Biometric Security Issues: A Review

Er. Kanika Sharma and Dr. V. K. Banga

Abstract— As the world is heading towards paperless communication and transaction, the correct and authentic personal recognition is important to ensure that only legitimate users have access to the rendered services or information. Automatic recognition of individuals on the basis of their physiological or behavioral characteristics known as Biometric recognition or biometrics is now frequently used by service providers to authenticate personal recognition. Biometrics makes it possible to recognize the person on the basis of what he has (characteristics) rather than what he possesses (Id cards etc.)

This paper provides an insight into various biometric characteristics their advantages, disadvantages, limitations and strengths. A systematic review of literature is carried out to identify future areas of research.

Keywords— Biometric recognition, Iris, Retina, Unimodal systems.

I. INTRODUCTION

It is a common practice in our day to day life to identify a person on the basis of voice, walking, standing and gesticulation styles. We are able to recognize a person even when the person may not be visible to us clearly. Biometrics refers to the recognition of humans by their characteristics or traits called as biometric identifiers. Biometric identifiers may be classified into physiological characteristics/identifiers and behavioral characteristics/identifiers. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, face recognition, DNA, Palm print, hand geometry, iris recognition, retina and odor/scent. Behavioral characteristics are related to the behavior of a person, including but not limited to: typing rhythm, gait, and voice. As such, many different aspects of human physiology, chemistry or behavior can be used for biometric authentication. The selection of a particular biometric for use in a specific application involves a weighting of several factors. Jain et al. (1999) identified seven such factors to be used when assessing the suitability of any trait for use in biometric authentication.

Universality: Characteristic should have universal presence i.e. each person in the population should have the characteristic.

- Distinctiveness: no two persons should exhibit similarity in terms of the characteristic.
- Permanence: the characteristic should be sufficiently invariant or stable (with respect to the matching criterion) over a period of time.
- Collectability: the characteristic can be measured quantitatively.

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

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

A biometric system is comprised of the following four main modules (see Fig. 1).

1) Sensor module: This captures the biometric data of an individual. An example is a fingerprint sensor that images the ridge and valley structure of a user’s finger.

2) Feature extraction module: This involves processing of biometric data for extracting a set of salient or distinguishable features. For example, the position and orientation of minutiae points (local ridge and valley singularities) in a fingerprint image are extracted in the feature extraction module of a fingerprint-based biometric system.

3) Matcher module: This involves the process of recognizing the features extracted and comparing against the stored templates to generate matching scores. For example, in the matching module of a fingerprint-based biometric system, the number of matching minutiae between the input and the template fingerprint images is determined and a matching score is reported. The matcher module also encapsulates a decision making module, in which a user’s claimed identity is confirmed (verification) or a user’s identity is established (identification) based on the matching score.

4) System database module: which is used by the biometric system to store the biometric templates of the enrolled users. The enrollment module is responsible for enrolling individuals into the biometric system database. During the enrollment phase, the biometric characteristic of an individual is first scanned by a biometric reader to produce a
digital representation of the characteristic. In order to facilitate matching, the input digital representation is further processed by a feature extractor to generate a compact but expressive representation, called a template.

A biometric system is typically a pattern recognition system operating on the basis of biometric data acquired from an individual, extracting desired feature set from the acquired data, and matching this feature set against the template set in the database.

A biometric system may operate either in verification mode or identification mode.

- In the verification mode, the system authenticates a person’s identity on the basis of matching between the captured biometric data with the same person’s biometric templates stored in the system database. Identity verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity [2].
- In the identification mode, the system performs one-to-many comparisons for identification of an individual by searching the templates of all the users in the database for a match.

Identification is a critical component in negative recognition applications where the system establishes whether the person is who she (implicitly or explicitly) denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities [2]. Identification may also be used in positive recognition for convenience (the user is not required to claim an identity). While traditional methods of personal recognition such as passwords, PINs, keys, and tokens may work for positive recognition, negative recognition can only be established through biometrics.

In terms of set theory verification process may be expressed as follows:

Let $I_f$ represent input feature vector (extracted from the biometric data)

$I_c$ represents claimed identity

$I_t$ represents the biometric template corresponding to user $I$

$C_t$ represents true claim

$C_f$ represents a false claim

To determine whether the veracity of the claim following condition needs to be satisfied:

$$(I, I) \in \begin{cases} 
C_t & \text{if } S(I_f, I_t) \geq t, \\
C_f & \text{otherwise}
\end{cases}$$

where $S$ is the function that measures the similarity between feature vectors $I_f$ and $I_t$, and $t$ is a predefined threshold. The value $S(I_f, I_t)$ is termed as a similarity or matching score between the biometric measurements of the user and the claimed identity. Therefore, every claimed identity is classified into $C_t$ or $C_f$ based on the variables $I_f, I_t, t$ and function $S$. Threshold $t$ takes into consideration the fact that same biometric feature measured at different times may not be exactly similar (like iris may be damaged or finger tips may be scarred etc.)

In terms of set theory verification process may be expressed as follows:

Let $I_f$ represent input feature vector (extracted from the biometric data)

$I_c$ Identity to be determined

$d \in \{1, 2, 3, 4 \ldots, N, N + 1\}$

Here $I_1, I_2, I_3, I_4$ are the identities enrolled in the system and $I_{N+1}$ indicates the reject case where no suitable identity can be determined for the user.

![Fig. 1 Enrollment, verification, and identification tasks using the four main modules of a biometric system](image)

**Types of Biometric Models**

Biometric models can be classified into two types, based upon their mode of application:

1. **Unimodal** - Biometric system that operates using any single biometric characteristics.
2. **Multimodal** – Biometric system that operates on the basis of multiple biometric characteristics.

Although unimodal biometrics have found extensive commercial applications requiring low level of recognition these have certain inherent limitations.
1) **Noise** – There may be distortion or contamination of the sensed data. A fingerprint with a scar or background noise are some of the examples of contamination of data on account of noise.

2) **Intra-class variations** – There may be intra-class variations on account of difference in interaction pattern of the person with the sensors during enrollment and authentication.

3) **Distinctiveness** – While a biometric trait is expected to vary significantly across individuals, there may be large inter-class similarities in the feature sets used to represent these traits. This limitation restricts the discriminability provided by the biometric trait. [4] have shown that the information content (number of distinguishable patterns) in two of the most commonly used representations of hand geometry and face are only of the order of 10^5 and 10^3, respectively. Thus, every biometric trait has some theoretical upper bound in terms of its discrimination capability.

4) **Non Universality** – While it is expected that each individual in a population will possess the biometric traits, in reality it may not be possible. It will not be possible to acquire fingerprints or palm prints of a person with missing arms or iris scan of a person who is blind.

5) **Spoof Attacks** – There is a high probability of forging in case single biometric is used. Forging of signatures [7] and copying voices [8] is fairly common. It is also possible (although difficult and cumbersome and requires the help of a legitimate user) to construct artificial fingers/fingerprints in a reasonable amount of time to circumvent a fingerprint verification system [9].

**Multimodal**

Some of the limitations of the unimodal system listed above are overcome by multimodal systems. Such multimodal biometric systems [10] are expected to be more reliable due to the presence of multiple, independent pieces of evidence [11]. These systems are also able to meet the stringent performance requirements imposed by various applications [12].

A multimodal system may operate in series, parallel or hierarchical manner. While operating in series a multimodal system first uses a biometric to narrow down the options and then another biometric application is used to identify the individual. For example initially face biometric could be used to narrow down the option to a few and subsequently fingerprints may be used to recognize the individual. Parallel operations require using different biometric applications simultaneously. Parallel operations are usually time consuming as several biometrics are to be measured, this is in contrast to series process a decision could be arrived at without acquiring all the traits. This reduces the overall recognition time. In the hierarchical scheme, individual classifiers are combined in a treelike structure.

**Fusion in Multimodal Biometrics**

Multimodal biometric systems integrate information presented by multiple biometric indicators. The information can be consolidated at various levels. Figure 2 illustrates the three levels of fusion [1] when combining two (or more) biometric systems. These are as follows.

1) **Fusion at the feature extraction level.** The data obtained from each biometric modality is used to compute a feature vector. If the features extracted from one biometric indicator are (somewhat) independent of those extracted from the other, it is reasonable to concatenate the two vectors into a single new vector, provided the features from different biometric indicators are in the same type of measurement scale. The new feature vector has a higher dimensionality and represents a person’s identity in a different (and hopefully, more discriminating) feature space.

Feature reduction techniques may be employed to extract a small number of salient features from the larger set of features.

2) **Fusion at the matching score (confidence or rank) level.** Each biometric matcher provides a similarity score indicating the proximity of the input feature vector with the template feature vector. These scores can be combined to assert the veracity of the claimed identity. Techniques such as weighted averaging may be used to combine the matching scores reported by the multiple matchers.

3) **Fusion at the decision (abstract label) level.** Each biometric system makes its own recognition decision based on its own feature vector. A majority vote scheme [13] can be used to make the final recognition decision.

![Fig. 2 Different levels of fusion in a parallel fusion mode: (a) fusion at the feature extraction level, and (b) fusion at matching score (confidence or rank) level, and (c) fusion at decision (abstract label) level.](image-url)
Different Types of Biometrics

Different biometric characteristics are existing and being used in various applications. Each biometric has its strengths and weaknesses and the choice of any one biometrics depend upon intended application. No single biometric is expected to effectively meet the requirements of all the applications. A brief description of various biometrics is provided below:

a) Deoxyribose Nucleic Acid (DNA) - ultimate unique code for one’s individuality— except for the fact that identical twins have identical DNA patterns [1]. DNA molecules are double-stranded helical structures.

![DNA structure](Image)

It is predominantly used in forensic sciences for person recognition. DNA biometrics differs from other biometrics in three ways.
1. DNA requires a tangible physical sample as opposed to an impression, image, or recording
2. DNA matching is not done in real-time, and currently not all stages of comparison are automated.
3. DNA matching does not employ templates or feature extraction, but rather represents the comparison of actual samples.

Further [1] have listed three inherent limitations in using DNA as a biometrics.
1. Contamination and Sensitivity-- it is easy to steal a piece of DNA from an unsuspecting subject that can be subsequently abused for an ulterior purpose.
2. Automatic Real-time Recognition Issues-- the present technology for DNA matching requires cumbersome chemical methods (wet processes) involving an expert’s skills and is not geared for on-line noninvasive recognition
3. Privacy Issues – DNA is a molecule that encodes genetic instructions used in the development and functioning of all living organisms. In case of humans DNA may contain information pertaining to certain hereditary diseases and DNA analysis may thus impinge upon privacy of the individual.

b) Ear: The shape of the ear and the structure of the cartilagenous tissue of the pinna are distinctive. The ear recognition approaches are based on matching the distance of salient points on the pinna from a landmark location on the ear. The features of an ear are not expected to be very distinctive in establishing the identity of an individual [1].

![Ear](Image)

c) Face - The human face plays an important role in social interaction, conveying people’s identity. Using the human face as a key to security, biometric face recognition technology has received significant attention in the past several years due to its potential for a wide variety of applications in both law enforcement and non-law enforcement.

As compared with other biometrics systems using fingerprint/palmprint and iris, face recognition has distinct advantages because of its non-contact process. Face images can be captured from a distance without touching the person being identified, and the identification does not require interacting with the person. In addition, face recognition serves the crime deterrent purpose because face images that have been recorded and archived can later help identify a person. The most popular approaches to face recognition are based on either: 1) the location and shape of facial attributes such as the eyes, eyebrows, nose, lips, and chin, and their spatial relationships, or 2) the overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces [1]. Although, the verification performance of the face recognition systems that are commercially available is reasonable [3], they impose a number of restrictions on how the facial images are obtained, sometimes requiring a fixed and simple background or special illumination. These systems also have difficulty in recognizing a face from images captured from two drastically different views and under different illumination conditions. It is questionable whether the face itself, without any contextual information, is a sufficient basis for recognizing a person from a large number of identities with an extremely high level of confidence [4]. In order for a facial recognition system to work well in practice, it should automatically: 1) detect whether a face is present in the acquired image; 2) locate the face if there is one; and 3) recognize the face from a general viewpoint (i.e., from any pose).

![Face as a biometric](Image)

d) Facial, Hand and Hand vein IR Thermogram – All human bodies emits heat and this emission is a characteristic of metabolism rate of each of the human beings. Since,
metabolic rates of any two individuals are not same, so the pattern of heat emission is also not same and can be captured by an infrared camera in an unobtrusive way much like a regular (visible spectrum) photograph. One major limitation of IR termogram is interference by the heat generated by the surroundings.

Fig. 6 Face thermogram as a biometric

e) Fingerprints – Finger prints have long been used for recognition and the matching accuracy using fingerprints has been shown to be very high [5]. A fingerprint is the pattern of ridges and valleys on the surface of a fingertip, the formation of which is determined during the first seven months of fetal development. Fingerprints of identical twins are different and so are the prints on each finger of the same person. Since, fingerprinting requires physical contact for data enrollment it cannot be used for certain fraction of population who are without limbs or in cases where some damage has happened to fingers.

Fig. 7 Fingerprint as a biometric

f) Gait – Gait refers to a person’s walking style. It is a complex spatio-temporal biometric. Gait cannot be considered as a distinctive biometric since it may change over a period of time owing to injuries, joint problems or behavior modification. However, it may be used in certain low security applications.

Fig. 8 Gait as a biometric

g) Hand and Finger Geometry - Hand geometry recognition systems are based on a number of measurements taken from the human hand, including its shape, size of palm, and lengths and widths of the fingers. The technique is very simple, relatively easy to use, and inexpensive. Environmental factors such as dry weather or individual anomalies such as dry skin do not appear to have any negative effects on the verification accuracy of hand geometry- based systems. The geometry of the hand is not known to be very distinctive and hand geometry-based recognition systems cannot be scaled up for systems requiring identification of an individual from a large population. Further, hand geometry information may not be invariant during the growth period of children. In addition, an individual’s jewelry (e.g., rings) or limitations in dexterity (e.g., from arthritis), may pose further challenges in extracting the correct hand geometry information.

Fig. 9 Hand and Finger Geometry as Biometric

h) Iris -- The iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side. The visual texture of the iris is formed during fetal development and stabilizes during the first two years of life. The complex iris texture carries very distinctive information useful for personal recognition. It is very difficult to surgically tamper Iris and further artificial irises (designer contact lens). These qualities along with fact that each iris is distinctive make them an ideal biometric tool.

Fig. 10 Human Iris as a biometric

i) Keystroke – There is a distinctive pattern in the way a person types on the key board. This behavioral biometric is not expected to be unique to each individual but it offers sufficient discriminatory information to permit identity verification.

Fig. 11 Keystroke as a biometric

j) Body Odor – Every human being has a distinctive body odor which depends upon its chemical composition. A whiff of air is blown over certain chemical sensors to identify the type of body odor. Camouflaging the body odor with
A high-resolution palmprint scanner, on the other hand will extract all the features of the palm such as hand geometry, ridge and valley features (e.g., minutiae and singular points such as deltas), principal lines, and wrinkles may be combined to build a highly accurate biometric system.

**k) Palm prints** – Just like finger prints, palms also contain contain pattern of ridges and valleys much like the fingerprints. The area of the palm is much larger than the area of a finger and, as a result, palmprints are expected to be even more distinctive than the fingerprints. Besides, human palms also possess additional distinguishing features such as principal lines and wrinkles that can be captured even with a cheaper lower resolution scanner [6]. A high-resolution palmprint scanner, on the other hand will extract all the features of the palm such as hand geometry, ridge and valley features (e.g., minutiae and singular points such as deltas), principal lines, and wrinkles may be combined to build a highly accurate biometric system.

**l) Retinal Scan** – Retina of each individual has a distinctive vasculature and since it is very difficult to change the pattern of blood vessels, retinal scans are very secure biometrics. However, capturing retinal scan requires not only cooperation from the person whose retina is being scanned – requires looking into a eye piece at a particular point – to ensure effective scanning, but also highly trained personnel who can execute the work.

**m) Signatures** – Signatures have been used and accepted as identifiers of a person. The way a person signs has a distinctive pattern facilitating recognition. Signatures are a behavioral biometric that change over a period of time and are influenced by physical and emotional conditions of the signatories. Signatures of some people vary substantially; even successive impressions of their signature are significantly different. Further, professional forgers may be able to reproduce signatures that fool the system. The major impediment in using voice as a biometric is pollution of the sample on account of background noise.

**n) Voice** - Signatures are a behavioral biometric that change over a period of time and are influenced by physical and emotional conditions of the signatories. Signatures of some people vary substantially; even successive impressions of their signature are significantly different. Further, professional forgers may be able to reproduce signatures that fool the system. The major impediment in using voice as a biometric is pollution of the sample on account of background noise.

II. LITERATURE REVIEW

It is an established fact that multimode biometric systems are better in personal recognition as compared to unimode biometric systems. Researchers have used various combinations of biometrics in pursuit of obtaining a most optimal multimode system. The present section aims to delve into the studies that have been carried out in the past.

Mingxing et al [14] in their study used three biometric characteristics fingerprint, face, and finger vein, while Fierrez et al [16] in their study proposed the use of eight biometric characteristics namely: speech, iris, face (still images, videos of talking faces), handwritten signature and handwritten text (on-line dynamic signals, off-line scanned images), fingerprints (acquired with two different sensors), hand (palmprint, contour-geometry) and keystroking. A fingerprint-codified templates, iris-codified templates, and iris and fingerprint-fused templates was proposed by Conti et al [18]. Kang et al [22] propose fusion of finger veins, fingerprints, and finger geometry features. While majority of these studies involve biometric parameters that require considerable involvement and cooperation from the user, which may not always be forth coming. Systems using biometrics with minimum involvement of users have also been proposed and suggested by the experts. Yazdanpanah et al [20] have used face, ear and gait database for biometric identification. While Giot et al [23] have used 2D face recognition pattern along with keystroke.

Review of literature has revealed many techniques for feature extraction of the biometrics to be used for fusion. While Conti et al [18] and Raghvendra et al [21] have recommended the use of Log-Gabor algorithm, Yazdanpanah et al [20] have used Gabor + PCA feature extarction method. Kang et al [22] in their study showed that finger geometry recognition is greatly enhanced by combining a Fourier descriptor with principal component analysis.

Normalization/Optimization of biometric characteristics prior to fusion is an important step. Different studies have suggested different techniques for normalization. Mingxing et
al [14] have used min–max normalization, z-score normalization, and tanh-estimators normalization. Besides these, a new transformation method which is derived from min–max normalization is proposed. Yazdanpanah et al [20] besides using min-max and z score have also employed median-MAD normalization. Giot et al [23] have used min, max, mul, svm, weighted sum configured with genetic algorithms, and, genetic programming for normalization. Kang et al [22] in their study found that fuzzy score normalization method is better than z-score method, while hybrid particle swarm approach was employed by Kumar et al [15] and Raghvendra et al [21].

The fusion of features have been carried out by Sum based rule; Mingxing et al [14]; Weighted sum Yazdanpanah et al [20] and Kang et al [22]; weighted product Yazdanpanah et al [20]; F-norm Poh et al [17]; Bayesian classifiers Poh et al [17], Poh et al [19]; SVM based Mingxing et al [14] and Kang et al [22].

A template-level fusion algorithm working on a unified biometric descriptor leading to a matching algorithm that is able to process fingerprint-coded templates, iris-coded templates, and iris and fingerprint-fused templates was proposed by [18]. In contrast to the classical minutiae-based approaches, the proposed system performs fingerprint matching using the segmented regions (ROIs) surrounding (pseudo) singularity points. This choice overcomes the drawbacks related to the fingerprint minutiae information: the frequency-based approach should consider a high number of ROIs, resulting in the whole fingerprint image coding, and consequently, in high-dimensional feature vector. At the same time, iris preprocessing aims to detect the circular region surrounding the feature, generating an iris ROI as well. A Log-Gabor-algorithm-based codifier to encode both fingerprint and iris features, thus obtaining a unified template. Successively, the HD on the fused template was used for the similarity index computation.

Poh et al [19] have compared, and categorised several state-of-the-art quality-based score normalization procedures, depending on how the relationship between quality measures and score is modelled, as follows: i) direct modelling, ii) modelling via the cluster index of quality measures, and iii) extending (ii) to further include the device information (device-specific cluster index). Experimental results carried out on the Biosecure DS2 data set show that the last approach can reduce both false acceptance and false rejection rates simultaneously. This was followed by fusion using Naïve Bayes principal.

In a novel multimodal biometric recognition system using three modalities including face, ear and gait, based on Gabor+PCA feature extraction method with fusion at matching score level is proposed by [20]. The performance of the proposed approach was studied under three different normalization methods (min-max, median-MAD and z-score) and two different fusion methods (weighted sum and weighted product). The new method was successfully tested using 360 images corresponding to 120 subjects from three databases including ORL face database, USTB ear database, and CASIA gait database. Because of these biometric traits, proposed method requires no significant user cooperation and also can work from a long distance. According to the experimental results the proposed method exhibits excellent recognition performance and outperforms unimodal systems. The best recognition performance that our proposed method achieved is 97.5.

Raghvendra et al [21] implemented a particle swarm optimization procedure prior to coding using Log-Gabor transformations. Results in both closed identification and verification rates show a significant improvement of 6% in performance when performing feature fusion in Log-Gabor space over the more common optimized match score level fusion method.

A single finger contains finger veins, fingerprints, and finger geometry features; by using multimodal biometrics, information on these multiple features can be simultaneously obtained in a short time and their fusion can outperform the use of a single feature. [22] propose a new finger recognition method based on the score-level fusion of finger veins, fingerprints, and finger geometry features. Their research is novel in the four ways. First, the performances of the finger-vein and fingerprint recognition were improved by using a method based on a local derivative pattern. Second, the accuracy of the finger geometry recognition is greatly increased by combining a Fourier descriptor with principal component analysis. Third, a fuzzy score normalization method is introduced; its performance is better than the conventional Z-score normalization method. Fourth, fingerprint, finger-vein, fingerprint, and finger geometry recognitions are combined by using three support vector machines and a weighted SUM rule. Experimental results showed that the equal error rate of the proposed method was 0.254%, which was lower than those of the other methods.

Giot et al [23] have used different fusion methods (min, max, mul, svm, weighted sum configured with genetic algorithms, and, genetic programming) on the scores of three keystroke dynamics algorithms and two 2D face recognition ones. The proposed multimodal biometric system improves the recognition rate in comparison with each individual method. On a chimeric database composed of 100 individuals, the best keystroke dynamics method obtains an EER of 8.77%, the best face recognition one has an EER of 6.38%, while the best proposed fusion system provides an EER of 2.22%.

III. CONCLUSION AND DISCUSSION

Biometrics refers to the recognition of humans by their characteristics or traits (Physiological or Behavioral characteristics) called as biometric identifiers. Like any other system biometric system also has certain advantages and limitations. On the positive side, biometrics can be used as one of the most effective means for protecting individual privacy by safeguarding identity and integrity. On the other hand, biometric information of an individual in the hands of a wrong person may be catastrophic as biometric characteristics may provide additional information about the background of an
individual (like presence or propensity towards a disease). Biometrics essentially is a risk management system. The endeavor is to ensure that only the authorized persons are able to access information, restricted areas or any other service. A sound trade-off between security and privacy is therefore necessary.

Success of a biometric system is largely dictated by the human factors. The ease and comfort in interaction with a biometric system contribute to its acceptance. Also, biometric technologies requiring very little cooperation or participation from the users (e.g., face and face thermograms) may be perceived as being more convenient to users.

IV. FUTURE SCOPE

While unimodal systems (systems using only a single biometric characteristics) are considered to be sufficient in case of services/issues requiring low level recognition (like attendance of employees in a small scale industry). Multimodal systems (combination of two or more biometric characteristics or a single biometric with multiple inputs eg finger prints of two or more fingers) may be required for high level recognition (like matters of national security or financial transactions). While in general it is acknowledged that normalization before fusion improves the performance of multi modal systems. There is no consensus on the most effective technique of normalization while some studies report min-max, median-MAD and z-score to be more effective others have reported Fourier descriptor with principal component analysis to be more useful. Further, there is considerable debate upon the use of biometric fusion methods some studies have adopted SVM and weighted SUM rule for fusion others have used Log- Gabor algorithm and still others have followed Hybrid Particle Swarm Optimization Method. It is therefore evident that there exists a considerable scope in identifying the optimum normalization as well as fusion method.

REFERENCES


[22] Romain Giot Baptiste Hemery Christophe Rosenberger; “Low Cost and Usable Multimodal Biometric System Based on Keystroke Dynamics and 2D Face Recognition”, 20th International Conference on Pattern Recognition, Istanbul : Turkey (2010)