Volume 4, Issue 4, April 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Comparative Analysis of Biometric Modalities

Gursimarpreet Kaur, Dr.Chander Kant Verma
Department of Computer Science and Application
Kurukshetra University Kurukshetra, India

Abstract: With the increasing concern for security, biometrics has become an inevitable tool. Biometrics is the science and technology of recognizing individuals based on physiological, behavioral or morphological characteristics. This includes fingerprint, face, gait, iris, hand geometry, signature etc. By using biometric techniques it is possible to establish one's identity. Nowadays biometrics is being successfully implemented in many fields like forensic, security, identification and authorization systems. Brief overview of biometrics is presented. Various biometric modalities are compared based on different perspectives. Feature sets of these modalities are also described.

Keywords: biometrics, identification, verification, modalities.

I. INTRODUCTION

In this fast changing world of global data communication, security has become an issue. The need to secure information, services, and systems has increased. Conventional methods of authentications are knowledge based like passwords and PIN or object based like tokens, ID. Problem with these methods is that passwords can be cracked, ID can be stolen, and PIN can be forgotten. But biometrics overcomes all these problems because the unique information is carried by individual with itself, so it is very secure method. The key advantages of using biometrics are non-repudiation, not guessable, not transferable, not forgettable, availability. There are many traits that can be used as biometric to identify and authenticate an individual like fingerprint, gait, iris, retina, signature, vein etc. biometrics is being successfully implemented in many fields like forensic, security, identification and authorization systems. The rest of the paper is organized as follows: introductory part in section I, overview of biometric system is given in section II, working of biometric system is defined in section III, various modalities are described in section IV, comparison is done in section V, section VI includes conclusion and finally references are given.

II. OVERVIEW OF BIOMERTIC SYSTEM

The term biometric is derived from two Greek words: bios=”life”, metron=”measure” Pato et al.stated that biometric has two meanings and thus can be described as [1]:

- A characteristic(measureable biological and behavioral property of living being)
- A process (automated method of recognizing an individual by means of identification of above mentioned kinds of characteristics).

This section describes a brief overview of biometric modalities that can be classified into three main categories i.e. physical, behavioral and both physical and behavioral. There are number of modalities in these categories which can be used according to application. Functionality of biometric system is defined in terms of identification and verification.

A. Classification of biometric modalities

There are various biometric traits a human being possesses which can be used.

1) Physical modalities: This is related to the shape of the body. This includes fingerprint, iris, hand geometry, face, retina, ear shape, DNA etc. recognition system.
2) Behavioral modalities: These are related to human behavior that may change over time, like signature, typing rhythm etc.
3) Both physical and behavioral: For example voice, as a physical characteristic voice is constant because it depends on the size or shape of the mouth, lips, vocal tracts and nasal cavities etc. But for the behavioral part, voice is not constant. It can be changed based on individual's emotion, sickness or age.

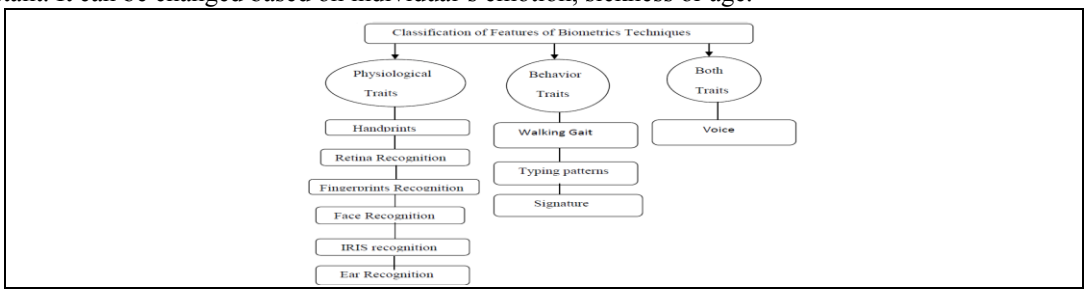

Fig. 1 Biometric Modalities

B. Functionality of biometric system

It is defined in terms of verification and identification.

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.

Identification: It refers to 1: m matching. In this situation user does not know its identity, it is simply presenting its biometrics for matching with whole database. User's template is matched with all the templates stored in database to identify with which template it has highest similarity [2].

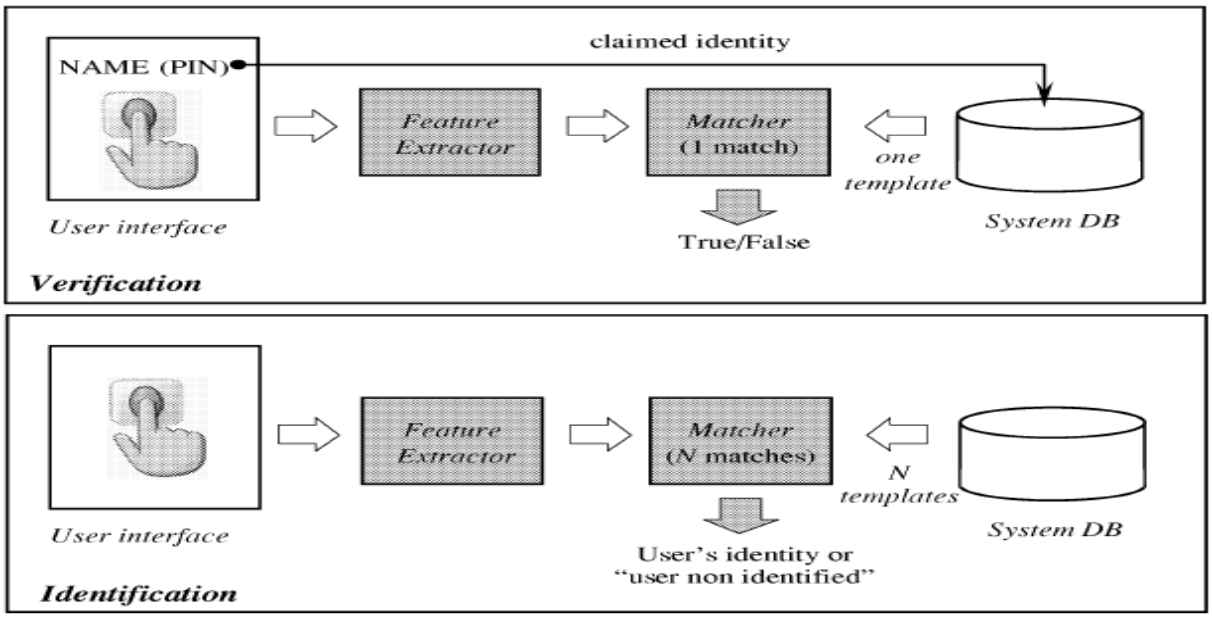

Fig. 2 Verification Vs Identification

III. WORKING OF BIOMETRIC SYSTEM

Biometric system works by going through four main modules. These include preprocessing, feature extraction, template generation and template matching.

Firstly a person enrolls to give its biometric data, which goes through preprocessing module. Preprocessing module reduces noise in data. Then feature set is extracted using various feature extraction algorithms. From these extracted features a template is generated which is stored in the database. At the time of authentication, input sample is matched with stored template in database to check whether the person is genuine or not. This section describes the working of biometric system in terms of various outputs that are produced at each level of the biometric system.

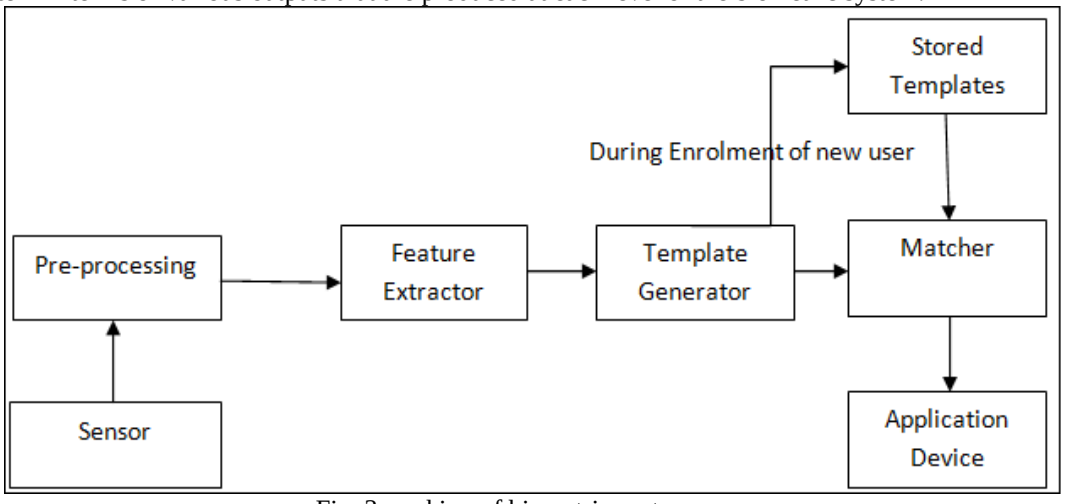

Fig. 3 working of biometric system

Enrollment: The first time user presents its biometric data. It is the process of accusation, processing and storing of biometric data. This data is further used in authentication process.

Biometric sample: The identifiable, unprocessed data presented during enrollment process is known as biometric sample. It is used to generate templates. It is also called raw biometric data. The biometric sample for various modalities is given in table I.

Table I Biometric samples of biometric modalities

Modality	**Biometric Sample**
Fingerprint	Fingerprint image
Voice recognition	Voice recording
Facial recognition	Face image
Iris scan	Iris image
Retina scan	Retina image
Hand Geometry	3D image of top and sides of hand and fingers
Signature Scan	Image of signature and record of related dynamics measurements
Gait	Dynamic measurements
Keystroke scan	Recording of characters typed and measurements

Presentation: The process of presenting the biometric data to the accusation device is called as presentation.
Accusation device: The hardware device used to collect biometric sample. List of accusation devices for various modalities are listed in table II.

Table II Accusation device for biometric modalities

Biometric modality	**Accusation Device**
Fingerprint	Sensor
Facial scan	Video camera, PC camera
Iris scan	IR enabled video camera
Hand Geometry	Proprietary wall-mounted unit
Signature-scan	Signature tablet, motion-sensitive stylus
Voice recognition	Microphone, telephone
Retina-scan	Proprietary desktop or wall-mountable unit
Keystroke-scan	Keyboard or keypad
Gait	Walking surface

Template: This is mathematical representation of biometric sample. It is used for matching. It is generated after applying certain feature extraction algorithms. The template created during enrollment phase is known as stored template while during authentication it is live template.
Feature extraction: The process by which distinct features of biometric data are located is known as feature extraction. Features extracted from various biometric modalities are listed in table III.
Matching: The process of matching live template with stored template to find degree of similarity is known as matching. A score is generated based on similarity and user is authenticated based on this score. There are many algorithms for matching process; some of the popular algorithms of various modalities are listed in table IV.

Table III Feature Extracted from biometric modalities

Modality	**Feature extracted**
Facial scan	Distance of specific facial features (eyes, nose, mouth)
Voice recognition	Words, tone
Iris scan	Texture of the iris such as freckles, coronas, strips, furrow, and crypts
Retina scan	Vessel pattern in the retina of the eye as the blood vessels at the back of the eye
Signature scan	pressure, direction, timing, acceleration and the length of the strokes
Keystroke scan	Keystroke time interval
Fingerprint	A friction Ridge curves-a raised portion, pore structure, indents and marks
Hand geometry	Estimation of length, width, thickness, shape and surface area of the hand.

Table IV Popular matching algorithms for various biometric modalities

Modality	**Popular Matching algorithm**
Fingerprint	String matching
Facial scan	Euclidian distance
Iris scan	Hamming distance
Retina scan	Silicon retina stereo matching
Hand geometry	Euclidian matching
Voice recognition	Hidden markov model

IV. BIOMETRIC MODALITIES

A. Physical modalities

1. Fingerprint recognition: A fingerprint is made up of ridges and furrows. Uniqueness is determined by ridges, furrows, 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 rings and furrows.

Fingerprint matching techniques are of three types:

a. Minutiae-based techniques: In these minutiae points are finding and then mapped to their relative position on finger. There are some difficulties like if image is of low quality it is difficult to find minutiae points correctly also it considers local position of ridges and furrows not global [4].
b. Correlation- based method: It uses richer gray scale information. It overcome problems of above method, it can work with bad quality data. But it has some of its own problems like localization of points.
c. Pattern based (image based) matching: Pattern based algorithms compare the basic fingerprint patterns (arch, whorl, and loop) between a stored template and a candidate fingerprint.

Advantages:

- It is the most developed method till now
- Relatively inexpensive
- Even twins have unique fingerprint patterns so highly secure
- Small template size so matching is also fast

Problems:

- Systems can be cheated by having artificial finger like finger made up of wax
- Cuts, scars can produce obstacle for recognition

Applications:

- Verification of driver-license authenticity and license validity check
- Law Enforcement Forensics
- Border Control/Visa Issuance

2. Face recognition: Face recognition is based on both the shape and location of the eyes, eyebrows, nose, lips and chin. It is non intrusive method and very popular also. Facial recognition is carried out in two ways [5] [6]:

a. Facial metric: In this location and shape of facial attributes (e.g. distances between pupils or from nose to lip or chin) are measured.
b. Eigen faces: Analyzing the overall face image as "a weighted combination of a number of canonical faces."

Another emerging technique is to use face recognition combining with other visual details of skin. This technique is called as skin texture analysis. The unique lines, patterns, and spots apparent in a person's skin is located. According to tests with this addition, performance in recognizing faces can increase 20 to 25 percent [8].

Advantages:

- Totally non intrusive
- Easy to store templates
- Socially accepted

Problems:

- Facial traits vary over time
- Uniqueness is not maintained ex. in case of twins
- Not proper recognition if person has different expressions like slight smiling can affect recognition
- Highly dependent on lightning

Applications:

- General identity verification
- Surveillance
- Access Control

3. Iris recognition: The iris is the elastic, pigmented, connective tissue that controls the pupil. The iris is formed in early life in a process called morphogenesis. Once fully formed, the texture is stable throughout life. It is the most correct 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. Eye color is the color of iris. Iris recognition uses camera technology with subtle infrared illumination to acquire images of the detail-rich, intricate structures of the iris [9].

Advantages:

- Highly accurate.1 chances in 10^{78} that iris pattern of two individual matches
- Highly scalable as iris structure remains same throughout lifetime
- Small template size so fast matching

Problems:

- Iris scanners are relatively expensive
- Scanners can be fooled by high quality image
- Require cooperation from user

Applications:

- All of the UAE's land, air and sea ports of entry are equipped with systems
- Adhaar card also has taken iris trait for recognition
- Google uses iris scanners to control access to their datacenters

4. Hand geometry: This recognition include Measuring length, width, thickness and surface area, overall bone structure of the hand. The fact is that a person's hand is unique and it does not change after certain age. Hand based system are of two types [7]:

a. Contact based: a hand is placed on a reader's covered flat surface. This placement is positioned by five guides or pins that correctly situate the hand for the cameras.

b. Contact-less based: In this approach neither pegs nor platform are required for hand image acquisition.

Advantages:

- High reliability and accuracy
- Robust, user friendly
- Environmental factors, such as, dry weather that causes the drying of the skin is not an issue

Problems:

- The hand geometry is not unique and cannot be used in identification systems
- Not ideal for growing children
- Jewelry (rings, etc), limited dexterity (arthritis, etc) etc may pose a challenge

Applications:

- Majority of the nuclear power plants in the US use hand recognition geometry for access control
- Used during 1996 Olympic Games
- U.S military has been using hand recognition geometry for access control

5. Retina scan: The blood vessels at the back of the eye have a unique pattern, from eye to eye and person to person. A light source is needed because retina is not visible. The infrared energy is absorbed faster by blood vessels in the retina than by the surrounding tissue. Based on this pattern of blood vessels can be easily recognized. It is required that a person remove its glasses, focus on a specific point for about 10-15 seconds. A coupler is used to read the blood vessel patterns. A coherent light source is also required for illumination [10].

Advantages:

- Retinal scan cannot be forged
- Error rate is 1 out of 10,000,000(almost 0%)
- Highly reliable

Problems:

- Reveals some medical conditions (e.g. hypertension), which causes privacy issues
- It is intrusive so not user friendly
- measurement accuracy can be affected by a disease such as cataracts[12][13]

Applications:

- utilized by several government agencies including the FBI, CIA, and NASA
- Used for medical diagnostic applications

6. DNA recognition: Human DNA is the genetic material that can be found in every single body cell of an individual. There are number of sources from which DNA patterns can be collected such as blood, saliva, nails, hair and others. The collected DNA samples are fragmented into shorter fragments which are organized by size and are then compared. Still this technology is not automated and need to be refined.

Advantages:

- It is highly unique feature
- Performance is high
- Its universality is very high

Problems:

- More informative so privacy issues
- More storage required
- Not automatic technique

Applications:

- In forensic
- Used in courts and law to prove guilt or innocence
- Physical and Network security

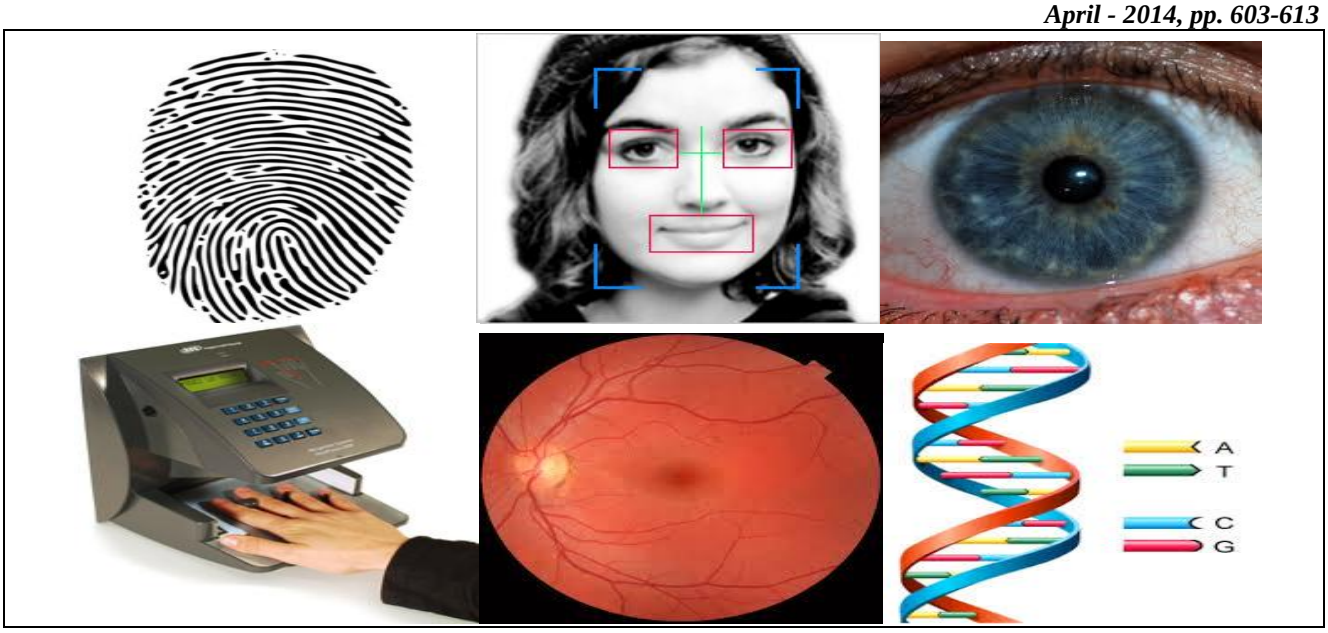

Fig. 4 Physical modalities

B. Behavioral modalities

1. **Gait recognition**: It means how the person walks. Gait is the pattern of movement of the limbs of animals, including humans, during locomotion over a solid substrate. Patterns include overall velocity, forces, kinetic and potential energy cycles, 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 [14].

Advantages:

- Details can be captured from distance
- Difficult to conceal
- Can be extracted without knowing user

Problems:

- Time to time it persons walking style changes
- Not necessarily unique

Applications:

- To detect suspicious people in sensitive areas.
- Can be used in conjunction with other biometric traits

2**. Signature**: A signature is a handwritten (and sometimes stylized) depiction of someone's name, nickname that a person writes on documents as a proof of identity. Signatures have been accepted in government, legal, and commercial transactions as a method of authentication. It is also a widely accepted method of authentication.

Advantages:

- Highly socially accepted
- Cheap hardware
- Low total error
- Low storage required

Problems:

- Professional forgers may able to reproduce signatures.
- From time to time person's style of signature changes
- Changes based on emotional and medical condition of person

Applications:

- Banking services
- contract / agreement execution

3. **Keystrokes**: It is the way a person types on keyboard. I include speed, how the buttons are pressed and released. It changes from person to person [16].

Advantages:

- Except keyboard no additional hardware required
- Simple to deploy
- No end user training required
- Cost effective

Problems:

- Dynamic changes in timing pattern
- Injury
- Changes in keyboard hardware

Applications:

- Multifactor authentication
- Very specific form of surveillance
- Passport verification system
- E-commerce applications

Fig. 5 Behavioral modalities

3. Both physical and behavioral

Voice recognition: It focuses on the vocal features that produce speech and not 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. There are three different techniques [11]:

a. Text-dependent systems: The user is requested to speak a word or phrase which was earlier during the enrollment process. It is matched with stored pattern.
b. Text-prompted systems: The user is prompted to repeat or read a word or phrase from a pre-recorded vocabulary displayed by the system (e.g., *"Please say the numbers 7 8 3 4!"*).
c. Text-independent systems: Systems have no initial knowledge /vocabulary. Reference templates are generated for different phonetic sounds of the human voice, rather than samples for certain words.

Advantages:

- Reliable
- Inexpensive
- Easy to use and no special instructions required

Problems:

- Affected by noisy environment
- Very large database
- Changes if person suffering from cold
- Depend on emotional condition of individuals

Applications:

- Robotics
- Automatic translation
- Interactive voice response

Fig. 6 Voice recognition

V. COMPARISONS

There are various biometrics methods are employed for authentication system. These vary from each other in various perspectives.

A. Based on properties

a. Universality: Most of the population should have this trait.
b. Uniqueness: Trait should be able to distinguish individuals.
c. Collectability: The ease with which the data can be captured.
d. Permanence: It should be almost constant for long run of time.
e. Performance: How well the trait performs. It includes speed, d security.
f. Acceptability: To what extent people are willing to support this.
g. Circumvention: Can this trait be cheated

Table V Comparison based on properties [17] [18]

	Universality	Uniqueness	Collectability	Permanence	Performance	Acceptability	circumvention
Fingerprint	M	H	M	M	M	H	M
Face	H	M	H	M	L	H	H
Iris	H	H	H	H	H	M	L
Hand Geometry	H	M	H	L	M	M	M
Retina	H	H	M	H	H	L	L
DNA	H	H	L	H	H	H	L
Gait	H	M	H	M	L	M	M
Signature	L	H	H	L	M	H	H
Keystroke	L	L	M	L	L	L	M
Voice	M	H	M	L	M	H	H

B. Comparison based on social point of view

Socially biometric modalities can be compared on privacy, hygiene, safety, cost, popularity, ease of use and when it was introduced.

Table VI Based on social view [18] [19] [21]

	Socially introduced	Privacy concept	Hygiene factor	Safety	Cost	Popularity	Ease of use
Fingerprint	1981	H	M	M	L	H	H
Face	2000	H	L	M	M	H	H

Iris	1995	H	L	H	H	M	M
Hand Geometry	1986	L	H	M	H	L	H
Retina	1999	L	L	H	H	L	L
DNA	1965	L	M	H	H	H	L
Signature	1970`	H	H	H	M	H	H
Keystroke	2005	L	H	L	M	L	L
Voice	1998	M	L	H	L	H	H

C. Comparison based on evaluation:

There are various techniques based on which various modalities can be compared. These include false acceptance rate, false non acceptance rate, crossover error rate, failure to enroll rate, failure to capture rate, receiver capture characteristics, sensor subject distance etc.

Table VII Based on evaluation [19] [21]

	False acceptance rate	False rejection rate	Crossover error rate	Failure to enroll rate	Failure to capture rate	receiver operating char.	Sensor subject distance
Fingerprint	2%	2%	2%	1%	-	-	30cm
Face	1%	20%	-	NA	NA	-	~20m
Iris	0.94%	0.99%	0.01%	0.5%	-	-	30cm
Hand Geometry	2%	2%	1%	NA	NA	-	10cm
Retina	0.91%	0.04%	0.8%	-	-	2cm	30cm
DNA	-	-	-	-	-	-	Zero
Signature	-	-	-	-	-	-	Zero
Keystroke	7%	0.1%	1.8%	-	-	-	Zero
Voice	2%	10%	6%	-	-	-	20cm

D. Comparison based on technical point:

Technically biometric modalities can be compared based on processing speed, accuracy, template size, devices that are used, technology used in devices and stability.

Table VIII Based on technical point of view [18] [19] [20] [21]

	Processing speed	Accuracy	Template size	Device used	Technology used in device	Stability
Fingerprint	H	M	-	Fingerprint reader	Optical, thermal, silicon, ultrasonic sensor	H
Face	M	L	3-5kb	Camera	CCD/CMOS image sensor	M
Iris	M	H	5-50kb	Camera	CCD/CMOS image sensor	M
Hand Geometry	H	M	-	CCD Camera	Laser light, IR light	M
Retina	M	H	-	Retinal scanner	Laser light, IR light	H
DNA	L	H	100kb	Lab environment	Testing in lab	H
Signature	H	M	20kb	Tablet, touch panel	Capacitive, resistive, acoustic	M
Keystroke	M	L	-	Keyboard, special software	Software based	L
Voice	H	L	-	Microphone	Converting signals	M

E. Comparison based on biometric market

Mostly face, fingerprint, iris and AFIS are used in market and hand geometry is used in lowest no of applications. The complete pie chart is shown below:

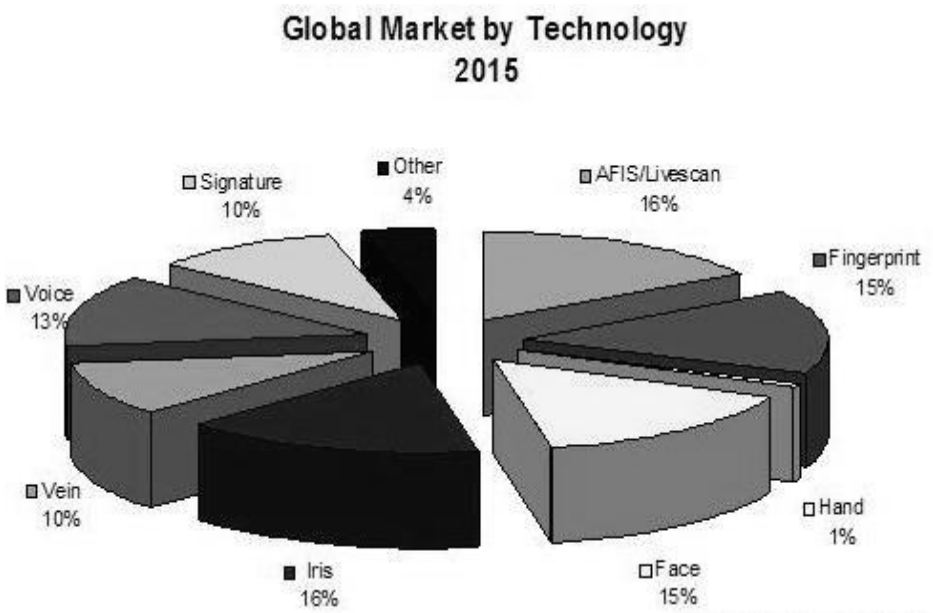

Fig. 7 Biometric market in 2015[22]

VI. CONCLUSIONS

Biometric is automated method of identifying an individual based on its biometric traits. It is highly secure as compared to conventional methods of authentications. Biometric is basically developed based on methods of pattern recognition Today biometric is playing key role in many application areas such as forensic, military, access controls, etc. In this paper various biometric modalities are defined and also these are compared based on various perspectives. Iris seems to be most accurate biometric but actual use depends on type of application. Although there are some problems with biometric systems but it is also becoming an emerging technology in the field of security.

REFERENCES

[1] Joseph N. Pato and Lynette I. Millett, Editors; whither Biometrics Committee; National Research Council (2010), "Biometric Recognition: Challenges and Opportunities".

[2] James L. Wayman, Anil K. Jain, Davide Maltoni, and Dario Maio, Biometric Systems: Technology, Design and Performance Evaluation, Springer.

[3] K P Tripathi,"Comparative Study of Biometric Technologies with Reference to Human Interface," *International Journal of Computer Applications(IJCA), vo.l 14, no.5, 2011.*

[4] Jain, A. K.; Ross, A. & Pankanti, S., "Biometrics: A Tool for Information Security," *IEEE Transactions on Information Forensics And Security*, vol. 1, no. 2, pp 125 – 144, 2006.

[5] S. Z. Li and A. K. Jain, Eds., Handbook of Face Recognition. New York: Springer Verlag, 2004.

[6] L. Hong and A. K. Jain, "Integrating faces and fingerprints for personal identification", IEEE Trans. Pattern Anal. Mach. Intell., Volume 20, No. 12, Dec. 1998, pp. 1295–1307.

[7] R. Sanchez-Reillo, C. Sanchez-Avilla, and A. Gonzalez-Macros, "Biometrics Identification Through Hand Geometry Measurements", IEEE Transactions on Pattern Anakysis and Machine Intelligence, Volume 22,Issue 18, Oct. 2000, pp. 1168-1171.

[8] Bonsor, K. "How Facial Recognition Systems Work". http://computer.howstuffworks.com/facial-recognition.htm.

[9] Sanjay R. Ganorkar, Ashok A. Ghatol, "Iris Recognition: An Emerging Biometric Technology", In Proc. of the 6th WSEAS International Conference on Signal Processing, Robotics and Automation, Greece, Feb. 2007, pp.91 – 96.

[10] C. Marin˜ o Æ M. G. Penedo Æ M. Penas Æ M. J. Carreira F. Gonzalez, "Personal authentication using digital retinal images", Journal of Pattern Analysis and Application, Springer, Volume 9, Issue 1, May. 2006, pp. 21–33.

[11] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Trans. Circuits Syst.Video Technology, Special Issue Image- and Video-Based Biomet., Volume 14, Issue 1, Jan. 2004, pp. 4–20.

[12] Hill, Robert. ―Retina Identification‖. Msu.Edu.

[13] Roberts, Chris. "Biometrics" Retrieved on 2009-06-11.

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

[15] Samir K. Bandopadhaya, Debnath Bhattacharyya, Swarnendu Mukherjee, Debashis Ganguly, Poulumi Das,"Statistical Approach for Offline Handwritten Signature Verification", Journal of Computer Science, Science Publication, Volume 4, Issues 3, May. 2008, pp. 181 – 185.

[16] S. Hocquet, J. Ramel, H. Cardot, "Fusion of Methods for Keystroke Dynamic Authentication", In Proc. of 4th IEEE Workshop on Automatic Identification Advanced Technologies, USA, Oct. 2005, pp. 224 – 229.
[17] Himanshu Srivastava, "Personal Identification Using Iris Recognition System, a Review," International Journal of Engineering Research and Applications (IJERA), vol. 3, pp. 449-453, 2013.
[18] P Tripathi, "A Comparative Study of Biometric Technologies with Reference to Human Interface," International Journal of Computer Applications (IJCA), vol. 14, no.5, 2011.
[19] Simon Llu and Mark Silverman, "A practical guide to biometric security technology," *IT Pro*, 2001.
[20] Tilo Burghardt, "A brief review of biometric identification," University of Bristol, UK.
[21] Himanshu Srivastava, "A Comparison Based Study on Biometrics for Human Recognition", IOSR Journal of Computer Engineering(IOSR-JCE),vol. 15,pp.22-29,2013.
[22] International Biometric Group, "Biometrics Market and Industry Report 2010-2015", 2010.

