IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 15, Issue 1 (Sep. - Oct. 2013), PP 22-29
www.iosrjournals.org

A Comparison Based Study on Biometrics for Human Recognition

Himanshu Srivastava
Department of Computer Science & Engineering Roorkee Institute of Technology, Roorkee (U.K.), India

Abstract: *A biometric system provides automatic recognition of an individual based on a unique feature or characteristic possessed by the individual. These biometric characteristic may physiological or behavioral. Unlike other identification methods such as id proof, tokens and password, the distinct aspect of biometric recognition comes into light from randomly distributed features in human being. In this paper, I describe the novel comparison based upon various aspects to make easy selection for biometric device deployment in specific environment. This paper proposes a comparison among all kind of biometric system available in the society. 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; it means one can be authorized by representing himself or herself. In this paper, the main focus is on working principal of biometric technique, the various biometrics systems and their comparisons.*

Keywords: *Biometrics, authentication, identification, recognition.*

I. Introduction

Now a days, one of the main threats that IT system and security environment can have, is the possibility of intruders in the system. This is normally solved by user authentication schemes based on passwords, secret codes and identification cards or tokens. Schemes based only on passwords or secret codes can be cracked by intercepting the presentation of such a password or by brute force attacks. On the other hand, an intruder can attack systems based on identification card or token by robbing, copying or simulating them. As it is a well-known, biometric deal with identification of individuals based on their physical and behavioral features. Biometric solutions, such as identification systems using fingerprint, iris, face, and palm print, hand geometry, signature, etc; have many advantages over the traditional authentication techniques based on what you know or what you possess. Instead of carrying bunk of keys, all those access cards or passwords you carry around with you, your body can be used to uniquely identify you. Among them, iris recognition is tested as the most accurate manner of personal identification. Therefore nowadays many automatic security systems based on iris recognition have been deployed worldwide for border control, restricted access and so on [1].

This paper represents the comparison about recognition of a person using a number of biometric systems available, after study a number of papers, articles, conference paper and real facts. My paper is organized as follows: working principle of biometric system in section II, types of biometric either physiological or behavioral based characteristics and their types in section III, a comparative tables based upon various aspects as biometric features, characteristic of biometric entities, social point of view, technical point of view, evaluation point of view, and biometric market point of view are given in section IV, the entire theme is given as conclusion in section V, in the last all the papers and websites which I have used to provide this study is given under the heading references in section VI.

1.1 Identification and verification: Sometimes verification and identification are interpreted as similar terms but in biometric recognition both the terms having different meanings. Verification refers to 1:1 matching, it means persons is claiming his/her identity to the system, and then getting verifying himself/herself. Identification refers to 1: m matching it refers to a situation where user does not know who is he or he is not claiming his identity but presenting his/her biometric for matching with entire database. Identification occurs when an individual's characteristic is being selected from a group of stored images. Identification is the way as human brain performs most day to day identifications. For example, if a person encounters a familiar individual, the brain process the information by comparing what the person is seeing to what is stored in memory. Recognition is a generic term and does not necessarily imply either verification or identification. All biometric system performs recognition.

1.2 Authentication Methods: As there exist a number of authentication methods, I can categorized as non biometric based and biometric based. Non biometric based include password, keys, token which can be steal or copying easily and biometric based include iris, face, signature and so on, which is very difficult to forgery.

Knowledge Based: Only the authenticator knows as password, PIN or answer to a security question.
Possession Based: Things are carrying by the person, being authenticate as keys or in the forms of cards which made up of plastic or using other material where we can find information regarding a person.
Physical Characteristic Based: A physical characteristic is related to the shape of the body. It is a stable human physical characteristic, such as fingerprint, iris pattern. It remains unalterable without significant issue.
Behavioral Characteristic Based: It depends upon the behavior of a person as signature and voice feature.

II. Working Principle of Biometric System

All the biometric system use the same basic principle as dictated below [2]. It consists predefined steps as well as we must know some basic terms related to biometric system as enrollment, biometric data, presentation, template, feature extraction, matching.

2.1 Enrollment or Registration: The process, by which a user's biometric data is initially obtained, processed and stored in the form of a template for ongoing use in a biometric system. It is called enrollment or registration process. This template will be use for further process as authentication.
2.2 Biometric Data: The data presented by the user during registration is called unprocessed image data, which is also referred as raw biometric data or biometric sample. Raw biometric data cannot be used to perform biometric matches so it is used to generate biometric template with the help of feature extraction process.
2.3 Presentation: The process by which user presents his/her biometric data to the acquisition devices, the hardware which is used to collect data. For example placing a finger on a plate at finger reader device.
2.4 Template: A mathematical representation of raw biometric data which is obtained after applying a number of feature extraction algorithms. A template size can vary in size as few bytes for hand geometry to several thousand bytes for facial recognition [3]. The template created at the time of registration is called stored template and at the time of authentication is called live template.
2.5 Feature Extraction: The process of locating and encoding distinctive characteristics from biometric data in order to generate a template is called *feature extraction.* Feature extraction takes place during enrollment and verification, any time a template is created.
2.6 Matching: A process where stored template is matched with live template at the time of verification and we obtained a score, on the basis of this score we conclude that a user is authenticate human or not.

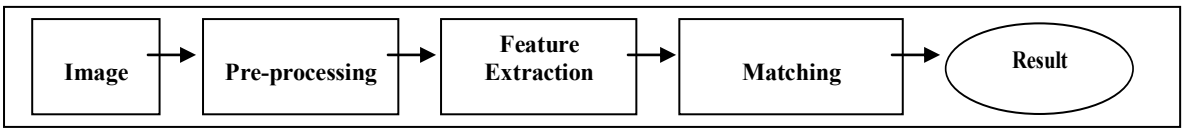

Figure 1: A biometric system [1]

III. Types of Biometrics

While referring to types of biometric, it is important to know and distinguish between physiological and behavioral human characteristic. Based upon physiological and behavioral characteristic of human we have two types of biometrics, where each type can define multiple biometrics as stated below.

3.1 Physiological Biometrics: A biometric related to the human body and difficult to forgery. It remains unaltered without significant issue. This type of biometric includes iris, retinal, fingerprint, palm print, hand geometry, face and DNA.

Figure 2: Iris [4]

Figure 3: Retinal [5]

Figure 4: Fingerprint [5]

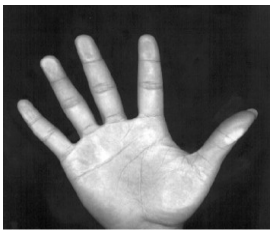

Figure 5: Palm Print [6]

Iris: This recognition method uses the iris of the eye which is colored area that surrounds the pupil. Iris patterns are unique and are obtained through digital image or video based image acquisition system. Each iris structure is

featuring a complex pattern. This can be a combination of specific characteristics known as corona, crypts, filaments, freckles, pits, furrows, striations and rings [7]. An iris image is shown in figure 2.

Retinal: Retina scans require that the person removes their glasses, place their eye close to the scanner, stare at a specific point, and remain still, and focus on a specified location for approximately 10 to 15 seconds while the scan is completed. A retinal scan involves the use of a low-intensity coherent light source, which is projected onto the retina to illuminate the blood vessels which are then photographed. The infrared energy is absorbed faster by blood vessels in the retina than by the surrounding tissue. The image of the retina blood vessel pattern is then analyzed [5]. A retinal image is shown in figure 3.

Finger Print: A fingerprint is an impression of the friction ridges of all or any part of the finger. A friction ridge is a raised portion of the on the pal mar (palm) or digits (fingers and toes) or plantar (sole) skin, consisting of one or more connected ridge units of friction ridge skin [5]. In modern approach, live finger print readers are used .These are based on optical, thermal, silicon or ultrasonic principles [8] [9]. A fingerprint image is shown in figure 4.

Palm Print: Palm print verification is a slightly different implementation of the fingerprint technology. Palm print scanning uses optical readers that are very similar to those used for fingerprint scanning; their size is, however, much bigger [6]. A palm print image is shown in figure 5.

Hand Geometry: It is based on the fact that nearly every person's hand is shaped differently and that the shape of a person's hand does not change after certain age. These techniques include the estimation of length, width, thickness and surface area of the hand. Various method are used to measure the hands- Mechanical or optical principle [10]. A hand geometry scanner image is shown in figure 6.

Figure 6: Hand geometry scanner [5]

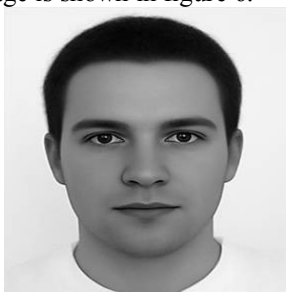

Figure 7: Face

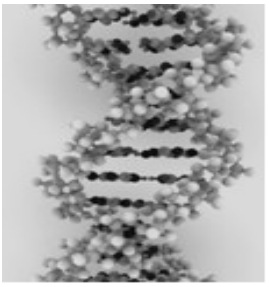

Figure 8: DNA [11]

Face: A facial recognition technique is an application of computer for automatically identifying or verifying a person from a digital image or a video frame from a video source. Facial biometric technology relies on the manufacture of the specific facial features. The system usually look for the positioning of eyes, nose and mouth and distances between these features. It is the most natural means of biometric identification [12]. A facial image is shown in figure 7.

Ear: Identifying individuals by the ear shape is used in law enforcement applications where ear markings are found at crime scenes. Whether this technology will progress to access control applications is yet to be seen. An ear shape verifier (Optophone) is produced by a French company ART Techniques. It is a telephone type handset within which is a lighting unit and cameras which capture two images of the ear [13].

DNA: At present, there exists no technology to allow for automated recognition of DNA samples [11]. DNA analysis requires a lab environment and a form of tissue, blood or other bodily sample. This method of capture still has to be refined. So far the DNA analysis has not been sufficiently automatic to rank the DNA analysis as a biometric technology. The analysis of human DNA is now possible within 10 minutes. As soon as, the technology advances, DNA can be matched automatically in real time, it may become more significant [9] [14].

3.2 Behavioral Biometrics: It depends upon the behavior of human, i.e. psychologically dependent. It depends on the present state of mind and can vary frequently as per situation or environment. For example, voice of human being can be affected by various factors as sadness, happiness, disease as throat infection, environment and so on. This type of biometric includes voice print, signature and typing rhythm recognition.

Voice: Individuals (speakers) can be recognized by their voice print, the set of measurable characteristics of a human voice. Different algorithms are applied in text-dependent, text-prompted or text-independent speaker recognition systems, as explained. Text-dependent systems: The user is requested to speak a word or phrase,

which was saved earlier during the enrollment process. The spoken input is represented by a sequence of feature vectors and compared with previously recorded input vectors, to calculate the degree of similarity. 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 8 3 4 1!"*). 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 [11]. A voice signal image is shown in figure 8.

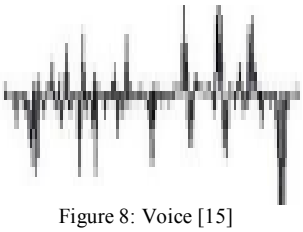

Figure 8: Voice [15]

Figure 9: signature reader [15]

Figure 10: Typing Rhythm [11]

Signature: Biometric signature recognition systems measure and analyze the physical activity of signing. Important characteristics include stroke order, the pressure applied, the pen-up movements, the angle the pen is held, the time taken to sign, the velocity and acceleration of the signature [16]. This method is known as dynamic signature recognition. There are various kinds of devices used to capture the signature dynamics. These are either traditional tablets or special purpose devices. A signature reader device image is shown in figure 9.

Typing Rhythm: The recognition of keystroke dynamics is the process of analyzing the way an individual types at a terminal by monitoring the keyboard inputs in an attempt to recognize the individual based on habitual typing rhythm patterns [17]. Keystroke dynamics are described by speed (the time a key is pressed, the time between keys pressed), rhythm, precision, keys used (e.g., left Shift key or right Shift key, Caps Lock), and other typing characteristics. A typing rhythm image is shown in figure 10.

IV. Biometric Comparison Based on Various Aspects

As the aim of this paper is to provide the comparative study about various biometrics, so in this section after studying a number of research papers and articles, I am giving a number of comparison tables based upon various aspects under the heading as biometric features used for authentication, characteristics of biometric entities, social point of view, technical point of view, evaluation point of view and biometric market point of view.

4.1 Biometric Features Used for Authentication: 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 this table representing biometrics with its features.

Biometrics	Feature Description
Iris	Texture of the iris such as freckles, coronas, strips, furrow, and crypts
Retinal	Vessel pattern in the retina of the eye as the blood vessels at the back of the eye
Finger Print	A friction Ridge curves-a raised portion, pore structure, indents and marks
Palm Print	Principal lines, wrinkles (secondary lines) and epidermal ridges
Hand Geometry	Estimation of length, width, thickness, shape and surface area of the hand.
Face	Distance of specific facial features (eyes, nose, mouth)
Ear	Dimension of the visible ear
Shape of X-Rayed Teeth	Shape of continuous teeth
DNA	DNA code can be extracted from blood, hair, skin cells and other bodily substances
Voice	Words, tone
Signature	It measures pressure, direction, timing, acceleration and the length of the strokes
Typing Rhythm	Keystroke time interval

Table 1: [1] [18]

4.2 Characteristics of Biometric Entities: Each biometric technology has its merit and shortcoming; it is difficult to make a comparison directly. Researchers have identified several factors for it [19] [20] [21] [22]. In table 2, High, Medium, and Low are denoted by H, M and L respectively. We can define first six characteristics as essential characteristic of biometric entities and last four as system dependent characteristic of biometric entities.

Uniqueness: Each individual should have features but different with other. It means distinctive information content.
Permanence: The biometric should be sufficiently invariant over a certain period of time
Universality: The population coverage. Each individual should have the biometric feature.
Measurability: Measurable with simple technical equipments. It means simplicity of extraction.
Comparability: Simplicity of comparison between two templates as one is stored and second one is live template.
Collect ability: How well can the identifiers be captured and quantified
Invasiveness: Introduction of instrument into a body part. For example DNA required blood for testing.
Performance: Accuracy, speed, security.
Acceptability: To which extent society is supporting.
Circumvention: The act of cheating someone.

	Uniqueness	Permanence	Universality	Measurability	Comparability	Collect ability	Invasiveness	Performance	Acceptability	Circumvention
Iris	H	H	H	M	M	H	M	H	M	L
Retinal	H	H	H	L	M	M	H	H	L	L
Finger Print	H	H	M	H	M	M	M	M	H	M
Palm Print	H	H	M	H	M	M	M	M	H	M
Hand geometry	M	L	H	H	M	H	M	M	M	M
Face	M	M	H	M	L	H	L	L	H	H
Ear	M	M	H	M	L	M	L	L	M	L
Shape of X-rayed teeth	L	L	M	L	L	M	H	L	L	H
DNA	H	H	H	L	L	L	H	H	H	L
Voice	L	L	M	M	L	M	L	L	H	H
Signature	H	L	L	M	M	H	M	M	H	H
Typing rhythm	L	L	L	L	L	M	M	L	L	M

Table 2: [23] [18] [24]

4.3 Social Point of View: In table 3, High, Medium, and Low are denoted by H, M and L respectively.
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 [25].
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.

	Privacy Concept	Hygiene Factors	Safety Concern	Cost	Socially Introduced	Popularity	Ease of Use	Error of Incidence
Iris	H	L	H	H	1995	M	M	Poor lighting, glasses
Retinal	L	L	H	H	1999	L	L	Glasses, contact lens
Finger Print	H	M	M	L	1981	H	H	Dryness, dirt, age, moisture
Palm Print	H	H	M	L	1994	L	M	Dirt, age, moisture
Hand geometry	L	H	M	H	1986	L	H	Hand injury, age
Face	H	L	M	M	2000	H	H	Lighting, age, glasses, hair
Ear	L	L	L	M	2002	L	H	Low Lighting
Shape of X-rayed teeth	L	L	L	H	1988	L	H	Equipments
DNA	L	M	H	H	1965	H	L	Equipments
Voice	M	L	H	L	1998	H	H	Noise, cold, weather
Signature	H	H	H	M	1970	H	H	Changing signature
Typing rhythm	L	H	L	M	2005	L	L	Weather, device

Table 3: [26] [18]

4.4 Technical Point of View: In table 4, High, Medium, and Low are denoted by H, M and L respectively.
Processing Speed: *The s*peed 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.
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.
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.

	Processing Speed	Accuracy	Template Size	Device Used	Technology used in device	Stability
Iris	M	H	5-50 kb	Camera	CCD/CMOS image sensor	H
Retinal	M	H	-	Retinal scanner	Laser light, IR light	H
Finger Print	H	M	-	Finger print reader	Optical, thermal, silicon or ultrasonic principles	H
Palm Print	H	M	-	Palm print reader	Optical, thermal, silicon or ultrasonic principles	M
Hand geometry	H	M	-	CCD Camera	Laser light, IR light	M
Face	M	L	3-5 kb	Camera	CCD/CMOS image sensor	M
Ear	M	L	-	Camera	CCD/CMOS image sensor	M
Shape of X-rayed teeth	M	L	-	X-ray machine	X-rays	L
DNA	L	H	100 kb	Lab environment	Testing in lab	H
Voice	H	L	-	Microphone	Converting signals	M
Signature	H	M	20 kb	Tablet, Touch panel	Capacitive, resistive, acoustic	M
Typing rhythm	M	L	-	Keyboard, special software	Software based	L

Table 4: [26] [18] [8]

4.5 Evaluation 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 Rejectance 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.
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 [23]. 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.

	False Acceptance Rate	False Rejectance Rate	Crossover Error Rate	Failure To Enrollment	Failure To Capture Rate	Receiver Operating Char.	Sensor Subject Distance
Iris	0.94 %	0.99 %	0.01 %	0.5 %	-	-	30 cm
Retinal	0.99 5	1 %	0.04%	0.8%	-	-	2 cm
Finger Print	2 %	2 %	2 %	1 %	-	-	Zero
Palm Print	-	-	-	-	-	-	Zero
Hand geometry	2 %	2 %	1 %	NA	NA	-	10 cm
Face	1 %	20 %	-	NA	NA	-	~ 20 m
Ear	-	-	-	NA	NA	-	~ 5 m
Shape of X-rayed teeth	-	-	-	-	-	-	50 cm
DNA	-	-	-	-	-	-	Zero
Voice	2 %	10 %	6 %	-	-	-	20 cm
Signature	-	-	-	-	-	-	Zero
Typing rhythm	7 %	0.1 %	1.8 %	-	-	-	Zero

Table: 5 [27]

4.6 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 11 and figure 12.

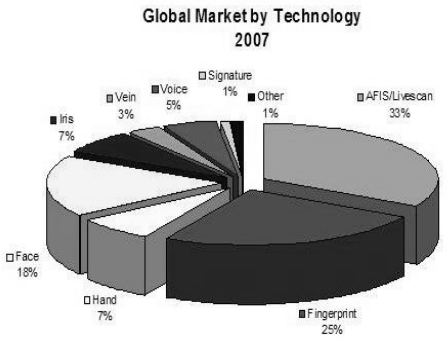

Figure: 11 [28]

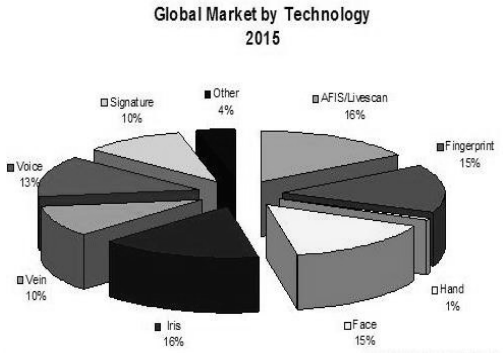

Figure: 12 [29]

V. Conclusion

A Biometric recognition or biometrics, refers to the automatic identification of a person based on his/her physiological (e.g., fingerprint, iris) or behavioral (e.g., signature) characteristics. This method of identification offers several advantages over traditional methods involving ID cards (tokens) or PIN numbers (passwords) for various reasons for example acquired and measured for the processing only in the presence of a person. Hence these systems are proved highly confidential computer based security systems. Each and every biometric system is useful and selection of particular biometric device depends upon the application area, i.e. where we are going to deployed biometric technology. Mainly it depends upon the number of persons, which are going to recognize himself or herself as well as environments. In case of limited persons we can use a biometric technology as less time taken but more secured than other biometric technology used where unlimited persons are recognized fastly but little bit accuracy. As my comparison show a number of differences based upon different aspects so one can easily choose the biometric technology for deployment in real time.

VI. References

[1] Himanshu Srivastava, "Personal Identification Using Iris Recognition System, a Review," *International Journal of Engineering Research and Applications (IJERA),* vol. 3, no. 3, pp. 449-453, 2013.

[2] 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.*

[3] Simon Liu and Mark Silverman, "A Practical Guide to Biometric Security Technology," *IT Pro* 27-32, 2001.

[4] http://www.amazingincredible.com/show/82-the-incredible-human-eye [Online] [26 April, 2013].

[5] Debnath Bhattacharyya, "Biometric Authentication: A Review," *International Journal of u- and e- Service, Science and Technology*, vol. 2, no. 3, 2009.

[6] D. Zhang and W. Shu, "Two Novel Characteristic in Palmprint Verification: Datum Point Invariance and Line Feature Matching," *Pattern Recognition*, vol. 32, no. 4, pp. 691-702, 1999.

[7] 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, 2007, pp. 91 – 96.

[8] 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.

[9] A. K. Jain, A. Ross, and S. Pankanti, "Biometric: A Tool for Information Security," *IEEE Trans. Information Forensics and Security*, vol. 1, no. 2, pp. 125–144, 2006.

[10] E. Kukula, S. Elliott, "Implementation of Hand Geometry at Purdue University's Recreational Center", *In Proc. of 35th Annual International Carnahan Conference on Security Technology*, UK, 2001, pp. 83 – 88.

[11] "Biometrics and standards ITU-T Technology watch report," 2009.

[12] M. A. Dabbah, W. L. Woo, and S. S. Dlay, "Secure Authentication for Face Recognition," *In Proc. of IEEE Symposium on Computational Intelligence in Image and Signal Processing*, USA, pp. 121 – 126, 2007.

[13] 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 Biometric*, vol. 14, no. 1, pp. 4–20, 2004.

[14] 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.

[15] Jitendra Choudhary, "Survey of Different Biometrics Techniques**,"** *International Journal of Modern Engineering Research (IJMER),* vol. 2, no. 5, pp-3150-3155, 2012.

[16] J. Ortega-Garcia, J. Bigun, D. Reynolds, J. Gonzalez-Rodriguez, "Authentication gets personal with biometrics, " *IEEE Signal Processing Magazine*, vol. 21, no. 2, pp. 50-62, 2004.

[17] F. Monrose, A.D. Rubin, "Keystroke dynamics as a biometric for authentication," *Future Generation Computer Systems*, vol. 16, no. 4, pp. 351-359, 2000.

[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] A. K. Jain, R. Bolle, and S. Pankanti, "Biometrics: Personal Identification in Networked Society," *Kluwer Academic Publishers*, 1999.

[20] Paul Reid, "Biometrics for network security," [Text book], [2004].

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

[22] D.Maltoni, A.K.Jain, "Hand book fingerprint recognition," [Online]. Available: http:// bias.csr.UnIbo.it/ maltoni/handbook, [2009].

[23] Padma, Manivannan, "Comparative and Analysis of Biometric Systems" *International Journal on Computer Science and Engineering (IJCSE,) v*ol. 3, no. 5, pp2156-2162, 2011.

[24] Tilo Burghardt, "A brief review of biometric identification," University of Bristol, UK.

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

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

[27] Ben Edgington, "Introducing Hitachi's Finger Vein Technology," *A White Paper*, 2007.

[28] International Biometric Group, "Biometrics Market and Industry Report 2007-2012", 2007.

[29] International Biometric Group, "Biometrics Market and Industry Report 2010-2015", 2010.