

Biometrics Security System

Divya Khandekar¹ and Shailesh Bendale²

Student, Department of Computer Engineering¹

Processor and Head, Department of Computer Engineering²
NBN Sinhgad School of Engineering, Pune, Maharashtra, India

Abstract: Due to its liability, biometrics are currently the most preferred technology. Because biometric authentication is very difficult to forget, steal, or guess, it is becoming more and more popular as a more reliable security solution than password-based ones. On the other side, biometric information that may be used to uniquely identify a person, such as fingerprints and iris patterns, can be used to follow people by connecting numerous different databases (such as where they have gone, what they have bought, etc.), which creates privacy issues.

Keywords: biometrics, authentication, verification, validation, recognition

I. INTRODUCTION

The first commercially available biometric device was developed more than 25 years ago at Shearson Hamill on Wall Street when a machine that restricted finger length was fixed for a time keeping request. Several organizations, including the Department of Energy, Western Electric, Naval Intelligence, and others, connected hundreds of these hand geometry devices at high-security locations in the years that followed. Currently, methods that look for a subject's unique physiological or behavioral characteristics are used to track access to more than 20,000 workstation rooms, vaults, exploratory labs, daycare centers, blood banks, cash machines, and military fixings. Reduced prices have made biometric machines more attentive; this, along with lower overall prices, will undoubtedly be good for this industry going forward.

II. BIOMETRICS SYSTEM

Biometrics: The rapidly developing field of science known as "biometrics" uses biological characteristics or behaviors to confirm people's identities. This entails taking a picture of a person's distinctive feature in advance and comparing it to a template, such as a fingerprint, hand, eye, or face. For the sake of clarity, this has been oversimplified, but this is essentially how biometric technology works. Use this document as a template and type your text into it to easily adhere to the Journal paper formatting specifications. The measurement of biological or behavioral characteristics that are used to identify people is known as biometrics. Most of these traits cannot be anticipated or taken; they are inherited.

Why we Need biometrics?

Biometrics-based verification helps us confirm your voice, finger prints, and iris pattern for your uniqueness at ATMs, Airports, etc. in order to avoid the problems of forgetting the passwords and ID codes. With just a flick of the eye, a tap of the finger, or by putting on an indifferent face, you can solve your family's problems with money withdrawals from or before a bank.

Classification of Biometric Traits:

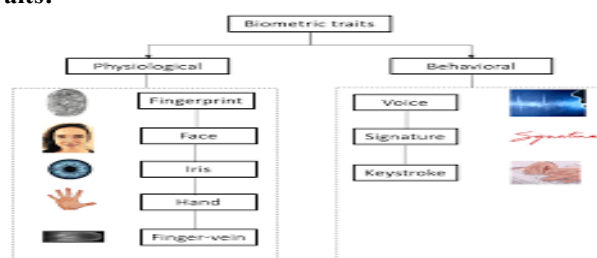


Figure 1. Classification of Biometric traits

Types of biometric devices

1. Physiological Biometrics
2. Behavioral Biometrics

Physiological Biometrics: In this type of biometrics, physical characteristics are assessed for identification and verification. The characteristic should be selected so that it is distinct from the population and resistant to changes due to illness, aging, injury, etc.

Fingerprint: The fingerprints on each individual are unique. There are numerous methods for quantifying them. As opposed to minutiae-based measurement, which uses graphs to match ridges, image-based measurement looks for similarities between a person's fingertips and fingerprint photos stored in the database. It is highly secure and used for both identification and verification. However, a fingerprint may change as a result of aging, illnesses, or injuries. Usage examples include using mobile devices for identification and verification.



Figure 2. Example of fingerprint

Face Recognition: In all of human history, faces have been used to distinguish one person from another. Face features like the distance between the nose, mouth, and ears, the length of the face, and the color of the skin are used for identification and verification. Accuracy can be affected by the weather, sunglasses, age, and other factors.



Figure 3. Example of face scanning

Iris Recognition: The iris, an incredibly thin, circular diaphragm, divides the cornea from the lens in the human eye. The pupil is a perforation that is a circular opening close to the iris's center. The iris and the sphincter and dilator muscles, which alter the pupil's size, cooperate to regulate how much light passes through the pupil.

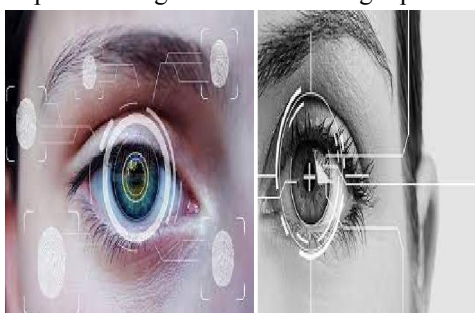


Figure 4. Example of Iris scanning

Hand Geometry: The use of the hand's geometric form for identification reasons is known as hand geometry. Ten years ago, this approach was rather common, but it is now rarely applied. The technique is based on the observation that at a certain age, a person's hand form remains constant and varies from that of another person. But it isn't special.

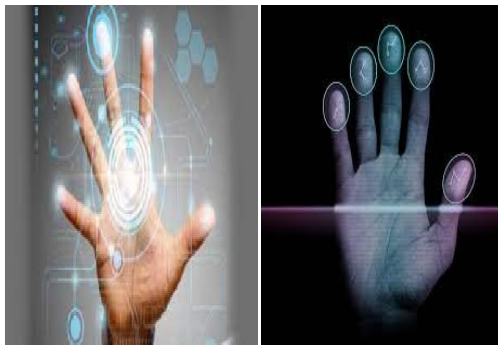


Figure 5. Example of hand scanning

Finger vein: A biometric identification technique called finger vein biometrics, also referred to as vein matching or vascular technology, looks at the blood vessel patterns that are visible from the skin's surface of fingers. This technique relies on photographing the veins inside a person's hand by shining a near-infrared light on their fingers. Because of this, counterfeiting is almost impossible. Additionally, the fact that blood is visible in the veins during identification proves the subject is a real person, not a fraudster.



Figure 6. Example of voice recognition

Behavioral Biometrics: In this type, human behavioral traits are being assessed. In this form of biometrics, monitoring is necessary to avoid claimant impersonation.

Voice Recognition: Like many other traits used in biometric techniques, voice is distinctive. A person's walking pattern and speech analysis both take very little time to complete. The voice in biometrics, also known as the "voice print," is given as a numerical representation of the sound.



Figure 7. Example of voice recognition

Signature scanning : An image of a handwritten signature that has been digitally transformed is known as a scanned signature. In order to create a scanned signature, a signatory will handwrite their signature on paper and then use some sort of equipment to convert the handwritten signature into a digital format, like a PDF, JPEG, or PNG.

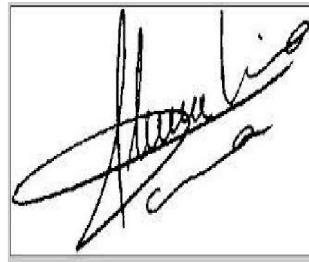


Figure 8. Example of signature recognition

Key Stroke : This method assesses how a person behaves when using a keyboard. The following are a few of the factors that are considered:

- Typing speed.
- Frequency of errors
- Duration of key depressions



Figure 9. Example of Key stroke

Privacy Issues Surrounding Biometrics:

The ability to identify and verify individuals using biometrics requires the preservation of personal information such as physiological and behavioral traits. Because of this, their fundamental right to privacy might be compromised. There is also worry that the data retained might be used against them. There are worries that since most biometric data on an individual is unique, it might be used to gauge and keep an eye on people. Data must be securely stored and database access must be hierarchical as a result.

III. ADVANTAGES OF BIOMETRIC SYSTEM

- Faster Authentication
- Convenient
- Accuracy
- Flexibility
- Scalability
- Access Control
- Can't be easily stolen

3.1 Faster Authentication

Using biometrics, we can unlock an application quickly. It becomes very quick to authenticate an individual using a fingerprint or face scan.

3.2 Convenient

We can keep track of employees' attendance data using biometric technology in databases or on sheets. We can quickly search for and update data in the sheets. The employee leaves are simple to search.

3.3 Accuracy

The information gleaned from biometric security is remarkably precise. The information will specify precisely when an employee entered or left the office.

3.4 Flexible

Long paper attendance records are not required to be kept on file by the company to store the data. Additionally, we don't need to repeatedly enter the password to unlock a device or application..

3.5 Scalability

The biometric features are useful for a variety of tasks and endeavors.

3.6 Access Control

The manager has access control thanks to the biometric. He has simple access control over adding and removing employees.

3.7 Can't be Easily Stolen

He cannot be observed in order to steal the biometric fingerprint or face lock.

IV. DISADVANTAGES OF BIOMETRIC SYSTEM

- False positives
- Scanner compatibility
- Expensive
- Malfunction
- Privacy issues

4.1 False Positives

False positives can be produced using stolen biometric data. False-positive biometric results occur when the system mistakenly recognizes the user as a match. False positives happen as a result of either very similar faces or stolen data used for authentication.

4.2 Scanner Compatibility

Due to long or irregular eyelashes, there may be problems with the scanner registering retina lock on the device.

4.3 Expensive

The cost of a secure biometric system can rise. The maker must maintain the biometrics' reliability, durability, and user safety possibilities.

4.4 Malfunction

The biometric software could malfunction as a result of a system bug. The biometric system could malfunction as a result of the power shortage.

4.5 Privacy Issues

The employee's fingerprint information can be misused by the employer. As a result, someone's or an employee's privacy may be at risk.

V. CONCLUSION

The biometric technology is now a secure, practical, and cost-effective way to identify people thanks to improvements in accuracy, usability, and efficiency. There are many well-known terms for scanning, including "iris scanning," "signature verification," "hand geometry," "voice verification," and others. Each has unique characteristics.

Their practical performance may frequently be higher than anticipated now that speed and band width are no longer limiting factors.

REFERENCES

- [1]. A. Jain, L. Hong and S. Pankanti, "Biometric Identification", Communications of the ACM, vol. 43, no. 2, pp. 91-98, 2000. Show Context Access at ACM Google Scholar
- [2]. Anil K. Jain and Arun Ross, "Introduction to Biometrics" in Handbook of Biometrics, Springer, pp. 1-22, 2008, ISBN 978-0-387-71040-2. Show Context CrossRef Google Scholar
- [3]. Sahidullah and Md, Enhancement of Speaker Recognition Performance Using Block Level Relative and Temporal Information of Sub band Energies, 2015. Show Context Google Scholar
- [4]. "Biometrics for Secure Authentication", (PDF)Retrieved. Show Context Google Scholar
- [5]. [online] Available: http://www.bioelectronix.com/what_is_biometrics.html. Show Context
- [6]. [online] Available: <http://www.biometricnewsportal.com/biometricsissues.asp>. Show Context
- [7]. [online] Available: <http://www.explainthatstuff.com/how-iris-scans-work.html>.
- [8]. L. O'Gorman "Comparing passwords, tokens and biometrics for user authentication". Proceedings of the IEEE, Vol. 91, No. 12, pp.2021-2040, December 2003.
- [9]. M. Faundez-Zanuy "Biometric recognition: why not massively adopted yet?". IEEE Aerospace and Electronic Systems Magazine. Vol.20 n° 8, pp.25-28, ISSN: 0885-8985. August 2005.
- [10]. M. Faundez-Zanuy "Privacy issues on biometric systems". IEEE Aerospace and Electronic Systems Magazine. Vol. 20 n° 2, pp13-15, February 2005