WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Review on Biometric Authentication

[1]Krishha Y S, [2]Jayaswethashree N.

[1]I BSc AIML Sri Krishna arts and science college, Coimbatore, Tamilnadu, India.
[2]I BSc AIML Sri Krishna arts and science college, Coimbatore, Tamilnadu, India.

ABSTRACT

Each human being has distinctive qualities that set him or her apart from everyone else. Physical traits like fingerprints, eye colour, hair colour, hand geometry, speech inflection and accent, signature, or the way a person types on a computer keyboard, among others, set a person apart from others. A biometric system is a piece of technology that examines an individual's physiological, behavioural, or both attributes as input and determines whether the person is a trustworthy or dishonest user. We are also adopting biometrics extensively due to the need for high security systems. This paper focuses on biometric authentication, including its varieties, benefits, drawbacks, and potential developments.

Keywords: Fingerprints, Geometry, Inflection, Accent, Biometrics, Technology, Physiological, Attributes, Security, Authentication

1. INTRODUCTION

The two terms that make up the name "biometrics" are "bio" (the Greek word meaning "life") and "metrics" (Measurements). A subset of information technology called biometrics works to establish a person's identity using personal characteristics. Due to its high level of identification accuracy, biometrics is currently a buzzword in the field of information security. Each human being has distinctive qualities that set him or her apart from everyone else. Physical traits like fingerprints, eye colour, hair colour, hand geometry, speech inflection and accent, signature, or the way a person types on a computer keyboard, among others, set a person apart from others .This uniqueness of a person is then used by the biometric systems to −

□ Identify and verify a person.

□ Authenticate a person to give appropriate rights of system operations.

□ Keep the system safe from unethical handling.

1.1 Are biometrics secure?

There is a critical necessity to safeguard the systems and data from unauthorised users given the expanding usage of information technology in fields like finance, science, medicine, etc.

A person can be authorised and authenticated using biometrics. Despite the frequent pairing, these phrases have different meanings. Although modern biometric systems frequently rely on acquiring biometric data locally and then cryptographically hashing it so that authentication or identification may be carried out without direct access to the biometric data itself, biometric data may be stored in a centralised database. The usage of biometrics is made possible by high-quality cameras and other sensors, but they can also make an assault easier. Because people do not cover their faces, ears, hands, voices, or gaits, it is easy to launch attacks by secretly collecting biometric information about them. In 2002, Japanese researchers demonstrated how an attacker could lift a latent fingerprint from a glossy surface using a gelatin-based candy. This attack, known as the "gummy bear hack," was the first to target fingerprint biometric authentication. Given that gelatin has a capacitance close to that of a human finger, the transfer of gelatin might trick capacitance-based fingerprint scanners. Other biometric components can likewise be defeated by determined attackers. In 2015, Jan Krissler, commonly known as Starbug, a biometrics researcher with the Chaos Computer Club, showed how to get enough information from a high-resolution photo to circumvent iris scanning authentication. The Samsung Galaxy S8 smartphone's iris scanner identification method was reportedly defeated in 2017 by Krissler. Krissler had previously shown that Apple's Touch ID fingerprinting authentication system was similarly vulnerable by recreating a user's thumbprint from a high-resolution photograph. Researchers were able to beat Apple's Face ID facial recognition system using a 3D-printed mask barely two weeks after the iPhone X's introduction by Apple. Face ID can even be defeated by family members of the verified user, such as children or siblings.

2. TYPES OF BIOMETRICS

The two main categories of biometric modalities are physiological and behavioural. Recognition of fingerprints, irises, faces, and palm veins are examples of physiological biometrics. A few examples of behavioural biometrics are voice and signature recognition. Nonetheless, the following are the known categories of biometrics:

2.1. Fingerprint recognition:

By photographing a person's fingertips and cataloguing the whorls, arches, and loops of the fingertip, fingerprint identification technology has been developed. For precise examination, it also records the patterns of ridges, furrows, and minute details. The process can be done in three ways:

- Minutae based
- Correlation based
- Ridge featurebased

A very safe, dependable, and robust biometric solution is the fingerprint. For decades, law enforcement organisations have used this technology to identify criminals. This technology is currently growing in popularity in areas such as workforce management, finance, and home security.

2.2. Iris recognition:

The best biometric identification technology, according to many, is iris recognition. It examines the features of the iris, which are located in the pigmented tissue around the pupil and include rings, furrows, and freckles. the video camera-equipped iris scanner that can be used while wearing spectacles or contact lenses. Generally, iris recognition can be done by two methods:

- Daugman System
- Wildes System

Iris recognition is deployed by many countries in crucial places like border crossings, banking, private companies, institutes, law enforcement agencies etc.

2.3. Face recognition:

Face photos are captured using a digital video camera, and a face recognition technique examines details like the separation between the borders of the eyes, nose, mouth, and jaw. These measurements are divided into facial planes and stored in a database where they can later be compared. Then, the system creates a template on the database for that person to compare the data for further uses.

2.4. Retina recognition:

Retina recognition is a biometric technique that records the distinctive patterns of each person's retinal blood vessels using infrared technology. Retina recognition is regarded as a trustworthy biometric authentication method because it is a protected internal organ of the eye.

2.5. Hand geometry:

The shape of a person's hands and their attributes are used in hand geometry recognition. The hand geometry reader takes multiple dimensions of a person's hand. After that, it archives the information for later analysis and measurement. It is most well-liked for its comfort, simplicity, and widespread acceptance. This approach isn't as distinctive as face or fingerprint recognition, though.

2.6. Voice/speech recognition:

Voice and voice recognition uses both behavioural and physiological biometrics. It functions with speech patterns that speech processing technology has recorded. To identify a person's speech, this system examines the basic frequency, nasal tone, cadence, inflection, etc. Other names for it include "speech to text" (STT), "computer speech recognition," and "automatic speech recognition" (ASR).

2.7. Palm vein recognition:

Pam vein recognition is one of the physiological subtypes of biometrics that examines the distinctive vein patterns in a person's hand palms. Like other biometric technologies, it begins by taking a picture of the user's palm before analysing and processing the data from their veins and storing it for further comparison.

2.8. Signature recognition:

One of the biometric behaviour kinds is signature recognition. It functions in both static and dynamic ways. In this recognition system, a person's signature is taken into account while identifying them. It is based on measures like the quantity of vertical slope components and the amount of internal contours.

2.9. Handwritten biometric recognition:

Similar to signature recognition, handwriting biometrics are unquestionably a behaviour kind of biometrics. It is a method of identifying someone based on their handwriting style. Similar to signature recognition, it can be divided into static and dynamic categories.

2.10.DNA Recognition:

DNA biometrics differ significantly from conventional biometric modalities. It cannot be done in real time and requires a tangible physical sample. It is a highly accurate recognition technology.

2.11. Ear Biometrics:

One of the most reliable biometric authentication methods is ear biometrics. Some think it offers more accurate results than a fingerprint and will dominate biometrics in the future.

2.12. Gait Recognition:

A biometric technology technique called gait recognition examines a person's gait, including their saunter, swagger, and sashay, among other walking styles. The technology used for surveillance analysis is very effective.

2.13. Odour Recognition:

Very unlike fingerprint or facial recognition systems, this biometric approach. It utilises a person's body odour for identification and verification.

2.14. Typing/ keystroke recognition:

One of the behavioural types of biometrics is the recognition of keyboard strokes or typing. It examines how a person types by seeing how they push the keys. The keystroke dynamics makes use of information about how and how quickly someone types on a keyboard.

2.15. Finger Vein recognition:

A biometric identification technique called finger vein recognition uses the vein patterns found in the fingernails below the skin's surface. It compares previously collected data with a person's finger's vascular pattern.

2.16. Eye vein recognition:

Eye vein recognition is a biometric technology that applies pattern-recognition methods to video pictures of a person's eye veins. It is one of the most accurate biometric authentication techniques since the veins are intricate and distinctive.

2.17. Skin Reflection:

Skin reflection biometrics is a rather rare biometric technique. With this technology, photodiodes read the scattered light that is then processed to carry out the authentication. Many LEDs transmit light into the human skin at different wavelengths.

2.18. Lip motion:

Using lip motion analysis technologies, a password is generated based on the user's activities. It then compares the new lip motion data with previously stored data to verify the information. Lip motion technology is a relatively recent biometric modality when compared to other modalities. 2015 saw the US grant a patent to Professor Cheung Yiu-ming of Hong Kong Baptist University for his invention of lip motion technology.

2.19. Brain Wave Pattern:

The biometric technique of brainwave recognition is unusual and startling. It analyses the brain's signals to build a distinctive, individual feature set on the database. Some studies think the biometric identification technique is 100% accurate.

2.20. Footprint and Foot Dynamics:

A distinctive physiological type of biometric identification, the footprint can be recognised similarly to fingerprint, finger vein, palm vein, iris, and retina recognition. Compared to other modalities, it is a biometric identification system that is relatively new.

This method records an individual's footprint-based biometric identification attributes. then put the information in a database for later comparison to confirm the identity.

2.21. Thermography Recognition:

Infrared cameras are used in facial thermography to record a person's blood flow beneath the skin. The underlying pattern then produces a strong biometric trait for accurate identification. This technology can be used to evaluate a person's "liveness."

3. ADVANTAGES OF BIOMETRICS:

Globally, biometric technology is becoming more and more popular every day. Many government agencies, international corporations, institutions, banks, and hospitals, to name a few industries, highly approve biometric solutions. Every industry is seeing growth, but national identity is expanding the fastest, along with finance, banking, workforce, and borders. According to research, consumers place more trust in contemporary biometric technology than in conventional security systems.

3.1. Security:

In the past, we used passwords that contained letters, numbers, and other symbols, but these are getting easier to crack every day. Every year, there are countless hacking incidences, and we continually lose money. In contrast to passwords, biometric technology offers a variety of solutions that are virtually impossible to hack. This is a huge assistance to us, especially for business owners who have long struggled with security issues.

3.2. Accuracy:

Conventional security systems frequently make mistakes that cost us a lot of time, money, and resources. Passwords, personal identification numbers (PINs), and inaccurate smart cards are the most popular security measures. Yet, biometrics uses your bodily characteristics, such as your fingerprints, palm vein, retina, and others, to precisely identify you wherever at any time.

3.3. Accountability:

Other means of verification make it possible for anyone to steal your password or security number and access your personal data, which is extremely unsafe and a persistent problem. Yet, biometric security requires your direct participation in order to login or pass the security system, ensuring complete accountability for all of your actions.

3.4. Convenient:

Consider how tense it would be if you continually lost your passwords. It's not just you. Everybody has experienced the difficulty of remembering or writing down every password, and we are prone to forgetting them in stressful situations. The convenience of biometric solutions, which stand to be the most convenient solution ever, can't be beaten by any of the useful tools that can perform the work for you. It doesn't require you to memorise or make a note of anything because your credentials are always with you.

3.5. Scalability:

Biometrics are extremely scalable solutions for all types of applications, unlike other alternatives. Several government initiatives, financial security systems, workforce management, etc. utilise biometric technologies. The scalability of its solutions makes it feasible.

3.6. ROI:

When compared to alternative security systems, biometric solutions will provide you the best return on investment. With just one biometric device and software, a major company's thousands of employees can be monitored. On the other hand, managing a large resource to do the same task would take more time than using the right biometric solution.

3.7. Flexibility:

Without a doubt, the most adaptable security solution is biometric systems. You don't need to bother learning the uncomfortable alphabets, numbers, and symbols needed to create a complex password because you already have your own security credentials with you.

3.8. Trustable:

According to reports, younger generations have a greater level of faith in biometric solutions than other solutions. Banks have already begun implementing biometric security solutions to increase client security and dependability..

3.9. Save Time:

Time is very efficiently saved by biometric solutions. Most of the time, all it takes to pass the system is placing your finger on a gadget or looking at a retina device. The layers of inconveniences and interrogations associated with traditional procedures, on the other hand, make them irritating and intolerable.

3.10. Save Money:

Governments are investing money to build a national biometric database so that citizens can receive government services more accurately and more affordably. Businesses are implementing biometric systems to obtain reliable data that saves time and money. Any business may watch its employees and cut the excess costs it has been incurring for years with a small investment. The era of information technology is now. Day by day, our traditional security measures will become obsolete. To improve our security and deter robbers, we must employ the newest technologies.

4. DISADVANTAGES OF BIOMETRICS

Technology is designed to make our lives better. Every part of our way of life is improved by it. Another remarkable breakthrough that significantly alters our way of life is biometric technology. The adage "with great power comes even greater responsibility" is particularly applicable to biometric technology. Despite all the excitement over the good news regarding biometrics, it also has a negative aspect of its own. In contrast to its well-known advantages, we know virtually little about biometrics' drawbacks. Although the adoption of biometrics had many advantages, it also had its share of issues. The drawbacks of biometrics technology may interest you.Here are some key points to consider regarding the disadvantages of biometrics:

4.1. Physical Traits are not Changeable:

The majority of biometric authentication methods use physical characteristics like fingerprints, iris scans, palm veins, etc. We all only have one set of eyes, a set number of fingerprints, and other fixed physical characteristics. We can change a password, but our fingerprints and retinas cannot be altered because they are fixed. Our biometric information is kept in the databases of the relevant governments or businesses that provide these services. Can they guarantee that the server won't ever be breached or the data stolen? Sadly, it is already taking place all around us. According to news reports, the Aadhaar database contains the private information of billions of Indians. In 2015, there was a significant data breach at the Federal Government Office of Personal Management in the US, where 5.6 million employees' fingerprints were taken. If your password is compromised, you can change it, but there is no way to modify your fingerprint.

4.2. Error Rate:

As biometric devices are not perfect, errors can occur. False Acceptance Rate (FAR) and False Rejection Rate (FRR) are typically the two sorts of mistakes made by biometric equipment (FRR). The gadget is referred to as FAR when it welcomes an unauthorised person and as FRR when it rejects an authorised person. In some instances, the error rate is so high that it seriously disrupts the security system as a whole. It could occur because to the weather, one's health, age, or other factors. An error in a large-scale authentication process could occur with a 1% error rate.

4.3. Cost:

Comparatively more expensive than other conventional security measures are biometric devices. The total cost of biometric software, hardware, programmers, servers, and other related equipment is high.

4.4. Delay:

A huge line of employees forms waiting to be enrolled in some biometric devices since they take longer than expected in large firms. People encounter difficulties in these situations when scanning the biometric device on a daily basis. When a person must daily pass through a biometric verification system to enter a school, office, or other location, it is difficult for them.

4.5. Complexity:

The mechanism that makes up the entire biometrics procedure is extremely technological and complex, which is one of its main drawbacks. If a non-technical individual tries to comprehend the system, they will flounder like a fish out of water. Businesses use highly qualified and experienced programmers to create the system, therefore programmers are also needed to maintain the system.

4.6. Unhygienic:

The biometric modalities come in a variety of forms. Some of them use touch technology, like palm vein and fingerprint scanners, while others, like iris and facial recognition, don't. An significant number of people utilise a biometric device countless times in contact-based modalities. Actually, everyone is using the equipment to spread their germs to one another. After putting your finger on the device, you can never be sure what you are bringing with you. You wouldn't be able to alter the system in any way.

4.7. Scanning Difficulty:

Certain biometric technologies, including iris scanning, may experience scanning issues. It occurs for a number of causes, including reflections from the cornea and eyelashes, eyelids, and lenses. These factors make iris scanning less likely to be effective.

4.8. Physical Disability:

Not everyone has the good fortune to be able to take part in the registration process. Body parts like fingers or eyes could have been lost or hurt. A fingerprint or iris identification device in this situation would be humiliating and downright disrespectful. These folks will undoubtedly find it difficult to get along with others in the system.

4.9. Environment and Usage Matters:

Not everyone has the good fortune to be able to take part in the registration process. Body parts like fingers or eyes could have been lost or hurt. A fingerprint or iris identification device in this situation would be humiliating and downright disrespectful. These folks will undoubtedly find it difficult to get along with others in the system.

4.10. Additional Hardware Integration:

Certain biometric modalities call for expensive, awkward, and complicated hardware integration. These modalities are challenging to manage. Despite all of the obvious problems of biometrics, people hardly ever discuss them. We will all undoubtedly jump on the biometrics bandwagon today or tomorrow, but not before exercising caution with this technology. For these few reasons, biometric technology's potential shouldn't be dismissed. With the development of technology, we anticipate that these issues will be resolved and that in the future, hassle-free biometric technology will be available for use in daily life.

5. CONCLUSION

The biometrics market is still expanding globally due to all of the aforementioned considerations. By 2024, the global market, according to Global Markets Insights, will be valued more than $50 billion. Its expansion is primarily being driven by significant investments made by security and governmental organisations in the United States as well as rising efforts to establish a digital identity in nations like China and India. Yet, in addition to these significant companies, the sector's greater democratisation will also contribute to biometrics' growth. The rising use of online and cloud-based verification platforms—many of which may be white-labeled to integrate with an organization's current digital footprint—has contributed to this. Biometric technology, such as facial recognition and liveness checks, used to be the exclusive domain of the biggest corporations with the biggest budgets and the best development teams. Yet now, even ambitious start-ups and smaller businesses may deploy them successfully. Just like their larger competitors, these enterprises require the advantages of security, convenience, and safety, and for the first time, it is now within their practical reach. In a nutshell, biometrics is the analysis of biological traits that are specific to each individual person in order to identify and validate that person. .The individual or group conducting the assessment can be certain that they are dealing with the person they believe they are dealing with by looking at certain information about them that sets them apart from others. Of course, things were a little easier when biometrics first became widely used. It first gained popularity in the 19th century when body measurements were employed in France to categorise and compare criminals, and it later expanded to include fingerprinting in the world of law and order. When biometrics' guiding principles were merged with computing power, this is when the field of biometrics became well known. The potential of biometrics increased as computing advanced quickly in the second half of the 20th century (and into the 21st century). Automated fingerprinting and face recognition allowed for considerably faster and more accurate identity verification than a trained person ever could. Voice recognition became feasible and useful, while artificial intelligence enabled using biometric data to get desired insights and outcomes simpler and faster than ever.

References

Biometric Technology: The Latest Guide | Veriff.com. Veriff. https://www.veriff.com/blog/the-future-of-biometric-technology

What is biometrics? (techtarget.com) - Bing. (n.d.-b). Bing. https://www.bing.com/search?q=What+is+biometrics%3F+(techtarget.com)&cvid=a5286894a18e4d819a1a5bf1693a95b0&aqs=edge.0.69i59j69i64.434j0j1&pglt=41&FORM=ANNTA1&PC=HCTS

21 Types of Biometrics with Detail Explanation - Biometric Today - Bing. (n.d.-b). Bing. https://www.bing.com/search?q=21+Types+of+Biometrics+with+Detail+Explanation+-+Biometric+Today&cvid=64e3340925334f35987b46350e1b7ec1&aqs=edge.0.69i59j69i64.385j0j9&FORM=ANAB01&PC=HCTS

10 Advantages and Disadvantages of Biometrics System You Should Know (biometrictoday.com) - Bing. (n.d.). Bing. https://www.bing.com/search?q=10+Advantages+and+Disadvantages+of+Biometrics+System+You+Should+Know+(biometrictoday.com)&cvid=78ecdfc787154296bf6b65e29e55c18d&aqs=edge..69i57j69i64.931j0j9&FORM=ANAB01&PC=HCTS

https://www.veriff.com/blog/the-future-of-biometric-technology. V. (n.d.-b). Biometric Technology: The Latest Guide | Veriff.com (n.d.-b).