Artificial Intelligence in Biometrics and Security

A.Kavitha

Head & Assistant Professor of Computer Science, Aditanar College of Arts and Science, Tiruchendur

Abstract- **Artificial intelligence is a way of making intelligent machines which can behave like a human so it can able to make decisions. AI is making our lifestyle easier and fast. It is becoming essential for today's time because it can solve complex problems with an efficient way in multiple industries, like healthcare, entertainment, finance, education, etc. Artificial Intelligence has various applications in today's society. Some of the applications of AI include Expert systems, Natural Language Processing, Vision systems, Speech Recognition, Intelligent Robots, Authentication by Biometric verification. AI system can be used in conjunction with the traditional forms of biometrics. Biometrics identifies and authenticates individuals based on their physical or behavioural characteristics. Biometric recognition offers well a promising approach for security applications. The emerging biometrics based identification and authentication technology is applicable in Banking security, ATM security, E-commerce etc. In this paper different types of biometric authentication methods that used as personal identifying factors are discussed.**

Index terms- **Artificial intelligence, Authentication, Biometrics, Fingerprint recognition, Iris recognition, Multimodal, Security, Unimodal, Voice recognition**

I.INTRODUCTION

Artificial intelligence makes it possible for machines to learn from experience and performs the tasks like human being. Nowadays it is used in many fields such as Psychology, Philosophy, Cognitive science, Linguistics, Operation Research, Economics, etc., AI technology is used in Speech recognition, Facial recognition, Data mining, Robotics, Biometrics authentication and control systems. In our day to day life, the verification of person is very important task to access sensitive data. That's why we can use a new modern way to identify a person is biometric authentication. Biometrics uses methods for unique recognition of humans based upon one or more intrinsic physical traits which includes fingerprint, retina, face recognition or behavioral traits which includes voice, signature and keystroke that can be used to identify an individual or to verify the claimed identity of an individual [1]. In computer science, particularly, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance.

II. BIOMETRICS AUTHENTICATION PROCESS

The application that uses biometrics for authentication consists of the following three steps.

- Enrollment
- Verification
- Identification

Enrollment

Enrollment is the first stage for biometric authentication. Before authentication, a user must be enrolled into a database. In this stage administrator adds a biometric sample of a user to the system by creating a biometric template of the user. A biometric sample is a data representation of the user's biological characteristics. This data is based on features extracted from the user's live scanned fingerprint, iris, face, voice by using an enrollment utility [2].

Verification

Each time a user accesses a computer system, the user is verified to authenticate the correctness of the user's claimed identity. In this stage a biometric sample of the user is generated, this biometric sample is matched with the existing biometric templates that are stored in a database. Here the comparison is done on a one-to-one basis. If the biometric sample matches the previously generated biometric template, the identity of the user is verified.

Identification

In this stage the biometric sample of the user is compared with all the templates that are stored in the database. This is known as one-to-many comparison.

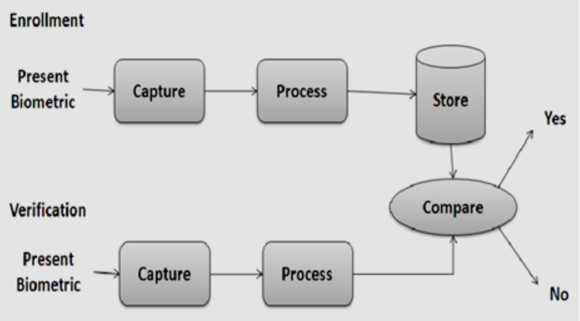

Fig. 1 Biometric Authentication System Architecture

The above block diagram Fig. 1 state the architecture of biometric authentication system.

III. BIOMETRIC TECHNOLOGY

There are various traits present in humans, which can be used as biometric modalities. The biometric modalities fall into two types.

- Physiological
- Behavioral

Physiological modalities are based on the direct measurement of parts of human body such as iris, retina, face, fingerprint etc., Behavioral modalities include voice, signature, keystroke etc., The types of biometric modalities is shown in the following diagram Fig. 2.

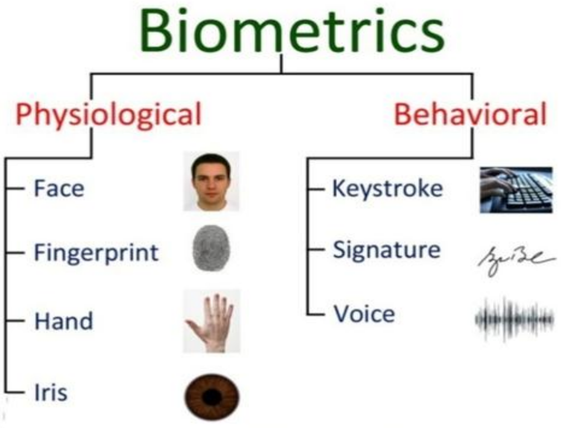

Fig. 2 Types of Biometric Modalities

Face Recognition

The biometric system can automatically recognize an individual by the face. This technology works by analyzing specific features in the face like - the distance between the eyes, width of the nose, position of cheekbones, jaw line, chin etc. These systems involve measurement of the eyes, nose, mouth, and other facial features for identification. To increase accuracy these systems also may measure mouth and lip movement. Face recognition captures characteristics of a face either from video or still image and translates unique characteristics of a face into a set of numbers. These data collected from the face are combined in a single unit that uniquely identifies each person [3]. Nowadays facial recognition is more effective with the help of machine learning. AI learns from millions of images and utilizes 3D biometrics to successfully authenticate an individual's face. It also can use predictive modeling to analyze the effects of aging on human faces [4].

The following block diagram Fig. 3 describes the face recognition process done by biometric system.

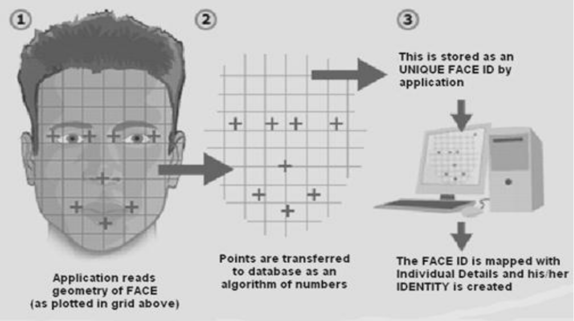
①
②
③
This is stored as an UNIQUE FACE ID by application
Application reads geometry of FACE (as plotted in grid above)
Points are transferred to database as an algorithm of numbers
The FACE ID is mapped with Individual Details and his/her IDENTITY is created

Fig. 3 Face Recognition

Eye Recognition

This technique involves scanning of retina and iris in eye. The iris is one of the most recognizably distinctive feature in the human body that is the unique pattern and characteristics of human iris remain unchanged throughout one's lifetime and no two persons in the world can have the same iris pattern. Retina scan technology maps the capillary pattern of the retina, a thin nerve on the back of the eye. It analyses the iris of the eye, which is the colored ring of tissue that surrounds the pupil of the eye. This is a highly mature technology utilized in many areas. Retina recognition is used in airports for travelers. Organizations use retina scans primarily for authentication in high-end security applications to control access, for example, in government buildings, military operations or other restricted quarters, to authorized personnel only [3].

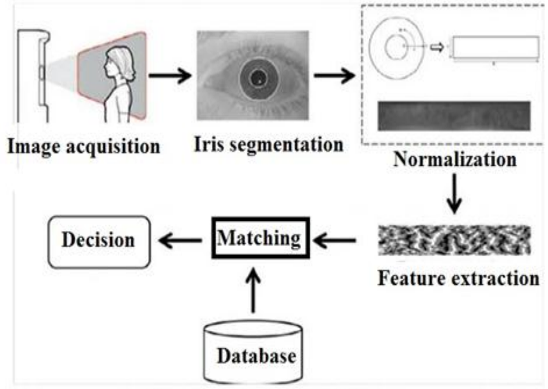

Fig.4 Eye Recognition

The above diagram Fig. 4 describes the eye recognition process done by biometric system.

Fingerprint Recognition

The fingerprint is such a pattern of ridges and valleys on the surface of the finger that are unique for each person, even in twins. The ridges themselves have a non-continuous flow, where the discontinuity brings about feature points called minutiae and the pattern can be of arches, whorls and loops, which are the basis of fingerprint recognition. Fingerprints are the oldest and probably best known biometric identifiers and because of the long and widespread experience with fingerprint technology. Fingerprints scanners are included in many consumer electronic devices like laptops, smart phones, etc. There are two main technical approaches for fingerprint recognition: minutia matching and pattern matching, of which minutia matching approach is most used in the fingerprint recognition systems. The following diagram Fig. 5 describes the fingerprint recognition.

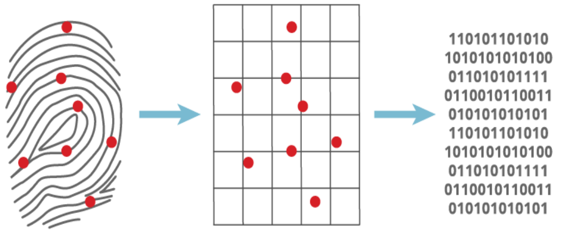

Fig. 5 Fingerprint Recognition

Voice Recognition

Voice biometrics, uses the person's voice to verify or identify the person. A microphone attached with PC is required to identify the person's characteristics. For enroll, Particular phrase will be spoken by users using microphone. The system then creates a template based on numerous characteristics, including pitch, tone, and shape of larynx. Voice verification is one of the least intrusive of all biometric methods. However in some situations voice authentication may not give foolproof results For example if a user has a sore throat or cough the voice recognition system may not work properly. Furthermore, voice verification is easy to use and does not require a great deal of user education [2] [3][5]. The below diagram Fig. 6 describes the basicc structure of voice recognition

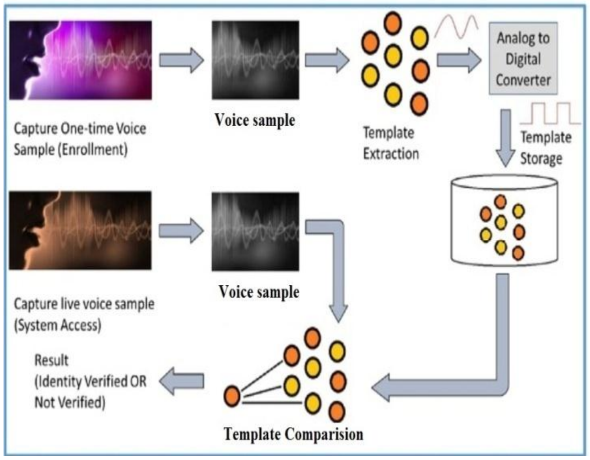
Capture One-time Voice Sample (Enrollment)
Voice sample
Template Extraction
Analog to Digital Converter
Template Storage
Capture live voice sample (System Access)
Voice sample
Result (Identity Verified OR Not Verified)
Template Comparision

Fig. 6 Voice Recognition

Keystroke Dynamics

Keystroke dynamics refers to the the automated method of identifying the individual based on the manner and the rhythm of typing on a keyboard [6]. Based on keystroke dynamics the user's typing speed and rhythm are stored as biometric template in the database. The software tracks the user's unique typing pattern to ensure that the person keying your password is authentic.

Signature Recognition

Signature Recognition technology is that the analysis of an individual's written signature, including the speed, acceleration rate, stroke length and pressure applied during the signature. There are different ways to capture data for analysis i.e. a special pen can be used to recognize and analyze different movements when writing a signature, the data will then be captured within the pen. Information can also be captured within a special tablet that measures time, pressure, acceleration and the duration the pen touches it. As the user writes on the tablet, the movement of the pen generates sound against paper an is used for verification[7].

IV. UNIMODAL BIOMETRIC SYSTEM

Biometric identification systems which use a single biometric trait of the individual for identification and verification are called unimodal systems.

Disadvantages of Unimodal Biometric Systems

- *Environment:* The environment in which biometric data is captured may have an effect on the ability of the system to identify an individual. For example, the accuracy of facial recognition is affected by illumination, pose, and facial expression.
- *Noise in sensed data:* A fingerprint with a scar and voice altered by a cold are examples of noisy inputs.
- *Intra-class variations:* Fingerprint data acquired from an individual during authentication may be very different from data used to generate the template during enrollment due to a misplacement of the finger on a capture device, thereby affecting the matching process.
- *Non-universality:* Some people cannot physically provide a standalone biometric credential due to illness or disabilities.
- *Spoof attacks:* An impostor may attempt to spoof the biometric trait of a legitimately enrolled user in order to circumvent the system.

V. MULTIMODAL BIOMETRIC SYSTEM

Biometric identification systems which use combination of two or more biometric modalities to identify an individual are called multimodal biometric systems. Multimodal biometrics overcomes the above unimodal biometrics problems. Recently, multimodal biometric fusion techniques have attracted increasing attention and interest among researchers.

Working of Multimodal Biometric System

In multimodal biometric systems more than one feature of humans are first sensed by sensor and then its features are extracted and then it is matched by using database and then with the help of algorithm scores of matching from all of the features are added to get exact score to identify a person. The following block diagram Fig. 7 describes how the Multimodal Biometric system works.

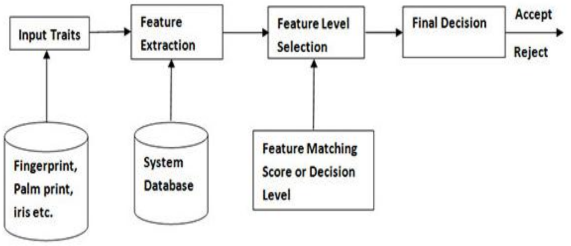

Fig. 7 Multimodal Biometric System

Advantages of Multimodal Biometric System

- *Accuracy:* Multi-modal biometric uses multiple modalities to identify a person which ensures higher accuracy.
- *Security:* Multi-modal biometric systems increase the level of security by eliminating any chance of spoofing. It is unlikely that a person would be able to spoof multiple types of biometric traits at once.
- *Liveness Detection:* Multi-modal biometric systems ask end users to submit multiple biometric traits randomly which ensures strong liveness detection to protect from spoofing or hackers.
- *Universality:* A multimodal biometric system is universal in nature, even if a person is unable to provide a form of biometric due to disability or illness, the system can take other form of biometric for authentication.
- *Cost-effective:* Multimodal biometric systems are cost effective by providing higher levels of security to lessen the risk of breaches or criminal attacks[8][9].

VI.CONCLUSION

In the digital age, security is one of the primary concerns of any field. With the advancement of technology and its increased use in various areas of life, a major aspect that needs to be considered is security. The security of data is crucial for every company and cyber-attacks are growing very rapidly in the digital world. AI can be used to make your data more safe and secure. Today’s modern computing world gains a lot of benefits from various AI approaches. Their ability to learn by example makes them very flexible and powerful. We have seen that the growth of biometric technology throughout the world for many reasons but mostly due to the fact that personal identification is considered more and more important. Biometric based authentication is becoming increasingly appealing and common for most of the human computer interaction devices. This paper presents how the various biometrics technologies help to authenticate a person effectively.

REFERENCES

[1] Sushma Jaiswal, Dr.Sarita Singh Bhadauria, Dr.Rakesh Singh Jadon, Journal of Global Research in Computer Science, Volume 2 , No.10, October 2011, Biometric : Case Study

[2] Information security An Overview, PHI 2004. pp. 117

[3] N.C.Kaneriya et. al., International Journal of Advance Research in Engineering, Science & Technology e-ISSN: 2393-9877, p-ISSN: 2394-2444, An Emerging Development Of Biometric System: A Novel Approach of Security

[4] https://www.allerin.com/blog/biometrics-is-smart-but-ai-is-smarter-heres-why

[5] https://emerj.com/ai-sector-overviews/ai-in-biometrics-currentbusiness-applications

[6] http://www.biometricsolutions.com/keystroke-dynamics.html

[7] Manasi G. Vaidya, International Journal of innovation in engineering And Technology, ISSN 2319- 1058, Volume 5 , Issue 2 April 2015, A Study of Biometrics Technology Methods and Their Applications- A review

[8] https://www.tutorialspoint.com/biometrics/multimodal_biometric_systems.htm

[9] http://www.m2sys.com/blog/important-biometric-terms-to-know/the-advantages-of-multimodal-biometric-system-for-human-identification/

BIOGRAPHY

A.KAVITHA [M.C.A] is presently working as Head & Assistant Professor in the department of Computer Science in Aditanar College of Arts And Science, Tiruchendur, Tuticorin District, Tamilnadu. She has qualified in Tamilnadu State Eligibility Test (SET) Lectureship in 2016.