Volume 5, Issue 7, July 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey of Biometric Techniques

B. Lavanya*, Dr. H. Hannah Inbarani
Department of Computer Science, Periyar University,
Salem,Tamilnadu, India

Abstract— Biometrics is becoming very essential in computer security world. Biometrics refers to an automated system that can identify a person by measuring their physical and behavioral uniqueness or patterns, and comparing it. By using biometric techniques a person can be identified/verified based on "who she/he is" rather than "what she/he has" (card, token, key) or "what she/he/ knows" (password, PIN). In this paper, present a review of biometric standards, both unique and multi model, and their advantages and disadvantages will be presented.

Keywords— Biometrics, Multibiometrics, Identification, Recognition, Fusion,

I. INTRODUCTION

The word biometric appears the Greek words "bios (life)" and "metrics (measure)" [1]. The biometric is well known that humans intuitively use somebody, the component such as eye, gait and voice to recognize each other. Biometrics is an automated method of verifying the identity of a person or identifying a person based on behavioral and physiological characteristics. Examples of behavioral characteristics are learned or acquired from their traits. Dynamic signature verification, keystroke dynamics and speaker verifications are examples of behavioral characteristics. Physiological characteristics include hand or finger recognition, facial characteristics, and iris recognition.
The bit of work is prepared as follows; Section two briefly described biometric technologies discussed in standards, types of biometrics and their advantages and disadvantages. Next section explained their performance of biometrics. Finally Multi Biometrics section describes the system's advantages and disadvantages.

1.1 Biometric Systems

A system recognizes a" verification" (authentication) system or an "identification" system, which are defined below [2] [5].
Verification - One to One: Biometrics can also be used to authenticate a person's identity. For example, one can grant physical access to a secured area in a building by using finger scans or can grant access to an access to a bank account at an ATM by using retinal scan.
Identification - One to Many: Biometrics can be used to find out a person's identity even without his knowledge or permission. For example, scanning a crowd with a camera and using face recognition technology one can determine matches against a known database.

II. BIOMETRIC TECHNOLOGIES

The Biometric technologies describe four Biometric operational stages of uni-model recognition system [1]. Figure.1. gives the generic structure of biometric recognition system. The systems are

- Image Acquisition- It is the first step of image processing. Image acquisition is creation of digital image.
- Image Evaluation and Feature Extraction
- Corresponding Scores Creation – analyzed image is then compared with what images are really saved in database.
- Enrollment- initial scan of a trait by a biometric reader, create its digital representation and form a template, even a few in the majority of the systems.

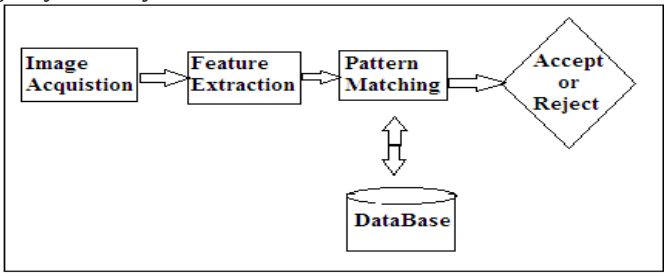

Fig.1. Biometric recognition system

2.1 Biometric Standards

The biometric standards are shown below [1] [5],

- Universality-Properties should be available from as many individuals as possible
- Uniqueness-must be distinguished when compared to others
- Permanence-biometric features that remain constant over time
- Collectability-data gathering techniques must be as simple as possible

Other important aspects to consider in a practical biometric system

- Performance- accuracy, speed and robustness of technology
- Acceptability/user Friendliness- ease of use
- Circumvention-how easy it is to cheat the system

2.2 Types of Biometrics

There are number of biometric methods in use (few commercial, few "not yet") and an overview of various biometric characteristics will be given in fig. 2 which shows the various types of biometrics[2]. Each technology used in our day to day life brings us in a manner to limit the access to a system, allowing the entrance only to those persons who know a specific code, have determined physic marks or own card. Table 1 provides the features of the biometric techniques, advantages and disadvantages. Biometrics is distinct, measurable features of an individual (e.g., facial features, fingerprints, gaits, ear, etc.) that can be utilized to discern their identity. Biometric types are shown below.

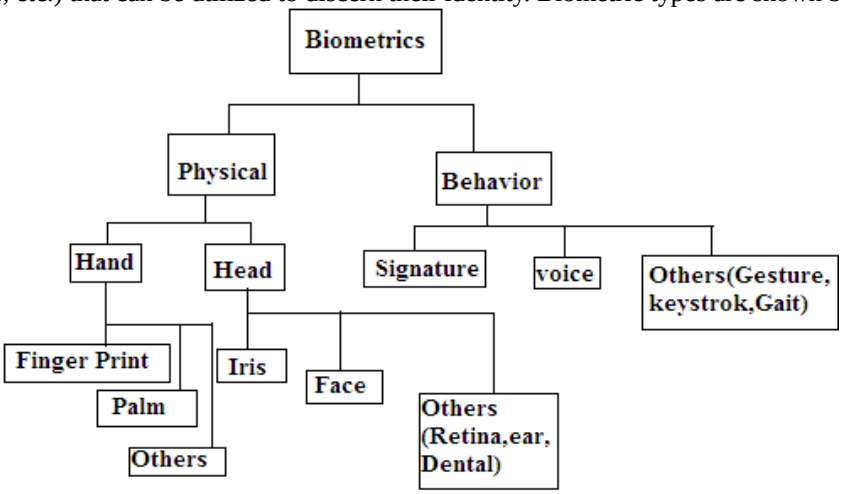

Fig. 2. Types of Biometrics

A. Fingerprint: Fingerprint biometrics is very closely related to hand geometry. Humans have used fingerprints for own identification for matching accuracy. So using fingerprint has been shown to be very high [1] [4].

B. Iris: Iris is a separate; it is a unique ring shaped colored area around the pupil and sclera (white of the eye). It is the angular region of the eye [4].

C. Keystroke: keystroke dynamics is the development by analyzing the way a user types at a terminal by monitoring the keyboard inputs thousands of times per second in an attempt to identify users based on typing patterns. It is considered that each person types on a keyboard in a characteristic way [1].

D. Palm print: palm has unique characteristics to be used in personal identification. The Human's hand contains a pattern of ridges and valleys like the fingerprint.

E. Retinal scan: The retinal vasculature is rich in structure and is hypothesized to be a characteristic of the individual [l] [2].

F. Signature: The way a person signs his/her name is known to be a characteristic of those individuals. It is a special case of handwriting which includes special characters and flourishes [4] [1].

G. DNA: Deoxyribo Nucleic Acid is the one dimensional ultimate, unique code for one's individually except for the fact that identical twins have identical DNA patterns [9].

H. EAR: Ear has been recommended that the shape and structure of cartilegenous tissue of the pinna are distinctive [9].

I. Face: Face Recognition is a non intrusive technique. Face images are most likely the most common biometric characteristic used by humans to make a personal recognition [8].

J. Voice: Voice recognition is a combination of physiological and behavioral biometrics. Voice signal recognition consists of the process to translate a speech waveform. The feature of an individual's based on the shape and size [9].

K. Gait: Gait means how the people walk. It is the pattern of movement of limbs of animals, humans during locomotion over a solid substrate. Pattern includes overall force, kinetic and potential energy, velocity and changes in the contact with the surface. Gait recognition also takes into account the gender of the person because there is a difference in the way of walking [2].

Table 1 List Of Features, Advantages And Disadvantages Of Biometric Characteristics

Biometric characteristic	**Description of the features**	**Advantages**	**Disadvantages**
Fingerprint[4]	Finger lines, pore structure	1.It is the most developed method till now 2.Relatively inexpensive 3.Even twins have unique fingerprint patterns show highly secure 4.Small template size so matching is also fast	1.Systems can be cheated by having an artificial finger like finger made up of wax 2.Cuts, scars can produce obstacle for recognition
Signature (dynamic)[4][1]	Writing with pressure and speed differentials	1.Highly socially accepted 2.Cheap hardware 3.Low total error 4.Low storage required	1. Professional forgers may able to reproduce signatures. 2.From time to time person's style of signature changes 3.Changes based on emotional and medical condition of the person
Facial geometry[9]	specific facial features like eyes, nose, mouth	1.Totally non intrusive 2.Easy to store templates 3.Socially accepted	1.Facial traits vary over time 2. Uniqueness are not maintained ex. In case of twins 3.Not proper recognition if person has different expressions like slight smiling can affect recognition 4.Highly dependent on lightning
Iris[9][4]	Iris pattern	1.Highly accurate.1 chances in 1078 that iris pattern of two individual matches 2.Highly scalable as the iris structure remains same throughout the lifetime 3.Small template size so fast matching	1.Iris scanners are relatively expensive 2.Scanners can be fooled by high quality image 3.Require cooperation from the user 4.Uses iris scanners to control access to their data centers
Retina[2][9]	Eye background (pattern of the vein structure)	1.Retinal scan cannot be forged 2.The error rate is 1 out of 10,000,000 (almost 0%) 3.Highly reliable	1.Reveals some medical conditions (e.g. Hypertension), which causes privacy issues 2.It is intrusive, so not user friendly 3.Measurement accuracy can be affected by a disease such as cataracts [2]
Hand geometry[4]	Measurement of fingers, vein structure and palm	1.High reliability and accuracy 2.Robust, user friendly 3.Environmental factors, such as, dry weather that causes the drying of the skin is not an issue	1.The hand geometry is not unique and cannot be used in identification 2.systems Not ideal for growing children 3.Jewelry (rings, etc.), limited dexterity (arthritis, etc.) etc may pose a challenge

Ear form[9]	Dimensions of the ear	1.Passive, easily captured 2.The shape does not change due to emotion 3.Smaller size	Affected by appearance
Voice[4]	Tone or timbre	1.Reliable 2.Inexpensive 3.Easy to use and no special instructions required	1.Affected by noisy environment 2.Very large database 3.Changes if person suffering from cold 4.Depend on the emotional condition of individuals
DNA	DNA code as the carrier of human hereditary	1.It is a highly unique feature 2.Performance is high 3.Its universality is very high	1.More informative so privacy issues 2.More storage required 3.Not automatic technique
Gait[2]	The person there is a difference in the way of walking of males and females	1.Details can be captured from a distance 2.Difficult to conceal 3.Can be extracted without the user knowing	1.Time to time it persons walking style changes 2.Not necessarily unique
Keyboard strokes[9]	Rhythm of keyboard strokes (PC or other keyboard)	1.Accept keyboard no additional hardware required 2.Simple to deploy 3.No end user training required 4.Cost effective	1.Dynamic changes in timing pattern 2.Injury 3.Changes in keyboard hardware

III. PERFORMANCE

Biometrics brings together and evaluates varying types of biometric related data to help to achieve various business objectives for performance. The performance metrics for biometric system as follows [5].

A. False Accept Rate or False Match Rate (FAR or FMR): The possibility that the system mistakenly matches the input pattern to non matching template in the database [1] [5].

B. False Reject Rate or False Non-match Rate (FRR or FNMR): The possibility that the system fails to discover a match between the input pattern and matching template in database [1] [5].

C. Receiver Operating Characteristic (ROC): The ROC scheme is a illustrate the characterization of the tradeoff between the FAR and the FRR.

D. Equal Error rate or Crossover Error Rate (EER or CER): The rates at which equally accept and reject errors are equal. The value of the EER can be simply obtained from the ROC curve [1] [5].

E. Failure to Enroll Rate (FTE or FER): The rate at which attempts to create a template from an input is failed. It is mostly used for low quality inputs.

F. Failure to Capture Rate: The possibility that the system fails to detect a biometric input when currently correct.

G. Template capacity: The maximum number of sets of data which can be stored in the system.

IV. MULTIBIOMETRICS SYSTEM

The Multi biometric system performs two or more combined biometric recognition technologies. The system determines a high security because one or more identity indicators are desired from the user. This makes it much difficult for an intruder to fool the system as various fake identifiers would need to be provided at the same time. Jain et. al. illustrate at the three levels of information similar combination in a multi biometric system [1] [6][11].

- *Fusion at the feature extraction level* is believed to be the effective and harder to perform at the same time.
- *Fusion at score matching level* –combination of similarity scores provided by the biometric matcher provides higher accuracy of identification.
- *Fusion at decision level*- after each system can accomplish its own recognition; the majority is selected scheme can be used to make the final decision.

A Multi biometric system denotes the fusion of different types of information. Information's are: 1)Multi sensor used to collect the same biometric trait, 2)Multi modal are collect from the same individuals, 3) Multiple units of same biometrics, 4)Multi sample used to collect same biometric trait during the enrollment or authentication phase, 5)Multiple algorithms used for feature extraction and matching on the same biometric samples. Fig.3. shows the scenarios of multi biometric system.

Combination's advantages are [1] [3]:

- High accuracy in a short time
- Safe and accepted by its users
- High level of security against fraud

Jain et. al. emphasize the main reasons why multimodal biometrics are not usually used in civilian applications [1] [5]:

- Possible user inconvenience -when multiple identifiers need to be provided
- The Combined system can be costly - due to the need of several scanning devices.

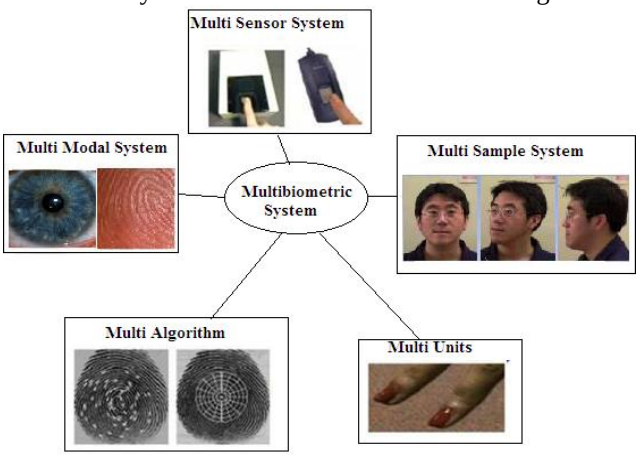

Fig. 3. Five scenarios of Multi biometric Systems

V. CONCLUSIONS

This paper presents an introduction of biometrics and techniques, undertaking the comparative study of commonly used biometric identifiers and also the identification methods. The biometric is an automated technique of identifying an individual's based on its traits. Today, biometric is playing a key role in many application areas such as forensic, military, access controls, etc. Although there are some problems with biometric systems, but it is also becoming an emerging technology in the field of security. It also discusses the multi biometrics system and their fusion levels, advantages and disadvantages. Multi biometric system can integrate information at various levels of fusion.

REFERENCES

[1] AnilK. Jain, Arun Ross and Salil Prabhakar (2004) "*An Introduction to Biometric recognition*".

[2] Ramen V.Ramen, V.yampoolskiy, "*Biometrics: a survey and classification*," Biometrics, vol. 11, no. 1, 2008.

[3] L. Hong, A. K. Jain, S. Pankanti, "*Can Multibiometrics Improve Performance?*," in Proc.AutoID'99, Summit, NJ, October 1999, pp. 59-64

[4] K P Tripathi, "*A Comparative Study of Biometric Technologies with Reference to Human*" Interface International Journal of Computer Applications (0975 – 8887) Volume 14– No.5, January 2011

[5] Kresimir Delac , Mislav Grgic," *A Survey Of Biometric Recognition Methods*" 46th International Symposium Electronics in Marine, ELMAR-2004, 16-18 June 2004, Zadar, Croatia

[6] Gursimarpreet Kaur, Dr.Chander Kant Verma,"*Comparative Analysis of Biometric Modalities* "International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 4, April 2014 ISSN: 2277 128X.

[7] Sushma Jaiswal et al., "*Biometric: Case Study*", www.jgrcs.info

[8] Ephin M et al., "Survey *On Multimodal Biometric Using Palm Print And Fingerprint*", Amrita International Conference of Women in Computing (AICWIC'13)

[9] Arun Ross, Anil K. Jain "*Human Recognition Using Biometrics: An Overview*", Springer pp. 11-35

[10] Harbi AlMahafzah , Ma'en Zaid AlRwashdeh "*A survey of multi biometric systems*" International journal of computer application, Volume 43 No15 April 2012.

[11] AnilK. Jain, Arun Ross "*Multibiometric System*" Communication of the ACM, volume 47 No 1January 2004

