Volume 8, Issue 3
June 2019

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Fuzzy Fusion of Face and Fingerprint Using Novel Threshold Estimation Technique for User Authentication

[1]Aparna Tiwari
[1] UPTU, Lucknow, India
E-mail: [1]aparnatiwari2710@gmail.com

ABSTRACT

With the advancement of internet, use of facebook, twitter, online banking, etc has increased tremendously. All of these applications require login and password for the authentication of user. But sometimes password can be stolen or lost and online application can be hacked. Therefore, to enhance security biometrics can be used, where any unique feature of user is also accompanied with passwords. But the recognition rate of various biometric which are user friendly is not very good. Therefore, sometimes it is beneficial to use more than one biometrics for user identification. This mixed form of biometrics provides better security. Here more than one type of biometric identifiers are combined together to obtain more accurate identification of the user. The biometrics can be combined by using probabilistic approach or by using other methods such as Fuzzy fusion etc. in this paper a fuzzy fusion technique is used, and it has been fund that recognition rate of combined system improves significantly.

Keywords: *PCA, Biometrics, Eigen Values and Eigen Functions, Fingerprint, Fuzzy Logic*

1. INTRODUCTION

Biometrics could be characterized as the science of making the reorganization of a person on the basis of his/her behavioral or physical characteristics. The uni-modal systems provide decent results in terms of recognition of users. However, accuracy is limited and as far as surveillance and security, the above mentioned methods alone are not quite effective. Still the computational complexity is quite less. Uni-modal systems are mingled together in this paper to evolve a multimodal system which makes use of two or more than two biometric identifier for the making the verification and authentication of the user. Biometric systems, that co-ordinate data at an early phase of processing are more effective in comparison to integration at a later stage. This happens due to the set of key feature that comprises whole information about the input biometric data than available at little later stage therefore it is expected to get improved recognition outputs by fusion at the feature level. However, in real systems fusion at this level is a quite hard job because of the fact that a majority of vendors doesn't give access to the set of feature data. Hence, the only possible solution is the fusion at the decision level. Moreover, in biometrics user acceptability is very important, and most of the biometric identifiers which provide very good recognition rate are not user friendly.

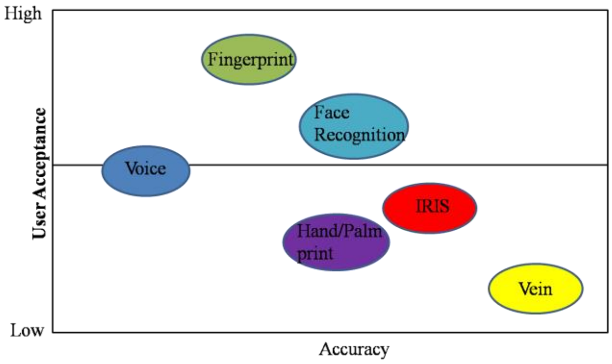


Fig. 1 User Acceptance vs.accuracy

Face and fingerprint are two biometrics which shows good accuracy with high user acceptability. Moreover in real system it is necessary that, the processing time of system should be as small as possible. Therefore complex algorithms cannot be used.

In this paper, face and fingerprint based multimodal system is discussed. For face recognition PCA algorithm is selected with novel threshold method which improves the results significantly. For fingerprint minutiae based method is considered. Finally, fuzzy fusion is done to obtain final recognition.

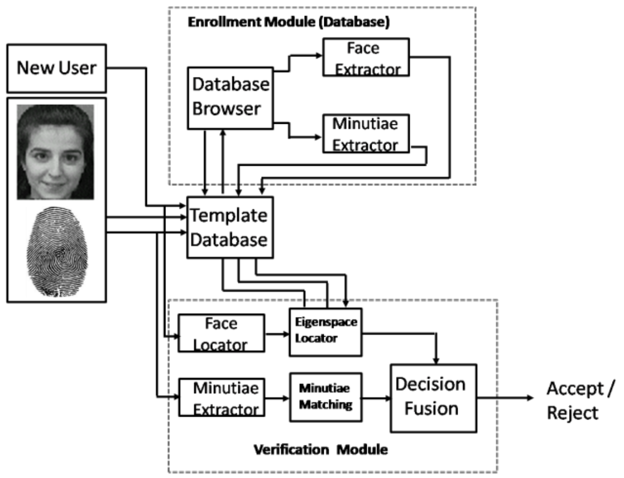


Fig. 2 Enrollment and verification module of multimodal system

The generic design for multimodal biometric using face and fingerprint is shown. Here, feaure of incoming user is extracted and matched with already stored in database.

The paper is organized in six sections, section 2 of the paper details the face recogntion process, section 3 of the paper details about fingerprnt recogntion. Fuzzy fusion is discussed in section 4 of the paper, section 5 of the paper discusses the simulation results and major conclusions of the paper discussed in section 6 of the paper.

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

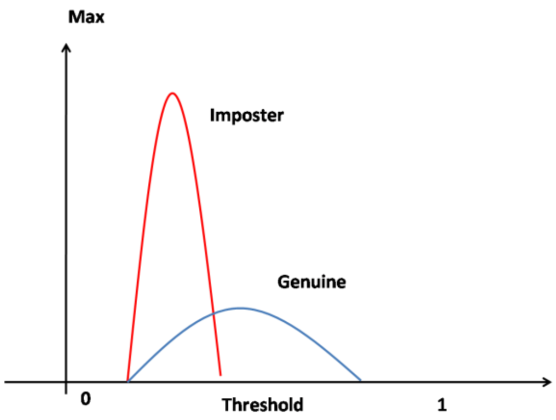


Fig. 3 Imposter and genuine wrong decision

Figure 3, shows how imposter and genuine user can be wrongly recognised. It is possible when feature of an imposter matches with a genuine person and user is accepted. Similarly, for genuine person feature does not match with database.

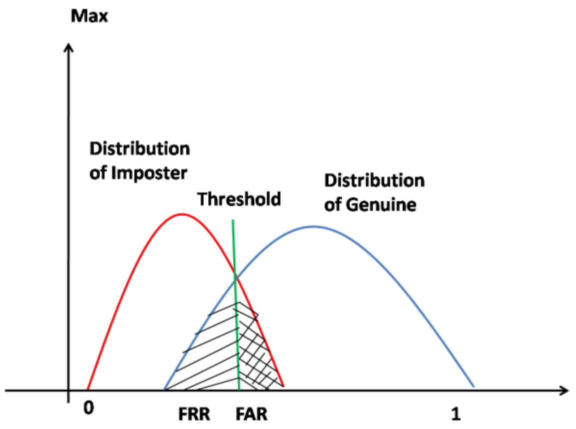


Fig. 4 Imposter and genuine distribution function with threshold

In figure 4, distribution of imposter and genuine person is illustrated. Here, as threshold increases FRR (False Rejection Rate) increases. But if threshold is decreaased FAR (False Acceptance Rate) increases. Therefore, threshold should be selecetd very carefully to minimimze both FAR and FRR, and where FAR becomes equal to FRR is known as EER (Equal Error Rate). Major problem with biometrics system is that distribution of imposter and genuine is not known, therefore optimum threshold cannot be set. To counteract such problems heuristic methods are used.

2. FACE RECOGNITION

A. *Principal Component Analysis*

In PCA a two dimensional image is represented as one dimension vector by putting all the row and column together. Then mean is obtained and mean image is subtracted from each image. Then for the co-variance matrix, eigen values and eigen vectors are obtained. An ortho normal basis is developed by the eigen vectors corresponding to non zero eigen values of the covariance matrix for the sub space inside of which a major number of image information can be referred with a little measure of flaw. The sorting of eigen vectors is accomplished as per the eigen values that corresponds them in a descending order. In the image, the eigen vector that corresponds to the greatest eigen value has the highest variance [5]. In the similar way, the least eigen value corresponds to the minimum variance. At this point, emphasis must be given on the fact that the decreased dimensions are initial five to ten percent of the whole dimensions.

The straight forward process for finding out which face class gives the perfect description of an input facial image is to discover the face class *k* that reduces the Euclidean distance

$$\varepsilon_k = \left\| \Omega - \Omega_k \right\| \tag{1}$$

where, Ω_k is a vector describing the k^{th} face class. If ε_k is less than some predefined threshold, a face belongs to the class *k*.

3. FINGERPRINT RECOGNITION

Among a number of biometrics, identification with fingerprint is one of the mostly used and popular processes. Due to its inherent benefits, these have been quite effective for the purpose of identifying for about over a century. In few years back, a person was identified by making use of thumb impression. As far as modern method is concerned, this process has turned out to be automated (i.e. a biometric) and this is possible because of the developments in sensor and computer applications. The reason behind the popularity of fingerprint identification is the inherent comfort in acquisition, the number of sources (ten fingers) that make the collection easy and reliable, and also their established application and collections by immigration and enforcement of law. As fingerprint recognition methods are very popular, numerous algorithms are proposed for the enhancement of the accuracy. Many algorithms show some improvement in the accuracy, but on the darker side the complexity of the algorithms increases drastically.

A. *Minutiae Based Matching:*

Considering *Q* and *T* and are the feature vectors, which refers the minutiae points, from the query and template fingerprint, respectively. All elements of the above mentioned feature vector is a minutiae point. The representation of a minutiae is the triplet x, y, θ, where x, y is the minutiae location and θ is the minutiae angle. Assuming that number of minutiae in *T* and *Q* be *m* and *n*, respectively [6]. Then *T* and *Q* can be represented as

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

$$Q = m_1^{'}, m_{2,..........,}^{'} m_m^{'}, m_j^{'} = x_j^{'}, y_j^{'}, \theta_j^{'}, j = 1......n$$

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

$$sd(m_j^{'}, m_i) = \sqrt{\left(\left(x'_j - x_i \right)^2 + \left(y'_j - y_i \right)^2 \right)} \le r_o \tag{3}$$

$$dd(m_j^{'}, m_i) = \min\left(|\,\theta_j^{'} - \theta_i\,|, 360 - |\,\theta_j^{'} - \theta_i\,| \right) \le \theta_0 \tag{4}$$

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

In the case an appropriate arrangement between template and query fingerprints can be balanced then the "matching" minutiae point's number can be set to maximum. Perfect alignment of two fingerprints demands for discovering a complex geometrical transformation function (map ()), that maps the two minutia sets (*Q* and *T*). The map () function should be capable to deal with distortion, and it should have the ability of recovering translation, rotation and parameters of scale with a good measure of precision. Let match () be a function defined as:

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

$$match(m''_j, m_i) = \begin{cases} 1, & if\ m''_j\ and\ m_i \\ 0 & otherwise \end{cases} \quad (5)$$

where, map $\left(m'_j\right) = m''_j$. Therefore, the minutiae matching issue can be formulated as

$$\max_P \sum_{i=1}^{m} match\left(map\left(m'_{P(i)}\right), m_i\right) \quad (6)$$

where P() is the minutiae correspondence function that find out the pairing between the minutia points in Q and T.

The classification of the minutiae-based matching could be done into three stages: coarse matching, fine and fusion matching. At first, coarse matching is done on a number of seeds, and the outputs we get from this matching are afterwards merged to get a relationship between minutiae in the template and query minutiae sets. At this point, the one-to-one correspondence is at last determined with the help of support degree of the elements in the constrained relations. This is accomplished by comparing of local structures similarity. The measure of similarity here is provided as: Let us assume that we got only *H* pairs of matched points at the time of the matching process then the score we got could be computed as follows

$$Score = \frac{H}{\min(M, N)} \quad (7)$$

where, *M* and *N* are the minutiae number in query and database image respectively.

4. FUZZY FUSION

A. Uni-modal to Multimodal Combining Process

From uni-modal to multimodal combining process, score normalization and biometric fusion methods are important.

(a) Score normalization

The primary goal of the score normalization is to maintain the matching score value in the certain fixed range for each of the uni-modal biometric in the event of their fusion. A score of raw matching is represented as s from the set S of each score for that matcher, and n represents the corresponding normalized score.

Min-Max (MM): This process figures out the raw scores to the [0, 1] range. The measures *min(S) and max(S)* denotes the minimum and maximum value of the score range:

$$n = \frac{s - min(S)}{max(S) - min(S)} \quad (8)$$

(b) Biometric Fusion

Simple sum, Max score and Min score are well known fusion methods. The term n_i^m denotes the normalized score for matcher m ($m = 1, 2, \ldots, M$, where M is the number of matchers) applied to user i ($i = 1, 2, \ldots, I$, where I is the number of individuals in the database). The fused score for user i is denoted as f_i.

Max-Score (MAS): (9)

$$f_i = max(n_i^1, n_i^2, \ldots, n_i^M), \forall i$$

However, these methods have shown limited accuracy, therefore new methods needs to be investigated. In this work Fuzzy logic based fusion methods is applied which is more adaptive and large set of variations on the data can be performed.

Fuzzification of Face and Fingerprint Recognition Method

Fig. 5 shows the fusion at decision level. This level of fusion allows equal weightage to both the biometric identifier.

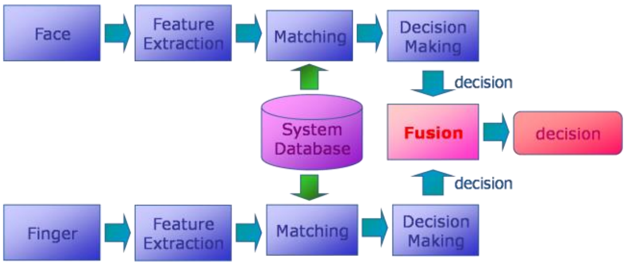


Fig. 5: Fusion System

In fuzzy system Mamdani model is used [8]. For face and finger, Gaussian membership functions are considered. Normalized value 1 is divided into five equal intervals of 0.2 and membership functions are defined as VL, L, M, H, and VH. The output is defined by two triangular membership functions L and H. Twenty fuzzy rules are derived, and centroid method is used for de-Fuzzification.

5. SIMULATION RESULTS

A. Face Recognition

For face AT&T data base is used. The database consists of 400 images. In the experiment we have shown 9 images.

In the first case 9 images are taken as training set, each with mean 100 and standard deviation of 80. In the second step the mean and standard deviation of all images are changed for normalization. This is done to reduce the error due to lighting conditions and background.

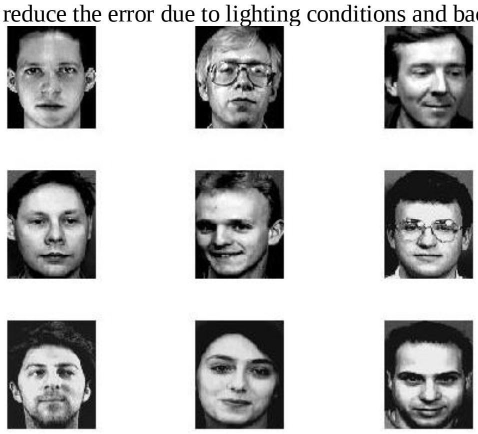


Fig. 6 Training Set (AT&T)

The considered image set is shown in figure 6. For displaying nine images are considered. Mean image is shown in figure 7. Which basically consist of feature of all the trained images, and thus helpful in identification of query images feature.

Fig. 7 Mean image

In the next step, co-variance matrix is created, thereafter the Eigen-values are obtained, and the Eigen values close to zero are dropped and for the left over Eigen values, Eigen vector are obtained. Finally, after the normalization of Eigen vectors, Eigen faces are calculated (Figure 8).

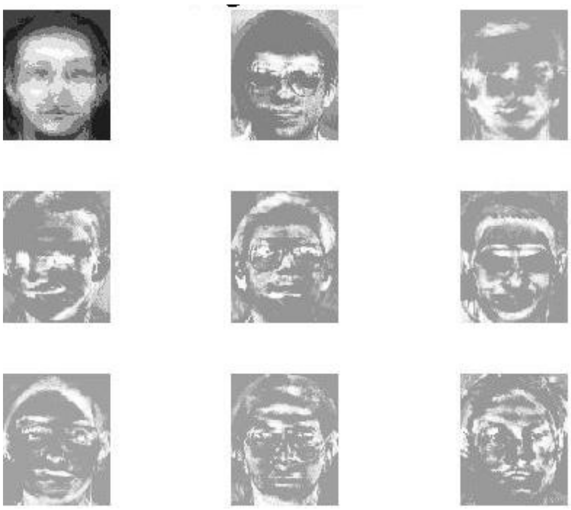
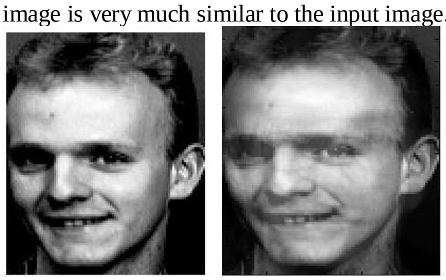


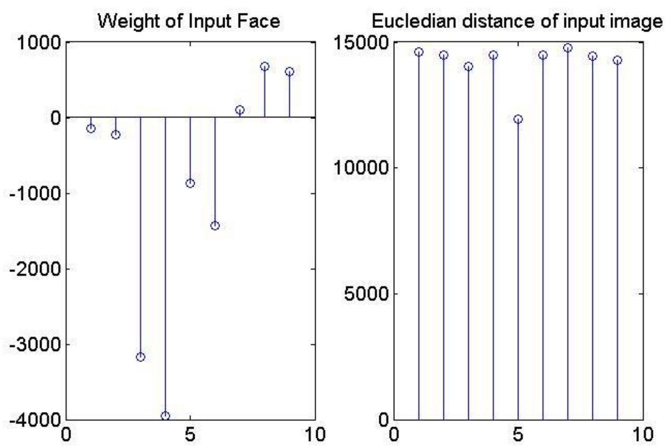
Fig. 8 Eigenfaces

In case of user authentication, template matching is done. In figure 9, the input image and the re-constructed images are shown. The re-constructed image is very much similar to the input image.



(a) **(b)**

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



(a) (b)

Fig. 10(a) weight (b) Euclidean distance of input image

In figure weight of input image with respect to other images is shown Fig. 10(a). Similarly the Euclidean distance of the query image with other images is shown in figure 10(b). It is clear from the figure that, the query image is similar to the 5^{th} image present in the database. However, how much similar they are, is an open question. Thus a threshold point is needed to mathematically identify an user. In biometric based system, correct threshold detection is not straight forward, as if threshold is kept low, then chances of false acceptance increases, similarly, if threshold is kept high enough, then FRR increases. Therefore, threshold is selected heuristically. In this paper, a threshold detection based method based on Euclidean distance is presented, which has much better recognition rate in comparison to earlier method where threshold is taken to be $0.8I_{max}$ [7]. Defining the maximum Euclidian distance with query image as I_{max} , minimum Euclidean distance as I_{min} and average of Euclidean distances with other database images as I_{avg}.

We define threshold as:

$I_{th}= I_{min} +0.06\ I_{max}$

if

$I_{th} < I_{avg}$

Authentication succeed

else

Authentication fails

end

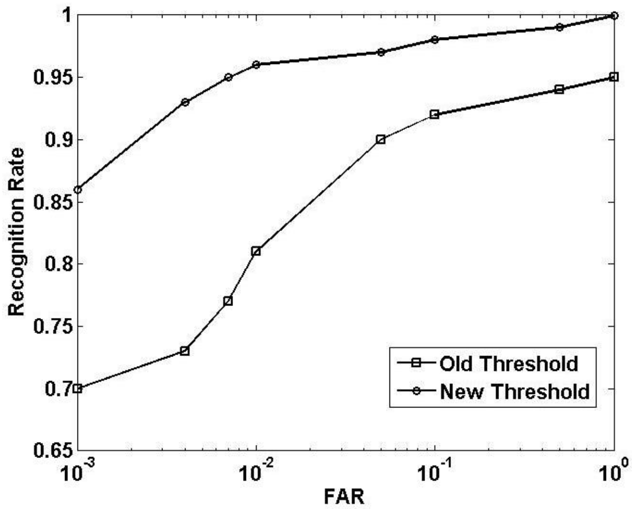


Fig. 11 FAR vs. Recognition Rate

In Fig 11, FAR vs. Recognition rate is presented, here results for both old and new thresholds are shown. It is clear from the figure, that with new threshold results improves tremendously. Comparing the results at FAR level of 10^{-3} with old method recognition rate is 70% and with novel threshold method recognition rate is nearly 86%. Still this recognition rate is not at per with the required recognition rate in most surveillance applications.

B. Fingerprint Recognition

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.

Fingerprint matching techniques require initial image processing of the finger set that has been obtained. The various processes are as under:

Initial Image Processing
Histogram Equalization
Fingerprint Enhancement by Fourier Transform
The RGB to Grayscale Conversion
Gray to binary conversion
Ridge Thinning
Minutiae Marking
False Minutiae Removal

After performing the above mentioned processes we get fingerprint as shown below:

Volume 8, Issue 3
June 2019

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

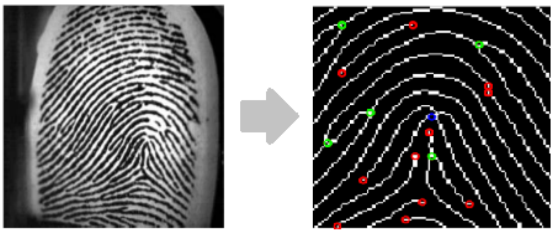


Fig. 12: Input Print to Database Image

In fig. 12, input and image after various processing step is shown.

In fig.13, similarity score vs. image index is plotted for minutiae 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 (fig.14).

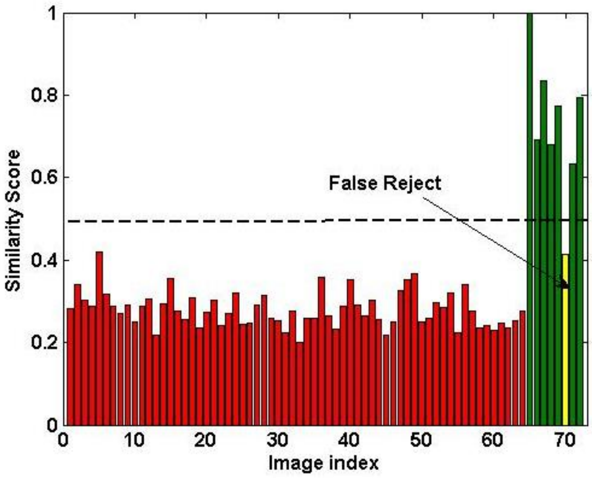


Fig. 13: Similarity Score vs. image index (test images 65-72, false reject 70)

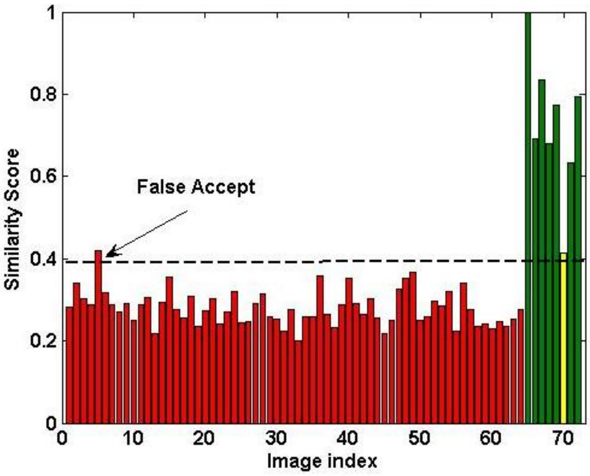


Fig. 14: Similarity Score vs. image index (test images 65-72, false accept 5)

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 these techniques are that they are image dependent and the quality and orientation of the image also affects the results. The simple procedure for accepting the test images is as follows

if

$$T_{Score} > T_{th}$$

Fingerprint matched

else

discard image

end

In fig.15, given below, matched fingerprints are identified at different threshold scores. In fig.15, test and matched fingerprints are shown at different thresholds. In the experiment, images numbers from 9 to 16 are tested at the threshold levels of 0.40, 0.46, 0.48 and 0.54.

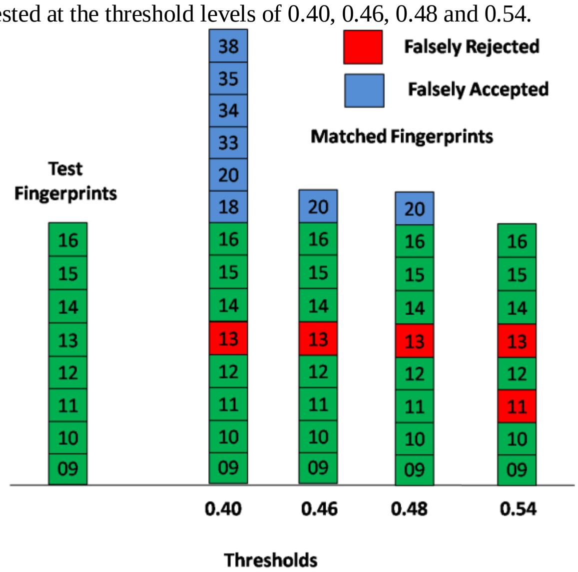


Fig.15: Minutiae based fingerprint matching at various thresholds

It is clear from the figure that when the threshold is at low level of 0.40, the falsely accepted fingerprints are 3, 18, 20, 33, 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.

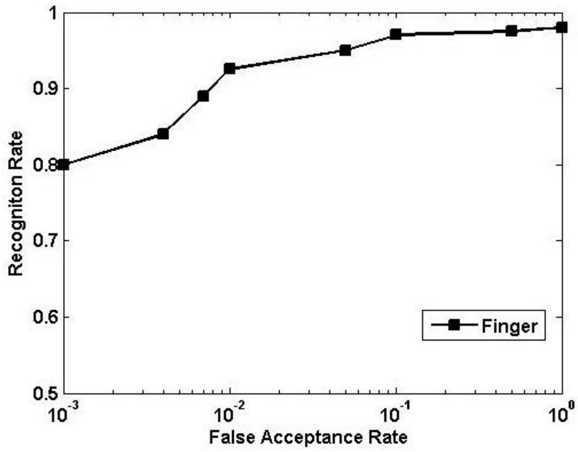


Fig. 16 Recognition Rate vs. False Acceptance rate

Fig. 16, shows the recognition rate vs. FAR for fingerprint. For FAR 0.001 the recognition rate is 80% which increases with FAR. However, for FAR<0.1 the recognition rate is 86%. As discussed above the face and fingerprint methods are not free form errors, thus a further improvement is needed to reduce the errors.

Fig. 17, shows the face recognition rate for Face, Finger, and for the fuzzy fusion [8] of these two processes. With old threshold, 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

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

recognition rate is 86 %. The performance of the Fingerprint identification method is better (old threshold) in comparison to Face recognition method.

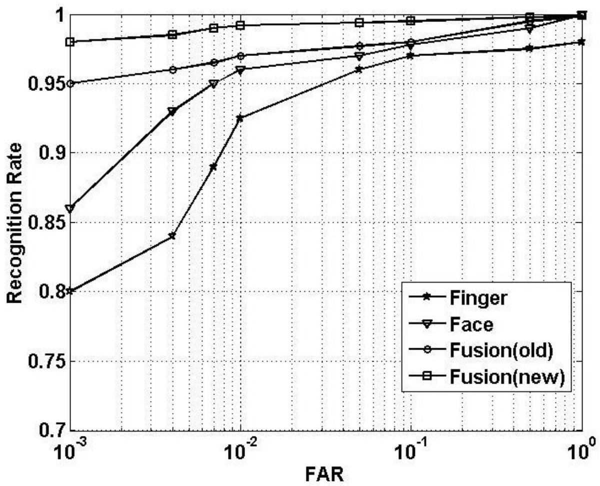


Fig. 17 Fuzzy Fusion (Face and Finger) with old and new threshold

In fingerprint identification technique for the FAR < 0.001, the recognition rate is 80 %, and is much better in comparison to face methods. With new threshold method, face recognition method performs better than fingerprint recognition. For both face and finger 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 95.07 %, (old threshold) and with new threshold the recognition rate is as high as 98%.

6. 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. In this paper, both face and fingerprint recognition is considered. For face recognition a new threshold method is developed based on Eigen values. The results of face and finger recognition is combined together using the fuzzy fusion and through this process accuracy of 98% is achievable.

REFERENCES

[1] Jain, A.K., Bolle, R. & Pankanti, S. (Eds.).1999. "Biometrics: Personal Identification in Networked Security," Dordrecht, Netherlands: Kluwer Academic Publishers.

[2] Jafri, Rabia & Arabnia, Hamid R.2009. 'A Survey of Face Recognition Techniques', *Journal of Information Processing Systems*, Vol.5, No.2, June 2009.

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

[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**, 5:252-260.

[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*, CVPR, 2001: Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Published by *IEEE*, Vol.**1**, 1:535:542.

[6] Alessandro Farina, Zsolt M.Kovacs-Vajna, Alberto leone, "Fingerprint minutiae extraction from skeletonized binary images," Pattern Recognition, Vol.32, No.4, pp. 877-889, 1999.

[7] Marijeta Slavković1, Dubravka Jevtić1, "Face Recognition Using Eigenface Approach" Serbian Journal Of Electrical Engineering, Vol. 9, No. 1, February 2012, 121-130.

[8] Dubois, D. and H. Prade, " Fuzzy Sets and Systems: Theory and Applications," Academic Press, New York, 1980.

AUTHOR PROFILES

Aparna Tiwari received the M.Tech. degree in computer science from Kashi Institute of Technology Varanasi, INDIA. His are of interest includes image processing and biometrics.