Survey of Different Biometrics Techniques

Jitendra Choudhary
Asst.Prof.Computer Science &Engineering Department, IES College Bhopal, India

ABSTRACT: *Biometrics is the study of automatically recognizing humans by means of inherently unique physical or behavioural 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 alleviate 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, computer based security systems, Feature Extraction, Biometrics recognition system, false reject rate, false accept rate.

I.   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.

II.   TAXONOMY OF BIOMETRICS
According to biometrics applications and technologies, we can mainly classify biometrics systems into the following two types-

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, biometrics system can be divided into four categories.

2.2. Personal Authentication
We may use biometrics technology to identify individual since this is popular biometrics application.

2.3. 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.

2.4. 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.

2.5. 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.
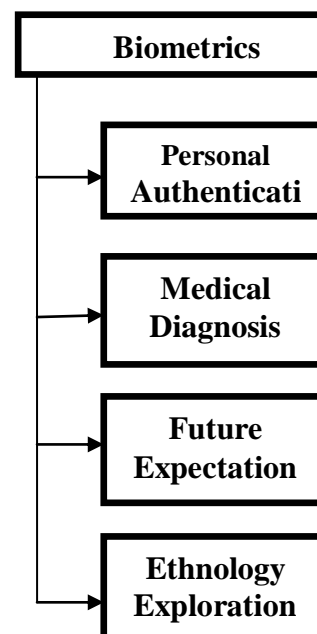

Fig. 1: Taxonomy by Application Type

III. TECHNOLOGY TYPE

System are categorized in terms of 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.
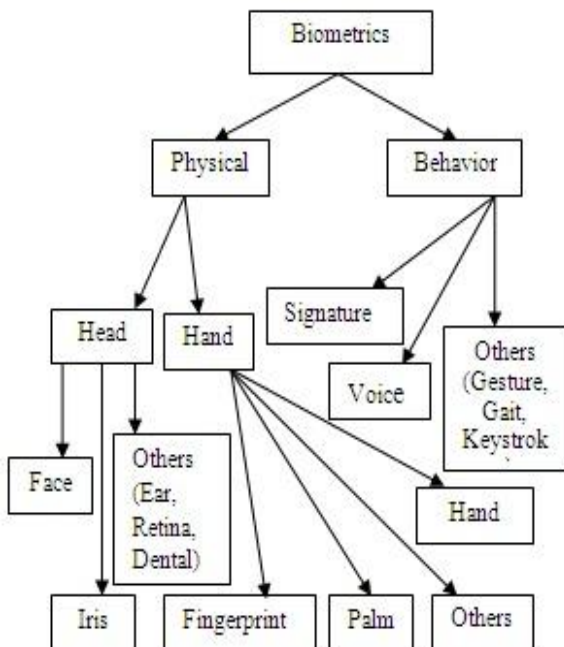

Fig.2: Taxonomy by Technology Type.

3.1. Description of the different types of biometrics

Biometrics can be physiological or behavioural. Physiological biometrics is more common and accurate than behavioural. Some of physiological biometrics, that was the most commonly used in many fields, is facial scan, iris scan, hand scan and fingerprint scan. However keystroke, signature and voice recognition are some of behavioural biometrics. A brief introduction of some of this biometrics, are described below [1].

3.2. 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 [3].

Fig.3: Facial image variations amongst the same subject

3.3. 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 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].

Fig.4: Commercial three-dimensional scanner

3.4. Iris

Iris recognition is based on the features that exist in the coloured tissue surrounding the pupil which has many interesting points that can be used for comparison, including rings, rows and spots [4]. 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 [12].
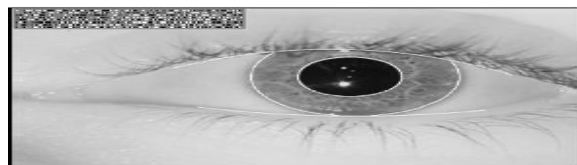

Fig.5: Example of an iris pattern.

3.5. 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 behavioural 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.

3.6. 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.

Fig .6: Signature biometrics

3.7. Voice

Voice recognition is the identification of a person based on unique characteristic on their voice. Voice characteristic is the combination between physical and behavioural 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 behavioural part, voice is not constant. It can be changed based on individual's emotion, sickness or age. Due to this behavioural effect, voice recognition system can't not be considered as a distinctive biometric [6].

Fig .7: Voiceprint

3.8. 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 [5]. Fingerprint biometrics is very distinctive, not expensive, unique and permanent and has a very good balance from all the properties.

Fig .8: Samples recorded from a gait cycle.

3.9. Fingerprint

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 [7].

Fig.9: Fingerprint sensors in everyday products.

IV. ENROLLMENT AND AUTHENTICATION

In enrollment the biometrics of 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 behavioural 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 [8]. These includes

1. Non-repudiation
2. Accuracy and Security
3. Screening

4.1. 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.

4.2. 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.

4.3. 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. The various biometric modalities can be broadly categorized as the various stages of a typical fingerprint recognition system are shown in Figure 4.3 the fingerprint image is acquired using off-line methods such as creating an inked impression on paper or through a live capture device consisting of an optical, capacitive, ultrasound or thermal sensor. The first stage consists of standard image processing algorithms such as noise removal and smoothening.
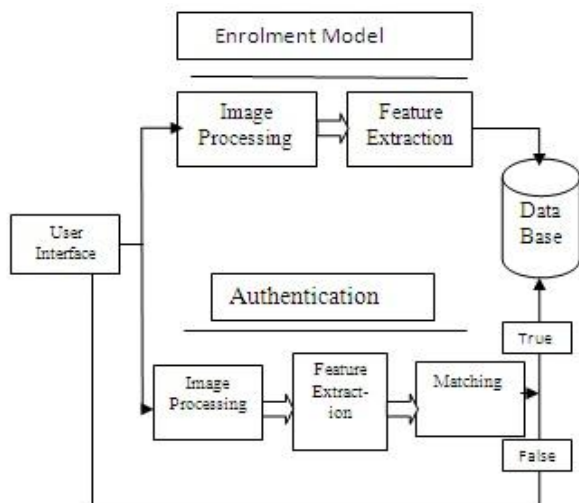

Fig.10: General processes to recognize a fingerprint

However, it is to be noted that unlike regular images, the fingerprint image represents a system of oriented texture and has very rich structural information within the image. Furthermore, the definition of noise and unwanted artifacts are also specific to fingerprints. The fingerprint image enhancement algorithms are specifically designed to exploit the periodic and directional nature of the ridges. Finally, the minutiae features are extracted from the image and are subsequently used for matching. Although research in fingerprint verification research has been pursued for several decades.

4.4. Biometrics and Pattern Recognition

As recently as a decade ago, biometrics did not exist as a separate field. It has evolved through interaction and confluence of several fields. Fingerprint recognition emerged from the application of pattern recognition to forensics. Speaker verification evolved out of the signal processing community. Face detection and recognition was largely researched by the computer vision community. While biometrics is primarily considered as application of pattern recognition techniques, it has several outstanding differences from conventional classification problems as enumerated below

1. In a conventional pattern classification problem such as optical character recognition (OCR) recognition the number of patterns to classify is small (A-Z) compared to the number of samples available for each class. However in case of biometric recognition, the number of classes is as large as the set of individuals in the database. Moreover it is very common that only a single template is registered per user.

2. The primary task in biometric recognition is that of choosing a proper feature representation. Once the features are carefully chosen, the act of performing verification is fairly straight- forward and commonly employs simple metrics such as Euclidean distance. Hence the most challenging aspects of biometric identification involve signal and image processing for feature extraction.

3. Since biometric templates represent personally identifiable information of individuals, security and privacy of the data is of particular importance unlike other applications of pattern recognition.

4. Modalities such as fingerprints, where the template is expressed as an unordered point set minutiae do not fall under the category of traditional multi-variety features commonly used in pattern recognition.

4.5. Fingerprints as a Biometric

Fingerprints were accepted formally as valid personal identifier in the early twentieth century and have since then become a defect to authentication technique in law-enforcement agencies worldwide. The federal bureau of investigation (FBI) currently maintains more than 400 million fingerprint records on file. Fingerprints have several advantages over other biometrics such as the following.

1. High universality

2. High distinctiveness

3. High permanence

4. Easy collectability

5. High performance

6. Wide acceptability

V.   BIOMETRIC RECOGNITION SYSTEM

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 [10]. These systems are person authorized systems hence offer more secure and convenient 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 [11].

5.1. Fingerprint Recognition Systems

Fingerprint recognition systems consist of the following parts
- Sensing or Image acquisition
- Pre-processing
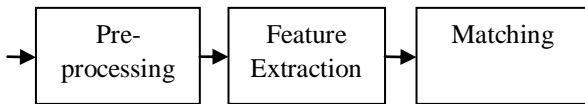- Feature or minutiae extraction
- Matching

Fig.11: Fingerprint Recognition Systems

5.2. Fingerprint matching techniques

The large number of approaches to fingerprint matching can be coarsely classified into three families.

5.2.1. Correlation-based matching

Two fingerprint images are superimposed and the correlation between corresponding pixels is computed for different alignments (e.g. various displacements and rotations).

5.2.2. Minutiae-based matching

This is the most popular and widely used technique, being the basis of the fingerprint comparison made by fingerprint examiners. Minutiae are extracted from the two fingerprints and stored as sets of points in the two- dimensional plane. Minutiae-based matching essentially consists of finding the alignment between the template and the input minutiae sets that result in the maximum number of minutiae pairings

5.2.3. Pattern-based (or image-based) matching

Pattern based algorithms compare the basic fingerprint patterns (arch, whorl, and loop) between a previously stored template and a candidate fingerprint. This requires that the images be aligned in the same orientation. To do this, the algorithm finds a central point in the fingerprint image and centers on that. In a pattern-based algorithm, the template contains the type, size, and orientation of patterns within the aligned fingerprint image. The candidate fingerprint image is graphically compared with the template to determine the degree to which they match.

5.3. The metrics of Biometrics
- FTE – Failure To Enroll
- FTA – Failure To Accept
- FAR – False Acceptance Rates
- FRR – False Reject Rates

5.4. Essential parameters
- Livens testing
- Tamper resistance
- Secure communication
- Security Threshold level
- Fall back node

5.5. Fingerprint techniques
- Optical
- Capacitive
- Thermal
- Ultrasonic

Fig.12: Fingerprint Image

VI. BIOMETRIC CHARACTERISTIC

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.

6.1. Feature Extraction Module

In the feature extraction module, the preprocessed image voice is used to extract the features. The feature extraction algorithms are applied to get feature vector of the biometric image / voice. There are various feature extraction techniques like Independent Component Analysis, Linear discriminate component, principal component analysis, wavelet transform, LPC, MFCC, etc [13][14][15][16]. According to the biometrics selected and its application the feature extraction technique can be applied.
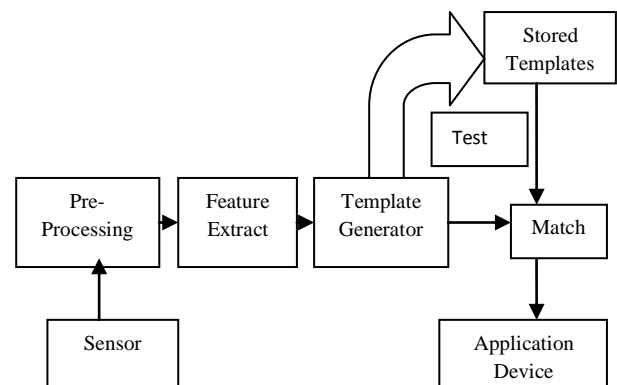

Fig.13: Biometric System

VII. APPLICATIIONS OF THE BIOMETRIC RECOGNITION SYSTEMS

Which uses the physical biological or behavioral characteristics that can be processed to perform automatic recognition of a person Hence this requires achieving low cost, reliable human identification system by using feature set of individual characteristics. The biometric concentrates on physical aspects like finger print, hand geometry, face, voice and iris of a person [12].

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 of 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.

VIII.   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]   Faundez-Zanuy, M. Biometric verification by means of hand geometry.39th Annual 2005 International Carnahan Conference on Security Technology, 61-67(2005).

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

[3]   Rafael C. Gonzalez, Richard E Woods and Steven L Eddins "Digital Image Processing using MATLAB", Pearson Education, 2004.

[4]   Sulochana Sonkamble, Dr. R.C. Thool, Balwant Sonkamble, "An Effective Machine-Vision System for Information Security and Privacy using Iris Biometrics", in The 12th World Multi-Conference on Systemics, Cybernetics and Informatics: WMSCI 2008 at Orlando, Florida, USA during June 29th - July 2nd , 2008.

[5]   Boulgouris, N.V., Hatzinakos, D., &Plataniotis, K.N. Gait recognition: a challenging signal processing technology for biometric identification. IEEE Signal Processing Magazine, 22, 78-90(2005).

[6]   L. Rabiner, B. H. Juang, "Fundamentals of Speech Recognition", Pearson Education.

[7]   K. Karu, A.K. Jain, "Fingerprint classification, Pattern Recognition", 1996.

[8]   Ton van der Putte and JeroenKeuning "Biometrical Fingerprint Recognition", Fourth Working Conference on Smart Card Research and Advanced Applications, pp 289-303, 2000.

[9]   F.A. Afsar, M. Arif and M. Hussain, "Fingerprint Identification and Verification System using Minutiae Matching", National Conferenceon Emerging Technologies, 2004.

[10] K.V.Kale, R.R.Manza, V.T.Humbe, Prapti Deshmukh" fingerprint image enhancement using composite technique"f-14-14/2003(SR).

[11] Jain, A., Hong, L., Pankanti, S., and Bolle, R. An identity authenticationsystem using fingerprints. In Proceedings of the IEEE (September1997), vol. 85, pp. 1365–1388.

[12] John Carter, Mark Nixon, "An Integrated Biometric Database" Department of Electronics and Computer Science, University of Southampton, Highfield, Southanpton, SO95NH.

[13] Peng Wang; Qiang Ji; Wayman, J.L., "Modeling and Predicting Face Recognition System Performance Based on Analysis of Similarity Scores", Pattern Analysis and Machine Intelligence, IEEE Transactions on Volume 29, Issue 4, April 2007.

[14] Steve Lawrence C. Lee Giles Ah Chung Tsoi, Andrew D. Back, "Face Recognition: A Convolutional Neural Network Approach", IEEE Transactions on Neural Networks, Special Issue on Neural Networks and Pattern Recognition.

[15] Wei Han, Cheong- Fat Chan, Chiu Sing Choy and Kong Pang Pun, "An Efficient MFCC Extraction Method in Speech Recognition", IEEE 2006.

[16] John Daugman, "How Iris Recognition Works", ieee transactions on circuits and systems for video technology, vol. 14, no. 1, january 2004.