International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 3, 2023. ISSN: 2348-6600
Reference ID: IJCS-467 PAGE NO: 3183-3187

ADVANCEMENTS IN BIOMETRIC SECURITY APPROACHES

P. Manish
Department of I MCA,
Sourashtra College, Madurai. Tamil Nadu, India.
E-mail: manishsabarish007@gmail.com

B. Prasath
Department of I MCA,
Sourashtra College,
Madurai. Tamil Nadu, India.
E-mail: prasath3428@gmail.com

Dr.K.Anuratha
Assistant Professor and Head,
Department of MCA,
Sourashtra College, Madurai. Tamil Nadu, India.
E-Mail: anu_ksyo@yahoo.com

Abstract:

Information security has become a key component of information technology as a result of its development. User authentication plays a vital role in managing privacy and security. A human being can be authenticated using biometrics based on specific physiological characteristics. This paper represents various viewpoints on the usability of biometric authentication systems, advantages and disadvantages of each. It also summarizes the advancements in biometric security approaches.

Keywords: Artificial Intelligence (AI), Biometrics, Security.

1. Introduction

The basis of biometrics is the measurement and analysis of the human face, iris, fingerprint, etc. Biometric categories are based on physical characteristics related to the shape of the body and behaviour. So, it is unique. "Uniqueness [1] is a state or condition wherein someone or something is unlike anything else in comparison, is remarkable, or is unusual."

Components of a Biometric System

A biometric system (Figure:1) has three components: a data capture component, a signal processing (feature extraction) component, and a data storage component. It

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 3, 2023. ISSN: 2348-6600
Reference ID: IJCS-467 PAGE NO: 3183-3187

has enrolment and verification stages. To generate a biometric template [2], a particular algorithm is used to select a person's collected biometric data.

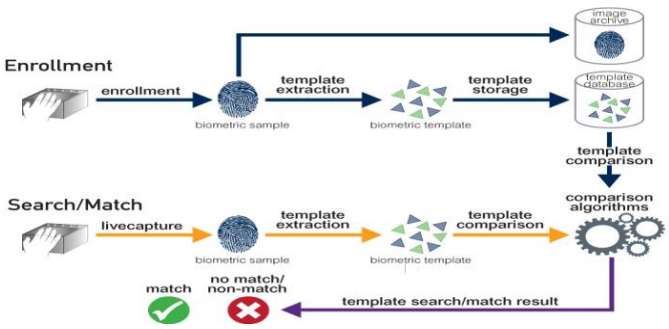

Figure 1: A Biometric Process (Source: https://www.aware.com/what-are-biometrics-biometric-processes)

2. Background of Study

Semi-automated facial recognition methods were created in the 1960s, requiring managers to examine facial characteristics in a picture and extract valid feature points. We can use a lot more manuals than the ones we can use to unlock our phones.

By 1969, fingerprints and face recognition had become so common in law enforcement that the FBI allocated funds to create automated procedures. This sparked the creation of increasingly advanced sensors for collecting biometric information and data extraction.

The National Institute of Standards and Technology established a voice section in the 1980s to research and advance methods for speech recognition technology. The voice command and recognition technologies we use today are based on these investigations.

The idea that irises were similar to fingerprints in that they were unique to each individual was put forth in 1985, and the first iris recognition algorithm was patented in 1994.

Real-time recognition became feasible in 1991 because of the development of face detection technologies. Despite the fact that these methods had several flaws, they greatly increased interest in face recognition research.

In the year 2000, the USA had hundreds of working and patented biometric authentication, recognition, and recognition algorithms. Biometric technologies are not being used by the government or huge corporations.

3. Types of Biometric Devices and Services

Types of biometrics [4] are categorized according to physical and behavioural characteristics. They are:

Physical Type of Biometrics

Since there are so many distinctive physiological characteristics that are very simple to detect, biometrics are considerably more frequent.

Facial Recognition

Facial recognition is another well-known security feature that has been utilized for years in large-scale venues that require high security, such as casinos. Today's technology is so sophisticated that many phones can link unique characteristics on a person's face to their identification.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 3, 2023. ISSN: 2348-6600
Reference ID: IJCS-467 PAGE NO: 3183-3187

Vein Recognition

As it occurs, everyone has different vein patterns. Now, technology exists to analyze the vein patterns in the palm or finger. Because it's hard to figure out how a vein pattern, rather than a fingerprint, could be changed in a meaningful way, vein identification is more secure than fingerprint identification.

Iris Recognition

Retina recognition is another widely used biometric identification technique. The user simply stares into an eye reader, which compares it to a pre-approved user profile by examining the retinal or iris patterns.

Ear Recognition

Certain authentication and authorization systems may perform by only analysing the unique form of a person's ear, as opposed to recognizing the full face.

DNA Matching

If collecting a user's DNA every time they attempt to log into a system can be viewed as a little overly personal, there is no doubting the high efficacy of DNA analysis in identifying people.

Finger Geometry

Everyone has unique fingerprints, which is a well-known fact. It makes sense to use fingerprints as a biometric since they have been used to identify people long before the internet came into being. The accuracy of fingerprint recognition is usually very high.

Smell Recognition

It is feasible to recognize a person by their unique smell, even though such systems are currently uncommon.

Behavioural Type of Biometrics

Methods of behaviour identification focus on a person's activities, allowing the user the opportunity to control his actions.

Keystroke

The component that enables computer communication is the keyboard. Several people use keyboards in various ways. Typing speed varies from person to person. The time of day and a person's mood both affect how quickly they type. A system called biometric keystroke recognition uses a person's typing to identify them. It is crucial to realise that this technology doesn't concern itself with "what" is written but rather "how" it is written.

Digital Signature

Static systems that just compare the signature to an existing handwriting sample and dynamic systems that also monitor the hand's motion while writing.

Voice Recognition

The physical aspects that contribute to sound production, such as the throat, mouth, nasal cavities, and lips, determine the qualities of a person's voice. Certain aspects of human speech remain constant for a particular person, but the behavioural aspect varies over time due to age, sickness, and emotional

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 3, 2023. ISSN: 2348-6600
Reference ID: IJCS-467 PAGE NO: 3183-3187

states. This form of authentication examines a speaker's speech patterns.

4. Advantages and Disadvantages

The biometric advantages are:

- Faster Authentication: We can quickly and simply unlock the application.
- Convenient: The employee databases' attendance information is something we can store, making it convenient to search the employee's data.
- Accuracy: The data from biometric security is quite accurate.
- Scalability: The biometric features may be used for many tasks and activities.
- Access Control: The manager has access control according to the biometric. He has simple access control for adding and removing employees.

The biometric disadvantages are:

- Scanner compatibility: Given long or irregular eyelashes, there may be problems with the scanner recognising the iris lock on the device.
- Expensive: A safe and reliable biometric system can get costly.
- Malfunction: The biometric system may fail because of corrupt biometric software or a power shortage.
- Privacy issues: The fingerprint information of the employees may be misused by the company.

5. Recent Trends in Biometric Technology

Voice, behavioural, face recognition, and other consumer identification modalities are all part of biometrics. Authentication using artificial intelligence (AI) makes this crucial process faster, easier, and more secure than before. Businesses and people must adopt digital financial and data transactions as the world shifts towards digitalization. However, as hackers with sophisticated AI support develop over time, identity security has become a more major issue than ever.

By cracking passwords using social engineering and AI algorithms, hackers are aiming for personal information such as national ID numbers, financial information, demographic information, credit card information, medical information, and tax information. As technology advances, hackers can break into biometric systems. Gelatin film used to resemble fingerprints, the creation of a face mask to mimic a facial recognition camera, and the fabrication of a false picture of the iris might all be examples.

Identity theft is rising as more connected IoT devices are used. Identity theft can be prevented by using protected (encrypted biometric data) biometric authentication. Along with matching biometric data, liveness detection evaluates the physical characteristics that indicate life. Existing biometric devices might be used with additional hardware or software to check for liveness. Liveness detection can be done in two ways.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 3, 2023. ISSN: 2348-6600
Reference ID: IJCS-467 PAGE NO: 3183-3187

Active liveness detection

It recognises several living qualities of a person, such as the presence of veins, blood pressure, pulse, stride, and so on, in order to confirm their liveness.

Passive liveness detection

It is a technique for determining if the supplied biometric sample is dead. For instance, if someone wants to trick a facial recognition camera with a 2D image, the camera may have a flash that makes the image gallery.

6. Conclusion

The use of biometric technology is booming, along with demand in a number of industries. High adoption rates are seen in the following industries: are military, defence, and healthcare. The important future technological developments are the analysis of face recognition using artificial intelligence. AI makes use of biometric technology. AI may also be used to analyse a person's emotional reactions, iris, speaking manner, attitude and walking style. Liveness detection and encryption for biometric data play an important role in information security.

References

1. Headley, John M. (2012). The Problem with Multiculturalism: The Uniqueness and Universality of Western Civilization. Transaction Publishers. Retrieved 3 May 2017.
2. "The future of biometrics Technology: An overview by industry", available at https://incode.com/blog/future-of-biometrics/
3. Joseph N, Pato, Lynette I. Millett, "Biometric Recognition: Challenges and Opportunities", National Research Council (US) Whither Biometrics Committee; Washington (DC): National Academies Press (US); 2010.
4. Shilpa Shrivastava, "Biometric: Types and its Applications", National Conference on Knowledge, Innovation in Technology and Engineering (NCKITE), 10-11 April 2015. Available at https://www.ijsr.net/conf/NCKITE2015/100.pdf