# Human Recognition Methods based on Biometric Technologies

Annu Sharma
Research Scholar
Department of Computer Science & Technology, GKV, Haridwar, Uttarakhand, India

Praveena Chaturvedi, Ph.D
Associate Professor
Department of Computer Science & Technology, KGC, Dehradun, Uttarakhand, India

Shwetank Arya, Ph.D
Assistant Professor
Department of Computer Science & Technology, GKV, Haridwar, Uttarakhand, India

## ABSTRACT
Biometric has revolutionized the Human Recognition Technology .The base and reach of human recognition system has been expanded by the innovative uses of Biometric devices .Human recognition have becomes one of the most well-off fields in the past ten years. Biometrics is the science of establishing the identity of an individual based on physical, chemical or behavioural attributes of the person; it deals with the automated recognition of individuals based on biological and behavioural characteristics. Biometrics spread its wings in a wide range of applications and found itself as a reliable source in fields such as electronic data security, ecommerce, internet access, physical access control, PDA, Government applications such as national ID card, social security, welfare-disbursement, border control, military surveillance, etc As the application areas are emerging, the implementation of biometric systems in both commercial and government sectors is increasing and therefore leading to enormous security breaches in the installed systems. Currently, the most effective means of Human Recognition is to use biometric system. So while designing biometric system, security of the system is one of the factors which have to be considered along with the increasing performance at reasonable costs. The objective of this paper is to explore the potential of fast developing Biometric systems such as fingerprints, face recognition, iris recognition for human identification. This paper discusses the main features of the biometric system: architecture, evaluation methodology used in these system and also various issues related to security of the biometric system.

## Keywords
Biometric, Face Recognition, Iris Recognitions, template matching

## 1. INTRODUCTION
The human recognition system is now a desired requirement of our security and surveillance systems. Biometric recognition is a crucial tool being used in commercial, government and forensic applications .The term biometrics is derived from the Greek words bios and metron which literally translates as life measurement. The national Institute of Standards and Technology defines 'biometric' as the automatic recognition of a person based on physiological or behavioral characteristics [5]. Biometrics is the use of physical or behavioral traits to verify personal identity. It is defined as the automated use of physiological or behavioral characteristics to determine or verify an individual's identity. The above characteristics include visual images like fingerprints, face, iris and other human phenomena such as speech, gait, DNA, and indeed anything at all which might help to uniquely identify the individual [2][3]. In general terms, a biometric is observed data of a human that allows the identity of that person to be determined. Traditional personal authentication systems are either knowledge based (e.g., password) or possession based (e.g., ID card) they are not able to meet strict security performance requirements of a number of modern applications. The traditional approaches are unable to differentiate between an authorized person and an impostor (person pretending to be somebody he/she is not) Biometric systems are good alternatives to traditional methods because the traits used in these systems are not easily changed or imitated, and they cannot be forgotten as in the case for passwords, nor can they be lost in the same manner as identification cards. These biometric systems are more reliable as the data cannot be lost and are more user-friendly as the person has nothing to remember or carry. Every biometric system has its own strengths and weaknesses; however, for a biometric to be effective it should have the following requisite properties:

(1) Universality (every person should have that characteristic)

(2) Uniqueness (no two people should be exactly the same in terms of that characteristic)

(3) Permanent (invariant with time)

(4) Collectable (can be measured quantitatively)

(5) Reliable (must be safe and operate at a satisfactory performance level)

(6) Acceptable (non-invasive and socially tolerable)

(7) Non-circumvent able (how easily the system is fooled into granting access to impostors) [1] [4].

## 2. ARCHITECTURE OF BIOMETRIC SYSTEM
The system working of biometric system can be explained with the help of the following units which describes the architecture of the system

**2.1 Data Capturing Device:** it is a sensing device comprising of camera required to acquire the raw image of individual biometric data and this data is submitted to Feature extraction unit .The quality of the raw data is impacted by the characteristics of the sensing device.

**2.2 Feature Extraction Unit:** To improve the quality of acquired data it is subjected to image enhancement algorithm in order to improve its quality. The data is processed and a set of salient discriminatory features are extracted to represent the underlying trait. The feature set extracted is stored in database in form of template.

### 2.3 Matching and Decision making Unit:

Decision making depend on the matching of templates. The extracted features are compared against the stored template to generate match scores. The match score decides whether the enrolled individual is authentic or an impostor.

### 2.4 Database Unit:

It is repository of biometric information. During the enrolment process the templates generates from feature extraction module are stored in the database along with some information such as name, add, uid etc.[2][4].

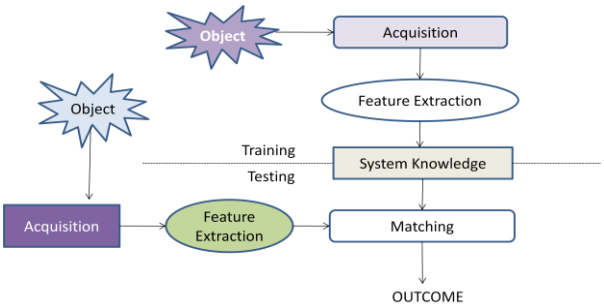


**Fig 1: Architecture of Biometric System**

## 3. BIOMETRIC SYSTEM EVALUATION

The success of any of the system depends on its performance evaluation. Identification and Verification is one of the factors for evaluating the performance of biometric system. A verification system authenticates a person's identity by comparing the captured **i**mage with her/his own biometric template(s) pre-stored in the system. It conducts one-to-one comparison to determine whether the identity claimed by the individual is true where as identification system recognizes an individual by searching the entire template of the database for a match. It conducts one-to-many comparisons to establish the identity of the individual. In Biometric system the feature set of individual are taken and compared by the process of verification and identification, it is very rare that the two feature sets of same biometric trait of a user are exactly same [22]. This may be due to sensor imperfection, alteration in user biometric characteristics or changes in ambient conditions. The variability observed in biometric feature set of an individual is referred to as inter-class variation and that between the feature set of two different individuals is known as intra-class variation. There must be small intra-class variation and large inter class variation to measure this the similarity score is used to indicate the degree of similarity between two biometric feature sets. Similarity score can be either authentic score or imposter score [23]. It is authentic or genuine if score is a result of matching two samples of same biometric trait of a user and an imposter score involves comparing two biometric trait of a sample originating from different user. The threshold value n is used to measure this score and on the basis of this threshold value the value of FAR (false accept ratio) and FRR(false reject ratio are drawn). An imposter score that exceeds the threshold value) results in a false accept. FAR of a system is defined as the fraction of imposter scores exceeding the threshold (n). A genuine score that falls below the threshold (n) results in false reject.FRR may be defined as fraction of genuine scores falling below the threshold(n)[22][23] .

The Genuine Accept rate is fraction of genuine score exceeding the threshold (n) therefore

$$GAR = 1 - FRR$$

Detection error tradeoff curve [22] is used to summarize FAR and FRR at various values of (n). It plots FRR against FAR at various thresholds on a normal deviate scale and interpolates between theses points and the resulting graph is known as ROC curve.

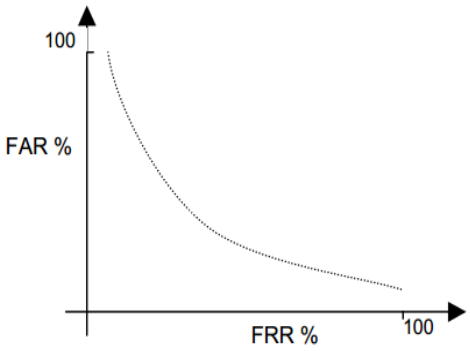


**Fig 2: Biometric System Evaluation**

The acronym ROC stands for 'Receiving Operating Characteristic', a term used in signal detection to characterize the tradeoff between hit rate and false alarm rate over a noisy channel [22]. The ROC curve with FRR's on X-axis and FAR's on Y-axis presents how these two rates are dependent each other. Biometrics systems are generally optimized towards minimizing the false accept rate, as it tends to be the more detrimental of the two error cases. Figure 2 presents an example of the ROC curve for some biometric system [23].Possibility of evaluating the ROC curve depends on the used pattern matching method. Besides the two types of error, a biometric system can encounter other types of failures such as failure to acquire (FTA) or failure to capture (FTC). FTA or FTC rate denotes the proportion of time a biometric system fails to capture a sample when characteristics trait is presented to it. This type of error is due to poor quality input or sensor wear tear.

## 4. BIOMETRIC IDENTIFICATION METHODS

### 4.1 Fingerprint Verification

Fingerprint biometric is most popular biometric and is being deployed in wide range of applications such as attendance system, e-commerce, ATM, mobile phones ,car, home, National Id card. As the sensor used to capture image are small and inexpensive, also the recognition rate in many applications is about one second, so it is well accepted by public. Fingerprints are fully formed at about seven months of fetus development and do not change throughout life and even the fingerprints of identical twins are different that is the reason it is quite popular biometric identifier [6]. The findings of [10] provide evidence to show that even our ancestors were aware of individuality of fingerprint. Earlier the acquisition of fingerprint images was performed by using ink-technique and the process was referred as offline sensing and it was mainly used for law enforcement applications. At present online finger print acquisition is done by directly sensing the finger surface with an electronic fingerprint scanner and these can be done via optical sensor(FTIR) , solid state sensor(silicon sensor) or ultrasounds sensor of these FTIR is the oldest and most used live-scan acquisition technique. The quality of fingerprint scanner, its sensing area, size and resolution influences the performance of recognition algorithm [8] [6].

### *4.1.1 Feature types*

The lines that flow in various patterns across fingerprints are called ridges and the space between ridges are valleys (width varies from 100nm to 300nm).Ridges and valleys often run in parallel; sometimes they bifurcate and sometimes they terminate. This termination and bifurcation of ridge is called minutiae which is an important feature of fingerprint. In fingerprint pattern there are regions where the ridge line assumes distinctive shapes, depending on the type of shapes these are classified into three topologies loop, delta and whorl and the core is the center of the pattern. See Figure3.1 (i) for a sample of Ridges as well as valleys and Figure 3.1 (ii) for loop, delta, whorl and core [9].

The performance of minutiae extraction algorithm and fingerprint recognition technique relies on quality of input fingerprint images. The process of fingerprint recognition involves following steps (i) Feature Extraction, (ii) Segmentation, (iii) Singularity detection, (iv) Minutiae detection and (v) Matching. The result of all these operations depend on quality of image captured and processed at various stages. The fingerprint is most accepted biometric till date although the performance evaluation of the system is very data dependent, large databases are required to obtain low error rate. Unfortunately, collection of large database is quite time consuming and expensive and also large number of attacks has been reported in fingerprint biometrics [7] [8].

## 4.2 Face Recognition

Face plays a specific role in the emerging biometric systems. Human being identify each other by recognizing each other's face rather than voice, fingers and palm when we meet someone looking at his face is the first thing we do , we recognize him and we know to whom we are interacting, if the person is stranger ,our brain store the face feature of the person along with his name so that we can recognize this person next time. Face Recognition is a similar process using a computational environment and is in great demand to solve the criminal cases, in law enforcement, homeland security, and identity management system **[18].** Numerous face recognition algorithms have been proposed which can be categorized as Feature based and Appearance based. Properties and geometric relations such as that the areas, distances, angles between the facial feature points are used as descriptor for face recognition. In geometry based face recognition various methods were proposed, which include filtering and morphological operations, Hough transform methods and deformable templates. But feature based had its limitation on auto recognition in face recognition.

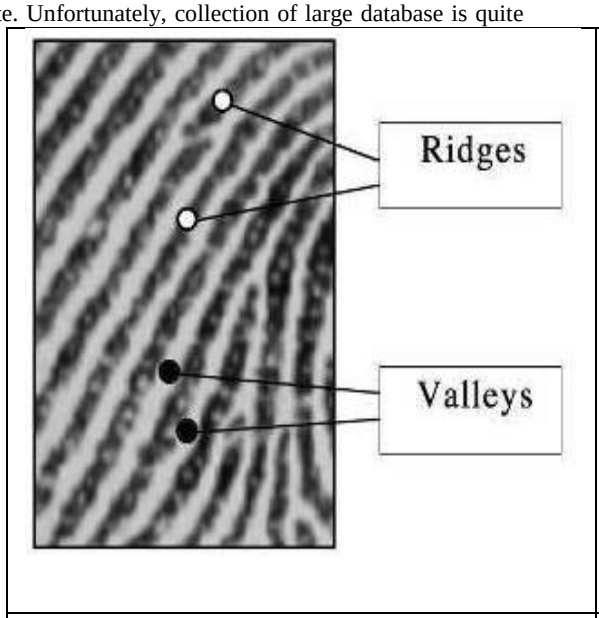


**Fig 3.1(i): Fingerprint image depicting Ridges and Valleys**

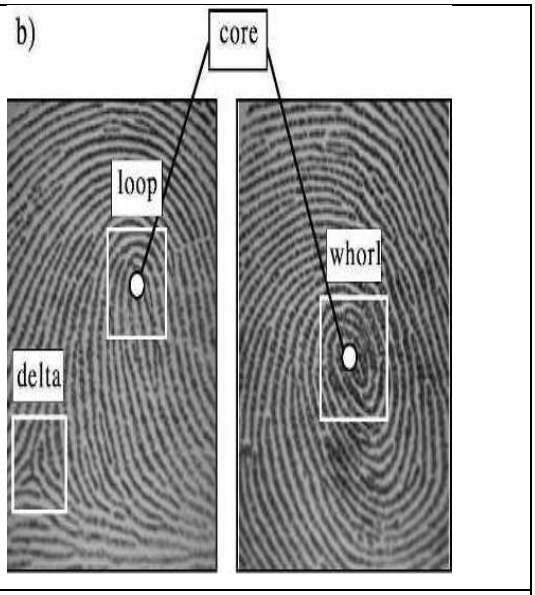


**Fig 3.1(ii): Depicting singular regions (white boxes)and core(small circles)**

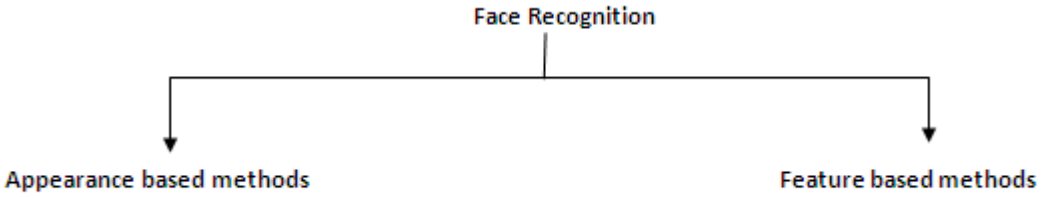


**Fig 4: Face Recognition**

Appearance based methods consider the global properties of face image intensity pattern and appearance based algorithm proceed by computing basis vectors to represent the face data efficiently .The faces are projected onto these vectors and the projection coefficient can be used for representing the face images.

Many popular algorithms such as PCA, LDA, ICA, and LFA are based on the appearance of face. In PCA the system function by projecting the face images onto a feature space that spans the significant variations among known face

$$W_{PCA} = \arg\max_{W} | W^T S_T W | = [ w_1 w_2 \dots w_m ] \quad \text{.....4.2.1}$$

images. The significant faces are known as "Eigen faces" because they are eigenvectors (principal components) of set of faces. They do not necessarily correspond to features such as eyes, ears and noses [18**]**. Eigen faces find the minimum mean squared error linear subspace that maps from the original N-dimensional data space into M – dimensional feature space. Eigen faces achieve dimensionality reduction by using the M eigenvectors of covariance matrix corresponding to largest Eigen values. The optimal basis PCA vectors are the ones that maximize the following objective function [11].

LDA seeks the optimal projection vectors which maximize the ratio of the between class scatter and the within class scatter. The optimal basis vectors of LDA can be denoted as

$$W_{LDA} = \arg\max |W^t S_B W| / |W^T S_W W| \text{.....4.2.2}$$

ICA seeks a non-orthogonal basis so that the transformed features are statistically independent .ICA generalize the concept of PCA to model high order statistical relationships.

EBGM constructs dynamic link architecture using image graphs to represent individual faces. An image graph representing a face image is a geometrical structure consisting of various nodes connected by edges. NN and SVM are usually used in low dimensional feature space due to computational complexity of the processing involved using high dimensional face data.SVM has been successfully applied for object recognition by utilizing the kernel trick which maps data onto higher dimensional feature spaces.

EBGM Face recognition algorithm uses image graphs to represent individual faces by constructing dynamic link architecture. An image graph representing a face image is a geometrical structure consisting of various nodes connected by edges .A set of complex Gabor wavelet coefficients are used as local features at each node. These Gabor wavelets contain information of multiple orientations and frequencies for each node .When performing face recognition on a new facial image , each graph in the training set is matched to the image and the best match indicates the identity of person [17][18][11].

## 4.3 Iris Recognition

The Iris recognition method is considered to be the most reliable biometric system. In this process of automated recognition person is recognized on the basis of his iris image by analyzing the random pattern of iris. The inner and outer boundaries of an iris image are demarcated at pupil and sclera by the process of segmentation. The iris is a muscle within the eye that regulates the size of the pupil, controlling the amount of light that enters the eye [29]. The iris inner and outer boundaries are termed as "Active Contours" based on discrete Fourier series expansions of the contour data. The iris develop during prenatal growth through a process of tight forming and folding of tissue membrane .prior to birth degeneration occurs , resulting in the pupil opening and the random unique pattern s of the iris .An individual irides are unique and structurally distinct, which allows for it to be used for recognition purposes [12][17].

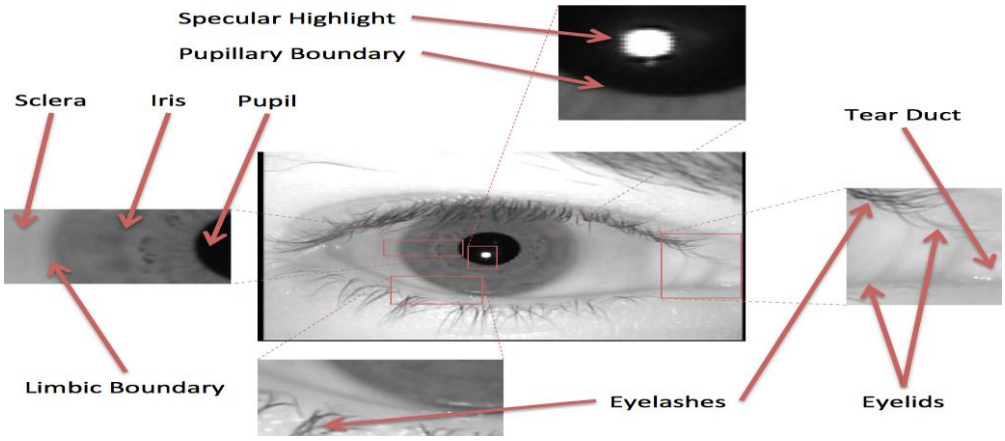


**Fig 5: Features of an Iris Image**

**Courtsey : [29]**

Iris recognition systems apply computer vision techniques to identify the pupillary and limbic boundaries to localize the iris region in an iris image. John Daugman in 1993 developed first

Iris recognition algorithm for iris biometrics. He introduced an algorithm to locate the iris region in an iris image, segment it, and produce a template that can be used for comparisons to fastly and correctly determine identity [13]. Time to time Daugman made various development to the original algorithm, and till date his system remains the basis of almost all iris recognition systems[14][15] .Iris recognition systems based on the original Daugman algorithm generally detect the iris boundaries by searching for circles, using an integro-differential operator. However, since the boundaries are not perfectly circular, alternative techniques have been implemented to segment the iris region based on ellipses or active contours [16]. After acquisition, segmentation, and normalization, iris texture features are extracted through the use of a complex filter. The author of [13] suggests a two-dimensional log-Gabor filter, which maps each pixel in the unwrapped image to a coordinate location in the complex

plane. After all processing is completed; an iris image is defined by its iris code and a corresponding mask, and is ready for matching. In matching two iris codes, Daugman's approach computes a fractional Hamming distance between iris codes as given by the following formula:

$$HD_{raw} = \frac{||(codeA \oplus codeB) \bigcap maskA \bigcap maskB||}{||maskA \bigcap maskB||} \quad \text{.....4.3.1}$$

The above equation does not consider the number of masked bits in the comparison. Comparisons with a large number of occluded bits have a higher probability of resulting in an artificially low match score [13].

## 4.4 Other Biometrics

A variety of biometrics such as speech recognition palm print, gait, ear geometry, odour, electrocardiogram, keystroke dynamics and other physiological and behavioral characteristics are being investigated to be deployed for human authentication. Speech recognition is the special area of interest of telecommunication companies [27]. The microphone is the only needed equipment its benefit is low cost in application. However the voice may be easily imitated, disguised and electronically transformed. Keystroke dynamics method is based on measuring the dynamics of the sequence of keystrokes when the user writes something on the keyboard. Raw measurements already available by the standard keyboard can be manipulated to determine Dwell time (the time one keeps a key pressed) and Flight time (the time it takes a person to jump from one key to another) Another properties may be measured when using specially designed keypads [28].

# 5. SECURITY ISSUES OF BIOMETRIC SYSTEMS

Biometrics offers greater security and convenience than traditional methods of personal recognition. In some applications, biometrics can replace or supplement the existing technology. But there are certain securities flaws present when using biometric and also some forms of biometric data do not work well in large groups such as facial scans, palm shape scans just like any other identification system, there are security issues inherent to biometric identification not only are standard security issues such as insecure databases present, but the presence of a biometric scanner invites other forms of manipulation, such as mimicking a person's gait, or providing a copied fingerprint. Biometric information is not at all private. Although privacy expert may consider it as private but Biometrics cannot be regarded as secret, our facial images are captured every time we enter a bank, airport, mall etc. Our voices are recorded by many phone based service providers. People touch door, cup, table, glass etc and leave their fingerprints everywhere. Someone may be interested in stealing our biometric credentials in order to assume our biometric identity. And we know that our facial, eye images, voice pattern, fingerprint are publically available and therefore are threat to Biometric system.

It has already been shown ,through various experiments that many if not all biometric technologies including finger print, iris ,face recognition are susceptible to spoofing attacks [19][21][5][6] .

**Table 1. Security Issues of Biometric System**

| Technology | Registration Problems | Security Problems |
|---|---|---|
| **Finger Scan** | **Dryness, cuts, bruises** | **Fingerprint Imitation** |
| **Iris and Retina** | **Drooping, Lenses** | **Iris and retina image synthesis** |
| **Face Recognition** | **Pose variation, illumination conditions** | **Face Reconstruction and mimics animation** |

There can be two basic types of failures in a biometric system, first intrinsic failures due to the limitations in hardware or software which are not caused by an outside attack. The second failure can be caused by an outside agent directly manipulating, either intentionally or accidentally, the hardware or software used in biometric system[20] .Biometric systems are vulnerable to a number of security threats. Six major types of threats are Circumvention, Repudiation, Contamination, Collusion, Coercion and Denial of service. A number of attacks have been reported in Biometric system such as a fake biometric (e.g., an artificial finger) is presented at the sensor, illegally intercepted data is resubmitted , feature detector is replaced by a Trojan horse program and It produces feature sets chosen by the attacker, legitimate features are replaced with a synthetic feature set, matcher is replaced by a Trojan horse program and It produces scores chosen by the attacker, templates in the database are modified, removed, or new templates are added, the transferred template information is altered in the communication channel or the matching result is overridden.[21] [26]. A fake biometric may be presented at the sensor, for example Synthetic Biometric Submission in which Dummy finger is created from a lifted impression of the finger without cooperation of the user with silicon cement. The Author of [24] reported that 6 fingerprint verification systems were attacked with dummy finger 5 out of 6 accepted the dummy finger in the first very attempt . Recently, the study of [25] discovered several detailed methods of creating a fake finger from silicone and gelatin to fool many commercially available fingerprint sensors. it has also been reported that Gelatin fingers are accepted with a probability of 67-100%[24]. Although producing a gummy clone of an available real finger (from a consenting user) is relatively simple, reconstructing a fake finger from a latent fingerprint remains quite complicated. In case of Face Recognition, Face reconstruction is a classical problem of criminology [18]. Many biometric systems are confused when identifying the same person smiling, aged, with various accessories (moustache, glasses), and/or in badly lit conditions. Also iris and retina image synthesis is main security threat in case of iris recognition. Many commercial applications could improve their personal recognition systems' security by adding required credentials or building

blocks—for example, using a token or password together with biometric recognition. However, in high-security applications it is important that each component of the recognition system is secured in itself and that the many components provide additional layers of security. Academic and industry experts have been researching methods to counter the threat of spoofing the biometric samples. In particular various methods have been proposed like multimodal biometrics, liveness detection biometrics, spectral biometrics, thermal biometrics to enhance the security of the system.

## 6. CONCLUSION

Biometric systems play a vital role for automated human recognition .It is being deployed in various authentication systems like attendance system, Aadhar card , ATM, etc. The paper introduces the concept of human recognition system and highlights the pros and cons of traditional authentication system and biometric system. Traditional authentication techniques fail to address the issues of negative recognition and non repudiation whereas the biometric system addresses both these issues and enhances the recognition of person based on personal authentication system by the evidence presented by physiological or behavioral characteristics. The paper has covered the most widely used biometric systems that provide efficient solutions for identity management system which include fingerprint, face recognition, iris scanning and others however each method has its own drawbacks . While the biometrics of an individual is unique and extremely difficult to impersonate, weaknesses or vulnerabilities can be introduced into the system based largely on how it is implemented. Several type of attacks has been reported in case of these automated recognition systems , which open a wide scope for researchers to build a safe and secure biometric systems taking into consideration the existing problems in the present biometric systems. Spoofing attacks is a fatal threat for biometric authentication systems, the paper has also briefly demonstrated the various security issues such as covert identification, privacy and discrimination and concealable biometrics pertaining to identity management system and also the methods of dealing with these issues.

## 7. REFERENCES

[1] R. Bolle, J. Connell, S. Pankanti, N. Ratha and A. Senior, “Guide to Biometrics”, Springer, 2004

[2] J. Wayman, A. Jain, D. Maltoni, and D. Maio, Eds. “Biometric Systems Technology, Design and Performance Evaluation”, Springer, 2005.

[3] National Science and Technology Council Subcommittee on Biometrics, “Biometrics Glossary”, September 2006. http://www.biometrics.gov/Documents/Glossary.pdf.

[4] Anil K. Jain, Arun Ross, “Introduction to Biometrics”, Springer, 2011.

[5] Bori Toth, “Face Biometric liveness Detection, Information Security Bulletin”, October 2005, Volume 10.

[6] Maio, D., Maltoni, D., Cappelli, R., Wayman, J.L., Jain A.K.: FVC2002: “Second Fingerprint Verification Competition”, Proc. Int. Conf. on Pattern Recognition (16th), vol. 3(2002) 811−814.

[7] Hong, L., Wan, Y., Jain, “A.K.: Fingerprint Image Enhancement: Algorithms and Performance Evaluation”, IEEE Transactions on Pattern Analysis and Machine Intelligence,vol. 20, no. 8 (1998) 777−789.

[8] Bazen, A.M., Gerez, S.H. “Systematic Methods for the Computation of the Directional Fields and Singular Points of Fingerprints”, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 24, no. 7 (2002) 905−919.

[9] Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S., “Handbook of Fingerprint Recognition”, Springer, New York (2003).

[10] Lam, L., Lee, S.W., Suen, C.Y. “Thinning Methodologies: A Comprehensive Survey”, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 14, no. 9 (1992) 869−885.

[11] Marios Savvides, Jingu heo and Sung Won Park, “Face Recognition”, “Dept. of electrical and computer engineering Carnegie Mellon University, Pittsburgh, pennysylvania,USA.

[12] Barbara Westmorel, Michael Lemo,and Richard snell,”cinical anatomy of eye 2nd ed Oxford” ;Blackwell Science Inc.,1998.

[13] J. Daugman. “High confidence visual recognition of persons by a test of statistical independence”, IEEE Transactions on Pattern Analysis and Machine Intelligence, 15(11):1148{1161, 1993.

[14] J. Daugman. “The Importance of Being Random: Statistical Principles of Iris Recognition”, IEEE Transactions on Pattern Analysis and Machine Intelligence, 36(2):279{291, 2003.

[15] J. Daugman. “How Iris Recognition Works” IEEE Transactions on Circuits and Systems for Video Technology, 14(1):21{30, 2004.

[16] J. Daugman. “New Methods in Iris Recognition”, IEEE Transactions on Systems, Man, and Cyernetics, 37(5):1167{1175, 2007.

[17] Government of India. Unique Identification Authority of India, February 2011. http://uidai.gov.in/.

[18] Ferdinando Samaria and Steve Young. “HMM-based architecture for face identification. Image and Vision Computing”, 12(8):537{543, 1994.

[19] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld. “Face recognition: A literature survey. ACM Comput. Surv”, 35:399{458, December 2003.

[20] Jain, A. K., Nandakumar, K., and Nagar, “A.Biometric template security”. EURASIP J. Adv. SignalProcess 2008 (January 2008), 113:1{113:17.

[21] B.toth, “Biometric ID card Debates, Newsletter ‘Biometrie”, of ISACA chapter Switzerland, Germany and Austria, June 2005

[22] Egan J. P.: Signal “Detection Theory and ROC Analysis”, Academic Press (1975)

[23] Wayman J. L.: “Fundamentals of Biometric Authentication Technologies”. National Biometric Test Center Collected Works 1997-2000, San Jose University Press (2000)

[24] Putte, Keuning2000: T. Putteand J. Keuning, “Biometrical fingerprint recognition: don’t get your fingers burned”, *Proc. IFIP TC8/WG8.8, Fourth Working Conf. Smart Card Research and Adv. App*., pp. 289-303, 2000.

[25] Matsumoto et al. 2002: T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of Artificial Gummy Fingers on Fingerprint Systems", *Proc. of SPIE, Optical Security and Counterfeit Deterrence Techniques IV*, vol. 4677, pp. 275-289, 2002.

[26] Uludag, Jain 2004 (1): U. Uludagand A.K. Jain, "Attacks on biometric systems: a case study in fingerprints", Proc. SPIE-EI 2004, Security, Steganographyand Watermarking of Multimedia Contents VI, vol. 5306, pp. 622-633.

[27] Cholet G.: "Automatic Speaker Recognition: Technologies, Evaluations and Possible Future", Presentation during 1st BioSec and Biometric Technologies Workshop, Barcelona (2004)

[28] Ord T., Furnell S. M.: "User authentication for keypad-based devices using keystroke analysis". Proceedings of the Second International Network Conference (INC 2000), Plymouth, UK (2000)

[29] James S. Doyle, Jr, Patrick J. Flynn, Director, "QUALITY METRICS FOR BIOMETRICS", thesis of Graduate Program in Computer Science and Engineering Notre Dame, Indiana April 2011