their physiological or behavioural characteristic and those already enrolled in the system. Whenever a user who has never been enrolled before enrolls for the first time, the user's identifying information is entered and stored in the programme for future use [1].

The development of modern biometric systems may be traced back to the scientific method, empirical evaluation, and the categorization of a given physical or behavioural attribute into sub-types. Image processing, pattern identification, statistics, simple signalling, and some machine learning models like knowledge based systems and neural networks are at the heart of contemporary biometrics. To measure and then electronically recognize such characteristics automatically is the essence of a modern biometric system. Forensic criminology and government security were two of the primary areas that stood to benefit from fingerprint technology in the form of AFIS until the late 1980s. However, research into automatic and machine recognition for image processing and pattern identification has continued to improve our ability to separate patterns of interest from their context and to make informed judgements about the categories to which they belong. In this context, "pattern" refers to a quantitative or structural representation of an object or other entity of interest, such as a speech signal, DNA, PCB intensity image, multi-spectral image, fingerprint image, document image, iris image, face image, etc.

2. LITERATURE REVIEW

This section will review the literature based on various biometric techniques available till date.

Fingerprints

In terms of biometrics, it's been around the longest. Fingerprints can now be digitally imaged with this technology. It reads the imprint of human fingers' friction

ridges on the skin. The sensor picks up on the finger's individual creases and kinks in the skin. Palm scanning is subject to the same limitations.

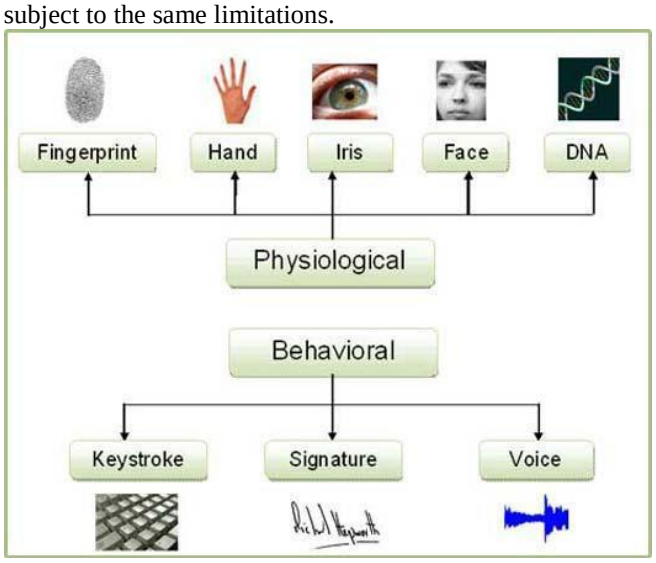

Figure 1 : Biometric Techniques [2]

Figure1 shows that how Above categories works.

2.1 Eye Scanning

Recognizing an individual by their eyes can be done in two different ways [7]:

2.2 Retina scanning

The user looks into a device that scans his retina with a laser. The user's vascular system is analyzed by the gadget. Each individual has a somewhat different set of blood vessel connections. The user has to keep his or her gaze steady while the laser examines the eye, which might be challenging.

2.3 Iris Recognition

One need not have their eyes close to the scanner, unlike with retinal scanning. Here, a camera takes the pictures. A video-based imaging method is utilized to acquire the iris patterns. The gadget then analyses the acquired image. There are 266 individual dots in this picture, and they all represent different iris features like furrows and rings. There is no age-related change in the iris. There is no need for regular picture updates.

Iris recognition is a form of biometric identification that identifies individuals based on the distinctive patterns of their irises. The coloured part of the eye that surrounds the pupil is called the iris, and it is composed of distinctive patterns of ridges, furrows, and other characteristics that can be used for identification purposes. The iris can be distinguished from other people's irises by comparing its ridges and furrows. Iris recognition technology works by taking a picture of the subject's iris and analysing its individual characteristics before comparing those characteristics to a library of pre-existing iris templates.

The method of iris identification is broken down into three primary steps: acquiring a picture, extracting features, and matching those features. In the initial step of the process, a photograph of the person's iris is taken with a camera. This photograph is typically obtained at a distance of approximately 10 centimetres and in a setting with ample lighting. After that, the image is processed to improve its quality and eliminate any noise it may include.

In the second step of the process, the distinctive aspects of the iris, such as its ridges, furrows, and other traits, are retrieved and included into the creation of a digital template. This template is then utilized to build an image of the iris. After that, the template is saved in a database so that it can be accessed at a later time.

In the final step, the digital template of the person's iris is compared to the previously stored templates in the database in order to identify or verify the person. The method of matching entails comparing the features retrieved from the iris with those stored in the database in order to establish the degree of similarity between the two sets.

Iris recognition provides a number of benefits that set it apart from other forms of biometric identification, such as facial recognition and fingerprint biometrics. Iris identification does not require physical contact and can be carried out at a distance, all of which make the process more hygienic and convenient. In addition, the distinctive patterns of the iris are quite stable and do not alter over the course of one's lifetime, making it a trustworthy method of biometric identification**.**

2.4 Face Recognition

Facial recognition often employs the usage of a simple camera or webcam with high enough resolution to capture faces in full detail. When recognizing people in the dark, the peripheral parts of the face are less important than the central part of the image. These qualities are eternal. Avoiding obvious details like hairstyles and facial expressions. If the representation matches an existing database, the user is verified as legitimate [3].

2.5 Handprint Imaging

A user's hand is scanned from an image. Digital signal processing methods are used to extract and store data such as finger spacing, finger length, and hand size. The formats are made automatically. It is possible to verify the qualities with these samples. Optical scanners are commonly used to capture hand geometry.

2.6 Palm print Recognition

Tiny details, ridges, principal lines, folds, orientation, and vein geometry are retrieved for identification. Vein geometry varies across individuals. The user authenticates themselves by placing their hand on the screen and having their veins scanned using infrared light. Vein patterns, which appear as a brilliant and dark pattern on the hand, are captured and removed. When infrared light is absorbed by the veins in the hand, a darker pattern is created. This biological pattern is recorded in the gadget and used as a sort of template. The transducer then converts the analogue signal into a digital one for further comparison.

2.7 DNA Analysis

The criminal justice system frequently use this method of verification. The user's DNA is verified through the collection of biological samples such blood, tissue, hair, and nails. The analysis of DNA is a time-consuming process. DNA is another distinguishing feature, albeit hair and nails can be easily taken [4].

2.8 Voice Verification

The user is prompted to verbally provide a passphrase or code for verification purposes. Both his physiological (the size and form of his vocal cords) and behavioural (the pitch of his voice) vocal features are measured. In this case, voice identification is not used in the verification procedure.

Identification is more of a many-to-one or many-to-many procedure, while verification relies on storing and comparing samples of a speaker's speech pattern with other recordings of that speaker. Voice verification has been trained on a certain speaker.

2.9 Signature scanning

It's a real-time examination of the user's signature in terms of things like shape, size, writing speed, time, and pressure applied by the user's hand while signing. The act of signing itself can be replicated, but the characteristics associated with it cannot [6].

2.10 Keystroke

It boils down to a specific method of pressing a key. The characteristics that can be measured are the length of time a key is depressed, the length of time it takes to release, and the sound that is produced at the beginning and end of each press.

3.OPPORTUNITIES IN BIOMETRIC TECHNOLOGY

Applications such as access control, identification, and security have contributed to biometrics' meteoric rise in popularity in recent years. While fingerprint recognition is the most popular biometric method, there are alternative methods, each with its own set of benefits and drawbacks. Some potential applications of various biometric methods are listed below:

3.1 Face Recognition

Recognizing an individual by their face characteristics is what we call a biometric approach. The process begins with a photo of the person's face, which is then compared to a databased template. Face recognition is non-intrusive and has many potential uses, including but not limited to identity, security, and access management. Its use in smartphones and other mobile gadgets, as well as on websites, is also on the rise. However, its accuracy may suffer in dim lighting or when the subject's face is partially concealed, compared to other biometric methods.

3.2 Iris Recognition

Individuals can be identified through the use of biometric methods by analyzing their iris patterns. A picture of the person's iris is taken and compared to a databased template. Access control and border security are only two examples of when iris recognition could be useful thanks to its reliability and versatility. However, it can be more intrusive than other biometric methods because the person being scanned must both physically approach the sensor and stare directly at it [7].

3.3 Voice Recognition

Voice recognition is a form of biometrics that identifies a person through their distinctive vocal patterns. Recording the person's voice and then analyzing it for characteristics like pitch and tone is part of this process. Voice recognition doesn't require any kind of physical contact from the user and has several potential uses in the realm of security and authentication. And its use in smart speakers and other digital assistants is gaining ground, too. If the person being screened has a cold or is speaking in a very noisy setting, however, this biometric method may not be as reliable as others.

3.4 Palm Print Recognition

One form of biometric identification known as "palm print recognition" takes advantage of a person's palm's distinctive patterning to establish their identity. A picture of the person's palm is taken and compared to a databased template. Accurate palm print recognition has several potential uses, including security and personal identification. Compared to other biometric methods, like fingerprinting, it is more durable and difficult to forge. However, because it needs the user to rest their palm on a sensor, it isn't always the most practical biometric method.

3.5 DNA Analysis

The use of a person's DNA sequence as a form of biometric identification is known as DNA analysis. Individual DNA is taken and analyzed for distinctive markers. DNA analysis has a wide range of applications, including forensics and paternity testing, and is known for its high level of accuracy. Taking a bodily sample from an individual can make this biometric method more intrusive than others. Furthermore, it may not be suited for real-time applications because to its high resource and time requirements.

4.CHALLENGES IN BIOMETRIC TECHNOLOGY

Some of the problems that can arise with various biometric methods are mentioned below:

4.1 Fingerprint recognition

Some people may have low-quality fingerprints that are challenging to capture and analyse, which is one of the key issues with fingerprint recognition. Age, skin disorders, and jobs that include regular contact with other chemicals or substances are only some of the causes. Some people may also try to trick the system by submitting fake or otherwise changed fingerprints, which can cause either a false positive or a false negative.

4.2 Face recognition

Face recognition can be affected by changes in lighting, pose, expression, and occlusion. These factors can make it difficult to capture a clear and accurate image of an individual's face, and can also affect the ability of the system to match the face to a stored template. In addition, some face recognition systems have been found to exhibit racial and gender biases, which can lead to inaccurate results [3].

4.3 Iris recognition

Although iris recognition is often regarded as one of the most reliable methods of biometric authentication, it can be compromised by factors including low-resolution images, occlusion, or age- or illness-related changes to the iris's appearance. In addition, the size or form of an individual's iris may make it difficult to capture, resulting in a false negative [7].

4.4 Voice recognition

A voice's ability to be recognized can be hampered by factors such as ambient noise, tonal shifts, and pronunciation or accent differences. Furthermore, there is always the risk of false positives and false negatives if someone tries to trick the system by utilizing a pre-recorded or synthetic voice [9].

4.5 Behavioral biometrics

Time-based behavioural changes can have an impact on behavioural biometrics, which includes techniques like

keyboard dynamics and mouse dynamics. A person's typing speed or mouse movement, for instance, may alter as a result of variables including exhaustion, distraction, or injury. Furthermore, attempts that try to mimic or recreate an individual's behaviour might cause either false positives or false negatives when using behavioural biometrics.

It is clear that rigorous system design and implementation, as well as continual monitoring and evaluation, are required to ensure that a biometric system's accuracy and security are maintained over time in light of the difficulties inherent in its use.

5.CONCLUSION

In conclusion, biometric technology presents various prospects for boosting both security and convenience in a wide variety of applications. These applications include law enforcement and access control, the authentication of mobile devices, and financial transactions, among others. Because of their one-of-a-kind and distinguishable characteristics, biometric identifiers are notoriously difficult to forge or steal. Meanwhile, the proliferation of low-cost sensors and technologically advanced algorithms has made biometric technology more accessible and efficient than it has ever been before.

However, there are also a number of serious difficulties involved with the use of biometric technology. These difficulties include concerns around privacy, accuracy, and security. Particularly in instances in which biometric data is stored in centralized databases, there is a risk that personal information could be compromised or misused as biometric technology becomes more widely adopted. This risk is compounded by the fact that there is also a risk that biometric data could be stolen. In addition, biometric technology is not failsafe and might be vulnerable to problems such as inaccuracies, bias, and attacks.

It is vital to address these obstacles and issues through thorough system design, implementation, and evaluation in order to fully achieve the potential of biometric technology. This can only be accomplished by taking these steps. This involves installing stringent security measures to prevent unwanted access or tampering, assuring the accuracy and reliability of biometric systems, and following best practices for data protection and privacy protection. Keeping these things in mind, biometric technology has the potential to alter the way we safeguard our digital and physical environments. This would provide us the ability to improve security and convenience while maintaining personal privacy and data protection.

REFERENCES

[1] Mohamad El-Abed, et al., “A study of users’ acceptance and satisfaction of biometric systems,” 2010 IEEE International Carnahan Conference on Security Technology (ICCST), IEEE, 2016.

[2] A.K. Jain, A. Ross, and S. Prabhakar, An introduction to biometric recognition, IEEE Transactions on Circuits and Systems for video Technology, 14(1), 2014, 4-20.

[3] T. Chiara, M.C. Viola, and I. Leo, New borns face recognition: Role of inner and outer facial features, Child Development, 77(2), 2016, 297-311.

[4] Y. Du, C. Belcher, Z. Zhou, and R. Ives, Feature correlation evaluation approach for iris feature quality measure, Elsevier, Signal Processing, 90, 2015.

[5] Joseph Romanowski, Kirsanov Charles, Patricia Jasso, Shreyansh Shah, and Hugh W. Eng, “A Biometric Security Acceptability and Ease-of-Use Study on a Palm Vein Scanner,” Proceedings of Student-Faculty Research Day, CSIS, Pace University, May 6, 2016.

[6] Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Conference on Fairness, Accountability and Transparency, 77-91

[7] Waghmare, L. M., & Holambe, R. S. (2019). A review on iris recognition techniques. 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 392-397

[8] Jain, A. K., Ross, A., & Nandakumar, K. (2016). Introduction to biometrics. Springer

[9] Jiang, Z., & Sahidullah, M. (2019). A comprehensive review of voice biometric technologies. Journal of Ambient Intelligence and Humanized Computing, 10(9), 3573-3590.