Volume 8, Issue 6
December 2019

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

A Study on Different Biometric Techniques

[1]Kanimozhi and [2]Dr. K. Thangadurai

[1] PG and Research Department of Computer Science, Ph.D research Scholar, Govt. Arts College, Karur

[2]PG and Research Department of Computer Science, Assistant Professor & Head, Govt. Arts College, Karur

E-mail: [1]Kani.cs91@ gmail.com, [2] ktramprasad05@gmail.com

ABSTRACT

Biometrics is the study of recognizing humans by their unique physical characteristics. The human physical characteristics like fingerprints, face, hand geometry, voice, Signature, palm and iris are known as biometrics. These features are used to provide an authentication for computer based security systems. The existing computer security systems used at various places like banking, passport, credit cards, smart cards, PIN , access control and network security are using username and passwords for person identification. Biometric systems also introduce an aspect of user convenience. For example, they insist the need for a user to remember multiple passwords associated with different applications. A biometric system that uses a single biometric trait for recognition has to contend with problems related to non-universality of the trait, spoof attacks, limited degrees of freedom, large intra-class variability, and noisy data. Some of these problems can be addressed by integrating the evidence presented by multiple biometric traits of a user (e.g., face and iris). Such systems, known as multimodal biometric systems, In this paper, the main focus is on the various biometrics Techniques, their Types applications and the biometrics recognition systems.

Keywords: *Biometrics authentication; Biometrics identification and recognition; false reject rate; false accept rate.*

1. INTRODUCTION

Biometrics is the science and technology of measuring and analyzing biological data. In information technology, biometrics refers to technologies that measure and analyze human body characteristics, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes.

1.1. Physical biometrics

These involve some form of physical measurement and include modalities such as face, fingerprints, iris-scans, hand geometry etc.

1.2. Behavioural biometrics

These are usually temporal in nature and involve measuring the way in which a user performs certain tasks. This includes modalities such as speech, signature, gait, keystroke dynamics etc.

1.3. Chemical biometrics

This is still a nascent field and involves measuring chemical cues such as order and the chemical composition of human perspiration. A number of biometric identifiers are in use in various applications. Each biometric has its strengths and weaknesses and the choice typically depends on the application.

2. TAXONOMY OF BIOMETRICS

According to biometrics applications and technologies, we can mainly classify biometrics systems into the following two categories:

2.1. Application Type

As the general knowledge, biometrics technology is basically applied to security services infect, a few other applications using biometrics are also very effective based on a summary of different applications, and biometrics system can be divided into four categories.

2.1.1. Personal Authentication

more efficient algorithm. Though GA has been extensively We may use biometrics technology to identify individual since this is popular biometrics application.

2.1.2 .Medical Diagnosis

Tongue, color of face beat of heart and other aspects of our body can be also used as biometrics features for medical diagnosis. Traditional chine's medicine (TCM) particularly needs to measure such kind of body characteristics.

2.1.3 .Future Expectation

Egypt and china have some specialists on this biometrics application. by looking at one's palm, the specialists can tell the personality as well as the future direction of a person.

2.1.4 .Technology exploration

Measuring body characteristics can also used to decide one's ethic .we may use this biometrics technology to monitor the population shifting among different areas.

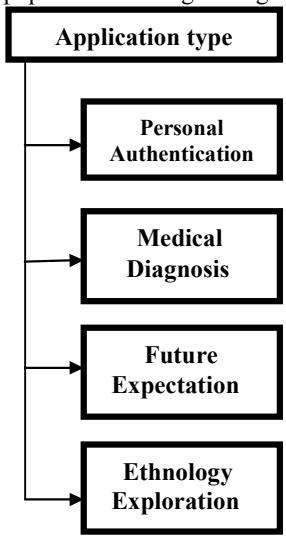

Figure 1. [Taxonomy by Application Type]

2.2. Technology Type

In terms of technology, systems are categorized in terms of

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

the employed physical or behavioral characteristics type, biometrics system are categorized in terms of the employed physical or behavioral characteristics. Since we will emphasize on the application of personal authentication.

No single biometric is expected to effectively meet the requirements of all the applications. The match between a biometric and an application is determined depending upon the characteristics of the application and the properties of the biometric. These various biometric identifiers mentioned above are compared in table below fingerprint recognition has a very good balance of all the desirable properties.

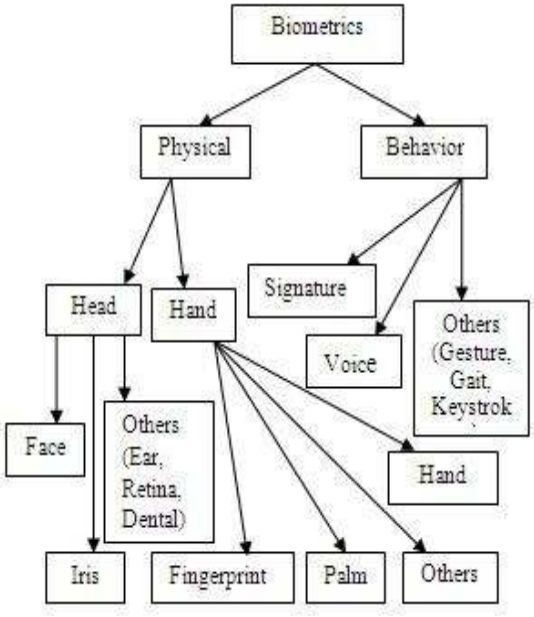

Figure.2.[Taxonomy by Technology Type.]

2.2.1. Face

Facial features are the most normal feature used by human to recognize one another. Face recognition is based on both the shape and location of the eyes, eyebrows, nose, lips, and chin or on the overall analysis of the face image that represent a face as a number of recognized faces. In a face recognition system, it is hard to match face images taken from two different views and under different illumination conditions. Moreover the face of individual can be changed by times. All this criteria make face recognition system to be uncertain if really the face itself is enough to recognize a person from a large number of identities[9].

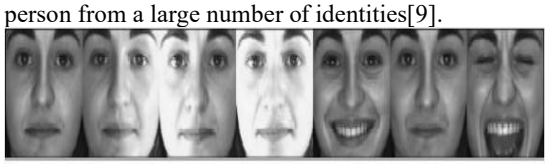

Figure 3. [Facial image variations under different emotions]

2.2.2. Hand Geometry

This method is simple, easy and inexpensive. It has been established in many locations in the world. Hand geometry recognition systems are based on a number of the measurements taken from the human hand. It measures the shape of hand, the size of palm, and the lengths and widths of the fingers. Many environmental or anomalies factors don't affect any change in the accuracy of this recognition system. However this system can't be generalized to recognize from a large number of population. In addition the geometry of the hand is not constant; it can be changed in proportion of the age. Moreover the size of the hand is big and it is not currently in wide deployment for computer security applications primarily because it requires a large scanner [2].

Figure 4. [Commercial three-dimensional scanner]

2.2.3. Iris

Iris recognition is based on the features that exist in the colored tissue surrounding the pupil which has many interesting points that can be used for comparison, including rings, rows and spots [10]. The texture of the iris is very complex and distinctive which is very useful for the recognition system. Even the irises of identical twins are different. Although based on this complexity and this distinctness, the system is more accurately deployed and supports the probability of extensive identification systems [5].

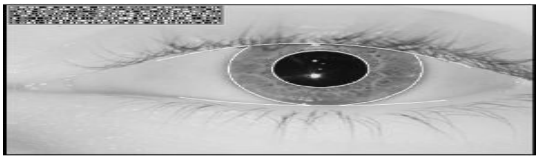

Figure 5.[Example of an iris pattern.]

2.2.4. Keystroke

The way and the manner of typing on computer keyboard vary from individual to individual. This biometric is not considered as unique but it can be sufficient for some applications. Identification of this behavioral biometrics is basically what a person types is less important than how he types it. Using this approach several things can be analyzed: time between key-pressed and key-released, type of keyboard used or the emotional and physical state of the person. So no special hardware is required for keystroke analysis, just the usual computer keyboard.

2.2.5. Signature

Signature is the way a person signs his name. Depending on this sign, the individual can be identified. Signature recognition examines the unique way in which the signature is written. In the signature recognition system, the signature is compared by examining how the signature was written or it is verified by estimating how the signature was created. Sometimes, this type of biometric can be changed over time. The same person can sign in different way. In addition, it is affected by physical conditions such as sickness or sentimental condition such as individual's feeling.

Figure 6. [Signature biometrics]

Volume 8, Issue 6
December 2019

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

2.2.6. Voice

Voice recognition is the identification of a person based on unique characteristic on their voice. Voice characteristic is the combination between physical and behavioral biometric. For the physical part of view, voice is constant because it depends on the size or shape of the mouth, lips, vocal tracts and nasal cavities and so on. However for the behavioral part, voice is not constant. It can be changed based on individual's emotion, sickness or age. Due to this behavioral effect, voice recognition system can't not be considered as a distinctive biometric [8].

Figure 7. [Voice Print]

2.2.7. Gait

Gait recognition is a particular type of biometric due to its capability to identify a person at distance. Gait is related to the way of the person walking. The gait recognition system use standard camera in any conditions and develop algorithms to extract the silhouette of the person in case he is moving. Therefore the system can track the person over time. However the algorithm is not very efficient for this trait is affected by many conditions such as the type of cloth's or shoes the individual's wearing, the walking surface or the health. All these biometrics are acceptable in different environment and none of them is optimal. However the most accurate ones are iris and fingerprint techniques. Due to the fact iris recognition is expensive and it requires advance requirement, fingerprint is one of the most mature biometrics and suitable for many applications [1]. Fingerprint biometrics is very distinctive, not expensive, unique and permanent and has a very good balance from all the properties.

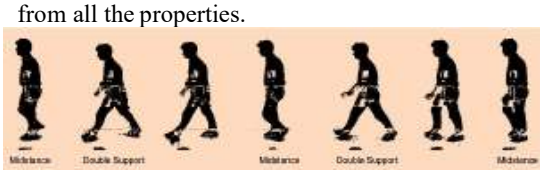

Figure 8.[Samples recorded from a gait cycle.]

2.2.8. Finger Print

Fingerprint recognition system is the oldest recognition system among all the biometrics techniques. Everyone have a unique and unchangeable fingerprint. Like iris, fingerprints of the twins are even different. Based on this uniqueness and distinctness, fingerprint identification is used in many applications for a long period. A fingerprint is the pattern of ridges and valleys on the surface of the finger. It can be changeable only by some environmental and job-related factors such as cuts or injuries on the finger. These factors cause to be the system unsuitable in some degree. Generally the accuracy of the fingerprint recognition is sufficient in many applications especially in Forensics. To allow great identification systems for a large number of identities, the systems require having a multiple fingerprint

from the same person to give additional information [6].

Figure 9. [Fingerprint sensors]

3. ENROLLMENT AND RECOGNITION PHASE

3.1. Biometric Enrollment Phase

In this Phase the user is captured and the extracted features templates are stored in the database. In authentication the biometrics of the user is captured again and the extracted features are compared with the ones already existing in the database to determine a match. The specific record to fetch from the database is determined using the claimed identity of the user. The database itself may be central or distributed with each user carrying his template on a smart card.

Biometrics is the science of verifying the identity of an individual through physiological measurements or behavioral traits. Since biometric identifiers are associated permanently with the user they are more reliable than token or knowledge based authentication methods. Biometrics offers several advantages over traditional security measures [4]. These includes

- Non-repudiation
- Accuracy and Security
- Screening

3.1.1. Non-repudiation

With token and password based approaches, the perpetrator can always deny committing the crime pleading that his/her password or ID was stolen or compromised even when confronted with an electronic audit trail. There is no way in which his claim can be verified effectively. This is known as the problem of deniability or of 'repudiation'. However, biometrics is indefinitely associated with a user and hence it cannot be lent or stolen making such repudiation infeasible.

3.1.2. Accuracy and Security

Password based systems are prone to dictionary and brute force attacks. Furthermore, such systems are as vulnerable as their weakest password. On the other hand, biometric authentication requires the physical presence of the user and therefore cannot be circumvented through a dictionary or brute force style attack. Biometrics has also been shown to possess a higher bit strength compared to password based systems and is therefore inherently secure.

3.1.3. Screening

In screening applications, we are interested in preventing the users from assuming multiple identities e.g. a terrorist using multiple passports to enter a foreign country. This requires that we ensure a person has not already enrolled under another assumed identity before adding his new record into the database. Such screening is not possible using traditional authentication mechanisms and biometrics provides the only available solution.

3.2. Biometric Recognition Phase

The Biometric Recognition Systems are used to identify the person based on the feature vectors of any one of the biometric that the person possesses [7]. These systems are person authorized systems hence offer more secure and convenient

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

process of identification compared to alternative methods of identification. The biometric System uses the individual's physical characteristics like fingerprint, hand geometry, face, voice or iris. They are more reliable and secure as they provides the access to authorized users in their physical presence [3].

4. CHARACTERISTICS OF BIOMETRIC SYSTEMS

Every biometric characteristic require satisfying the following properties:

- **Universality:** The characteristic should be encountered in each person.
- **Uniqueness:** The characteristic should be unique between individuals.
- **Permanence:** The characteristic should be sufficiently constant over long time.
- **Collect ability:** The characteristic can be measured from a quantity point of view.
- **Performance:** The characteristic give an accurate result under different environment.
- **Acceptability:** The entire people accept to give their traits to the system without any Problem.
- **Circumvention:** The characteristic must be hard to deceive and imitate.

5. APPLICATIONS OF BIOMETRIC SYSTEMS

In the last years has considerably increased the area of application of biometrics and it's expected that in the near future, we will use biometry many times in our daily activities such as getting in the car, opening the door of our house, accessing to our bank account, shopping by internet, accessing to our PDA, Mobil phone, laptops, etc. Depending on where the biometrics is deployed, the applications can be categorized in the following five main groups:

- Forensic
- Government
- Commercial
- Health-care and
- Traveling and immigration.

However, some applications are common to these groups such as physical access, PC/network access, time and attendance, etc.

CONCLUSION

Biometric recognition, or biometrics, refers to the automatic identification of a person based on his/her anatomical (e.g., fingerprint, iris) or behavioral (e.g., signature) characteristics or traits. This method of identification offers several advantages over traditional methods involving ID cards (tokens) or PIN numbers (passwords) for various reasons: (i) the person to be identified is required to be physically present at the point-of-identification; (ii) identification based on biometric techniques obviates the need to remember a password or carry a token.

With the increased integration of computers and Internet into our everyday lives, it is necessary to protect sensitive and personal data. By replacing PINs (or using biometrics in addition to PINs), biometric techniques can potentially prevent unauthorized access to ATMs, cellular phones, laptops, and computer networks. The biometric features can be easily acquired and measured for the processing only in the presence of a person. Hence these systems are proved highly confidential computer based security systems.

REFERENCES

[1] Boulgouris, N. H. (2005). recognition: a challenging signal processing technology for biometric identification. *IEEE Signal Processing Magazine* , 22, 78-90.

[2] F.A. Afsar, M. A. (2004). Fingerprint Identification and Verification System using Minutiae Matching. National Conferenceon Emerging Technologies.

[3] Jain, A. H. (1997). An identity authenticationsystem using fingerprints. *IEEE* , 1365–1388.

[4] JeroenKeuning, T. v. (2000). "Biometrical Fingerprint Recognition . *Fourth Working Conference on Smart Card Research and Advanced Applications*, (pp. pp 289-303).

[5] John Carter, M. N. An Integrated Biometric Database. Southanpton.

[6] K. Karu, A. J. (1996). *Fingerprint classification, Pattern Recognition.*

[7] K.V.Kale, R. V. (2003). *fingerprint image enhancement using composite technique.* Prapti Deshmukhf.

[8] L. Rabiner, B. H. (1996). *Fundamentals of Speech Recognition.* Pearson EducatioN.

[9] Rafael C. Gonzalez, R. E. (2004). *Digital Image Processing using MATLAB.* Pearson Education.

[10] Sulochana Sonkamble, D. R. (2008). An Effective Machine-Vision System for Information Security and Privacy using Iris Biometrics.