Volume 4, Issue 7, July 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Biometrics: 21st Century Technology of Authentication and Security

Prachi P Bansal
CSE, M.Tech Scholar
Galaxy Global Imperial Technical Campus
India

Saurabh Mittal
CSE, Associate Professor
Galaxy Global Imperial Technical Campus
India

Maanak Gupta
CSE, Assistant Professor
DIT University, Dehradun
India

Abstract- with the advancement in information technology, information security has become an indispensable part of it. Authentication plays an inevitable role when it comes to security and privacy. This is a review paper which briefs the various biometric authentication techniques and the future prospects in this area. In biometric recognition, automated recognition of individuals is done based on a feature set(s) derived from their behavioral and/or physiological characteristic. Computing systems require reliable and secure personal recognition and authentication schemes to either determine or confirm the identity of an individual requesting their services. Applications include secure electronic banking, computer systems security, credit cards, mobile phones, health and social services, secure access to buildings. By using biometrics a person could be identified based on "who she/he is" rather than "what she/he has" (card, token, key) or "what she/he knows"(password, pin). In this paper, how the biometrics has become the integral part of security has been discussed. We have also discussed and compared various techniques based on their performance metrics.

Keywords- Biometrics, Multimodal Biometrics, Recognition, verification, Identification, Security

I. Introduction

Today, large numbers of applications require reliable verification schemes to confirm the identity of an individual. Conventional ways like password and id cards can easily be breached and are unreliable. Body characteristics of humans such as face, voice, gait, etc. have been used since ages for recognition. Biometric cannot be stolen, forgotten or borrowed and forging the biometric is practically impossible. The term *biometric* comes from the Greek words *bios* (life) and *metrikos* (measure). Biometric authentication supports the facet of identification, authentication and non-repudiation in information security. The features in biometrics are face recognition, fingerprints, handwriting, hand geometry, iris, vein, voice and retinal scan. Biometric technique is now the foundation of numerous highly secure identification and personal verification. As the level of security breach and transaction scam increases, the need for well secure identification and personal verification technologies is becoming apparent. A biometric system can be either an 'identification' system or a 'verification' (authentication) system. In this paper, we comprehensively discuss on Biometric technology and we believe that this review will definitely provide a limelight on the past, present and future aspects of this field.

II. Biometric Systems

A biometric system is a pattern-recognition system that recognizes a person based on a feature set derived from a specific physiological or behavioral characteristic that the person possesses [1]. That feature set is usually stored in a database after being extracted. Based on requirements, the system can have two modes: *verification* or *identification*. Verification validates the person's identity by comparing the captured feature set with his/her own biometric feature set that is already stored in the database. In such a case the individual has an identification number, user name etc. and the system performs one to one comparison to validate the claim. For example one can grant access to bank account at ATM using retina scan or finger print scan. Formally verification can be posed as: given a feature set Y_e (taken from biometric data) and identity I, the system need to determine if (I, Y_e) belong to class c_1 *or* c_2, where c_1 indicates true identity and c_2 indicates false. Y_e is matched against Y_d (the biometric template of identity I), to determine its category. Hence,

$$(I, Y_e) \epsilon \quad \begin{vmatrix} \mathbf{c_1} & \textbf{if } S(Y_e, Y_d) \geq \mathbf{t,} \\ \mathbf{c_2} & \textbf{otherwise,} \end{vmatrix}$$

where S measures the similarity between Y_e and Y_d , and t is defined threshold. The value $S(Y_e, Y_d)$ is termed as matching score between two feature set. Identification involves recognizing an individual by searching the acquired biometric information against templates corresponding to all users in the database. Hence it is a one to many comparisons to establish individual's identity. This is used to determine a person's identity without his approval. For example, scanning a crowd with the help of a camera and using face recognition technology, one can verify matches with already stored database template [2].

Identification, on the other hand can be defined as: given an input feature set Y_e determine the identity I_f , f= {1,2,3,4…N, N+1}. Here I_1 , I_2 , ...I_N. are the identities of people enrolled in the database and I_{N+1} defines the rejection case where no suitable identity can be found. Hence

$$Y_e \in \left| \begin{array}{ll} I_f & \text{if } \max\{S(Y_e, Y_{If})\} \geq t, \text{ k=1,2,..N,} \\ I_{N+1} & \text{otherwise,} \end{array} \right.$$

where Y_{If} is the template corresponding to identity I_f and t is threshold.

Figure 1 shows the block diagram of biometric system. The system has various modules.

1) *Sensor module* is used to acquire the biometric data of an individual.

2) *Feature extraction module,* in which the acquired data from the sensor is processed to extract salient feature set of an identity.

3) *Matcher module* where feature during recognition are compared against those stored in the template to generate matching scores.

4) *Decision-making module* in which the user's identity is created or a claimed identity is accepted or rejected [10,21,28].

5) Database module which is used to store the biometric templates and features of the enrolled users.

Any physiological or behavioral feature can work as a biometric characteristic as long as it satisfies the requirements of universality, distinctiveness, permanence, collectability etc. [3].

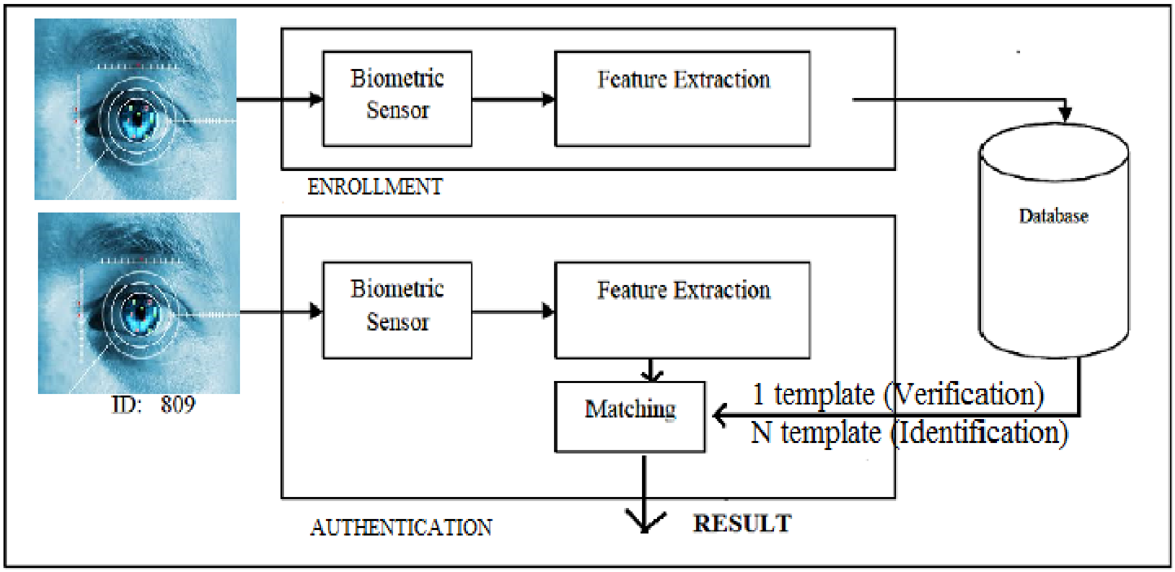

Fig. 1 Block diagram of Biometric system and various modules associated

III. Technologies Involved In Biometrics

There are various technologies being used in biometrics. Each biometric has its advantages and disadvantages over each other based on the various performance characteristics. The choice of the biometric depends on the application in which it is used. A brief introduction of various biometric technologies will be discussed below:

A. Facial, hand, and hand vein infrared thermo gram

Human body radiated heat and this pattern is unique for each person. This pattern is captured using the infrared camera in an unobtrusive way similar to normal photography. The technology could be used for covert recognition [4, 5, 10]. Though the technology is noninvasive but image capture is difficult if other heat emitting surfaces are their near to body. Although it is true that face thermo grams are unique to each individual, it has not been proven that face thermo grams are sufficiently discriminative. Near infrared imaging technology can also be used to scan the rear side of a clenched fist to determine the structure of hand vein. Infrared light is absorbed by the veins under the skin and thus have a darker pattern on the image of the hand taken by an infrared camera. The hand vein geometry is one of the upcoming technology and in the process of development. The price of infrared sensors is high which makes this technology less pervasive.

© 2014, IJARCSSE All Rights Reserved

B. Ear shape

The shape of the ear and structure of cartilaginous tissue of the pinna are assumed to be distinct for each individual. Matching the distance of salient points on the pinna from a landmark location of the ear is the suggested method of recognition [6]. This method is not very distinctive. Identifying individuals by the ear shape is used in law enforcement applications where ear markings are found at crime scenes.

C. Gait

It is a manner in which one walks and involves complex spatio-temporal biometric technology. The technology is not considered to be very distinctive but could be used for low level security applications. Since gait is a behavioral biometric, it may not remain the same over a long period of time as it depends on body weight and other factors. Acquiring gait is similar to acquiring facial picture. Gait-based systems are input intensive and computationally expensive as the video-sequence footage of a walking person is used to measure various different movements of each articulate joint [3,9].

D. Hand Geometry

It is based on the fact that various dimensions of human hand, including its shape, location of joints, size of palm and length and width of fingers can be used as biometric characteristic. These characteristics do not change after certain age. Hand geometry-based biometric systems have been installed at hundreds of locations around the globe. The technique is very easy, simple, and comparatively less expensive. External factors like dry skin do not have an impact on the identification accuracy. It is generally used as a verification technique and using in identification mode is not desirable. Limitation of this is low discriminative capability [7,18].

Hand geometry information may not be invariant over the lifetime of an individual, specifically during childhood. In addition, an individual’s jewelry or limitations in dexterity (for example, from arthritis), may pose challenges in digging out the accurate hand geometry information and specification. Verification systems based on fingers are also used and could be easily seen in laptops also.

E. DNA

Deoxyribonucleic acid (DNA) is probably the most reliable biometrics. Presently DNA sampling is intrusive and requires a form of tissue, blood or other bodily sample. It is in fact a one-dimensional code unique for each person. Exception is identical twins. This method, however, has some drawbacks: 1) contamination and sensitivity, as it is easy to take a piece of DNA from an individual and use it for an illegally, 2) DNA matching requires complex chemical compositions involving dexterous skills, hence real-time application is not possible, 3) privacy issues since DNA sample taken from an individual is likely to show susceptibility of a person to some diseases [11,14] .

Biometric Systems DNA, at present, is inevitable in crime detection and will be an integral part of law enforcement for long time.

F. Odor

Each object emanates odor or smell which characterizes its chemical composition. This odor can also be used to distinct two individuals. The air surrounding the object is blown into a number of chemical sensors, each sensitive to a certain group of compounds. Human smell is composed of chemicals known as volatiles. These volatiles are extracted by the system and converted into a template. The use of deodorants and perfumes make it more difficult to distinguish objects [12].

G. Speech

Voice is both, physiological and behavioral biometrics because every person has a different pitch but voice recognition is mainly the way a person speaks, commonly as behavioral. Physical characteristics like mouth, vocal tracts, lips, nasal cavities do affect the features of a person’s voice. The physiological characteristics of speech are do not change for an individual, but the behavioral part changes over time due to medical conditions (such as common cold), age, emotional state, etc. Acoustic feature, which is considered different for each individual is used in speaker recognition [13,17].

A predetermined phrase is used in case of text-dependent voice recognition system. In case of text-independent voice recognition, the speaker is recognized irrespective of what he/she speaks. A text independent system is more difficult to design than a text-dependent system but offers more protection against fraud. However, speech-based features are sensitive to a various factors such as background noise as well as the physical and emotional state of the speaker. Speech-based authentication is currently restricted to low-security applications because of high variability in an individual’s voice and poor accuracy performance of a typical speech-based authentication system.

H. Face

This is the most pervasive technology used for personal recognition. It is a non-intrusive method and is suitable for covert applications. The facial recognition applications range from a static, controlled “mug-shot” verification to a dynamic, uncontrolled face identification in a cluttered background (e.g., airport). Feature set is extracted from a two-dimensional image of the user's face and is matched with the stored template in database. Commonly used approaches to face recognition are based on location and shape of facial attributes like eyes, nose, lips, eyebrows etc.; the overall (global) analysis of the face image that represents a face as a combination of canonical faces. Although the systems performance is reasonable, the systems have difficulties in recognizing face from images captured from various angles and different ambient illumination conditions. It is also questionable if face itself is sufficient for recognizing a person from a large group with an extremely high level of confidence [16,25]. Another issue is the fact that different expressions display face in different figure.

I. Palmprint

Similar to fingerprints, palms also have unique pattern of ridges and valleys. As, surface of palm is bigger, it is expected to be more reliable than fingerprint. As the scanners scan larger area, they are bulkier and more expensive. Human palms also have additional distinctive features such as wrinkles and principal lines that can be captured with a lower resolution scanner, which is cheaper. A more accurate biometric system could be combined by using a high-resolution palmprint scanner that would collect all the features of the palm such as hand geometry, ridge and valley features, principal lines, and wrinkles [17,20,27].

J. Retina scan

Blood vessels at the rear side of the retina, have pattern which is unique for each individual forms the basis of retina scan biometric technique. These patterns create an eye signature from the vascular configuration of the retina. It is most secure as retinal vasculature is not easy to change. Digital images of retinal patterns can be acquired by projecting a low intensity beam of visual or infrared light into the eye and capturing an image of the retina using optics similar to a retina scope. The image acquisition involves cooperation of the identity, requires contact with the eyepiece, and a conscious effort of the user. The technique requires user to see into an eye piece and focus on a specific spot in the visual field so that the predetermined and stored part of the retinal vasculature could be imaged. Also retinal scan can reveal some medical conditions and as such public acceptance is questionable [15,19].

K. Keystroke dynamics

It is assumed that each person types on a keyboard in a characteristic manner. This is not very distinctive but offers enough uniqueness to discriminate identities. As key stroke is a behavioral biometric, one could expect large variations in typing patterns. The user can be verified at the log-on stage or they can continually monitor the Biometric Systems 32 typist. These systems are cheap to install as it requires only software package [19,21,22].

L. Fingerprint

Fingerprint is an impression of the ridges and furrows located on the surface of a fingertip. The formation of fingerprint is determined during the first seven months of fetus development. A friction ridge is a raised portion on the digits (fingers and toes) or plantar (sole) skin or palmar (palm), which consists of one or more connected ridge units of friction ridge skin. These ridges are also called "dermal "or "dermal ridges “. Traditionally, finger prints were taken by applying ink on the fingertip and taking the impression of the finger on the paper. Nowadays sensors are used to create digital image of the pattern. The accuracy of available fingerprint systems is good enough for verification systems. Since the scanning device is actually touched by the finger, its surface can become greasy and oily after using repeated which in turn could reduce the reliability, sensitivity and accuracy of optical scanners. This problem could be resolved with solid state sensors as the coated silicon chip itself is the sensor. In real-time verification systems, the feature extraction module use the image captured by sensors to derive the feature set. The feature values usually correspond to the orientation and position of certain critical and important points known as minutiae points. Minutiae based and Correlation based is two types of Finger print matching techniques [20, 23].

In Minutiae based techniques, minutiae points are figured out and are then mapped to relate their placement on the finger. In Correlation based techniques, the exact location of a registration point is required. The positions could be affected by image translation and rotation. In matching process, the two-dimensional minutiae patterns extracted from the user's print are compared with those in the stored template. One drawback of fingerprint recognition systems is that they require a large amount of computational resources.

M. Iris

The colored area that surrounds the pupil is called iris. These Iris patterns are unique and are obtained with the help of video based image acquisition system. The visual texture of the iris is created during fetal development and gets stabilized during the first two years. This complex iris texture contains very distinctive information which is used for personal recognition. The pattern can contain many distinct features such as furrows, crypts, freckles, arching ligaments, rings, ridges, corona and a zigzag collarets. Surgically tampering the texture of the iris is very difficult. Since the iris response change with light, it can provide an important supplementary verification that the iris presented belongs to a particular user. Two identical twins also have different iris. A careful balance of focus, resolution, light and contrast is required to extract a feature set from localized image. While the iris seems to remain the same during adulthood, it varies somewhat up to adolescence [22,24]. Although the early iris-based identification systems required considerable user participation and were expensive, efforts are underway to build more user-friendly and cost-effective versions.

N. Signature

Each person has a unique way to mark the signature. Signature is concrete, simple expression of the unique variations in human hand geometry. Signatures are a behavioral biometric that change over a period of time and are influenced by physical and emotional conditions of the signatories. The identification accuracy of systems based on this highly behavioral biometric is reasonable but does not appear to be sufficiently high to lead to large-scale recognition. Two approaches are used in identification based on signature: static and dynamic. The geometric (shape) features of a signature are used in static signature, whereas dynamic (online) signature identification uses both the geometric (shape) features and the dynamic features such as acceleration, velocity, pressure, and trajectory profiles of the signature. Apart from the general shape of the signed name, velocity and pressure of the point of stylus across the sensor writing pad can also be measured by signature recognition system [25].

A brief comparison of various technologies is outlined in Table I [2,4].

TABLE I
COMPARISON OF VARIOUS BIOMETRIC TECHNOLOGIES. HIGH, MEDIUM, AND LOW ARE DENOTED BY H, M, AND L, RESPECTIVELY.

Biometric Technique	**Distinctiveness**	**Permanence**	**Performance**	**Circumvention**	**Universality**	**Collectability**	**Acceptability**
Facial thermo gram	H	L	H	L	H	L	L
Ear shape	M	H	M	M	M	M	H
Gait	L	L	L	M	M	H	H
Hand Geometry	M	M	M	M	M	H	M
DNA	H	H	H	L	H	L	L
Odor	H	H	L	L	H	L	M
Speech	L	L	L	H	M	M	H
Face	L	M	L	H	H	H	H
Palm print	H	H	H	M	M	M	M
Retina scan	H	M	H	L	H	L	L
Keystroke dynamics	L	L	L	M	L	M	M
Fingerprint	H	H	H	L	M	M	H
Iris	H	H	H	L	H	M	L
Signature	L	L	L	H	L	H	H

IV. Performance Of Biometric Systems

Security is an important issue when it comes to use of biometric authentication. Evaluating the performance of a technique is a challenging research area. Due to different positioning on the acquiring sensor, imperfect imaging conditions, environmental changes, deformations, noise and bad user's interaction with the sensor, it is impossible that two samples of the same biometric characteristic, acquired in different sessions, exactly coincide. Biometric systems are not perfect, and will sometimes mistakenly accept an impostor as a valid individual (a false match) or conversely, reject a valid individual (a false non match) [27,28].

© 2014, IJARCSSE All Rights Reserved

The main system errors are usually measured in terms of:

A. *False Reject Rate (FRR) or False Non-Match Rate (FNMR):* It is the probability that the system incorrectly declares failure of match between the matching template and input pattern. It measures the percentage of valid inputs being rejected.

B. *False Match Rate (FMR) or False Accept Rate (FAR):* The probability that the system incorrectly determines a successful match between the input pattern and a nonmatching pattern in the database. These systems are important as they are commonly used to stop certain actions by disallowed people [1,10]. It measures the percentage of invalid matches

FNMR and FMR are basically functions of the system threshold *t*: if the system's designers decrease *t* to make the system more tolerant to input variations and noise, FMR increases. On the other hand, if they raise *t* to make the system more secure, FNMR increases accordingly.

C. *Relative Operating Characteristic (ROC)*: In biometric systems the FAR and FRR can typically be traded off against each other by changing those parameters. The values of FRR and FAR can be graphed to create a ROC plot. A Detection Error Tradeoff (DET), which is a common variation , can be obtained using normal deviate scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).

Figure 2 shows the trade-off between a system's FMR and FNR at different operating points; it's called the "Receiver Operating Characteristics (ROC)" and is a comprehensive measure of the system accuracy in a given test environment. High-security access applications, where concern about break-in is great, operate at a small FMR. Forensic applications, where the desire to catch a criminal outweighs the inconvenience of examining a large number of falsely accused individuals, operate their matcher at a high FMR. Civilian applications attempt to operate their matchers at the operating points with both a low FNR and a low FMR. The error rate of the system at an operating point where FMR equals FNR is called the equal error rate (EER) which may often be used as a terse descriptor of system accuracy [25,26].

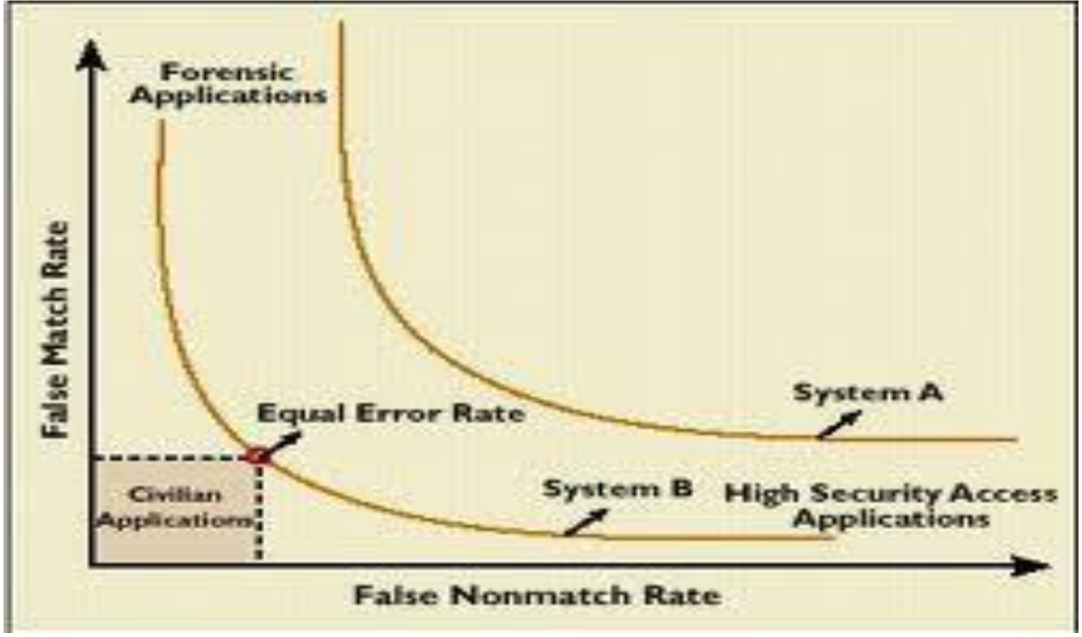

Fig. 2 Receiver Operating Characteristic

There are two other recognition error rates that can be also used and they are: *failure to capture* (FTC) and *failure to enroll* (FTE). FTC denotes the percentage of times the biometric device fails to automatically capture a sample when presented with a biometric characteristic. This usually happens when system deals with a signal of insufficient quality. The FTE rate denotes the percentage of times users cannot enroll in the recognition system. Figure 2 shows the ROC characteristics of a system illustrating FNR and FNMR of a matcher at various operating points [22,23,25].

Accuracy performance of a biometrics system is considered acceptable if the risks (benefits) associated with the errors in the decision-making at a given operating point on ROC for the given test environment are acceptable. Similarly, accuracy of a biometrics-based identification is unacceptable/poor if the risks (benefits) associated with errors related to any operating point on the ROC for a given test environment are unacceptable (insufficient). The human factors issue is also important to the success of a biometric-based identification. Additionally, biometric technologies requiring very little cooperation/participation from the users (such as face and thermo grams) may be perceived as more convenient to users [27].

V. Discussion And Conclusion

Biometric authentication and security is highly reliable since forging the physical human characteristics are much more difficult than passwords, security codes and hardware keys. There are lots of applications and solutions in biometrics technology used in security systems, which can improve our lives such as: improved security, it is reduced con and password administrator costs, easy to use and make life more secure and comfortable. Standardized token-based and knowledge-based methods do not provide positive personal recognition as they are based on surrogate representations of the person's identity [28]. Though biometric are highly secure, they are not a perfect solution. The use of biometrics raises several privacy questions. A robust security system design will require the blend of both biometric and non-biometric components to provide reliable personal authentication and recognition. Just the inclusion of biometric in security is not enough to make systems more secure, the strong and basic principles of system design and engineering are still required. Distribute database used in biometric can easily be compromised, in particular where the privacy of individuals and hence irrevocability and non-repudiation are a matter of concerned. Meticulous importance and deliberation should be given to how biometric data can be secured and legally protected. A sound trade-off between security and privacy may be necessary; but we can only enforce collective accountability and acceptability standards through common legislation. As biometric is upcoming and booming field its future cannot be predicted so early. How biometrics can be embedded in day to day use and in applications still need to be more researched. But still it is true that biometric will have a profound influence on our life in days to come.

REFERENCES

[1] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric Recognition: Security and Privacy Concerns", *IEEE Security and Privacy Magazine*, Vol. 1, No. 2, pp. 33-42, 2003.

[2] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, NY, 2003.

[3] K P Tripathi, *International Journal of Computer Applications* (0975 – 8887) Volume 14– No.5, January 2011

[4] Zdeneˇk R íhaVáclav Matyáš "*Biometric Authentication Systems*", FI MU Report Series, November 2000.

[5] Bonsor, K. "*How Facial Recognition Systems Work*". Retrieved 2008-06-02.

[6] Yongsheng Gao; Leung, M.K.H., *"Face recognition using line edge map"*, Pattern Analysis and Machine Intelligence, IEEE Transactions on , Volume: 24 Issue: 6 , June 2002, Page(s): 764 -779.

[7] Pentland, A.; Choudhury, T. *"Face recognition for smart environments "*, Computer, Volume: 33 Issue: 2, Feb. 2000, Page(s): 50 -55.

[8] Yooyoung Lee, James J. Filliben, Ross J. Micheals, P. Jonathon Phillips, "Sensitivity analysis for biometric systems: A methodology based on orthogonal experiment designs", Computer Vision and Image Understanding, Volume 117, Issue 5, May 2013, Pages 532-550.

[9] Ujwalla Gawande, Mukesh Zaveri, Avichal Kapur," Bimodal biometric system: feature level fusion of iris and fingerprint", Biometric Technology Today, Volume 2013, Issue 2, February 2013, Pages 7-8.

[10] Hisham Al-Assam, Sabah Jassim, "Security evaluation of biometric keys", Computers & Security, Volume 31, Issue 2, March 2012, Pages 151-163.

[11] Prokoski, F.K. Disguise detection and identification using infrared imagery. In the P*roceedings of SPIE, Optics, and Images in Law Enforcement II*. A.S. Hecht, Ed. (Arlington, VA, May, 1982), 27–31.

[12] Amioy Kumar, Shruti Garg, M. Hanmandlu, " Biometric authentication using finger nail plates", Expert systems with applications, Volume 41, Issue 2, 1 February 2014, Pages 373-386.

[13] Soumyasree Chakraborty, Indrani Bhattacharya, Amitava Chatterjee, "A palmprint based biometric authentication system using dual tree complex wavelet transform", Measurement, Volume 46, Issue 10, December 2013, Pages 4179-4188.

[14] L. I. Kuncheva, C. J. Whitaker, C. A. Shipp, and R. P. W. Duin, "Is Independence Good for Combining Classifiers?", *Proc. International Conference on Pattern Recognition (ICPR)*, Vol. 2, pp. 168-171, Barcelona, Spain, 2001.

[15] J.A. Unar, Woo Chaw Seng, Almas Abbasi, "A review of biometric technology along with trends and prospects", Pattern Recognition, Volume 47, Issue 8, August 2014, Pages 2673-2688.

[16] R. Brunelli and D. Falavigna, "Person Identification Using Multiple Cues", *IEEE Trans. onPattern Analysis and Machine Intelligence*, Vol. 12, No. 10, pp. 955-966, Oct 1995.

[17] R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, A. W. Senior, *Guide to Biometrics.* Springer, 2003.

[18] Martti Juhola, Youming Zhang, Jyrki Rasku, " Biometric verification of a subject through eye movements", Computers in Biology and Medicine, Volume 43, Issue 1, 1 January 2013, Pages 42-50.

[19] FVC2004: Fingerprint Verification Competition, http://bias.csr.unibo.it/fvc2004.

[20] A. Ross and A. K. Jain, "Information Fusion in Biometrics", *Pattern Recognition Letters*, Vol. 24, Issue 13, pp. 2115-2125, September 2003.

[21] A. K. Jain, S. C. Dass and K. Nandakumar, "Soft Biometric Traits for Personal Recognition Systems", To appear in *Proceedings of International Conference on BiometricAuthentication*, Hong Kong, July 2004.

[22] A. K. Jain and A. Ross, "Multibiometric Systems", *Communications of the ACM, Special Issue on Multimodal Interfaces*, Vol. 47, No. 1, pp. 34-40, January 2004.

[23] A. Ross, S. Dass and A. K. Jain, "A Deformable Model for Fingerprint Matching", *Pattern Recognition*, 2004.

[24] C. Ensibi, M. Pérez-López, F. Soler Rodríguez, M.P. Míguez-Santiyán, M.N. Daly Yahya, D. Hernández-Moreno," Effects of deltamethrin on biometric parameters and liver biomarkers in common carp", Environmental Toxicology and Pharmacology, Volume 36, Issue 2, September 2013, Pages 384-391.

[25] Peiyang Shen, Yingfeng Zheng, Xiaohu Ding, Bin Liu, Nathan Congdon, Ian Morgan, Mingguang He," Biometric measurements in highly myopic eyes", Journal of Cataract & Refractive Surgery, Volume 39, Issue 2, February 2013, Pages 180-187.

[26] Abiyev, R.H. Altunkaya, K., "Neural Network Based Biometric Personal Identification", Frontiers in the Convergence of Bioscience and Information Technologies, Jeju, Oct. 2007, pp. 682 – 687.

[27] Umarani Jayaraman, Surya Prakash, Phalguni Gupta," Use of geometric features of principal components for indexing a biometric database", Mathematical and Computer Modelling, Volume 58, Issues 1–2, July 2013, Pages 147-164

[28] Amioy Kumar, M. Hanmandlu, H.M. Gupta, "Fuzzy binary decision tree for biometric based personal authentication", Neurocomputing, Volume 99, 1 January 2013, Pages 87-97