Process of Biometric Authentication and Its Application-A Review

Prof. Kaushik Vipul R.[1], Dr. Tanaji Dabade[2], Dr. Vijay N. Patil[3]

[1]Assistant Professor, Parikrama Group of Institutions, Kashti, Ahmednagar, Maharashtra, India
[2]Director, Parikrama Group of Institutions, COM, Kashti, Ahmednagar, Maharashtra, India
[3]Director, Parikrama Group of Institutions, Kashti, Ahmednagar, Maharashtra, India

ABSTRACT: The Biometrics are become the most popular technique now a day due to its liability and security. Earlier method of establishing a person's Authenticate includes knowledge based like password or token base like ID cards. These identities may be lost stolen or shared by any person. It prevents fraud usage of ATMs, mobiles, PCs, smart cards etc. Another feature of biometric is its efficiency. It is very easy to use and handle. Biometric uses fingerprint, eye patterns (IRIS recognition), hand geometric, facial expression, voice recognition, and signature analysis etc which are detailed explained in this paper. With the use of unique characteristics of person; various biometrics authentication devices have been developed and in use which are also reviewed in this paper.

KEYWORDS: Biometrics Authentication, Face Recognition, Fingerprint Scanning, DNA, Hand Recognition, Iris Recognition, Voice Recognition, Key Stroke and Signature Scanning.

I.INTRODUCTION

Biometric Authentication is any process that validates the identity of a user who wishes to sign into a system by measuring some intrinsic characteristic of that user. The traditional methods involving passwords and PIN numbers do not require the candidate to be present there at the time of authentication, while biometrics techniques does not require password, PIN numbers or any RFID cards. Now a day the Biometric is becomes the most popular technique due to its liability**.** Automatic person authentication is an important task in our day to day life. Earlier method of establishing a person's Authenticate includes knowledge based like password or token base like ID cards. These identities may be lost stolen or shared by any person. It prevents fraud usage of ATMs, mobiles, PCs, smart cards etc. The characteristics are measurable and unique. Identity verification occurs when the user claims to be already enrolled in the system (presents an ID card or login name); in this case the verification biometric data obtained from the user is compared to the user's data already stored in the database [1][2][3]. Identification (also called search) identification occurs when the identity of the user is a priori unknown. In this case the user's biometric data is matched against all the records in the database as the user can be anywhere in the database or he/she actually does not have to be there at all. In biometric-based authentication, a legitimate user does not need to remember or carry anything and it is known to be more reliable than traditional authentication schemes. Biometric authentication offers a convenient, accurate, irreplaceable and high secure alternative for an individual, which makes it has advantages over traditional cryptography-based authentication schemes. Biometric authentication or simply biometrics refers to establishing identity based on the physiological and behavioral characteristics (also known as traits or identifiers) of an individual such as face, fingerprints, hand geometry, iris, keystroke, signature, voice, etc. Biometrics systems offer several advantages over traditional authentications schemes [4][5][6]. They are inherently more reliable than password – based authentication as biometric traits cannot be lost or forgotten; biometric traits are difficult to copy, share and distribute; and they require the person being authenticated to be present at the time and point of authentication. Thus, a biometrics – based authentication scheme is a powerful alternative to traditional authentication schemes.

Biometrics System: Biometrics is the automated use of physiological or behavioral characteristics to determine or verify identity. Several aspects of this definition require elaboration. All biometric identifier scan be divided into two big groups:

1) Physiological.
2) Behavior.

1. Physiological characteristics: Biometrics is based on the measurement of distinctive physiological and behavioral characteristics. Finger-scan, facial-scan, iris-scan, hand-scan, and retina-scan are considered physiological biometrics, based on direct measurements of a part of the human body. Voice-scan and signature-scan are considered behavioral biometrics; they are based on measurements and data derived from an action and therefore indirectly measure characteristics of the human body. The element of time is essential to behavioral biometrics-the characteristic being measured is tied to an action, such as a spoken or signed series of words, with a beginning and an end. The physiological/behavioral classification is a useful way to view the types of biometric technologies, because certain performance- and privacy related factors often differ between the two types of biometrics [7][8]. However, the behavioral/physiological distinction is slightly artificial. Behavioral biometrics is based in part on physiology, such as the shape of the vocal cords in voice-scan or the dexterity of hands and fingers in signature-scan. Physiological biometric technologies are similarly informed by user behavior, such as the manner in which a user presents a finger or looks at a camera.

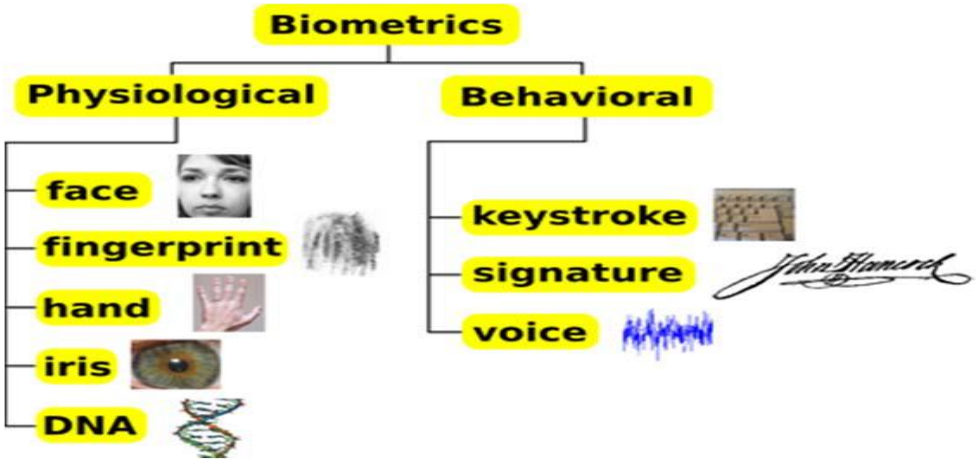

Fig 1: Classification of Biometrics

Face Recognition: During the whole history of humanity, people used face to distinguish one person from the other. Facial (face) recognition is a computer application that automatically identifies or verifies a person with the help of a digital image or a video frame from a video source. A simple camera or a web cam with good resolution use in face recognition, after capturing face image the device computes a digital representation based on some features of the face. The representation is compared with one which is stored in a database, and if there is a match, the user is authenticated. It is easy to implement and cheap authentication method with unique recognition. Facial recognition in visible light typically models key features from the central portion of a facial image. Using a wide assortment of cameras, the visible light systems extract features from the captured image(s) that do not change over time while avoiding superficial features such as facial expressions or hair. The accuracy of the face recognition systems improves with time, but it has not been very satisfying so far.

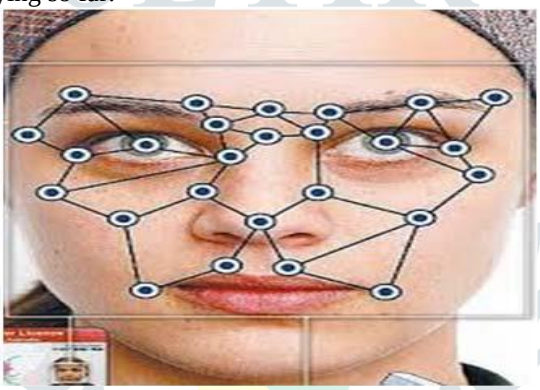

Fig 2: Face Recognition

Fingerprints scanning: - Today fingerprints consider being one of the oldest and popular among other bio-metric technologies. This is the oldest biometric authentication approach. Itanalyzes finger characteristics. The first is by scanning optically the finger. The other method is by using electrical charges that determines which parts of the finger are directly in contact with the sensor. Each fingerprint has some characteristics, such as curves, bifurcations, deltas. One set of these characteristics is unique for each person. Fingerprint matching techniques can be placed into two categories: minutiae-based and correlation based [9]. Minutiae-based techniques find the minutiae points first and then map their relative placement on the finger. Minutiae are individual unique characteristics within the fingerprint pattern such as ridge endings, bifurcations, divergences, dots or islands. In the recent years automated fingerprint comparisons have been most often based on minutiae. The problem with minutiae is that it is difficult to extract the minutiae points accurately when the fingerprint is of low quality. This method also does not take into account the global pattern of ridges and furrows.

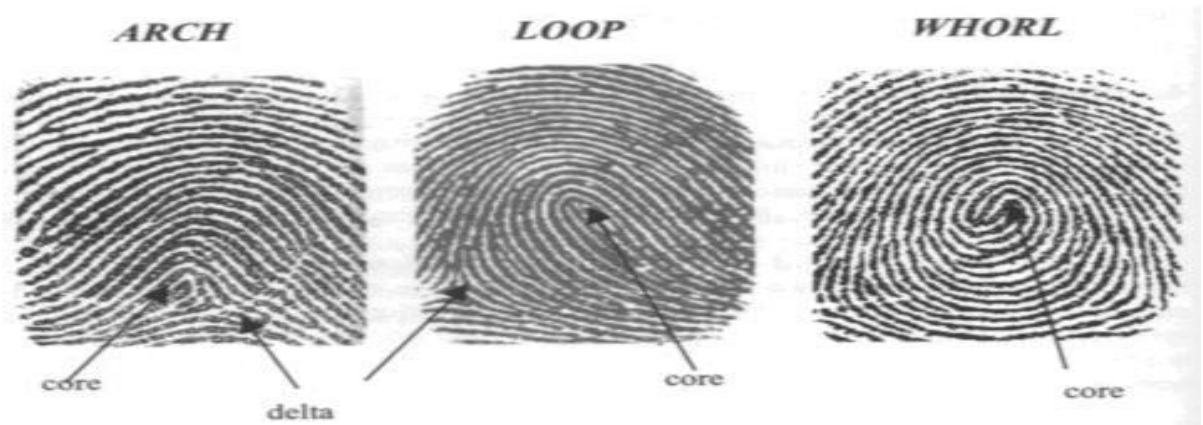

Fig 3: Fingerprints scanning

DNA: - Not long ago Russian show business was full of rumors that one of the popular Russian singers has two fathers and each father tried his best to influence on the son. Special programs were created and the situation was discussed but only one thing was interested to public: who was the real father of the singer. The singer himself was confused. In one of the programs the singer and both of his father's decide to take DNA test.

Fig 4: DNA testing

Hand Recognition: Palm print is inner part of hand. Palm prints possess features such as principal lines, orientation, minutiae, singular points etc. Also palm print modality is unique. Palm print recognition is used in civil applications, law enforcement and many such applications where access control is essential. Palm has features like geometric features, delta point's features, principal lines features, minutiae, ridges and creases. Principal lines are heart line, head line and life line. Palm print contains three principal lines which divides palm into three regions: Interdigital, Hypothenar and Thenar. An Inter-digital region lies above the Heart line [10]. The Thenar lies below the Life line. And Hypothenar is between Heart and Life line. From palm print principal lines, minutiae, ridges features can be extracted for identification. Hand vein geometry is based on the fact that the vein pattern is distinctive for various individuals. The veins under the skin absorb infrared light and thus have a darker pattern on the image of the hand taken by an infrared camera .The hand vein geometry is still in the stage of research and development. One such system is manufactured by British Technology Group. The device is called Veincheck and uses a template with the size of 50 bytes.

Iris Recognition: There are two methods using the eyes characteristics for authentication.

The first is based on the retinal recognition. The user has to look in a device that performs a laser-scanning of his retina. The device analyzes the blood vessels configuration of the acquired retinal picture. This blood vessels configuration is unique for each eye. The device is not friendly, because you have to fix a point while a laser is analyzing your eye. The second method is based on the iris recognition. The scan is done by a camera. Unlike the retinal method, you don't need to be close to the device to be authenticated. The acquired picture is analyzed by the device, and contains 266 different spots. Moreover iris is stable through the whole life. The 266 spots are based on characteristics of the iris, such as furrows and rings. The iris patterns are obtained through a video-based image acquisition system. Systems based on iris recognition have substantially decreased in price and this trend is expected to continue. The technology works well in both verification and identification modes. The main drawback of the retina scan is its intrusiveness. The method of obtaining a retina scan is personally invasive. A laser light must be directed through the cornea of the eye. Also the operation of the retina scanner is not easy.

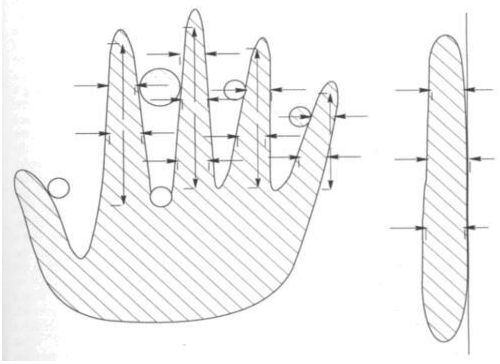

Fig 5: Hand Recognition

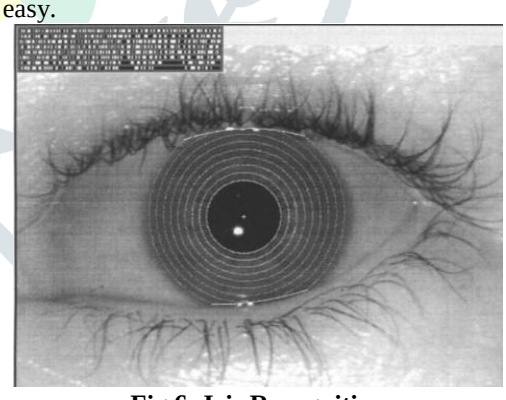

Fig 6: Iris Recognition

2. Behavioral characteristics

Voice recognition: Voice, like many other characteristics that are used for biometric methods, is unique. Like style of gait, it takes quite little time to analyze the voice and to identify the person. Voice in biometrics or "voice print" is presented as a numerical model of the sound. The user speaks in a microphone, and voice is recorded and computed. It is done by using some frequency analysis of the voice. It can be useful to authenticate someone through a telephone, and it allows users to work on a remote location. It is less accurate than other biometrics authentication methods, and some errors can occur.

Fig 7: Voice Recognition

Key stroke and Signature scanning:- The keystroke is the behave of the human mean to say that the different humans have the different techniques of pressing keys on such basis the identification takes place. Another behavioral biometric is signature by which the data can be extract by the signature of that particular person.

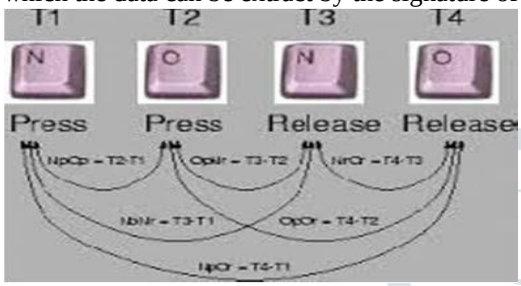

Fig 8: Keystroke and Signature Scanning

Characteristics of Biometric: Any physical and/or behavior characteristics of a human can be considered as a biometric if it exhibits following characteristics.

- **Universality:** Each person accessing the biometric application should possess a valid biometric trait.
- **Uniqueness:** The given biometric trait should exhibits distinct features across individuals comprising the population.
- **Permanence:** The biometric characteristics should remain sufficient invariant over a period of time.
- **Measurability:** The biometric characteristics can be quantitatively measured i.e. acquiring and processing of biometric trait should not cause inconvenience to the individual.
- **Performance:** The biometric trait should the required accuracy imposed by the application
- **Acceptability:** The chosen biometric trait must be accepted by a target population that will utilize the application.
- **Circumvention:** This indicates how easily the chosen biometric trait can fooled using artifacts.

II. Working of Biometric System

The block diagram illustrates the two basic modes of a biometric system.[3] First, in verification (or authentication) mode the system performs a one tone comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Three steps are involved in the verification of a person. In the first step, reference models for all the users are generated and stored in the model database. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. Third step is the testing step. This process may use a smart card, username or ID number (e.g. PIN) to indicate which template should be used for comparison. 'Positive recognition' is a common use of the verification mode, "where the aim is to prevent multiple people from using the same identity".

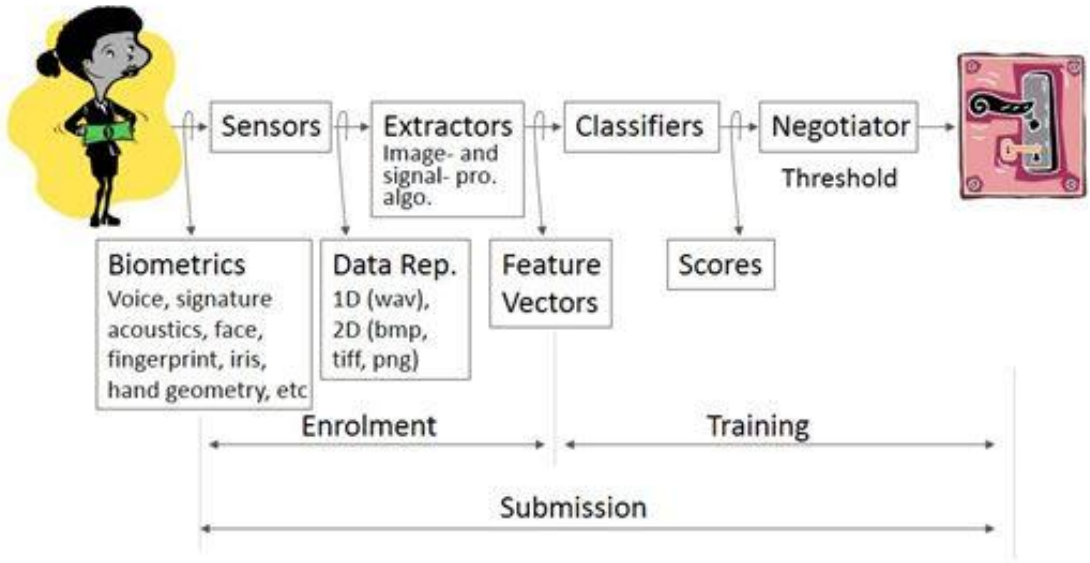

Fig 9: Block Diagram of Biometric System

III. Conclusion

In this paper Biometric Authentication is reviewed and explained in detail. A biometrics technique does not require password, PIN numbers or any RFID cards. Biometric technique is also used broadly due to its high security. Another feature of biometric is its efficiency. It is very easy to use and handle. Biometric uses face recognition, fingerprint scanning, DNA, hand recognition, iris recognition, voice recognition, key stroke and signature scanning which are explained in detail. In this paper the complete review of Biometric authentication is provided.

REFERENCES

[1] Pravin J, Deepak Sankar A, "Industrial pollution monitoring system using LAB VIEW and GSM", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Issue 6, June 2013

[2] Vipul Ranjan Kaushik et al., "IOT based energy meter billing and monitoring system -A case study," International Research Journal of Advanced Engineering and Science, Volume 2, Issue 4, pp. 64-68, 2017.

[3] V. N. Patil et al., "Criminal Identification Using Arm7," International Research Journal of Engineering and Technology, Vol: 04, Issue: 3, pp.677- 680, Mar -2017.

[4] Souvik Manna, Suman Sankar Bhunia, "Vehicular Pollution Monitoring Using lOT", IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014.

[5] Vipul Ranjan Kaushik et al., "IOT based Vehicle Tracking & Vehicular Emergency System-A Case Study and Review", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 6, Issue 10, pp. 8001-12, October 2017.

[6] V. N. Patil et al., "Voice over Internet Protocol Technology for Automation," Wulfenia Journal Klagenfurt , Austria, Vol 24, No. 3, pp. 321-330, Mar 2017.

[7] Jiong Jin, Jayavardhana Gubbi, Slaven Marusic, Marimuthu Palaniswami, "An Information Framework for Creating a Smart City Through Internet of Things," IEEE Internet of Things Journal, Volume: 1, Issue: 2, April 2014: DOI:10.1109/JIOT.2013.22965168.

[8] V. N. Patil et al., "Digital Static Timing Path Analyzer for DSCH Program," International Research Journal of Engineering and Technology, Vol: 04, Issue: 3, pp.674- 677. | Mar -2017

[9] Shadrach Tunde,Akinkaude, Kowawole, Peter Fasae, "A Survey of Noise Pollution in Ado-Ekiti Metropolis Using Mobile Phone," Science Technology Department, Science Research Publishing, October-2015.

[10] Navreetinder Kaur, Rita Mahajan, Deepak Bagai,"Air Quality Monitoring System based on Arduino Microcontroller", International Journal Innovative Research in Science, Engineering and Technology (IJIRSET), Vol 5, Issue 6- June 2016.