Scientific Journal of Impact Factor(SJIF): 3.134
e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 6, June -2015

Multimodal Biometric System for User Authentication with Fuzzy Fusion of Face and Fingerprint

Shiv Ratan Singh[1], *Prof Jai Prakash*[2]

[1]Sr. Lecturer, Department of ECE,Guru Nanak Dev Institute of Technology, Govt of NCT of Delhi
Research Scholar Mewar University
[2]*Visiting facult, Mewar University*

Abstract—*The vast majority of the successful commercial biometric systems at present depend on fingerprint or face. Moreover, these biometric indicators complement one another in their strengths and advantages. While fingerprint gives exceptionally high verification precision, but still carry some verification errors. The Face recognition is second most preferred method with reasonably good accuracy. In this paper, integration of face and fingerprint recognition techniques using fuzzy fusion method is detailed. The introductory results are promising and indicate that the fusion of face recognition and fingerprint methods further improves the accuracy of the user identification system.*

Index Terms— *Face recognition, Finger recognition, Fuzzy Logic*

1. INTRODUCTION

A biometric system which relies on a single biometric identifier is most of the time unable to meet the desired requirements in making a personal identification and verification. This happens due to the algorithms limitations. Now days various biometric identifiers like, face, finger, voice, palm, retina and hand writing etc. are used. However, each of these methods has their pros and cons. In this work we have concentred on finger and face recognition based system as these are more preferred methods over others.

In past, the biometric systems were mostly used as an identity service, but in surveillance these methods were not used (Fig. 1).

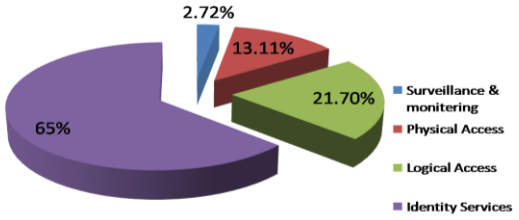


Fig. 1: Global Market by Application (2009)

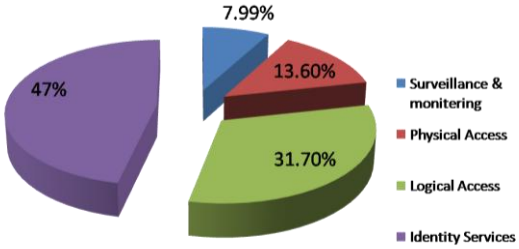


Fig. 2: Global Market by Application (2017)

But in past few years trend has changed, and now the biometric is also preferred in surveillance application. This acceptance of biometric system over the traditional methods over the years is increased and expected to grow in coming years (Fig. 2).

Biometrics, which points out to the automatic individual identification based on his behavioural or physiological characteristics, depends on "something which he is or he does" (e.g. placing his finger on a scanner) in order to make identification of a person. As compared to the token-based and/or knowledge-based approaches, biometrics methods are more reliable. The reason behind this is the uniqueness of the physiological or behavioural characteristic of each user. As of now, nine distinctive biometric indicators are either broadly used or are under investigation, including fingerprint, signature, facial thermo gram, face, hand geometry, hand vein, iris, voice-print and retinal pattern. Each one of these biometric indicators has their own advantages as well as disadvantages in terms of the applicability, accuracy and user acceptance [1]. The choice of a particular biometric indicator relies on the necessities of the application domain.

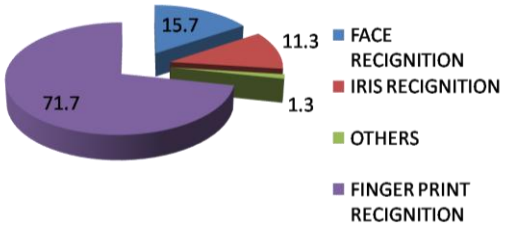


Fig. 3: Biometric indicators

Still in most of the biometric based authentication system Fingerprint is most preferred choice, followed by face recognition. This work focusses in developing a fuzzy logic based multimodal biometric system which integrates fingerprint and face to identify a personal. Our choice of these two specific biometric is based on the fact they have been used routinely in the community of law enforcement. The vast majority of the successful commercial biometric systems at present depend on fingerprint or face (Fig. 3). Moreover, these biometric indicators complement one another in their strengths and advantages. While fingerprint gives exceptionally high verification precision, it is not easy for an untrained human to match fingerprints. On the other hand, face is routinely used by each one of us as a part of our day by day recognition tasks [2]. Our system is focused for verification applications to authenticate the identity claimed by a user such as in authentication of a multiuser account.

In this work face LDA (Linear Discriminator Analysis) and fingerprints (minutia based) algorithms are studied and finally these algorithms results are fused using the fuzzy logic based system. In this system, the capabilities of both the algorithms are utilized. The integrated system can restrict some of the limitation of a sole biometric system. The introductory results are promising and indicate that the fusion of face recognition and fingerprint methods establishes a more reliable and accurate identity of user in comparison of the identity established by either face of finger recognition system in alone.

2. Need for biometrics

In the current electronically/optically wired internet media where much information is shared, user may come across a situation where he has to make access of a multi-user computer account and thus, as a user, needs to be verified by an electronic device. Generally, this verification of a user is based on either on a certain token, for example, an ID card ("something that she has") and/or he has a particular knowledge such as password ("something that she knows") which is expected to be known by him only. These approaches have various disadvantages. Tokens may be stolen, misplaced, lost, forged, or forgotten. Password may be forgotten or can be changed. In such a situation it will be difficult for the system to differentiate between a registered authorized user and an imposter who some how know the token of the authorized user. Hence, knowledge or token -based authentication doesn't provide the sufficient security in critical application e.g., financial transactions.

The block diagram of our system is demonstrated in Fig. 4, which comprises of four segments: (i) acquisition module, (ii) template database, (iii) enrollment module, and (iv) verification module. It is the responsibility of acquisition module to obtain face images, fingerprint images, and speech signal of a user who expects to access the system. The template database is a system database where the template of the user who are registered in the system is located. The enrollment module which includes enrollment, deletion, updating user, training, parameter specification manages the system. Further, the verification module is in charge of authentication the identity claimed by a user at the point-of-access. This process of verification essentially comprises three stages. These are: (i) fingerprint verification, (ii) face recognition, and

(iii) decision fusion. It is the responsibility of Finger print verification module to match the input fingerprint template(s) stored in the database to get the fingerprint matching score. The input face is matched against the face template to obtain the fingerprint matching score and Face recognition is responsible for this process. The decision fusion integrates the matching scores from fingerprint verification and face recognition to make the final conclusion.

3. The Multimodal Biometric System

Each one of the biometrics in our multimodal system has a quite different matching scheme. Subsequently, it is more sensible to integrate the various biometrics at the decision level instead of at the sensor level.

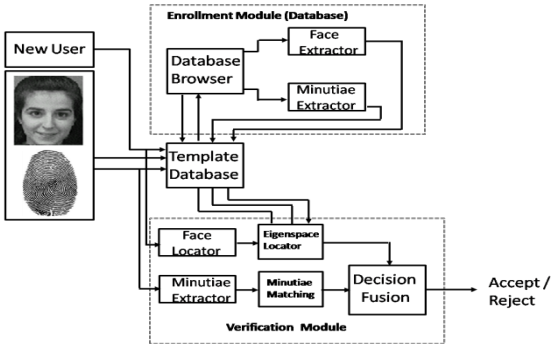


Fig. 4: Multi-modal Biometric system

2.1Problem Formulation

Let β denote a given biometric system, and let $\Phi^1, \Phi^2, \ldots\ldots\ldots \Phi^N$ are the template of the N users which are enrolled in β, and have indicator number as, $1, 2, \ldots\ldots\ldots N$. Each enrolled user has only two templates one for each face and finger are stored in the system. Thus for the i^{th} user, the template $\Phi^i = \left\{\Phi_1^i, \Phi_2^i\right\}$, has two components, where Φ_1^i, Φ_2^i are the templates for fingerprint and face biometric, respectively. Let $\left(\Phi^0, \mathrm{I}\right)$ denote the biometric indicator. Again Φ^0 have two components, $\Phi^0 = \left\{\Phi_1^0, \Phi_2^0\right\}$ corresponding to the measurement of the two biometric indicators. The claimed identity, I, either belongs to category w_1 which indicates a true identity (a genuine user) or in w_2 indicates the false identity (an imposter). The biometric system β decides in favour of, w_1 or w_2 using the relation:

$$I \in \begin{cases} w_1, & \text{if } F\left(\Phi^0, \Phi^1\right) > \in, \\ w_2, & \text{otherwise,} \end{cases} \qquad (1)$$

Where $F\left(\Phi^0, \Phi^1\right)$ is a function which measures the similarity between Φ^0 and Φ^1 and $\in$ is a threshold.

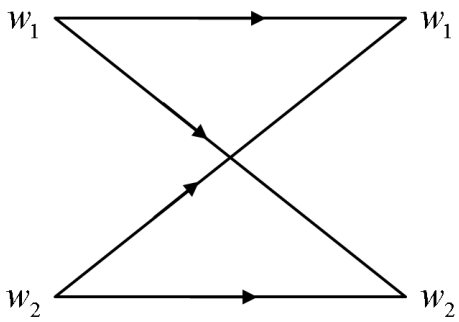


Fig. 5: system

A	B	Outcome	F
p	q	Genuine Accepted	T
p	1-q	Genuine Rejected	F

1-*p*	*q*	Imposter Accepted	F
1-*p*	1-*q*	Imposter Rejected	T

Identity Summary

For a claimed identity I, there are four possibilities: (i) a claimed identity in w_1 is determined to be in w_1, (ii) a claimed identity in w_1 is determined to be in w_2, (iii) a claimed identity in w_2 is determined to be in w_2, (iv) a claimed identity in w_2 is determined to be in w_1. Outcome (i) corresponds to a genuine user being accepted,outcome (ii) corresponds to a genuine user being rejected, outcome (iii) corresponds to an imposter user being rejected, and outcome (iv) corresponds to an imposter being accepted. Obviously, outcomes (i) and (iii) are correct whereas outcomes (ii) and (iv) are incorrect. Logically the outcome can be expresses as

$F = \overline{A}\overline{B} + AB$, however, the logical values are not '0' and '1' and are depends on some threshold as in table 1. Ideally, a biometric system should make only right decisions.In practise, because of the large intraclass variations in the acquired digital representation of the biometric indicator, incorrect decisions cannot be avoided. The performance measure of a biometric system are (i) false acceptance rate (FAR) and (ii) false reject rate (FRR). The false acceptance rate corresponds to the probability of outcome (iv) and the false reject rate is defined as the probability of outcome (ii). As the lower the values of the FAR and FRR goes lower and lower, the reliability of the decision made by the system increases. The FAR and FRR values of a particular biometric system are determined by the inherent interclass and intraclass variations of the indicator and the design (e.g., feature extraction, decision making) of the system.

4. Distance Metrics

In this work Mahalanobis Cosine distance measured is used which is detailed below:

Euclidean: The Euclidean distance measure (L^2) between two vectors *u, v* in any image space is calculated as

$$D_E(u,v) = \sqrt{\sum_{i=1}^{N}(u_i - v_i)^2} \qquad (2)$$

Mahalanobis Cosine: For each vector pair u and v in image space the transformed vector pair m and n in Mahalanobis space. The transformed vector pair now given as $m_i = \frac{u_i}{\sigma_i}$ and $n_i = \frac{v_i}{\sigma_i}$ .Here σ_i is the standard deviation of the i^{th} dimension.

The Mahalanobis Cosine distance between two vectors *u, v* in image space is calculated as in

$$S_{MCos}(u,v) = -\frac{m.n}{|m||n|} = -\frac{\sum_{i=1}^{N}(m_i n_i)}{\sqrt{\sum_{i=1}^{N}(m_i)^2}\sqrt{\sum_{i=1}^{N}(n_i)^2}} \qquad (3)$$

$$S_{MCos}(u,v) = -\frac{\sum_{i=1}^{N}\left(\frac{u_i}{\sigma_i}.\frac{v_i}{\sigma_i}\right)}{\sqrt{\sum_{i=1}^{N}\left(\frac{u_i}{\sigma_i}\right)^2}\sqrt{\sum_{i=1}^{N}\left(\frac{v_i}{\sigma_i}\right)^2}}$$

and $D_{MCos}(u,v) = 1 - S_{MCos}(u,v)$.

6. Face recognition

Face recognition is a process which investigates the similarity between the user face and the stored template to recognise the user identity.

The eigenface approach for the face recogntion is well investigated and it performes very well. This is a two step approach : (i) training stage and (ii) operational stage. In this method the dimention of the traing images are reduced.

Thereafter, a representation of the facial images in the eighenspace is created, and finally the trained facial images are protected onto the eighenspace. A user facial image is finally projected onto the same eighenspace as in the operational stage and the similarity between the input facial image and the template is computed. Assume that Φ_2^0 represents the input face image with claimed identity I and Φ_2^1 is the representation of the I^{th} template. The similarity between Φ_2^0 and Φ_2^I can be computed as follows:

$$F_2(\Phi_2^0, \Phi_2^I) = -\left\|\Phi_2^I - \Phi_2^0\right\| \qquad (4)$$

Where $\|\bullet\|$ denotes the L^2 norm.

6.1 Linear Discriminant Analysis

LDA is a powerful face recognition technique that overcomes the limitation of Principle component analysis technique. The LDA maximize the ratio of the determinant of the between-class scatter matrix to the determinant of the within class scatter matrix of the projected samples. Linear discriminant group images of the same class and separates images of different classes of the images [3-6].

Considering a *C*-class problem with each class *i* consisting of a set of N_i, *d*-dimensional samples

$\{x_1^i, x_2^i ... x_{N_i}^i\}\}$, where the superscript $(.)^i$ represents the class label. Defining the total number of samples as $N = \sum_{i=1}^{C} N_i$ and the probability of occurrence of class '*i*' as $p_i = \frac{N_i}{N}$, the sample mean for class '*i*' as $\mu^i = \frac{1}{N_i}\sum_{j=1}^{N_i} x_j^i$ and the grand sample mean as μ [13]

$$\mu = \frac{1}{N}\sum_{i=j}^{C}\sum_{j=1}^{N_i} x_j^i = \sum_{i=j}^{C} P^i \mu^i \qquad (5)$$

The within and between class scatter matrices represented as $\sum w$ and $\sum B$, respectively, and computed as:

$$\sum_W = \sum_{i=1}^{C} P^i \sum_W^i = \frac{1}{N}\sum_{i=1}^{C}\sum_{j=1}^{N_i}\left(x_j^i - \mu^i\right)\left(x_j^i - \mu^i\right)^T$$

$$\sum_B = \sum_{i=1}^{C} P^i \sum_B^i = \frac{1}{N}\sum_{i=1}^{C} N_i \sum_{j=1}^{N_i}\left(\mu^i - \mu\right)\left(\mu^i - \mu\right)^T \qquad (6)$$

In above expression $\sum_w^i$ is the covariance matrix estimate for class *i* and computed as

$$\sum_w^i = \frac{1}{N_i} = \sum_{j=1}^{N_i}\left(x_j^i - \mu^i\right)\left(x_j^i - \mu^i\right)^T \qquad (7)$$

and $\sum_B^i$ is the scatter matrix between the class *i* and the 'grand class' and computed as

$$\sum_B^i = \left(\mu^i - \mu\right)\left(\mu^i - \mu\right)^T \qquad (8)$$

In other words, $\sum w$ is estimated by 'pooling' together $\{\sum_w^i, i = 1...C\}$. Similarly, this is also holds for $\sum B$. Then, finally LDA evaluates a projection matrix *W*, say of size $r \times d$, that maximizes the criterion function [13]

$$J_W = \frac{\det\left\{W^T \sum_B W\right\}}{\det\left\{W^T \sum_W W\right\}} \qquad (9)$$

Above det{.} is matrix determinant. The maximum value of r is $d - 1$. For a test pattern y, its class label C_y can be computed as

$$C_Y = \arg \min_{i=1,2,..C}\{W^T(y-\mu^i)^2 + D_i\} \quad (10)$$

where D_i take into account of prior information.

Fig. 6 Training database images (LDA)

The AT&T lab database is used which consists of 40 folders each folder contains 10 images of a particular person with different facial expressions. Some of the training database images are shown in figure 6, and the normalized dataset is presented in figure 7.

Fig. 7 Normalized Training database images (LDA)

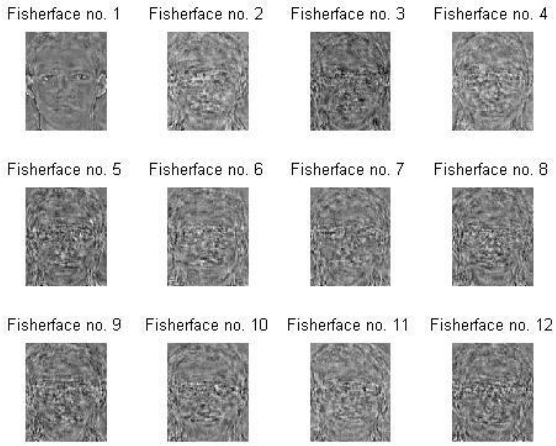


Fig. 8 Fisherface Images

The fisher faces for the normalized training datasets are shown in figure 7. The mean image is shown in figure 8, which consists of feature of all the training images.

Fig. 8 Mean Images

(a) **(b)**

Fig.9 (a)Input and (b)Re-constructed images

Table: 2: The Rank one Recognition Rate for different Methods using different number of Input images

In figure 9, input and reconstructed image is shown. These images are very much similar, with slight difference in intensity.

Table 2, the Rank one Recognition Rate for different number of Input images

Test Sample sizes (number of images)	LDA
400 (280+120)	86.07%
300 (210+90)	90.48%
200 (140+60)	93.57%
100 (70+30)	95.71%

In Table 2, the Rank one Recognition Rate for different number of Input images is shown. It must be remembered that first three images of each folder, i.e., 30% of the total images are used as training images. For 100 images the recognition rate is 95.71% and for 400 images, the recognition rate is 86.07%. Moreover, as the number of images increased form 100 to 400 the performance is not deteriorated much. But in alone LDA algorithm does not provide very effective solution when rank one recognition rate is considered.

7. Fingerprint Identification

Fingerprint identification is well-accepted and popular biometrics. Fingerprints have been used for identification for over a century due to its inherent advantages. In past thumb impression was used for the identification of a person. Now this methods has become automated (i.e. a biometric) due to advancements in sensor and computer based applications..

7.1 Minutia Based Matching:

Considering T and Q are the feature vectors, which represents minutiae points, from the template and query fingerprint, respectively. Each element of these feature vectors is a minutia point. The representation of a minutia is the triplet x, y, θ, where x, y is the minutia location and θ is the minutia angle. Assuming that number of minutiae in T and Q be m and n, respectively [7-9]. Then T and Q can be represented as

$$T = m_1, m_{2,\ldots\ldots\ldots,} m_m, m_i = x_i, y_i, \theta_i, i = 1\ldots\ldots m$$

$$Q = m_1^{'}, m_{2,\ldots\ldots\ldots,}^{'} m_m^{'}, m_j^{'} = x_j^{'}, y_j^{'}, \theta_j^{'}, j = 1\ldots\ldots n \quad (11)$$

A minutia m_i in T and $m_j^{'}$ in Q are considered as matched if:

$$sd(m_j^{'}, m_i) = \sqrt{\left(\left(x'_j - x_i\right)^2 + \left(y'_j - y_i\right)^2\right)} \le r_o \quad (12)$$

$$dd(m_j^{'}, m_i) = \min\left(|\theta_j^{'} - \theta_i|, 360 - |\theta_j^{'} - \theta_i|\right) \le \theta_0 \quad (13)$$

Here, r_0 and θ_0 are the parameters of the tolerance window.

If a proper alignment between query and template fingerprints can be adjusted then the number of "matching" minutia points can be maximized. Correct alignment of two fingerprints demands for finding a complex geometrical transformation function (map()), that maps the two minutia sets (Q and T). The map() function should be tolerant to distortion, and it should be able to recover rotation, translation and scale parameters with fair accuracy. Let match() be a function defined as:

$$match(m_j^{''}, m_i) = \begin{cases} 1, & if\ m_j''\ and\ m_i \\ 0 & otherwise \end{cases} \quad (14)$$

where, map $\left(m_j^{'}\right) = m_j^{''}$.Thus, the minutia matching problem can be formulated as

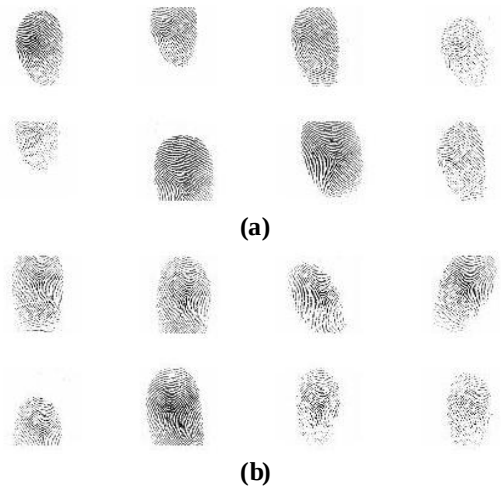
$$\max_P \sum_{i=1}^{m} match\left(map\left(m'_{P(i)}\right), m_i\right) \quad (15)$$

where P() is the minutia correspondence function that determine the pairing between the minutia points in Q and T.
The minutia-based matching can be divided into three stages: coarse matching, fusion and fine matching. Initially, on a number of seeds coarse matching is performed, and the obtained results are then fused to obtain a relationship between minutiae in the template and query minutiae sets. Then using the support degree of the elements in the constrained relations, the one-to-one correspondence is finally determined by comparison of similarity of local structures. Here, the similarity measure is given as follows: Assume that only H pairs of matched points are found during the matching process then the computed score obtained as

$$Score = \frac{H}{\min(M, N)} \quad (16)$$

where, M and N are the number of minutia in query and database image respectively.

The Fingerprint Verification Competition (FVC2002) database is used for the analyzing the algorithm. The database consist 8 fingerprint images with different orientations per person and a total of 9 persons are considered. Thus, in all a total of 72 finger images are in the database and are indexed as1 to72.



(a)

(b)

Fig. 10 (a) Loaded Fingerprints person1 (2) Loaded Fingerprints person1

In Figure 10, for an example, loaded images of the first two persons are shown. It can be visualized from the figure that various possible image orientations are considered. The algorithm test is performed on the all 72 images.

7.2 Processes

Fingerprint matching techniques require initial image processing of the finger set that has been obtained.

(a) Initial Image Processing

Fingerprint Image enhancement is a process which makes the image clearer for further operations. Sometimes the fingerprint images captured from scanner or any other image capturing media are not of perfect quality. These enhancement methods, increases the contrast between ridges and valleys. These processes are also helpful in connecting the false broken points of ridges due to lack of ink. Hence, these methods are very useful for keeping a higher accuracy to fingerprint recognition.

(b) Histogram Equalization:

Histogram equalization is a simple process which increases the pixel value distribution of an image thus increases the perception information. The original fingerprint image is shown in 11(a), and the image after the after the histogram equalization is shown in 11(b).

(a) (b)

Figure 11 (a) Image before equalization (b) Image after equalization

(c) Fingerprint Enhancement by Fourier Transform

This process is based on Fourier Transform. In this process the image under investigation is further divided into small processing blocks (32 by 32 pixels) and then, spatial Fourier transform is performed as:

$$F(u,v)=\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\exp\left\{-j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)\right\} \quad (17)$$

for u = 0, 1, 2, ..., 31 and v = 0, 1, 2, ..., 31.

Above $F(u,v)$ is Fourier transform of $f(x,y)$. A specific block can be enhanced by its dominant frequencies, according to

$$g(x,y)=F^{-1}\left\{F(u,v)\times\left|F(u,v)\right|^{K}\right\} \quad (18)$$

Where the magnitude of the original FFT = $\left|F(u,v)\right|$ and $F^{-1}\left\{F(u,v)\right\}$ is obtained as

$$f(x,y)=\frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}F(u,v)\exp\left\{j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)\right\} \quad (19)$$

for x = 0, 1, 2, ..., 31 and y = 0, 1, 2, ..., 31.

The 'K' in formula (18) is obtained experimentally and found to be K=0.45. A higher 'K' fills up small holes in ridges and improves the appearance of the ridges. High value of 'K' can result in false joining of ridges and it may possible that a termination might become a bifurcation.

(a) (b)

Figure 12 (a) Image before FFT (b) Image after FFT

In figure 12, it is clear that the lines are smoother now as compared to the histogram image. Hence to take advantages of both the methods, we first pass an input image though histogram equalization process, and the obtained image is passed through FFT enhancement method and the obtained image is shown in figure 13 (b).

Figure 13 (a) Input Image After Histogram Equalization (b) Image after FFT

While finger prints are in RGB, thus finger print enhancement is applied which includes following step:

1. RGB to gray conversion.
2. Gray to binary conversion.
3. Enhancing image to remove break point in Ridge and adjusting intensity of image.
4. Thinning Ridge Points.
5. Locating Core Point.
6. Locating Terminations and Bifurcations
7. Calculating ROI and Cropping around core point.

After all the above mentioned steps we get as shown below (Fig.14):

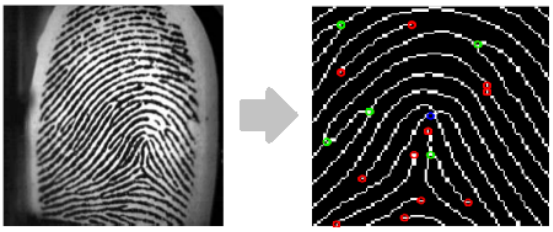


Figure 14: Input Print to Database Image

In figure 15, similarity score vs. image index is plotted for minutia based matching scheme. If threshold is kept at the higher level of nearly 0.5, then image 70 will be falsely rejected. Similarly if threshold is kept at the lower level then the image 5 will be falsely accepted (figure 16).

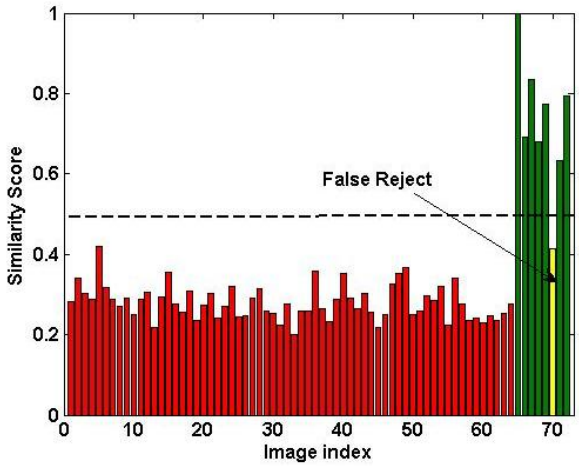


Figure 15: Similarity Score vs. image index (test images 65-72, false reject 70)

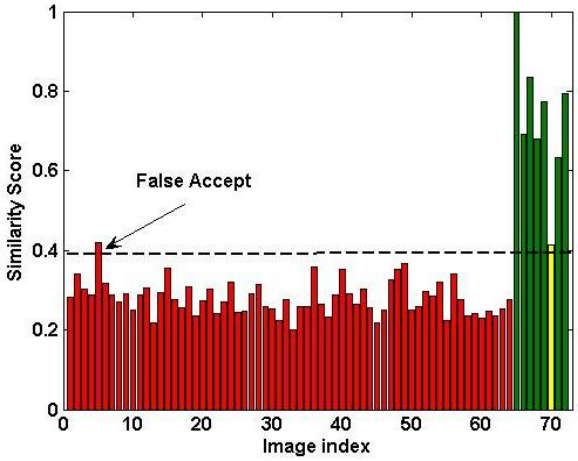


Figure 16: Similarity Score vs. image index (test images 65-72, false accept 5)

The above mentioned techniques are based on the principle of learning and matching. As we increase the threshold value for the matching, false rejection rate increases and similarly for the lower values of threshold false acceptance rate increases. The main problems with fingerprint techniques are that algorithms are dependent on the quality and orientation of the image and thus affect the results.

In the Table 3, given below, matched fingerprints are identified at different threshold scores. The simple procedure for accepting the test images is as follows

if

$T_{Score} > T_{th}$

Fingerprint matched

else

discard image

end

In table, test and matched fingerprints are shown at different thresholds. In the first set of experiment, images numbers from 9 to 16 are tested at the threshold levels of 0.40, 0.46, 0.48 and 0.54.

Table 3 Minutia based fingerprint matching at various thresholds

Threshold Score	Test images	Matched Fingerprints
0.40	9,10,11,12,13, 14,15,16	9,10,11,12,14,15,16, 18,20,3,34, 35, 38
0.46	9,10,11,12,13, 14,15,16	9,10,11,12,14,15,16, 20
0.48	9,10,11,12,13, 14,15,16	9,10,11,12,14,15,16, 20
0.54	9,10,11,12,13, 14,15,16	9,10,12,14,15,16

It is clear from the table that when the threshold is at low level of 0.40, the falsely accepted fingerprints are 3, 18, 20, 34, 35 and 38 and the falsely rejected image is 13. Now when the threshold is kept at the level of 0.48, the only false acceptance is image 20 while the false rejection is 13. Now when the threshold is kept at the level of 0.54, the falsely rejected fingerprints are 11 and 13.

As discussed above the face and fingerprint methods are not free form errors, thus a further improvement is needed to reduce the errors.

8. Decision Fusion

On the basis of the integration of the decision made by the face recognition module and fingerprint verification module, the ultimate decision is made by fuzzy system. In the event of having the output of each module is only a category label, either w_1 (claimed identity is true) or w_2 (claimed identity is not true) can be done with certain level of accuracy. A more precise decision can be made by accumulating the decision of individual methods if the output of each module is a similarity value.

For fingerprint verification and face recognition, let X_1 and X_2 be the random variables which denote the similarity (dissimilarity) between an input and a template for fingerprint verification and face recognition, respectively. Let $p_j\left(X_j|w_i\right)$ where $i, j = 1,2$ be the class-conditional probability density functions of X_1 and X_2. As X_1 and X_2 are statistically independent thus intersection is equivalent to multiplication. Hence the joint class-conditional probability density function of X_1 and X_2, can be written as:

$$p\left(X_1 \text{ and } X_2|w_i\right) = \prod_{j=1}^{2} p_j\left(X_j|w_i\right), \quad i = 1,2 \qquad (20)$$

Let R^2 denote the three-dimensional space spanned by $\left(X_1 \text{ and } X_2\right)$; R_1^2 *and* R_2^2 denote the w_1 - region and w_2 - region, respectively $\left(R_1^2 + R_2^2 = R^2\right)$; ε_0 is the acceptable FAR. According to the Neymen-Pearson rule for hypothesis testing, an observation $X^0\left(X_1^0, X_2^0\right)$, can be classified as:

$$\left(X_1^0, X_2^0\right) \in \begin{cases} w_1, & \text{if } \dfrac{p_1\left(X_1^0, X_2^0|w_1\right)}{p_2\left(X_1^0, X_2^0|w_2\right)} > \lambda \\ w_2 \end{cases} \qquad (21)$$

Where λ denotes the minimum vales and satisfies the relation

$$\lambda = \frac{p_1\left(X_1, X_2|w_1\right)}{p_2\left(X_1, X_2|w_2\right)} \text{ and } \in_0 = \int_{R_1} p_2\left(X_1, X_2|w_2\right) dX_1 dX_2 \qquad (22)$$

8.1 Fuzzification of Face recognition method

The idea of Fuzzification of the Face and fingerprint recognition techniques is shown in figure 17 [10]. For the input of the Fuzzifier the selected membership function is $\prod$ and at the output of the fuzzy system the membership function is chosen to be Δ. As the samples follow I.I.D. process. Therefore, a truncated Gaussian membership function known as $\prod$ function is selected. In the function α, β and γ defined as minimum, maximum and mean value of the training data set. The c_1, c_2 define the values at which the membership function takes a value of 0.5.

$$\Pi(z;\alpha,\gamma,\beta) = \begin{cases} 0 & z \le \alpha \\ 2^{m-1}\left(\dfrac{z-\alpha}{\gamma-\alpha}\right)^m & \alpha < z \le c_1 \\ 1-2^{m-1}\left(\dfrac{\gamma-z}{\gamma-\alpha}\right)^m & c_1 < z \le \gamma \\ 2^{m-1}\left(\dfrac{z-\gamma}{\beta-\gamma}\right)^m & \gamma < z \le c_2 \\ 1-2^{m-1}\left(\dfrac{\beta-z}{\beta-\gamma}\right)^m & c_2 < z \le \beta \\ 0 & z \ge \beta \end{cases} \qquad (23)$$

The value of the *m* can be selected to alter the shape of the $\prod$ function. In this work the value of *m* is taken to be 2.

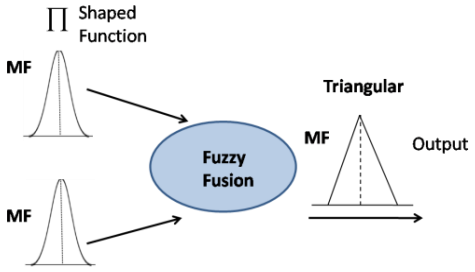


Figure 17: Fuzzy fusion of Face and Fingerprint Techniques

It is clear from above expression that the shape and structure of the Π function can be altered by varying the mentioned parameters.

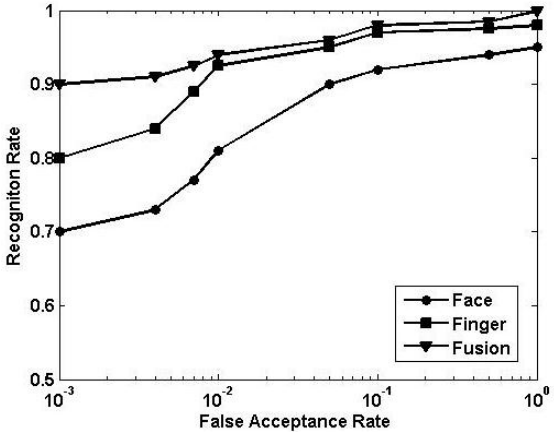


Figure 18 FAR vs. Recognition rate

Figure 18, shows the face recognition rate for Face, Finger, and for the fusion of these two processes. The performance of Face recognition method is poorest, as for the FAR < 0.001, the recognition rate is only 70 %, and for the FAR < 0.1, the recognition rate is 86 %. The performance of the Fingerprint identification method is better in comparison to Face recognition method. In fingerprint identification technique for the FAR < 0.001, the recognition rate is 80 %, and is much better in comparison to face methods. For both the methods, as the FAR increases, the recognition rate increases. However as the large FAR is not acceptable in most of the applications, therefore above two methods are combined using fuzzy methods and the obtained results are superior in comparison to others as FAR < 0.001, the recognition rate is 90.07 %, which can be reached at the level of 100% for FAR of 1. The obtained preliminary results are promising and provide a basic foundation for the future research.

CONCLUSIONS

A biometric system which basically relies on a single biometric identifier is most of the time unable to meet the desired performance requirements in making a personal identification. User identification based on the combination of various biometrics is an emerging trend nowadays. In this work a multimodal biometric system, which integrates fingerprint verification, and face recognition in making an individual identification is used. In this system, the capabilities of each individual biometric can be fully utilized. It can be applied to restrict some of the limitations of a single biometric system. The results presented in the paper clearly show that an integrated system generates a more reliable identity of user in comparison of the identity established by either face recognition or a fingerprint verification system alone.

REFERENCE

1. A. K. Jain, R. Bolle, and S. Pankanti, "Biometrics: Personal Identification in Networked Security,", Eds.: Kluwer Academic Publishers, 1999.

2. Rabia Jafri and Hamid R. Arabnia ‘A Survey of Face Recognition Techniques Journal of Information Processing Systems, Vol.5, No.2, June 2009.

3. M. Turk and A. Pentland," Eigenfaces for recognition, *"J. Cognitive Neuroscience*, Vol. 3, 71-86., 1991.

4. Delac, K.; Grgic, M. & Grgic, S. (2006). Independent Comparative Study of PCA, ICA, and LDA on the FERET Data Set, *International Journal of Imaging Systems and Technology*, Vol. 15, No. 5, 2006, pp. 252-260

5. Beveridge, J.R.; She, K.; Draper, B.A. & Givens, G.H. (2001). A Nonparametric Statistical Comparison of Principal Component and Linear Discriminant Subspaces for Face Recognition, *Proc. of the IEEE Conference on Computer*

6. P. N. Bellhumer, J. Hespanha, and D. Kriegman, "Eigenfaces vs. fisherfaces: Recognition using class specific linear projection," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 17, no. 7, pp. 711–720, 1997.

7. Zhong Wei-Bo, Ning Xin-Bao and Wei Chen-Jian, "A Fingerprint Matching Algorithm Based on Relative Topological Relationship Among Minutiae," *IEEE International Conference on Neural Networks and Signal Processing*, 2008, pp. 225-228.

8. Jiong Zang, Jie Yuan, Fei Shi and Si-dan Du, "A Fingerprint Matching Algorithm of Minutiae Based on Local Characteristic," *Fourth International Conference on Natural Computation*, 2008, pp. 13-17.

9. Xuzhou Li and Fei Yu, "A New Fingerprint Matching Algorithm Based on Minutiae," *Proceedings of International Council of Chemical Trade Associations*, 2009, pp. 869-873.

10. G. Riley, Expert Systems – Principle and programming (Pws-Kent, Boston, 1981),1-59.

