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

Aparna Tiwari
1 UPTU, Lucknow, India
E-mail: 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.

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, feature 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 recognition process, section 3 of the paper details about fingerprint recognition. 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.
In a biometric system, the recognition process involves identifying a biometric feature, usually a fingerprint, to authenticate an individual. This process can be divided into two main stages: feature extraction and matching.

### Feature Extraction

Feature extraction is the process of converting the biometric data into a form that is suitable for comparison. For fingerprint recognition, this involves identifying key features such as minutiae points, which are the small details on the fingerprint ridges. These features are extracted from the fingerprint image, and a feature vector is created for each fingerprint.

### Matching

Matching involves comparing the extracted feature vectors of the fingerprint to be identified with the feature vectors stored in the database. The goal is to find the feature vector in the database that is most similar to the query feature vector.

#### Minutiae Based Matching

In minutiae based matching, the extracted minutiae points from the query fingerprint are compared with the minutiae points in the template fingerprint. The matching process involves finding the best alignment of the two fingerprints, which is typically determined by minimizing the Euclidean distance between the corresponding minutiae points.

#### Principal Component Analysis (PCA)

PCA is a statistical method used for dimensionality reduction. It transforms high-dimensional data into a lower-dimensional space by identifying the directions of maximum variance (principal components). In the context of fingerprint recognition, PCA is used to reduce the dimensions of the feature vectors, making the matching process more efficient.

### Error Rate

The error rate in biometric systems is typically measured using two metrics: False Acceptance Rate (FAR) and False Rejection Rate (FRR). FAR is the probability of accepting an imposter as genuine, while FRR is the probability of rejecting a genuine person as an imposter.

The EER (Equal Error Rate) is the threshold where FAR becomes equal to FRR. It is a critical metric for evaluating the performance of biometric systems, as it indicates the point at which the system is equally likely to make a false acceptance or rejection.

### Conclusion

Biometric systems are becoming increasingly important in various applications due to their high accuracy and reliability. However, they also face challenges such as the need for efficient feature extraction and matching algorithms. Future research in this area should focus on developing methods that can handle larger datasets, improve accuracy, and reduce the computational cost of biometric systems.

---

**References:**


match\( (m'_{ji}, m_i) = \begin{cases} 1, & \text{if } m'_{ji} \text{ and } m_i \\ 0, & \text{otherwise} \end{cases} \) \tag{5}

where, map \( (m'_{ji}) = m_{ji} \). Therefore, the minutiae matching issue can be formulated as

\[
\max_P \sum_{i=1}^{I} \text{match} \left( \text{map} \left( m'_{pi(1)} \right), m_i \right)
\]

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

\[
\text{Score} = \frac{H}{\min(M, N)}
\]

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:

\[
n = \frac{s - \min(S)}{\max(S) - \min(S)}
\]

(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 \( m \) \((m = 1, 2, ..., M, \) where \( M \) is the number of matchers) applied to user \( i \) \((i = 1, 2, ..., I, \) where \( I \) is the number of individuals in the database). The fused score for user \( i \) is denoted as \( f_i \).

Max-Score (MAS):

\[
f_i = \max(n_i^1, n_i^2, ..., n_i^M), \quad \forall i
\]

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.

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.

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.
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

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\textsuperscript{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. 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:

\[ I_{th} = I_{min} + 0.06I_{max} \]

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\textsuperscript{-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 to 72. 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:
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).

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

\[ T_{\text{Score}} > T_{\text{th}} \]

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.

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. 15: Minutiae based fingerprint matching at various thresholds

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.
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

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.