Volume 4, Issue 12, December 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Analysing of Various Biometric System Predicted on Different Criteria Affected By Various Factor

[1]Ms. Meghna B. Patel*, [2]Dr. Ashok R. Patel, [3]Dr. N. J. Patel
[1]Asst. Professor, MCA, U.V.Patel College of Engineering,Ganpat University, Kherva, Gujarat, India
[2]Director, FCA, Hemchandracharya North Gujarat University, Patan, Gujarat, India
[3]Professor & Head, MCA, U.V.Patel College of Engineering, Ganpat University, Kherva, Gujarat, India

Abstract: ***In today's society, technologies are increased and it increases the need for the security for private their personal data and information from the attack of intruders. To overcome this problem proper authentication technique is required, which reject the unauthorized persons. This paper describes the emerging technology: the biometric technology provides automatic recognition of an individual based on a unique feature or characteristic possessed by the individual. These biometric characteristics may physiological or behavioral. This paper provides the comparison of the different authentication system and show the biometric authentication is the best. Also provide the Verification, Identification and Screening process of the biometric authentication system. This paper gives a comparison and brief overview on different physiological and behavioral biometrics. It also presents pros and cons of different biometric technology with the application where it is used, as well as provides the information of features which are to be extracted for authentication and the methods are implemented in different biometric technologies. This paper also shows the comparison of biometric technologies based on different criteria like measurement, communal, technical, performance, and market point of view.***

Keywords: ***Physiological Biometrics, Behavioral Biometrics, Types of Applications, Comparisons on Different Criteria.***

I. INTRODUCTION OF BIOMETRICS

We Todays in technical era, proper authentication techniques are demanding in educational, research and industrial due to the need for security in a wide range of applications from intruders. This problem is solved by tree authentication techniques like Knowledge Based (i.e. Password), Token Based (i.e. Id card) and Biometric authentication (i.e. Fingerprint). This three authentication techniques are based on a set of information schema. See the below Figure 1.1. The passwords or secret codes can be cracked. An intruder can attack systems based on identification cards or token by robbing, copying or simulating them. Only the biometric authentication can deal with identification of individuals based on their physical and behavioral features. Biometrics (ancient Greek: bios ="life", metron ="measure") is the automated identification or verification of human identity through repeatable measurements of individuals based on their physiological and behavioral characteristics. Examples of physiological biometric characteristics include fingerprints, eye retinas and irises, facial patterns and hand measurements, while examples of behavioral characteristics include a signature, gait and typing patterns. Biometric characteristics are remaining permanently with the user. And they are more reliable than token or knowledge based traditional authentication methods. The following Table 1.1 shows the difference between Biometric Authentication and Knowledge/Token (Password/Key) based authentication.

Table 1.1. Difference between Biometric and Knowledge/Token based authentication

Biometric Authentication	**Knowledge/Token (Password/Key) Based Authentication**
Based on physiological measurements or behavioral traits	Based on something that the user 'has' or 'knows'
Authenticates the user	Authenticates the password/key
Is permanently associated with the user	Can be lent, lost or stolen
Biometric templates have high uncertainty	Have zero uncertainty
Utilizes probabilistic matching	Requires exact match for authentication

Fig 1.1: Set of Information Schema

II. PHYSIOLOGICAL AND BEHAVIORAL BIOMETRICS

Biometric can be grouped into the following two classes:

- **Physiological/Biological** – are the biometrics derived directly from the part of a human body. The most used examples are the fingerprint, eye retina and irises, facial pattern and hand measurements, DNA etc.
- **Behavioral –** are the biometrics by persons behavioral characteristics, such as signature, keystroke recognition, speech/voice recognition, gait-recognition etc.

The following Figure 3.1 shows the graphical representation of physiological and behavioral biometrics and Table 3.2 shows the difference of physiological and behavioral biometrics.

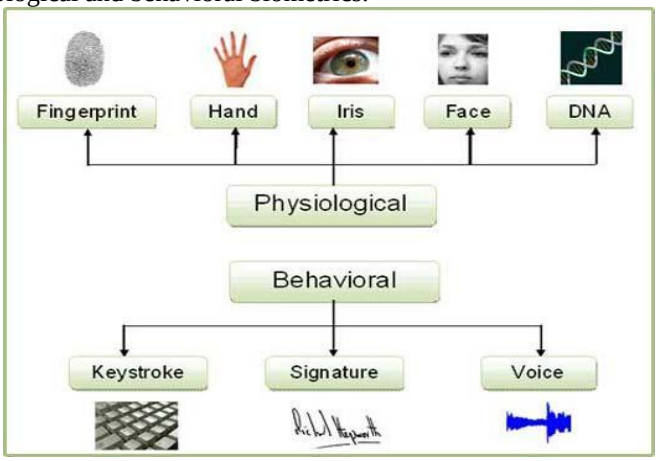

Fig 2.1 Graphical representation of Physiological and Behavioral biometric

2.1 Types of Physiological/Biological Biometrics

2.1.1 Fingerprint Recognition

Fingerprinting is one of the oldest and most well-known recognition technique [3]. A fingerprint is made up of ridges and valleys pattern. This pattern is remaining unique for a specific individual. The same fingers of identical twins will also differ. A user does not need to type passwords - instead, only a touch to a fingerprint device provides almost instant access.

One type of fingerprint reader reads in the fingerprint by flashing light through a glass plate, on which the user has placed his finger, and digitizing the reflections. All fingers may be analysed or just one or two. Computer software exists to encode the distinctive patterns found in the digitized image. The resulting templates can be optionally encrypted and stored on a central database or on each user's card individually.

2.1.2 Hand Geometry

Hand geometry recognition systems are based on a number of measurements taken from the human hand like shape of the hand - size of the palm, length and width of the fingers, thickness, joints, distance between the knuckles, etc. [4, 5]

A hand scanner is a fairly simple device that measures hand geometry to obtain a template of the user's hand. The user puts his or her hand in a small device, positions his or her fingers according to a set of pins on the device. A solid-state digital camera captures side and top views of the hand, and sends the data to a microprocessor for analysis. The data are compressed down to essential information and compared against a stored profile. If the comparison score is low, then the hands are nearly the same. New users can be enrolled easily. A new user places his hand on the device three times and is then ready for identification. The following figures show the image of Hand Scanner and Hand Geometry.

2.1.3 Face recognition

Biometric facial recognition systems analyse the overall structure of a person's face. Features such as the distance between the eyes, nose, mouth, eye sockets, location of the nose and eyes, and cheekbones are analysed.

At enrolment, several pictures are taken of the user's face, with slightly different angles and facial expressions, to allow for more accurate matching. For verification and identification, the user stands in front of the camera for a few seconds, and the scan is compared with the template previously recorded. The following figures show the image of Face Scanner and Face recognition.

2.1.4 Iris Recognition

The iris is the colourful part of the eye between the white (sclera) and the pupil. Its uniqueness in every person stems from variations in features such as furrows, striations, pits, collagenous fibers, filaments, crypts (darkened areas), serpentine vasculature, rings, and freckles. The iris of the eye has a unique pattern, from eye to eye and person to person. Eye colour is the colour of iris [6].

The user places him or herself so that the person can see his/her eye reflection in the iris biometric device. Afterwards, the user has to look into the device for a few minutes in order to capture the features of the iris. The unique code provided by the iris relies on very high-quality images provided by the software and the user [7]. The following figures show the image of Iris Scanner and Iris Recognition.

2.1.5 Retina Recognition

The retina, the backside of the eyeball, has unique patterns of blood vessels. This method of personal authentication uses the vascular patterns of the retina of the eye. [5] In healthy individuals, the vascular pattern in the retina does not change over the course of an individual's life.

The patterns are scanned using a low-intensity (e.g., near-infrared) light source. It requires the user to look into a device and focus on a given point. The image acquisition involves cooperation of the subject, entails contact with the eyepiece. [1,2]

User enrolment amounts to scanning the retina and recording the user's retinal templates. An infrared beam scans the user's retina and the reflected light is recorded by a CCD camera. The scanner may be stationary, in which case the user must position himself correctly in front of the scanner. Or the scanner may be hand-held, in which case the user must aim it correctly. Once the retina is scanned, special software creates a digital profile of the user's unique pattern of blood vessels. The image is processed. This image is compared to an image stored on the user's identification card or in a central database. A good match authenticates the user.

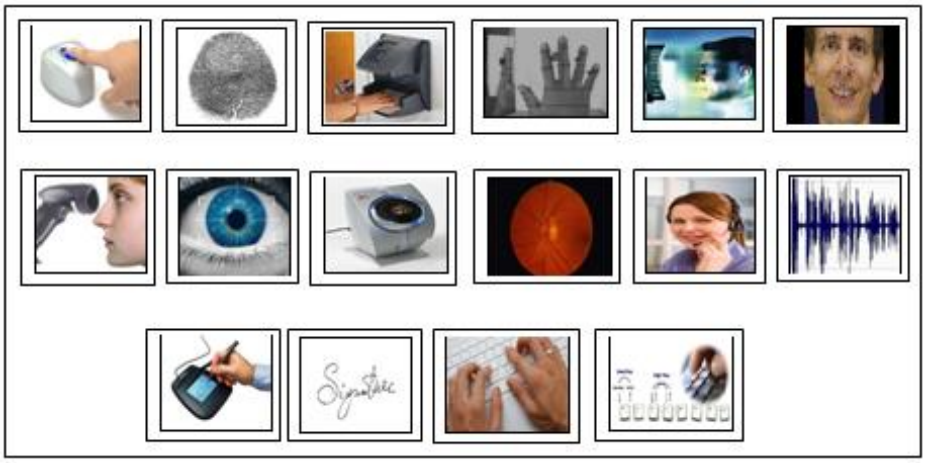

Fig. 2 Scanner and Types of Biometric Recognition

2.2 Types of Behavioral Biometrics

2.2.1 Voice Recognition:

One of the simplest systems is 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 [5].

In these systems, the user speaks a specific word into a microphone attached to the system. Software analyses his or her voice and abstracts significant measures on roughly twenty parameters (pitch, speech, energy density, waveforms, etc.). This live profile is compared against a profile stored on a central database or the user's card. A good match authenticates the user.

2.2.2 Dynamic Signature Recognition

The way in which an individual signs his/her name is considered to be characteristic of that person and as such could provide a feasible mode of biometric recognition. Dynamic signature recognition is an automated method of examining an individual's signature. In this assess specific features of the signature writing process, including the speed, direction and pressure of writing, the time the stylus (e.g. a pen) is in and out of contact with the surface (e.g. paper), the total time taken to write the signature and where the stylus is raised and lowered on the surface. It has been suggested that automated signature recognition should measure the degree of similarity in signature shapes.

A scanner is used to record the way a person writes on tablet, and even with a sensored pen. Another way of capturing a signature biometric is by using ultrasonic sensing. Once the signature is captured, it is verified against the database.

2.2.3 Keystroke:-

Keystroke dynamics is a behavioral characteristic. Keystroke dynamics means not what you type, but how you type. Keystroke dynamics is the process of analysing 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 habitual typing rhythm patterns [25]. Individual keystroke dynamics, such as speed of typing, pauses between words, and intervals between individual characters, could potentially provide on-going identity verification rather just onetime verification at the beginning of a computer session. Moreover, unlike other biometric systems which may be expensive to implement, keystroke dynamics is almost free only hardware required is the keyboard.

III. BIOMETRIC APPLICATIONS

On the most abstract level, biometric applications can be divided in three categories [28]:

Logical Access: Biometrics can be used to control access to data or information (intangible resources). This group of applications can be referred to as network security applications.

Physical Access: Biometrics can be used to control access to tangible resources or premises.

Identity Verification: Biometrics can be used to verify the identity of an individual or check his or her identity against other data.

On a more practical level, applications of biometrics can be divided into Forensic, Government and Commercial applications [29]. As presented below in Table 4.1 and Figure 4.1 each of these broad categories has a number of concrete applications.

Table 3.1: Categories of Biometric Application

Forensic	Government	Commercial
Corpse Identification	National ID Card Biometric Password	ATM Internet Banking
Criminal Investigation and Terrorist identification	Driver's License, Voter Registration	Access Control Computer Login
Parenthood determination	Welfare Disbursement	Cellular Phones, PDA
Missing Children	Border Crossing (US-Visit Program) and Passport Control	E-Commerce Smart card

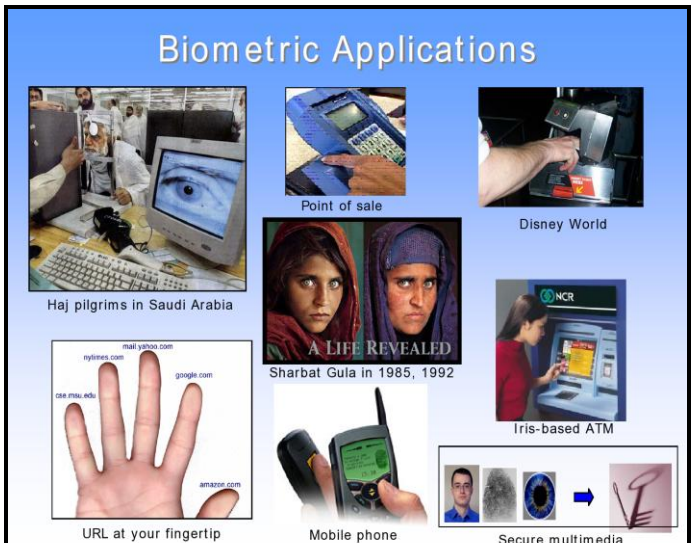

Fig 3.1: Biometric Applications

IV. SUMMARY OF PROS AND CONS WITH APPLICATIONS OF BIOMETRICS

In this topic we prepared one Table 4.1 which shows the pros and cons of different Physiological and Behavioral Biometric modalities with the variety of applications.

Table 4.1. Summary of Pros And Cons With Applications of Biometrics

Types of Biometric	Pros	Cons	Applications
Fingerprint [8]	• Mature technology • Easy to use	• Inability to enroll some users	• Time and attendance monitoring for employee and school

	/nonintrusive • High accuracy (comparable to PIN authentication) • Long-term stability and ability to enroll multiple fingers • Comparatively low cost	• Ridge patterns can be affected by cuts, dirt, or even wear and tear. • Sensor may get dirty • Association with forensic applications • Difficult to extract features from partial fingerprint.	• Used in laptop computers, USB storage devices, cars, household door locks, safes, and even mobile phones • Access bank ATMs • Used in National Identification cards, voter registration schemes, Driver's License, Welfare Disbursement, management of social service benefits (e.g. to work against fraud) and particularly border control and immigration programs. • In Forensic application like Corpse Identification, Criminal Investigation, Terrorist Identification, Parenthood determination, Missing Children, etc.
Hand Geometry [10]	• Not affected by environment • Mature technology • Non-intrusive • Relatively stable	• Lack of accuracy • High cost • Relatively size of the scanner is larger • Difficult to use for some users (arthritis, missing fingers or large hands)	• Used for physical access control, time and attendance in workplaces and schools • Access to restricted areas and buildings: Hand biometric systems are currently used in apartment buildings, offices, airports, day care centers, welfare agencies, hospitals, sperm banks and immigration facilities.
Face [11]	• Non-intrusive • Low cost • Ability to operate covertly	• Affected by appearance/environment • High false non-match rates • Identical twins attack • Potential for privacy abuse • User perceptions / civil liberty: Most people are uncomfortable with having their picture taken.	• Used for physical and logical access control in banks, casinos, offices, crèches, etc. • Employed to prevent unauthorized exit from certain locations. For example, a nursing home. • Used for passport identification. • Used for surveillance purposes and for screening individuals against watch lists of criminal's record.
Iris Scan [15,16]	• Potential for high Accuracy • Resistance to impostors • Long term stability • Fast processing	• Intrusive • Some people think the state of health can be detected • High cost • The user must hold still while the scan is taking place.	• Used for Immigration purposes, i.e. the Iris Recognition Immigration System (IRIS).
Retinal Scan [21]	• High accuracy • Long-term stability • Fast verification	• Difficult to use • Intrusive and slow • Limited applications	• Used where require maximum security, such as Government, military and banking. • Used by several government agencies including the FBI, CIA, and NASA.
Voice [22,23]	• Use of existing telephony infrastructure or simple microphones • Easy to use/nonintrusive/ hands free • No negative association	• Pre-recorded attack • Variability of the voice (ill or drunk) • Affected by background noise • Large template (5K to 10K) • Low accuracy • High false non-matching rates.	• Voice biometrics are usually used in verification-based applications, implemented in the financial services sector • Used in law enforcement for forensic purposes
Dynamic Signature [24]	• Resistance to forgery • Widely accepted • Non-intrusive • No record of the signature	• Signature inconsistencies • Difficult to use • Large templates (1K to 3K) • Problem with trivial signatures	• Used in banking and finance industry in order to restrict duplicate signature frauds • Used where paperless procedures are involved • Used in online insurance buying. Patient records and medical prescriptions are also protected using biometric signature recognition.

			• Used in various government offices and defense organizations to prevent the unauthorized access to sensitive data as well as for user identification. • Unauthorized access of Computer and cell phones.
Keystroke [25,26]	• No additional hardware required • Non-intrusive and wide user acceptance • Minimal training • Your type behavior can never be lost • Impossible to copy by observation	• Low accuracy • Narrow range of applications. • The keyboards of other countries are different (Germany, France)	• To access a computer.

V. FEATURES FOR EXTRACTION WITH IMPLEMENTED METHODS

As human present biometric data, a number of features extracted from that data are responsible for recognition process. The different biometric consists different biometric features, so the following Table 5.1 presents a summary of the biometrics with its features and with the implemented methodologies which are used to extract features.

Table 5.1. Features for Extraction with Implemented Methods

Types of Biometric	Implemented Methodologies		Features
Fingerprint [8]	• Minutiae-Based Methods [9] • Image Based Methods		• A friction Ridge curves-a raised portion, pore structure, indents and marks
Hand Geometry [10]	• Feature Based :Finger length, width, thickness curvatures and relative location of features		• Estimation of length, width, thickness, shape and surface area of the hand.
Face [11]	• Image Based ➢ Statistical methods ❖ Eigenfaces [12] ❖ Fischerfaces [13] • Feature based [14] ➢ Geometric ➢ Feature meteric ➢ Morphable models		• Distance of specific facial features (eyes, nose, mouth)
Iris Scan [15,16]	• Complex valued 2-D Gabor Wavelets [17]. • Laplacian of Gaussian filters [18]. • Zero Crossing Wavelet Transform[19] • Circular Symmetry 2-D Filters [20] .		• Texture of the iris such as freckles, coronas, strips, furrow, and crypts
Retinal Scan [21]	• Feature Based Retinal vein pattern		• Vessel pattern in the retina of the eye as the blood vessels at the back of the eye
Voice [22,23]	• Low level features • Pitch • MFCC • High level features	• GMM [28] • HMM[29] • ANN • VQ[30]	• Words, tone
Dynamic Signature [24]	• Feature based methods		• It measures pressure, direction, timing, acceleration and the length of the strokes
Keystroke [25,26]	• Latencies between successive keystrokes • Duration of each keystroke		• Keystroke time interval

VI. COPARISION OF BIOMETRICS

6.1 Comparison Based on Communal Point of View

- **Privacy Concept:** Worries that it might lead to remote tracking and one is giving its personal part information to other about some biometric.
- **Hygiene Factors:** Applies to contact technique such as finger print.
- **Safety Concern**: If my car starts only with my finger print, then thieves might chop off my finger. It happens [32].

- **Cost Factor:** The initial investment and operating cost both are important factors. The initial cost includes modifications to existing systems, initial training of operators as well as procuring biometric equipments. The operating cost depends on maintainability and reliability.
- **Socially Introduced:** The year when particular biometric comes into light and used for society.
- **Popularity:** To which extent a society aware about a particular biometric instrument.
- **Ease** of Use: It should be easy to use the device and especially for non-habituated applications.
- **Error of Incidence:** Various reason which occur and make sense of error.

6.2 Technological Point of View

- **Processing Speed:** The speed with which two templates can be generated and compared for problems involving identification, because the user's biometric data must be compared to each and every record in the database.
- **Accuracy:** How much accurately our device is working in the given environment.
- **Stability:** The time duration to which the biometric data changes over time. For example a person's voice can change due to cold or any other factors.
- **Template Size:** The size of template can impact the cost and performance of a system in several ways. A smaller code will require less system storage space and can be transmitted between sites more quickly than a larger code.
- **Device Used:** It describe about the hardware used by our application and give the answer of many questions as, It is handy or not, bulky in size or small, required operator or not. For example in iris recognition a camera is required.
- **Technology Used in Device:** We have a number of methods to implement our device.

Table 6.1.1. Comparison Based on Communal Point of View

Types of Biometric	Privacy Concent	Hygene Factors	Safety Concern	Cost	Socially Introduced	Popularity	Ease of Use	Error of Incidence
Fingerprint	H	M	M	L	1981	H	H	Dryness, dirt, age, moisture
Hand Geometry	L	H	M	H	1986	L	H	Hand injury, age
Iris Scan	H	L	H	H	1995	M	M	Poor lighting, glasses
Retinal Scan	L	L	H	H	1999	L	L	Glasses, contact lens
Face	H	L	M	M	2000	H	H	Lighting, age, glasses, hair
Voice	M	L	H	L	1998	H	H	Noise, cold, weather
Signature	H	H	H	M	1970	H	H	Changing signature
Keystroke	L	H	L	M	2005	L	L	Weather, device

Table 6.2.1. Comparison Based on Technological Point of View

Types of Biometric	Processing speed	Accuracy	Stability	Template size	Device used	Technology used in device
Fingerprint	H	M	H	-	Fingerprint reader	Optical, thermal, silicon or ultrasonic principles
Hand Geometry	H	M	M	-	CCD Camera	Laser light, IR light
Iris Scan	M	H	H	5-50 kb	Camera	CCD/CMOS image sensor
Retinal Scan	M	H	H	-	Retinal scanner	Laser light, IR light
Face	M	L	M	3-5 kb	Camera	CCD/CMOS image sensor
Voice	H	L	M	-	Microphone	Converting signals
Signature	H	M	M	20 kb	Tablet, Touch Panel	Capacitive, resistive, acoustic
Keystroke	M	L	L	-	Keyboard, special Software	Software based

6.3 Based on Measurement

Any human physiological and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

- **Universality:** each person should have the characteristic.
- **Distinctiveness:** any two persons should be sufficiently different in terms of the characteristic.
- **Permanence:** the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time.
- **Collectability:** the characteristic can be measured quantitatively.

However, in a practical biometric system (i.e., a system that employs biometrics for personal recognition), there are a number of other issues that should be considered, including:

- **Performance:** which refers to the achievable recognition accuracy and speed, the resources required to achieve the desired recognition accuracy and speed, as well as the operational and environmental factors that affect the accuracy and speed;
- **Acceptability:** which indicates the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives;
- **Circumvention:** This reflects how easily the system can be fooled using fraudulent methods.

6.4 Performance Point of View

Performance based upon various factors can be used to differentiate biometrics as dictated below.

- **False Acceptance Rate (FAR):** It refers to a situation where an unauthorized user is accepted by the authentication biometric machine as an authenticated person. It means the percentage of incorrectly accepted invalid users.
- **False Rejection rate (FRR):** It refers to a situation where an authorized person is rejected by the authentication biometric machine as an unauthenticated person. It means the percentage of incorrectly rejected valid users.
- **Equal Error Rate (EER) or Crossover Error Rate (CER):** The error rate at which FAR equals FRR. The minimum cross error rate, the more accurate and reliable the authentication biometric machine.

Table 6.3.1. Comparison Based on Measurement

Types of Biometric	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Iris Scan	H	H	H	M	H	L	H
Retinal	H	H	M	L	H	L	H
Face	H	L	M	H	L	H	L
Voice	M	L	L	M	L	H	L
Signature	L	L	L	H	L	H	L
Keystroke	L	L	L	M	L	M	M

Table 6.4.1. Comparison Based on Performance Point of View

Types of Biometric	False Acceptance Rate (%)	False Rejection Rate (%)	Crossover Error Rate (%)	Failure To Enrollment (%)	Failure To Capture Rate	Receiver Operating Char	Sensor Subject Distance
Fingerprint	2	2	2	1	-	-	Zero
Hand Geometry	2	2	1	NA	NA	-	10 cm
Iris Scan	0.94	0.99	0.01	0.5	-	-	30 cm
Retinal Scan	0.99	1	0.04	0.8	-	-	2 cm
Face	1	20	-	NA	NA	-	~20 m
Voice	2	10	6	-	-	-	20 cm
Signature	-	-	-	-	-	-	Zero
Keystroke	7	0.1	1.8	-	-	-	Zero

- **Failure to Enrollment (FTE):** The rate at which attempts to create a template from an input is unsuccessful. It can be defined as the probability that a user attempting to enroll yourself but unable to do so and it is normally defined by a minimum of three attempts [33]. This is most commonly caused by low quality inputs.
- **Failure to Capture Rate (FCR):** Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.
- **Receiver Operating Characteristic (ROC):** In general, the matching algorithm performs a decision using some parameters (e.g. a threshold). In biometric systems the FAR and FRR can typically be traded off against each other by changing those parameters. The ROC plot is obtained by graphing the values of FAR and FRR, changing the variables implicitly.
- **Sensor Subject Distance (SSD):** The distance between human biometric part and biometric part reader device. It may vary as zero distance to several meters.

6.5 Biometric Market Point of View

With the significant advances in computer processing, the automated authentication technique using various biometric features has become available over the last few decades. According to a report named biometrics market & industry presented by International Biometric Group (IBG) in 2007 and 2010, I can represent the percentage of market covered by different biometrics as shown in Figure 7.5.1 and Figure 7.5.2.

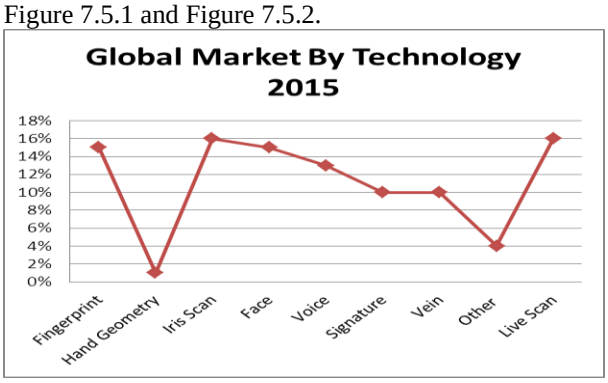

Fig 6.5.1 Comparison based on Market Point of View

VI. CONCLUSION

After the comparison of Token/Password based authentication and Biometric based authentication it proved that biometric authentication is more secured, safe and more reliable. This paper presents difference between physiological and behavioral biometric as well as a brief introduction of current numerous biometric techniques. It also describes the no. of applications alternative solutions used in security techniques. Biometrics is a rapidly evolving technology that is being widely used in forensics, security; prevent unauthorized access in bank or ATMs, in cellular phones, smart cards, PCs, in workplaces, and computer networks. Selection of a particular biometric technology for identifying and authenticating users depends of a number of factors such as measurement, communal, technical, performance and based on market. As this is a new technology for most of the peoples since it has simply been implemented in public areas for short time period. It provides benefits that may improve our lives in such a way by increasing security and efficiency, decreasing scams and reducing password administrator cost, ease of use and makes live more comfortable.

REFERENCES

[1] Anil K. Jain, Arun Ross and Salil Prabhakar: "An Introduction to Biometric Recognition" IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.

[2] L. O'Gorman, "Seven Issues with Human Authentication Technologies", Proc. of Workshop on Automatic Identification Advanced Technologies (AutoID), pp. 185-186, Tarrytown, New York, March 2002.

[3] Woodard, J. D., Orlans, N. M., & Higgins, P. T. (2003). Biometrics (electronic book). New York: McGraw-Hill/Osborne.

[4] 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.

[5] Fernando L. Podio: "Personal Authentication through Biometric Technologies" International Journal of Advanced Science and TechnologyVol. 4, March, 2009.

[6] 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.

[7] Garcia, J. O., Bigun, J., Reynolds, D., & Gonzalez-Rodriguez, J. (March 2004). Authentication Gets Personal with Biometrics. Increasing security in DRM systems through biometric authentication. , 50-62.

[8] Maltoni, D., D. Maio, A.K. Jain and S. Prabhakar, "Handbook of fingerprint recognition", Springer, New York, 2003.

[9] N. Yager and A. Amin, "Fingerprint verification based on minutiae features: a review", Pattern Analysis Application, Vol. 7, pp. 94–113, 2004.

[10] Reillo, R. S., Avilla, C. S. and Marcos, A. G., "Biometric Identification through Hand Geometry Measurements", IEEE Transactions on Pattern Analysis and Machine Intelligence Vol. 22, no. 10, October 2000, pp. 1168-1171.

[11] Chellapa, Rama, Wilson, Charles L, and Sirohey, Saad, "Human and machine recognition of faces: a survey" Proc. IEEE, Vol. 83, No 5, May 1995, pp-705-740.

[12] Turk,M. and Pentland , A. "Eigenfaces for Recognition," Journal of Cognitive Neuro Science, Vol. 3, No,1, pp-71-86,1991.

[13] Belhumeur,P., Hespanha, J. and Kriegman, D. "Eigenfaces vs. Fisherfaces: recognition using class specific linear projection," IEEE Transaction. on Pattern Analysis and Machine Intelligence, Special Issue on Face Recognition , July 1997, pp. 711-720.

[14] Brunelli,, R. and Poggio, T., "Face recognition: Features versus Templates" IEEE Transaction on Pattern Analysis And Machine Intelligence, Vol. 15, No.10, October 1993, pp. 1042-1052.

[15] Bowyer, K. W. Hollingsworth, K. and Flynn. P J. "Image understanding for iris biometrics: a survey" Computer Vision and Image Understanding 110 (2), May 2008, pp. 281-307.

[16] Ng, Richard, Tay, Y. H., and Mok, K. M., "A review of iris recognition algorithms," International Symposium on Information Technology Vol. 2, 26-28 Aug. 2008 pp.1 – 7.

[17] Daugman, J. G. "High confidence visual recognition of persons by a test of statistical independence," IEEE Transaction on Pattern Analysis and Machine Intelligence Vol. 15, 1993, pp. 1148–1161.

[18] Wildes,.R., Asmuth, J., Green, G., Hsu, S. , Kolczynski, R. , Matey, J. , McBride, J. " A machine-vision system for iris recognition," Machine Vision and Applications Vol. 9 (1996) 1-8.

[19] Boles, W.W., and Boashah, B. "A human identification technique using images of the iris and wavelet transform," IEEE Transactions on Signal Processing Vol. 46 (1998) 1185-1188.

[20] Li Ma, Yunhong Wang, and Tieniu Tan, "Iris recognition using circular symmetric filters" Proceedings of 16th International Conference on Pattern Recognition Vol. 2, 11-15 August 2002 pp. 414 – 417.

[21] H. Tabatabaee, A. Milani-Fard, and H. Jafariani, "A Novel Human Identifier System Using Retina Image and Fuzzy Clustering Approach," in Proceedings of the 2nd IEEE International Conference on Information and Communication Technologies (ICTTA 06), Damascus, Syria, April 2006, pp. 1031-1036.

[22] Kinnunen, T. and Li, H. "An overview of text-independent speaker recognition: from features to supervectors", Speech Communication, Vol. 52, Issue 1, January 2010, pp. 12-40.

[23] Campbell, Joseph P. Jr. "Speaker Recognition: A Tutorial," Proceedings of IEEE, Vol. 85, issue 9, Sep.1997, pp. 1437-1462.

[24] Zanuy, M. F., "Signature recognition state-of-the-art" IEEE A&E Systems Magazine, July 2005, pp. 28-32.[25] Fabian Monrose and Aviel Rubin "Authentication via keystroke dynamics", Proceedings of the 4th ACM conference on Computer and communications security, 1997, pp 48 -56.

[26] Shanmugapriya. D "A survey of biometric keystroke dynamics: approaches, security and challenges," International Journal of Computer Science and Information Security, Vol. 5, No. 1, 2009.

[27] Gafurov,D., "A survey of biometric gait recognition: approaches, security and challenges" NIK Conference ,2007.

[28] Nanavati, S., M. Thieme, and R. Nanavati (2002) Biometrics: Identity Verification in a Networked World, New York, NY: John Wiley & Sons, Inc.

[29] Jain, A., L. Hong, and S. Pankanti (2000) "Biometric Identification", Communications of the ACM, (43) 2, pp. 91-98.

[30] Simon Llu and Mark Silverman, "A practical guide to biometric security technology," IT Pro, 2001.

[31] A. Ross, S. Dass, and A. K. Jain, "A deformable model for fingerprint matching," Journal of Pattern Recognition, Elsevier, vol. 38, no. 1, pp. 95–103, 2005.

[32] Jonathan Kent, "Malaysia car thieves steal finger," [Online]. Available: http://news.bbc.co.uk/1/hi/world/asia-pacific/4396831.stm, [October 2, 2013].

[33] Meghna B. Patel, Ashok R. Patel, N. J. Patel, "Comparative Study on Different Fingerprint Classification Approaches", IJCTA, ISSN: 2229-6093, Volume-5, Issue-1, Page No. 189-197, Jan-Feb-2014.

[34] Meghna B. Patel, Ashok R. Patel, "Performance Improvement by Classification Approach for Fingerprint Identification System", IJRTE, ISSN:2277-3878, Volume-2, Issue-2, May-2013.

[36] Meghna B. Patel, Ashok R. Patel, Ronak B. Patel, "Components of Fingerprint Biometric System", IJERT, ISSN: 2278-0181, Volume 1 Issue 3, May-2012.

