IJCSC Volume 5 • Number 1 March-Sep 2014 pp.37-42 ISSN-0973-7391

A Comparative Study of Different Biometric Technologies

Arun Kumar Yadav, Sanjiv Kumar Grewal
Department of Computer Science and Applications, Kurukshetra University, Kurukshetra
arunkumar9429@gmail.com,sanjeev.grewal1990@gmail.com

ABSTRACT: Biometrics refers to the use of distinctive physiological (fingerprint, face, retina etc.) and behavioral (gait, signature etc.) characteristics for authentication. Every person has distinct physiological and behavioral characteristics. Traditional methods of establishing a person's identity include knowledge-based (e.g., passwords) and token-based (e.g., ID cards) mechanisms. These can easily be lost, shared or stolen . Therefore, they are not sufficient for identity verification in the modern day world. A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. As compared to traditional token based and password based technologies, biometric technologies are secure for reliable authentication. This paper presents a brief overview about biometric system, various biometric techniques and comparison among various biometric techniques based on the biometric characteristics.

KEYWORDS: Biometrics, Biometric Deformations, Biometric Technologies.

1. INTRODUCTION TO BIOMETRICS

Biometrics are the automated methods of recognizing an individual based on their physiological or behavioral characteristics [1]. Biometrics is the art of establishing the identity of individual based on the physical, chemical or behavioral attributes of a person. The relevance of biometrics in modern society has been reinforced by the need of large scale identity management systems whose functionality relies on the accurate determination of an individual's identity in context of several different applications. The identity of an individual may be viewed as the information with that person in a particular identity management system. For example an ATM card, will be defined by personal attributes name, address etc. By using biometrics it is possible to establish an identity based on who you are as it may be used to supplement ID cards. Based on the biological characteristics individuals are recognized. Biometrics offers certain advantages such as negative recognition and non repudiation that cannot be provided by tokens and password. Negative recognition is the process by which a system determines that a certain individual is indeed enrolled in the system although the individual might deny it. Non repudiation is a way to guarantee that an individual who accesses a certain facility cannot later deny using it. A number of biometric traits are in use in various applications. Each biometric has its strengths and weaknesses and the choice typically depends on the application [2]. While biometric systems have their own limitations such as expensiveness or sometimes less accurate they have an edge over traditional security methods in that they cannot be easily stolen or shared. These systems also enhanced user convenience by alleviating the need to design and remember password.

2. BIOMETRIC CHARACTERISTICS

Any human physiological or behavioral characteristic could be a biometrics provided it has the following [3]:

a. **Universality:** The biometric trait must be universal. Means every person should posses that biometric trait.
b. **Permanence:** The biometric trait of an individual should not be variable with time with respect to the matching algorithm. A trait that changes with time cannot be used as biometric.
c. **Uniqueness:** The biometric trait should be unique for individuals. In other words the trait should differ sufficiently in case of every two person so that each person can be identified individually.
d. **Measurability:** it should be possible to acquire and digitize the biometric trait using suitable devices. Furthermore, the acquired raw data should be valid to processing in order to extract representative feature sets.
e. **Performance:** The recognition accuracy and the resources required to achieve that accuracy should meet the constraints imposed by the application.
f. **Acceptability:** Individuals in the target population that will utilize the application should be willing to present their biometric trait to the system.
g. **Circumvention:** This refers to the ease with which the trait of an individual can be imitated using artifacts (e.g. fake fingers), in the case of behavioral traits.

3. BIOMETRIC SYSTEM MODULES

A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in verification mode or identification mode. In the verification mode, system conducts a one to one comparison to establish an individual's identity. In identification mode, system

conducts a one to many comparison to establish an individual's identity.

All the biometric systems have four main modules [4] (shown in figure 1):

a. **Sensor Module:** In this module the biometric data of the individual is been captured.
b. **Feature Extraction Module:** This module extract a set of salient or discriminatory features from the captured biometric data by sensor module.
c. **Matcher Module:** In this module the extracted features are compared against the stored template to generate matching scores.
d. **Decision Module:** Here the matching score is compared with the threshold value. If the matching score is greater than or equal to the threshold value, decision module gives positive result otherwise gives negative results.

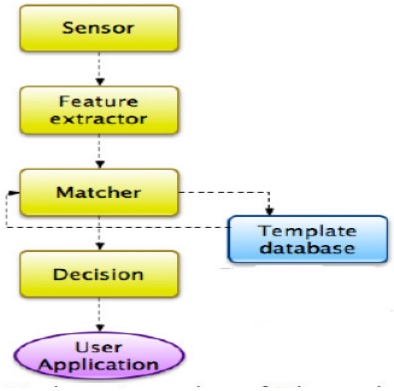

Figure 1 Biometric System Modules

4. BIOMETRIC TECHNOLOGIES

The function of a biometric technologies authentication system is to facilitate controlled access to applications, networks, personal computers and physical facilities. A biometric authentication system is essentially a method of establishing a person's identity by comparing the binary code of a uniquely specified biological or physical characteristic to the binary code of an electronically stored characteristic called a biometric. Biometric technologies are divided into two categories:

4.1 CONTACT BASED BIOMETRIC TECHNOLOGIES

A biometric technology that requires an individual to make direct contact with an electronic device(scanner) will be referred to as a contact biometric. Because of the inherent need of a person to make direct contact, many people have come to consider a contact biometric to be a technology that encroaches on personal space and to be intrusive to personal privacy. Some Contact biometric technologies are [5] :

a. **Fingerprint:** It has been used for personal identification for many decades. The matching accuracy using fingerprints has been shown to be very high. A fingerprint is the pattern of ridges and valleys on the surface of fingertip whose formation is determined during first seven months of fetal development. It has been empirically determined that the fingerprints of the identical twins are different. The accuracy of currently available fingerprint recognition system is adequate for authentication system in several applications, particularly forensics. One problem with large scale fingerprint recognition system is that they require a huge amount of computational resources, especially when operating in the identification mode.

Fingerprint

b. **Palmprint:** The palm of human hands contain patterns of ridges and valleys much like fingerprint. The area of the palm is much larger and hence are expected to be even more distinctive than fingerprints. Since palmprint scanners need to capture a large area, they are bulkier and more expensive than the fingerprint scanners. Human palms also contain additional distinctive features such as principal lines and wrinkles that can be captured even with a lower resolution scanner, which would be cheaper. Finally, when using a high resolution palmprint scanner, all features of the hand such as geometry, ridge and valleys features, principal lines, and wrinkles may be combined to build a highly accurate biometric system.

palmprint

c. **Signature:** The way a person signs her name is known to be characteristic of that individual. Although signatures require contact with the writing instrument and an effort on the part of the user, they have been accepted in government, legal, and commercial transactions as a method of authentication. Signature is a behavioral biometric that changes over a period of time and influenced by the physical and emotional conditions of the signatories.

Signature

d. **Hand Geometry:** These system are based upon number of measurements taken from human hand, including its shape, size of palm, and the lengths and widths of the

fingers. The technique is very simple, easy to use, and inexpensive. Environmental factors such as dry weather or individual anomalies such as dry skin do not appear to adversely affect the authentication accuracy of hand geometry based system.

Hand geometry

4.2 CONTACTLESS BIOMETRIC TECHNOLOGIES

A contactless biometric can either come in the form of a passive or active biometric. A contactless biometric can be used to verify a person's identity and offers at least two dimension that contact biometric technologies cannot match. A contactless biometric is one that does not require undesirable contact in order to extract the required data sample of the biological characteristics and in that respect a contactless biometric is most adaptable to people of variable ability levels. Some contactless biometric technologies are [5] :

a. Face : Face recognition is a non-intrusive method, and facial attributes are probably the most common biometric features used by human to recognize one another. The most popular approaches to facial recognition are based on either location, shape of facial attributes, such as eyes, eyebrows, nose, lips and their spatial relationship or the overall analysis of the face image that represent a face as weighted combination of a number of canonical faces. These systems also have difficulty in matching face images captured from two different views, under different illumination conditions, and at different times. It is a sufficient basis for recognizing a person from a large number of identities with an extremely high level of confidence.

b. Iris: The iris is the annular region of the eye bounded by the pupil and the sclera on either side. The visual texture of the iris is formed during fetal development and stabilizes during the first two years of life. The pigmentation, however, continues changing over an extended period of time. The complex iris texture carries very distinctive information useful for personal recognition. The accuracy and speed of currently deployed iris based recognition system is promising and support the feasibility of large scale identification system based on iris information .Each iris is distinctive and even the iris of identical twins are different. It is possible to detect the contact lenses printed with the fake iris. The hippus movement of the eye may also be used to measure of liveness for this biometric. Although early iris based recognition systems required considerable user participation and were expensive, the newer systems have become more user friendly and cost effective. While iris system have a very low false acceptance rate compared to other biometric traits, the false reject rate of these systems can be rather high.

Iris

c. Voice: Voice is a combination of physical and behavioral biometric characteristics. The physical features of an individual's voice are based on the shape and size of the appendages that are used in the synthesis of the sound. These physical characteristics of human speech are invariant for an individual, but the behavioral aspect of the speech changes over time due to age, medical conditions, emotional state etc. Voice is also not very distinctive and may not be appropriate for large scale identification. A text dependent voice recognition system recognizes the speaker independent of what he speaks. a disadvantage of voice based recognition is that speech features are sensitive to a number of factors such as back ground noise. Speaker recognition is most appropriate in telephone based applications but the voice signal is typically degraded in quality by the communication channel.

Voice

d. Gait : Gait refers to the manner in which a person walks, and is one of the few biometric traits that can be used to recognize people at a distance. Therefore, this trait is very appropriate in surveillance scenarios where the identity of an individual can be surreptitiously established. Most gait recognition algorithms attempt to extract the human silhouette in order to derive the spatio temporal attributes of moving individual. Hence, the selection of good model to represent the human body is pivotal to the optic flow associated with a set of dynamically extracted moving points on the human

body to describe the gait of an individual. Gait based systems also offers the possibility of tracking an individual over an extracted period of time. However, the gait of an individual is affected by several factors including the choice of footwear, nature of clothing, affliction of legs, walking surface, etc.

Gait

5. BIOMETRICS DEFORMATIONS

Biometric system performance varies according to sample quality and the environment in which the sample is being submitted; it is possible to locate and minimize factors that can reduce/affect system performance [6]. These factors are known as Biometrics- Deformations. The Biometrics-Deformations for various traits reported in the literature are given below:

- **Fingerprint**
  - Cold finger
  - Dry/oily finger
  - High or low humidity
  - Angle of placement
  - Cuts to fingerprint
- **Voice recognition**
  - Cold or illness that affects voice
  - Different enrollment and verification capture devices
  - Different enrollment and verification environments (inside vs. outside)
  - Variation in background noise
  - Poor placement of microphone / capture device
- **Facial recognition**
  - Change in facial hair
  - Change in hairstyle
  - Lighting conditions
  - Adding/removing glasses
  - Change in weight
- **Iris-scan**
  - Too much movement of head or eye
  - Glasses
  - Colored contacts
  - Too much movement of head or eye
- **Hand geometry**
  - Jewelry
  - Change in weight
  - Swelling of joints
- **Signature-scan**
  - Marking too quickly
  - Different marking positions (e.g., sitting vs. standing)

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

6. COMPARISION OF VARIOUS BIOMETRIC TRAITS BASED ON CHARACTERISTICS

A number of biometric characteristics are being used in various applications. Each biometric has its pros and cons and, therefore, the choice of a biometric trait for a particular applications depends on a variety of issues. Seven factors were identified by jain et al. [7] that determine the suitability of a physical or a behavioral trait to be used in biometric applications. (3-High, 2- Medium, 1-Low)

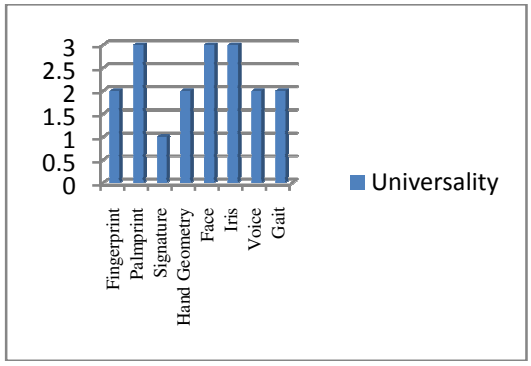

Fig. 2 – Comparison based on universality

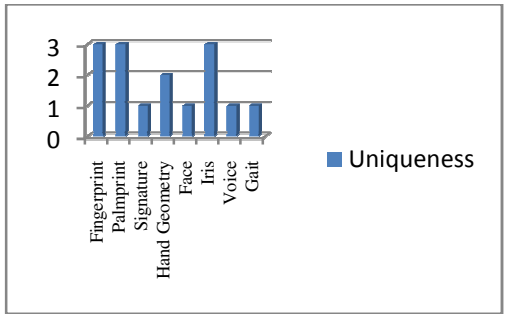

Fig. 3 : Comparison based on Uniqueness

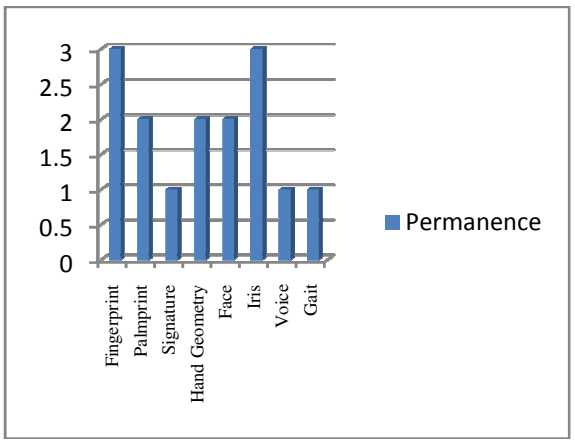

Fig. 4 : Comparison based on Permanence

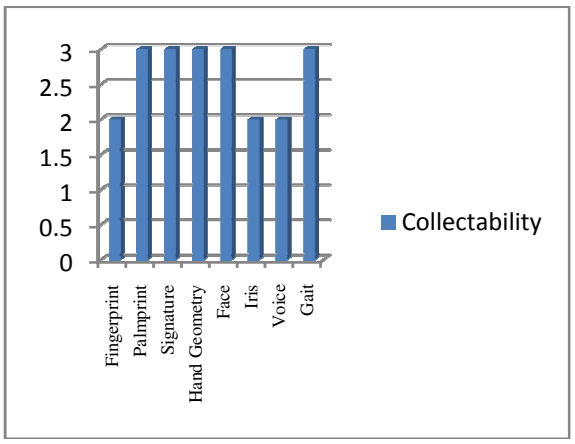

Fig. 5: Comparison based on Collectability

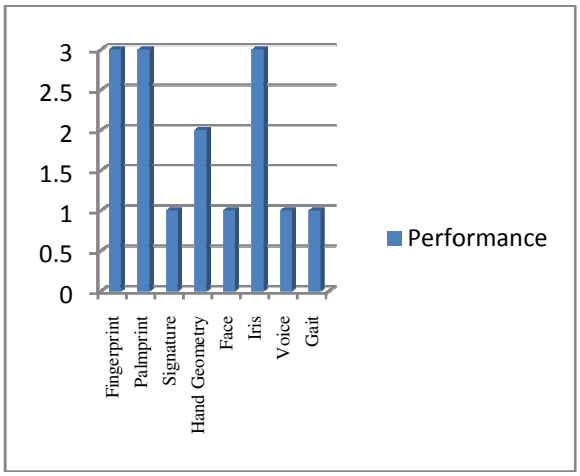

Fig. 6: Comparison based on Performance

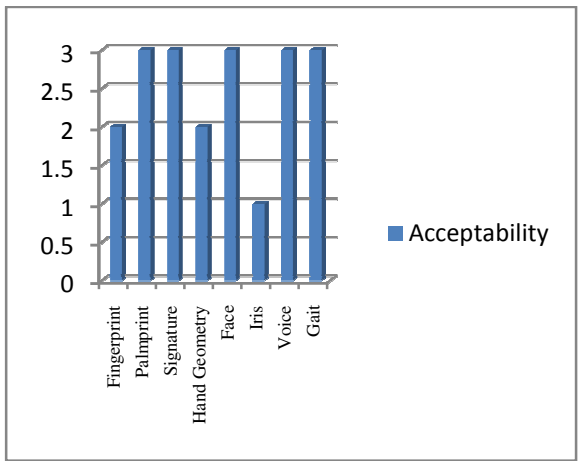

Fig. 7: Comparison based on Acceptability

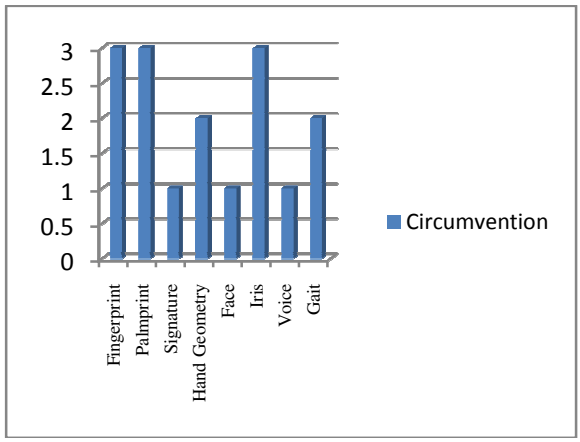

Fig. 8: Comparison based on Circumvention

7. CONCLUSION

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

REFERENCES

[1]. Anil K. Jain Michigan State University, E. Lansing, Michigan and Ruud Bolle and Sharath Pankanti IBM, T.J. Watson Research Center Yorktown Heights, New York Kluwer Academic,"Biometrics Personal Identification in Networked Society",2002 Kluwer

Academic Publishers New York, Boston, Dordrecht, London, Moscow.

[2]. Anil K. Jain, Michigan State University, USA, Patrick Flynn University of notre Dame, USA, Arun A. Ross West Virginia University, Usa, "Handbook of Biometrics", 2008.

[3]. R. Clarke, "Human identification in information system: Management challenges and public policy issues," Information Technology & People, Vol. 7, No. 4, pp. 6-37, 1994.

[4]. "An Introduction to Biometrics", White Paper by Motorola, 2006.

[5]. Anil K. Jain, Arun A. Ross, "Introduction to Biometrics", Handbook of Biometrics, Springer, New York, USA, 2008

[6]. D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. New York: Springer-Verlag, 2003.

[7]. A.K. Jain, editors, "Biometrics: personal identification in Networked Security" Kiuwer Academic Publishers,1999.