Biometric System: An Overview

Komal
M.Tech (Computer Science & Engineering)
Department of Computer Science and Application, K.U. Kurukshetra (Haryana), India
thakrankomal07@gmail.com

Abstract: Biometric is an automated recognition of an individual based on physiological and behavioural traits such as fingerprint, face, iris, voice, signature etc. Biometric recognition is very reliable and natural mechanism for ensuring that only authorized user can access the system. Biometric recognition is basically a sample recognition system that operates by capturing biometric data from an individual through sensor, extracting a feature set from the acquired data, and comparing this feature set against the templates stored in the database. Biometric system is more secure and reliable authentication system as compared to traditional token based and password based technologies. This paper discusses a brief overview of biometric system, various biometric modalities, their performance metrics and their comparison based on the biometric characteristics.

Keywords: Biometrics, Biometric Characteristics, Biometric Deformations, Biometric Modalities.

1. Introduction

Biometric is an automated recognition of an individual based on physiological and behavioral traits such as fingerprint, face, iris, voice, signature etc [1]. There are three levels of user authentication schemes as shown in table 1. First is token based and it relies on something a person carries such as ATM card, passport etc. Second is information based and it relies on something a person knows such as password, pin etc. Third is biometric based and it relies on physiological and behavioral characteristics of a person.

Table 1: Different Type of User Authentication Schemes

Method	Examples	Problems
Token based	ATM card, passport, smart card etc.	Lost or stolen, can be duplicated
Information based	Password, pin, id etc.	Forgotten, shared etc.
Biometric based	Fingerprint, iris, face etc.	Non-repudiable authentication

Biometric authentication system is more reliable or suitable for the users because there is no key to be lost or password to be forgotten and only single biometric trait can be used to access several accounts without the need of remembering anything like password, pin etc. Biometric based system can be used for personal data privacy or financial transactions in the federals, state or central governments, and in the military, in the banking, in health services, in commercial applications etc [2]. Biometric will become significant or essential component of identification technology because biometric sensors price continue to fall and user becomes aware of the strength of the biometric system. Biometric is fairly a new way to protect person's information. Alphonse Bertillon, chief of the criminal identification division of the police department in Paris, developed the idea of using a number of body characteristics to identify criminals in the mid of 19th century. He discovered the distinctiveness of the human fingerprint in the late 19th century. After this discovery many major law enforcement department uses the idea of first booking the fingerprint of criminals and storing it in their database. Later, the leftover fingerprint (i.e. latent) at the scene of crime could be lifted and matched with the fingerprints in the database to determine the identity of criminal. But there are also some limitations in the system i.e. system can be circumvented by the skilled imposter.

2. Biometric Operations

A biometric system is a sample recognition system that operates by acquiring biometric data from an individual through sensor, extracting a feature set from the acquired data, and comparing this feature set against the templates stored in the database. Depending on the application context, a biometric system may operate either in identification mode or verification mode. Before the system can be put into these modes, a system database must be created through to process of enrolment.

- **Enrolment -** Enrolment is the process where the user's initial biometric samples are collected, assessed, processed, and stored for use in a biometric system as shown in Fig. 1.1. If users are experiencing problems with a biometric system then they have to re-enroll to gather higher quality data.

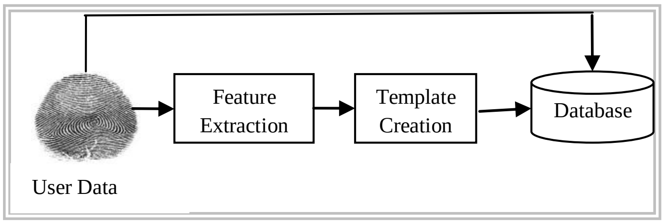

Fig. 1: Enrolment Process in Biometric System

Biometric system can provide two main functionalities after enrolment: - (i) verification (ii) identification.

(i) Verification: It refers to 1:1 matching. Verification is also known as authentication, the user claims an identity and system verifies whether the claim is genuine or not. Sample given by individual is matched with only one template i.e. stored template of that person only. As only one matching is performed so verification process is very fast and accurate.

DOI: 10.141079/IJITKM.2015.918

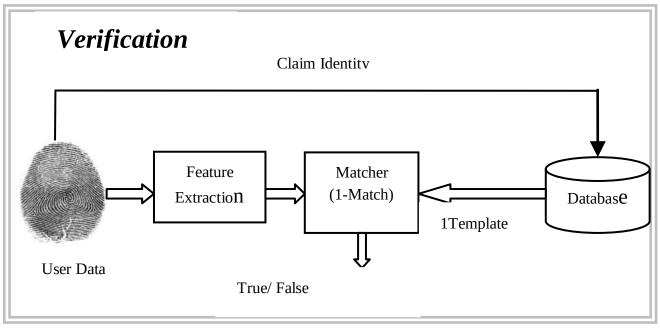

Fig. 2: Verification Process in Biometric System

(ii) Identification: It refers to 1: N matching where N is total number stored templates in database. In this situation user does not know his identity, he is simply presenting his biometrics for matching with whole database. User's data is matched with all the templates to identify with which template it has highest similarity.

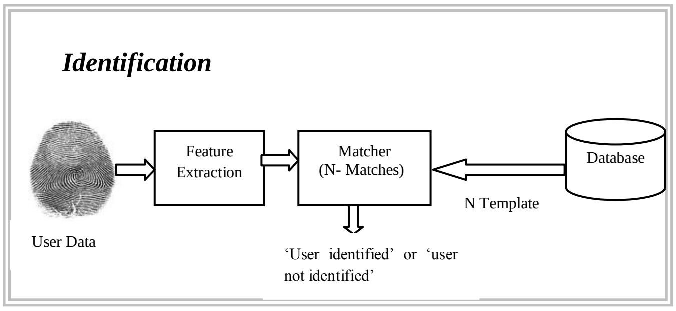

Fig. 3: Identification Process in Biometric System

3. Structure of Biometric System

Every biometric system consist of four basic modules. Modules are mainly used for converting the acquired image into some useful information and stored as a template [3] . The block diagram of biometric system is shown in Fig 4.

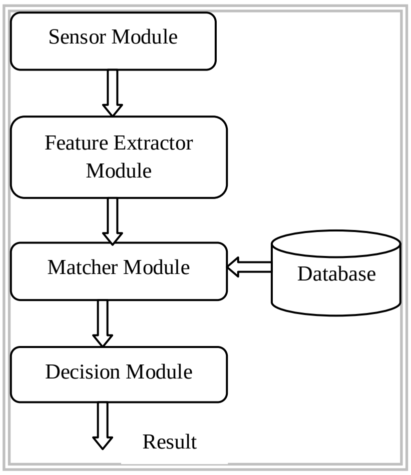

Fig. 4: Biometric System Modules

The description of modules are as follows [4] :

- **Sensor Module**
  Sensor module in biometric system is used for capturing biometric data(e.g. fingerprint, face, palm print etc.) and after scanning convert it into digital form.
- **Feature extractor module**
  The feature extractor module in a biometric system operate on data sent by the sensor module. As its name indicates, module extract feature set and store it in a compact representation called template database.
- **Matcher module**
  This module compare feature set received from feature extractor module with templates stored in database. Matching result are generated when all comparisons are done. This result is used for identification and verification of an user. This module is considered as main module in biometric system.
- **Decision module**
  This module accept or reject the user after comparing matching score with predefined security threshold value, if matching score is higher than predefined security threshold value, it will accept the user otherwise reject it.

4. Characteristics of a biometric system

Some characteristics of biometric system are [5]:

- **Universality:** It means that every person should possess the biometric traits.
- **Uniqueness:** It indicates that no two persons should be the same in terms of the traits.
- **Permanence:** It means that the traits should be invariant with time. A trait that changes significantly over time is not a useful biometric.
- **Collectability:** It means that it should be possible to acquire and digitize the trait using suitable devices without causing any inconvenience to the user.
- **Acceptability:** It indicates the extent to which people are willing to accept a particular biometrics in their daily life.
- **Circumvention:** It refers to how easy it is to fool the system by fraudulent methods**.**

5. Biometric Modalities

Biometric is broadly divided into two categories based on the individual's physiological or behavioral characteristics as shown in Fig.5.

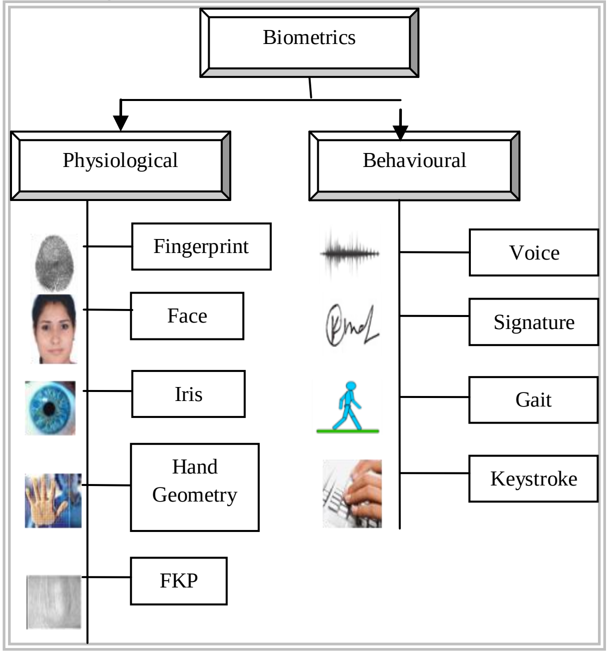

Fig. 5: Classification of Biometric Modalities

DOI: 10.141079/IJITKM.2015.918

Oldest trait that has been used for more than 100 years is fingerprint recognition. Behavioural methodologies are related to the behavior of a person e.g. voice, signature, gait etc. The commonly used behavioral trait that is still widely used is the signature recognition. Each biometric modality has its strengths and weakness and accordingly appeals to particular identification application

- **Fingerprint**
  A fingerprint is made up of ridges and furrows. Uniqueness is determined by ridges, furrows, and the minutiae points. Fingerprint is one of oldest and most popular recognition technique. Every individual possesses unique finger patterns, even twins has different patterns of ridges and furrows. Fingerprint matching techniques are of three types [6]: (i) Minutiae-based matching (ii) Correlation-based method (iii) Pattern based matching.
- **Face Recognition**
  Face recognition is based on both the location and shape of the eyes, eyebrows, nose, lips and chin. It is non intrusive method and very popular also. Facial recognition is carried out by measuring facial metrics (e.g. measure distances between pupils or from nose to lip or chin) [6][7].
- **Iris Recognition**
  The iris is the elastic, pigmented, connective tissue that controls the pupil. The process of iris formation in early life is called morphogenesis. Once completely formed, the texture is stable throughout life. It is the most accurate biometric recognition system so it is called as king of biometrics. The iris of the eye has a unique pattern, from eye to eye and person to person [8].
- **Hand Geometry**
  This recognition includes measuring length, width, thickness, surface area, or overall structure of the hand. The fact is that a person's hand is unique and it does not change after certain age [9].
- **Finger Knuckle Print (FKP)**
  FKP is a new biometric identifier which refers to the inherent skin pattern of the outer surface around the inter-phalange joint of one's finger. It can have a high user acceptance. There is no stigma of criminal investigation associated with the FKP. These characteristics make great potential to be widely accepted promising biometric identifier [10].
- **Voice Recognition**
  It focuses on the vocal features that produce speech and does not focus on the sound or the pronunciation of speech. The vocal properties depend on the dimensions of the vocal tract, mouth, nasal cavities and the other speech processing mechanism of the human body [11].
- **Signature**
  A signature is a handwritten depiction of someone's name, nickname that a person writes on documents as a proof of identity. Signatures have been accepted in government, legal, banking and commercial transactions as a method of authentication. It is also a widely accepted method of authentication [12].
- **Gait Recognition**
  It refers to how the person walks. Gait is the model of movement of the limbs of animals, including humans. Patterns include overall velocity, kinetic and potential energy cycles, forces, and changes in the contact with the surface (ground, floor, etc.). Gait recognition also takes into account the gender of the person because there is difference in the way of walking of males and females [13].
- **Keystrokes**
  It is the way a person types on keyboard. It includes speed, how the buttons are pressed and released. It changes from person to person [14].

Table 2: List of Popular Biometrics Modalities

Biometric Modalities	**Measurable Units**
Fingerprint	Finger lines, pore structure
Facial Geometry	Distance of specific facial features (mouth, nose, eyes)
Iris	Iris pattern
Hand Geometry	Measurements of fingers and palm
FKP	FKP image of all fingers except
Voice	Tone or timbre
Signature	Writing with pressure and speed
Gait	Gait energy image, user's height and walk length
Keystroke	Keystroke durations, finger placement and applied pressure on the keys

6. Biometric Deformations

Biometric system performance varies according to input sample quality and the environment in which the input is being submitted; it is possible to locate and minimize factors that can decrease/affect system performance [15]. These factors are called Biometrics- Deformations.

Deformations for various modalities are as given below:

- **Fingerprint**
  - Cold finger
  - Dry/oily finger
  - Cuts on fingerprint
  - Low or high humidity
  - Angle of placement
- **Voice recognition**
  - Cold or illness that affects voice
  - Different enrolment and verification Devices
  - Different enrolment and verification environments
  - background noise
  - Poor placement of capture device
- **Facial recognition**
  - Change in facial hair
  - Lighting conditions
  - Adding/removing glasses
  - Change in hairstyle
  - Change in weight

- **Iris-scan**
    - Too much movement of head or eye
    - Glasses
    - Colored contacts lenses
    - Too much movement of head or eye
- **Hand geometry**
    - Jewelry
    - Change in weight of body
    - Swelling of joints
- **Signature-scan**
    - Marking too quickly
    - Marking positions (e.g., sitting vs. standing)

In addition, for many systems, an additional problem occurs when a long period of time has elapsed since enrolment or since last verification. If significant time has elapsed since enrolment, physiological changes can complicate verification process and the user may have “forgotten” how she or he enrolled, and may place a finger differently or recite a pass phrase with different intonation. The performance of biometric systems varies for specific populations.

7. Performance Metrics

Different metrics can be used to rate the performance of a biometric factor, solution or application. Two most common performance metrics are False Acceptance Rate (FAR) and the False Rejection Rate (FRR).

- **False Acceptance Rate (FAR)**

It refers to the possibility where an unauthorized user is accepted by the authentication biometric system as an authenticated person. It measures the percentage of invalid inputs that are incorrectly accepted.

- **False Reject rate (FRR)**

It is the probability for an authorized person is rejected by the biometric machine as an unauthenticated person. It measures the percentage of incorrectly rejected valid users.
False Accept Rate is also known as False Match Rate, and False Reject Rate is known as False Non-Match Rate as shown in Fig 6.

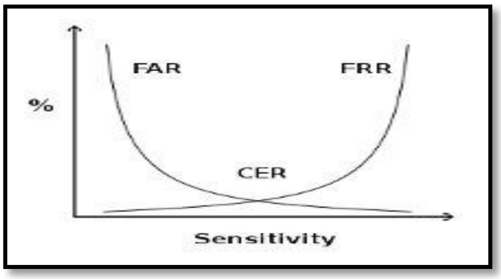

Fig.6: Graphical Representation of FAR and FRR Errors, Indicating CER

- **Crossover Error Rate (CER)**

It is the rate where both accept and reject error rates are equal. CER is also called Equal Error Rate (EER). Devices with lowest EER are most accurate.

- **Failure to Enroll Rate (FER)**

Failure to Enrollment Rate FER is the rate at which attempts to create a template from an input is unsuccessful. It can be defined as the probability that a user attempting to enroll itself but unable to do so. The reason for this is low quality inputs.

8. Comparison of Different Biometric Modalities

The comparison of various biometric traits in terms of above mentioned characteristics is shown in Table 3. Each biometric trait is ranked based on the categories as being low (L), medium (M) or high (H). A low ranking indicates poor performance, a medium ranking indicates good performance and a high ranking indicates a very good performance in the evaluation criterion [16].

Table 3: Performance Comparison of various Biometric Modalities

Identifier/ Criteria	**Universality**	**Uniqueness**	**Permanence**	**Performance**	**Acceptability**	**Collectability**	**Circumvention**
Fingerprint	M	H	H	H	H	M	H
Hand Geometry	M	M	M	M	M	H	M
FKP	M	H	H	H	H	M	M
Face	H	L	M	L	H	H	L
Iris	H	H	H	H	L	M	H
Voice	M	L	L	L	H	M	L
Signature	L	L	L	L	H	H	L
Keystroke	L	L	L	L	M	M	M
Gait	M	L	L	L	H	H	M

9. Conclusion

This paper presents a basic overview of biometric system and comparative analysis of various biometric techniques based on different parameters like universality, uniqeness, permanence, collectability, performance, acceptability, circumvention. This paper also presents the various issues associated with the biometric deformation and various performance matrics of the biometric system. Based on the above review it can be concluded that there is a considerable scope in enhancing the performance and efficiency of the biometric system.

DOI: 10.141079/IJITKM.2015.918

References

[1] Jain, A. Lansing, E., (2002), “Biometrics Personal Identification in Networked Society”, New York Kluwer Academic,” KluwerAcademic Publishers New York, Boston, Dordrecht, London, Moscow.

[2]. Jain A.K. (2008), “Handbook of Biometrics,” Michigan State University, USA.

[3]. Kant, C. and Jain, R. (2015). Attacks on Biometric System: An Overview. *International Journal of Computer Science and Application*, 3(2), pp. 1090-1094.

[4]. Obied, A. (2011). How To Attack Biometric System In Your Spare Time. *International Journal Of Scientific & Technology Research*, 4(1), pp. 1-9.

[5]. Sareen, P. (2014) "Biometrics – Introduction, Characteristics, Basic Technique, Its Types And Various Performance Measures," *International Journal Of Emerging Research In Management &Technology*, Vol. 03, No. 05, 2014.

[6]. Jain, A.K. Pankanti, A. and Ross, S. (2006). Biometrics: A Tool for Information Security. *IEEE Transactions on Information Forensics And Security*, 1(2), pp. 125-144.

[7]. Hong, L. and Jain, A.K. (1998). Integrating faces and fingerprints for personal identification. *IEEE Trans. Pattern Anal. Mach. Intel.*, 20(12), pp. 1295-1307.

[8]. Ghatol, S. and Ganorkar, R. (2007). Iris Recognition: An Emerging Biometric Technology. *In: Proc. of the 6th International Conference on Signal Processing, Robotics and Automation.* Greece, 2007, pp. 1348-1363.

[9]. Sareen, P. (2014) "Biometrics – Introduction, Characteristics, Basic Technique, Its Types And Various Performance Measures," *International Journal Of Emerging Research In Management &Technology*, Vol. 03, No. 05, 2014.

[10]. Kumar, A. and Zhou, Y. (2009). Personal identification using finger knuckle orientation features. *Electronic Letters*, 45(20), pp. 1-8.

[11]. Ross, A. Prabhakar, S. and Jain, A.K. (2004). An introduction to biometric recognition. *IEEE Trans. Circuits Sysems.Video Technology, Special Issue Image- and Video-Based Biomet.*, 14(1), pp. 4-20.

[12]. Rode, Y.S. Dabhade, S.B. Al-Dawla, N.H. Mane, A.V. Manza, R.R. and Kale, K.V. (2012). Multimodal Biometric System Using Face And Signature: A Score Level Fusion Approach. *Advances in Computational Research*, 4(1), pp. 99.

[13]. Yampoolskiy, V. and Ramen, V. (2008). Biometrics: a survey and classification," *International Journal of Biometrics*, 1(1), pp. 81-113.

[14]. Ramel, J. Cardot, H. and Hocquet, S. (2005). Fusion of Methods for Keystroke Dynamic Authentication. In: *Proc. of 4th IEEE Workshop on Automatic Identification Advanced Technologies*, USA, pp. 224-229.

[15]. Maltoni, D. Maio, D. And Prabhakar, S. (2003). Handbook of Fingerprint Recognition. New York: Springer-Verlag.

[16]. Jain, A.K. (1999). “Biometrics: personal identification in Networked Security” Kiuwer Academic
Publishers,1999.

DOI: 10.141079/IJITKM.2015.918