ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 10, March 2018

REVIEW OF BIOMETRICS SYSTEM

Inderpreet kaur
Research Scholar, Computer Applications, CT University, Ludhiana, India
inder5preet@gmail.com

Abstract: A comprehensive variation of systems demands authentic personal recognition schemes to either confirm or determine the identity of a person for their services requesting. The aim of such schemes is to ensure that the rendered services are accessed only by an authorized user, and not any other. For instance of similar applications include trouble-free access to computer systems, laptops, cellular phones, buildings, and ATMs. In the nonexistence of strong personal recognition schemes, these systems are unprotected to the wiles of a deceiver. Biometric identification refers to the automate identification of persons founded on their physiologic features. By using biometrics it is easy to prove a person's identity based on "who she is", rather than by "what she holds" (e.g., an ID card) or "what she remembers" (e.g., a password).The extended use of computers in information technology, it is essential to prevent unauthorized entrance to or fraudulent use of secret data. In this paper, a brief overview of the field of biometrics has been examined.

Keywords: Biometrics, Verification, Identification, Work Process

I. INTRODUCTION

Technology advancement makes possible variation of devices to increase the value or productivity of our lives, the requirement for such systems to be reliable and safe has become highly important [1]. Particularly, biometrics used in various applications and is specified as recognizing uncommon physical attributes of the human body. Biometric system is the procedure of verification of genuineness based on human's unique traits. It refers to automatic validation of a human being based on anatomical or behavioral features. Fingerprint, face, iris, ear etc. can be an example of anatomical characteristics and signature, keystroke, gait etc. can be an example of behavioral characteristics. Biometrics gives extensive comfort and various benefits over conventional security methods such as remembering a password or having an identification card. At the present time, users don't need to memorize personal identification number (PIN) or pass code and don't need to carry keys or cards which can be stolen because of the biometric system. In these days, biometric recognition system used in many military, non-military and government applications [2].

A. Biometric:

Biometric: The term biometric is a combination of two words bio i.e. life and metrics i.e. measurement and attained from Greek. Biometrics refers to the automatic identification or analysis of human's unique physiological and behavioral characteristics. A biometric system is necessarily a pattern detection system which makes a personal identification by defining the correctness of a precise physiological or behavioral feature owned by the user [3]. Nowadays, We are using biometric on regular basis in many places such as office workplace attendance, security checkpoints, and even our national UID card are created using biometric technology.

II. METHODS

Biometrics is used for two authentication methods (Illustrated in Fig. 1):

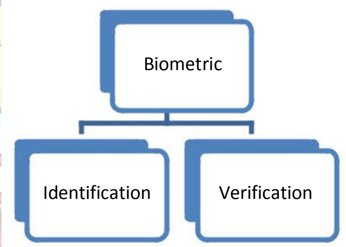
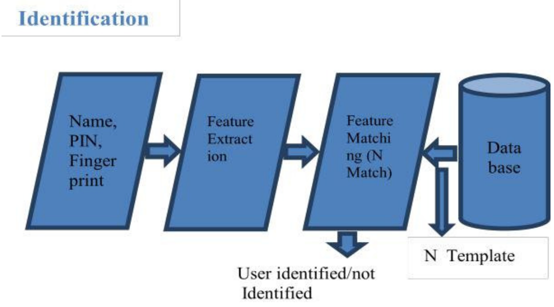


Fig.1. Types of method

A. Identification: In the identification process, the system verifies a person by seeking the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many (1: N) comparison to establish an individual's identity [4]. In 1: N matching individual's biometric is compared against multiple biometric templates in the system's database. In identification systems, the objective is to identify who a person is [1].Identification is pictorially represented in figure 2.



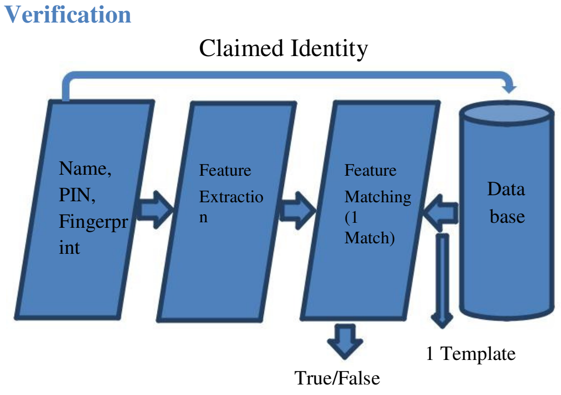


Fig. 2.Verification and identification tasks [4]

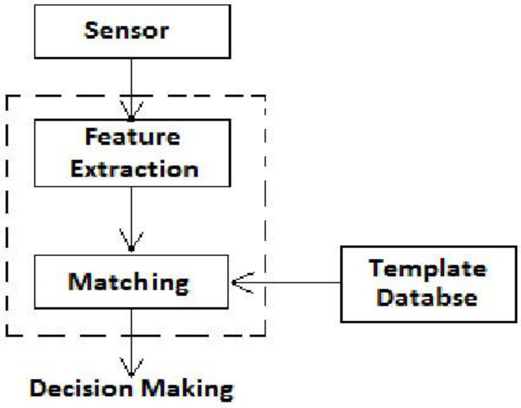


Fig. 3. Block diagram of the biometric process [7]

B. Verification: In the verification procedure, the system confirms a person’s identity by relating the taken biometric data with her own biometric template(s) accumulated system database. In this type of system, a person who needs to be identified requests an identity, usually through a PIN (Personal Identification Number), a username, a smart card, etc., and the system conducts a one-to-one comparison to decide whether the claim is true or not [4].In verification systems, the aim is to authenticate that a person is who he or she claims to be (i.e., the person who registered) [1].Verification is pictorially represented in figure 2.

Identification includes relating the attained biometric data in contrast to templates equivalent to all users in the database while verification includes a relationship with only those templates equivalent to the requested identity [5].

III. WORKING OF BIOMETRIC PROCESS

The detail of the human being which varies from one person to other is used as unique biometric data to provide as that person's unique recognition. The body parts such as retinal, fingerprint, iris, palm print, and DNA. Biometric system gathers and accumulates this data in order to authenticate any person’s identity. The combination of biometric data and biometric identification/recognition technologies creates the biometric security systems [6].

A. **Capturing biometric data**: When a user places the finger or palm at the sensor, the biometric data is presented to the capturing device [8].

B. **Pre-processing stage**: This is the stage before the feature extraction. Here biometric data is recorded and pre-processed by improved input from the sensor. It removes extra noises and distortions. The input is maintained to get the required format for maximum extraction.

C. **Feature extraction**: In this stage, the pre-processed data is extra processed and features are extracted in a best possible way. Because not all the data captured is required for biometric assessment.

D. **Template creation**: After feature extraction process is complete, a template is created from entire significant characteristics taken out from the users. The unnecessary data which is not required for the comparison algorithm is washout to reduce the file size and protect the privacy and security of user identity [9].

E. **Storage of the template**: Here template is getting stored in a reusable database, which can is needed at the time of execution of the matching process.

F. **Matching phase:** This is the last step that involves an algorithm to perform a comparison between the template already stored in the database and the template obtained for decision making. After the decision making the result is then passed on to some application device for further actions.

IV. TYPES OF BIOMETRICS:

Biometric types can be mainly categorized into two types i.e. physiological biometrics and behavioral biometrics. A fingerprint is an example of physiological biometric. In other hand behavioral biometrics which look at your own personal movements and gestures. There are various types of biometrics, which is pictorially represented in figure 4:

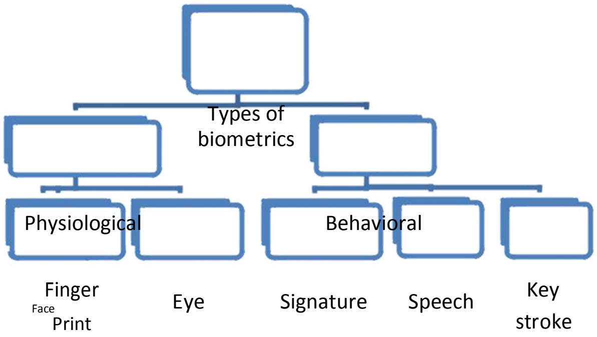


Fig:4 Different ways of biometrics [10]

V. CONCLUSION

As we can see that security fears have increased to very high levels of violence and other hidden dangers are around which origin vast damage to human life and intellectual property. To safeguard against all these high quality technical attacks and intrusions we need equally sophisticated biometric security systems. Biometrics security system has revolutionized the way people generally perceive security. Biometric systems along with the existing systems and technology can produce a very well protected system where a consumer can have rest from all their worries related to the money theft, identity theft etc. In this paper, various authentication methods, working process etc. of a biometric system have been examined. This paper will be beneficial to novice for understanding the fundamental concepts of image processing.

References:

1. *Biometric Analytics Cost Estimating.* **Sean McKenna, Joseph Sarage.** San Diego, CA : s.n., June 10, 2015. International Cost Estimating and Analysis Association (ICEAA) Conference.

2. *Ensuring Quality in Biometric Systems.* **Md. Mahbubur Rahman, Amit Karmaker, Md.Mahmudul Hasan and Samsuddin Ahmed.** Dumki, Bangladesh : s.n., 2015, International Journal of Security and Its Applications, Vol. 9, pp. 153-160. ISSN: 1738-9976 .

3. *BIOMETRICS : A FURTHER ECHELON OF SECURITY.* **Siddhesh Angle, Reema Bhagtani, Hemali Chheda.** Bandra, Mumbai : s.n.

4. *An Introduction to Biometric Recognition.* **Anil K. Jain, Arun Ross and Salil Prabhakar.** january 2004, Vol. 14.

5. *A SURVEY OF BIOMETRIC RECOGNITION METHODS.* **Kresimir Delac, Mislav Grgic.** Zadar, Croatia : s.n., 2004. 46th International Symposium Electronics in Marine.

6. *Biometric Authentications to Control ATM Theft.* **Siddiqui, Ahmad Tasnim.** Kingdom of Saudi Arabia : s.n., jun 2015, Asian Journal of Technology & Management Research , Vol. 5 . ISSN: 2249 –0892.

7. https://www.researchgate.net/figure/Block-diagram-of-Biometric-Process-Image-Source_fig2_274256399. *www.researchgate.net.* [Online]

8. *Biometric Security Enhancement using GLCM Method: A Review.* **Shelza Thakur, Shivani Rana, Vandana Thakur.** may 2015, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vol. 4.

9. *A Personal Verification and Identification using Palmprint and Hand Geometry Biometric Recognition System.* **Shiv Kumar, Vikas Kumar.** BAREILLY : s.n., september 2015, International Journal of Computer Science and Mobile Computing, Vol. 4, pp. 28 – 35. 2320–088X.

10. *SURVEYONRECOGNITIONOFDIFFERENT BIOMETRIC.* **S.N.Bharath, Tushar,Sachin Bharadwaj,Vidyalakshmi,Tashmitha Rao.** Mangalore : s.n., 2015, KAAV INTERNATIONAL JOURNAL OF SCIENCE, ENGINEERING, Vol. 2. 2348-5477.