# Multi Biometric System for Verification with Minimum Training Data

Mayank Vatsa, Richa Singh, P. Gupta
Indian Institute of Technology, Kanpur, 208016 INDIA
Email: {mayankv, richas, pg}@cse.iitk.ac.in

## Abstract

*This paper presents the multi biometrics system for identity verification based on face and signature. The proposed system is designed for applications where the training database contains one face and one or two signature image for each individual. This system has three modules namely face recognition, signature recognition and multi-biometrics. In face recognition, first the face is detected using the triangulation algorithm and then it is recognized based on KDDA and the Haar wavelet algorithm. In signature recognition, the signature is matched with stored database image using the Haar wavelet. Multi-biometrics algorithm considers the results of face and signature recognition and gives the final matching result based on the fusion rule. This system is tested on a database prepared by the authors and the overall accuracy of the system is found to be 94.37%.*

## 1. Introduction

In recent years, biometrics authentication has seen considerable improvements in reliability and accuracy, with some of the traits offering good performance. However, even the best biometric traits to date are facing numerous problems, some of them inherent to the technology itself. In particular, biometric authentication systems generally suffer from enrollment problems due to non-universal biometric traits, susceptibility to biometric spoofing or insufficient accuracy caused by noisy data acquisition in certain environments.

Multi-biometrics may be used to overcome these problems. Driven by lower hardware costs, a multi-biometric system uses multiple sensors for data acquisition. This allows it to capture multiple samples of a single biometric trait (called multi-sample biometrics) and/or samples of multiple biometric traits (called multi-source or multimodal biometrics). This approach also enables a user who does not possess a particular biometric identifier to still enroll and authenticate using other traits, thus eliminating the enrollment problems and making it universal.

As suggested in [1], [2] multibiometric systems are broadly categorized into three system architectures which are according to the strategies used for information fusion:

- Fusion at the Feature Extraction Level
- Fusion at the Matching Score Level
- Fusion at the Decision Level

In **Fusion at the Feature Extraction Level**, information extracted from the different sensors is encoded into a joint feature vector, which is then compared to an enrollment template (which itself is a joint feature vector stored in a database) and assigned a matching score as in a single biometric system.

In **Fusion at the Matching Score Level,** feature vectors are created independently for each sensor and are then compared to the enrollment templates which are stored separately for each biometric trait. Based on the proximity of feature vector and template, each subsystem computes its own matching score. These individual scores are finally combined into a total score, which is passed to the decision module.

In **Fusion at the Decision Level**, a separate authentication decision is made for each biometric trait. These decisions are then combined into a final vote. This architecture is rather loosely coupled system architecture, with each subsystem performing like a single biometric system.

This paper describes an efficient algorithm designed for face and signature based multimodal biometrics system using the "Fusion at the Matching Score Level" architecture. This system can be used at various competitive examinations, banks and other places where the training dataset is very less (only one face image and one or two offline signature images). For example, various competitive examinations are conducted at every level in the country in which hundreds of thousands of students appear every year. In these examinations there may be various types of unfair activities such as other person appears in the examination in place of the candidate or for the examinations in which the number of attempts are limited, a candidate may appear for several times and so on. To avoid such problems a multimodal biometric system for checking the various unfair means during the examinations is of current interest. This paper proposes an efficient verification algorithm that can be used for the purpose. Next section presents the algorithms. Experimental results are given in the third section and last section is the conclusion.

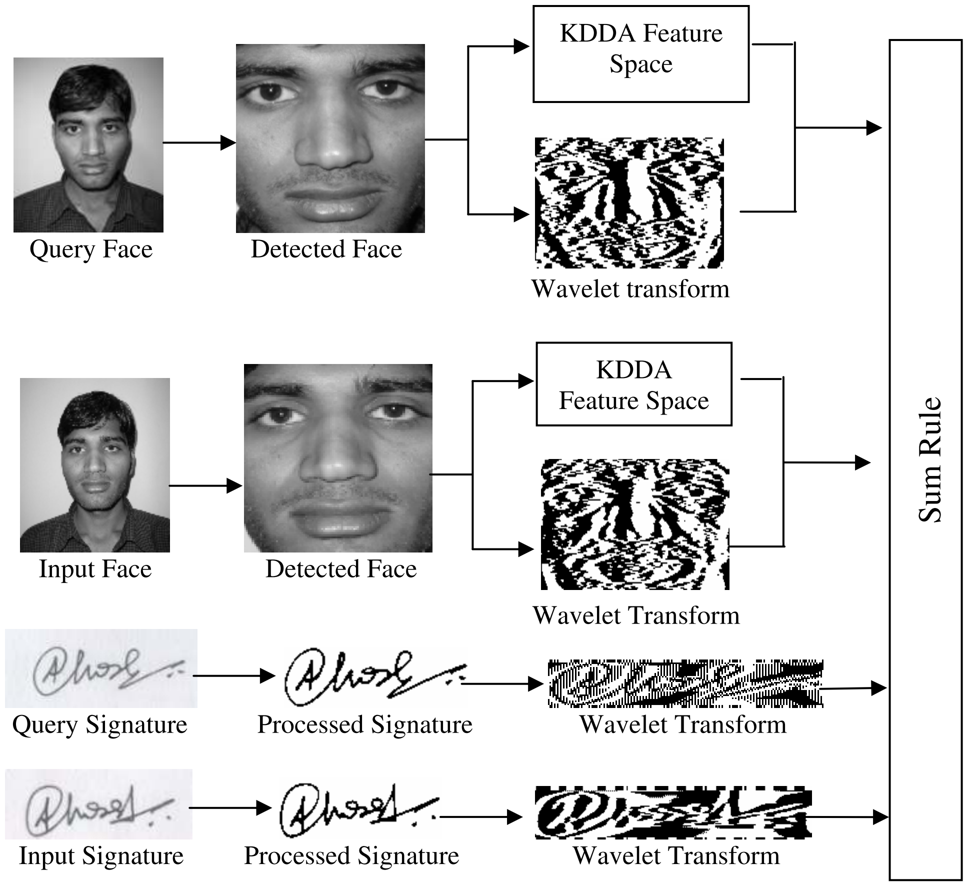



Figure 1: Block Diagram of the Multimodal System

## 2. Algorithms

This multi-biometric system is designed to use in the conditions where only one face image and one scanned signature image is stored in database, i.e. for training only a single face and signature image is available (Competitive examinations, Banks, Time and Attendance, etc). This system is divided into three modules: Face Recognition, Signature Recognition and Multi-biometrics. Figure 1 shows the block diagram of the system. In face recognition module, first the face is detected and then the matching score is calculated using the two face recognition algorithms. Similarly, in the signature recognition module, corresponding matching scores are calculated and finally using a sum rule based fusion algorithm; the two matching scores have been combined to get the result.

### 2.1 Face Recognition Module

Face recognition algorithm has been designed for matching scanned photographs with the digital or scanned images. The database of scanned images that we have collected is from different parts of India, from different cameras, in different background and lightning environments. The dataset contains around 135 images (both scanned and digital). The face recognition module is divided into four parts:

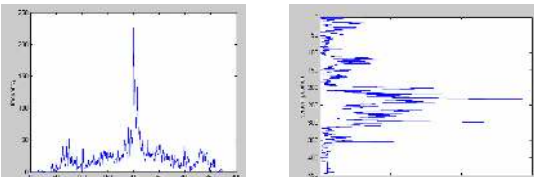
1. Face Detection,
2. KDDA based face verification,
3. Haar Wavelet based face verification and
4. Multi-classifier algorithm.

The following subsections explain the algorithm for face detection and recognition. Face image is taken and face is detected by extracting the eye and mouth coordinates from the face. Triangle based approach is applied on these coordinates to detect the face region. Haar wavelet and KDDA are then applied on the the detected face to get the maching score.

#### 2.1.1 Face Detection

In the face detection algorithm, bilateral symmetrry of the face parts and traingle detectioon algorithm is used. For eye and mouth detection, bilateral symmetry between and within the face parts has been utilized for this task. An edge detected version of the face image is given as the input for symmetry detection, this symmetry detection determins the locations on the image where symmetry is maximized. Eye region is shown in Figure 2(a) and Figure

2(b). After having narrowed the region where eyes are assumed to be present, template matching algorithm [3] is applied to search the precise location of the eyes. This method takes two templates for both the right and the left eye and lets it travel in the narrowed area pixel by pixel. At each location it calculates the normalized cross correlation between the template and the region on the original image where the template currently resides.

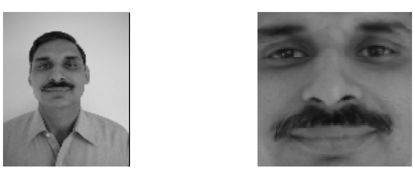


(a) Horzontal Axis (b) Vertical Axis

Figure 2: Symmetry Matrix Projection of a Face Image

After locating the eyes, symmetry detection is further utilized to detect mouth. İt is known that mouth lies on the midline of the face equidistant from the two eyes. A virtual line is drawn orthogonal to the line linking the two eyes from its midpoint. İt is assumed that the approximate location of mouth with respect to the two eyes on an ordinary human face is 4/3 times the eye to eye distance. At this region a peak in the vertical histogram of symmetry matrix is searched which corresponds to the high symmetry measure of mouth, the location of this peak gives the exact height and its intersection with the virtual line gives the exact location of the mouth. Then a traingle based algorithm [4] is applied to extract the face from the input image using the cordinates of the three facial features and the steps involved are:

1. Face image is taken and edge detection is done.
2. Bilateral symmetry detection on the edge detected image converges to the area for maximum symmetry.
3. Template matching is applied on this area of maximum symmetry to detect the eyes.
4. A line orthogonal to the line joining the two eyes is considered to detect the mouth location. At a distance of around 4/3 times the eye-to-eye distance, the peak in the vertical histogram of the symmetry matrix gives the location of mouth.
5. Triangle based algorithm is then applied to extract the face region depending on the value of eye and mouth coordinates.



Input face Image Detected face Image

Figure 3: Face Detection Algorithm

### 2.1.2 Face recognition using KDDA

The first step of face recognition using KDDA [5] is to make a feature space using some detected face images (for training). For creating the feature space, the following algorithm is applied on 25 training face images.

*Algorithm Feature Space Generation*

1. Make a set of training face images where each face image is represented as *n* dimensional vector.
2. Calculate the Kernel matrix, eigenfaces, eigenvectors (whose corresponding eigenvalues are greater than 0) and matrix containing the numbers equal to square of the eigenvalues.
3. Calculate the Kernel vector and a low dimensional Kernel matrix, which causes the low dimensional representation. Apply the KDDA equation from [5] to get the feature representation of the image.
4. Calculate and store the features extracted.

After creating the facial feature space *y*, query face and the database face are projected into the KDDA feature space, the features of the two faces are extracted, and a matching score [6] is calculated for matching the extracted features. The algorithm is given below

*Algorithm Matching* (*D*: Database, *Q:* Query)

Let there are *m* features in the database and *n* features in the query image. For each of the *m* features in the database and *n* features in the query image, reference features are chosen depending on the distance and rotation between the positions of features in the feature space.

1. Translate the database and the query feature sets with respect to the reference feature chosen and then convert into polar coordinate.
2. Import the relevant bounding box and for each of the *m* features in the database find those that lie within the bounding box. Increment the matching score accordingly.
3. Final matching score (*MS(KDDA)*) is the maximum score (among all the possibilities of reference features) divided by the maximum number of features (among the query and the database).

This matching score (*MS(KDDA)*) is used to determine whether the two faces are of the same person or not. If the matching score is greater than the threshold, the two images are matched else mismatched.

### 2.1.3 Face recognition using Haar Wavelet

Face recognition using discrete wavelet transform is based on the facial features extracted from a Haar Wavelet Transform [7]. Haar wavelet is widely used in texture recognition algorithms. Haar wavelet is taken because it is real, orthogonal, and symmetric. Its boundary conditions are the simplest among all wavelet-based methods. The minimum support property allows arbitrary spatial grid intervals. It can be used to analyze texture and detect edges of face. The equation of the Haar wavelet is given as

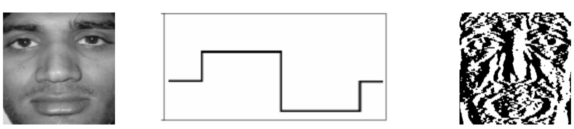
$$\psi(t) = \begin{cases} 1 & 0 \le t < 1/2 \\ -1 & 1/2 \le t < 1 \\ 0 & otherwise \end{cases} \qquad (1)$$

Wavelet is used to extract the facial features from the face image treating it as a texture image and encode it into the binary pattern. Detected face image is convolved with the Haar filter and the face image is converted into a binary template (Figure 4). This binary template is matched with the binary template of the database image using Hamming Distance algorithm [8]. Hamming distance (*HD*) for the two binary templates may be calculated using the equation below:

$$HD = \frac{1}{N}\sum_{i=1}^{N} A_i \oplus B_i \text{ and } MS(HAAR) = (1 - HD) \qquad (2)$$

where $A_i$ and $B_i$ are the two templates to be compared, $N$ is the number of bits represented by each template and $\oplus$ is the XOR operation. For handling rotation, templates are shifted left and right bit-wise and a number of *HD* values are calculated from successive shifts [8]. This bit-wise shifting in the horizontal direction corresponds to rotation of the original face template at an angle given by the angular resolution used. This handles the misalignments in the pattern caused by rotational differences during imaging. Matching score of this algorithm is calculated by (1 – *HD*) and is denoted as *MS(HAAR)* (Equation 2).

This recognition algorithm does not require a large dataset for training and is found to be robust for lightning variations and around $10^0$ angular rotations in all directions.



Detected Face Haar Wavelet Face Template

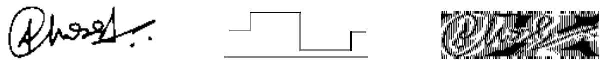
Figure 4: Generating the face template

## 2.2 Signature Recognition Module

Signature recognition module is also based on the Haar wavelet similar to face recognition. Signature module is divided into three algorithms:

1. Preprocessing,
2. Template generation
3. Matching.

In the preprocessing algorithm, signature is filtered by a low-pass filter [9] in order to eliminate spurious noise inherent to the acquisition process. Filtered image is then converted into binary image. The textural features of signature are extracted using the algorithm based on Haar wavelet, similar to the face recognition algorithm (as in this case also there is only one training image in the database). Here the binary signature image is convolved with the Haar wavelet and the corresponding binary template of signature is generated (Figure 5). Hamming Distance algorithm is used to match the two signature templates as given in Equation 2.



Binary Signature Haar Wavelet Signature Template

Figure 5: Generating the signature template

## 2.3 Multi Biometrics Algorithm

For calculating the final matching score, sum rule based multi-classifier algorithm is used. According to the studies on the multi-classifier algorithm [2], it has been proved that the sum rule base multi-classifier algorithm gives the best results even with the lesser complexity. In this algorithm first a matching score for face recognition module is calculated using the matching scores of two face recognition algorithms. A simple OR rule is applied on the matching scores i.e. a person is said to be verified if any of the algorithm verifies it and the matching score of the face module is calculated as follows:

$$MS(Face) = \begin{cases} MS(KDDA) * a > thresh1 \\ MS(HAAR) * b > thresh2 \end{cases} \qquad (3)$$

where *a* and *b* are the weight factors of the two face recognition algorithm and are determined by the experimental study. If a person is matched by KDDA and rejected by Haar, i.e. if the *MS(KDDA)*a* accepts the person and *MS(HAAR)*b* rejects then the matching score for face module *MS(Face)* is equal to *MS(KDDA)*a.* This is done because the false acceptance rate is low but the false rejection rate of algorithms is quite high. So, this approach is used as it lowers the false rejection rate but does not affect the false acceptance rate. If both the algorithms accept or reject the individual then *MS*(*Face*) takes bigger values of the two matching scores.

For signature recognition, Hamming Distance is used as the matching score (*MS*(*Sign*)). Finally, the sum rule is applied for merging the two sum rules because it has been proved that sum rule is the most efficient multi-classifier algorithm for any combining the biometric algorithms.

$$MS = MS(Face) + MS(Sign) \qquad (4)$$

This matching score is compared with a threshold that determines whether the person is genuine or not.

## 3. Experimental Results

The proposed multimodal algorithm is tested on the database prepared by the authors. The database consists of face and signature data from 135 different individuals (for each person four face images and signature images). One face and one signature image is used for the database and three face and signature images are used for testing. The time difference between two biometric samples for the same subject in the database is 6 months to one year depend upon the availability of the individuals. Other than these images, one another database of forgeries was prepared for 25 individuals which contains 25 face images and these 25 individuals forged the 100 signatures of the 100 individuals of the above database. This database is prepared to test the false acceptance. For preparing the face database, there were no restrictions on lighting conditions. These experiments were performed on a Pentium Xeon, 3.06GHz workstation. Thresholds of different values are fixed by analyzing the results obtained at different thresholds. FAR-FRR graphs (Figure 6(a) and Figure 6(b)) are used to determine the optimal thresholds for best performance. The thresholds of the three matching scores ($MS(Face)$, $MS(Sign)$ and $MS$) are found to be 0.56, 0.61 and 1.17 respectively. Using these thresholds the FAR-FRR graph (Figure 6(c)), the best performance and the accuracy of the multi-classifier decision algorithm is found to be 94.37%. The accuracy, stated here, has been computed using the equation below:

$$Accuracy = 100 - (FAR + FRR) \tag{5}$$

We have also tested the three algorithms individually and calculated the recognition rates. Table 1 shows the experimental results obtained from these algorithms.

| Algorithm | FRR | FAR | Accuracy |
|---|---|---|---|
| Face KDDA | 20.27 | 1.06 | 78.67 |
| Face Haar | 14.82 | 1.29 | 83.89 |
| Face | 10.72 | 1.12 | 88.16 |
| Signature | 19.54 | 2.11 | 78.35 |
| Multi Modal | 3.75 | 1.88 | 94.37 |

Table 1. Experimental Results

The results show that the multi-biometrics is more useful in compared to the single biometrics. It has been found that due to less training data, the false rejection rate is quite high in the single biometrics trait but in the multi biometrics, it has been reduced largely. Figure 7 shows the experimental results. In Case A and Case B, the face and signature images are genuine and the system accepts the user as genuine one. Case C is the example of skilled forgery in which a user has forged the signature of another user and has given her own face image as input. In this case, face was mismatched but the signature was accepted but the multimodal biometrics system rejected the user by the multi-biometrics algorithm. In Case D, user has given his own signature and face to match with other's identity and the system has rejected the case (both the face and signature were mismatched). This shows that the system is capable for handling various problems specially the high false rejection rate and less training dataset.

## 4. Conclusion

This paper presents a multi biometric system, which takes face and signature images as input, match it with the stored database and gives the verification result as the output based on the multi biometrics algorithm. The proposed system is designed for such applications where the training database contains minimum number (one each) of face and signature images, e.g. banks, competitive examinations, restricted access, etc. This system is tested on a database prepared by the authors and the overall accuracy of the system is found to be 94.37%. In future, other biometric traits such as fingerprint, iris, etc. can also be incorporated so that the accuracy can be improved.


## 5. Acknowledgement

This work has been done as a part of the project supported by the Ministry of Communication and Information Technology.


## 6. Reference


[1] L. Hong, A. Jain and S. Pankanti, "Can Multibiometrics Improve performance?", Proceedings of AutoID' 99, pp. 59-64, 1999.

[2] A. Ross and A. K. Jain, "Information Fusion in Biometrics", Pattern Recognition Letters, 24 (13), pp. 2115-2125, 2003.

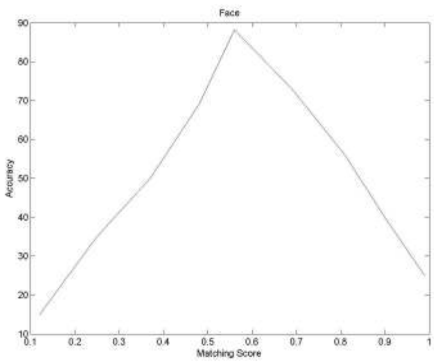
[3] I. Craw, D. Tock, and A. Bennett, "Finding Face Features," Proceedings Second European Conference Computer Vision, pp. 92-96, 1992.

[4] C. Lin, Kuo-Chin Fan, "Triangle-based approach to the detection of human face", Pattern Recognition, 34, pp. 1271-1284, 2001.

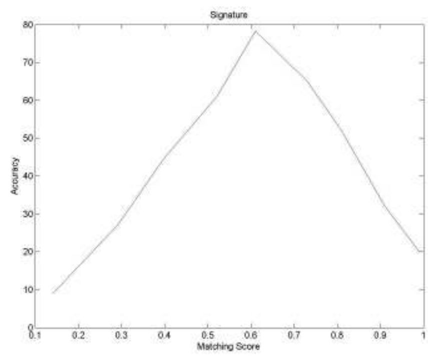
[5] Juwei Lu, K. N. Plataniotis and A. N. Venetsanopoulos, "Face Recognition Using Kernel Direct Discriminant Analysis Algorithms", IEEE Transactions on Neural Networks, 14 (1), pp. 117-126, 2003.

[6] J. Kittler, M. Hatef, R. P. W. Duin, and J. Mates, "On combining classifiers", IEEE Transactions on Pattern

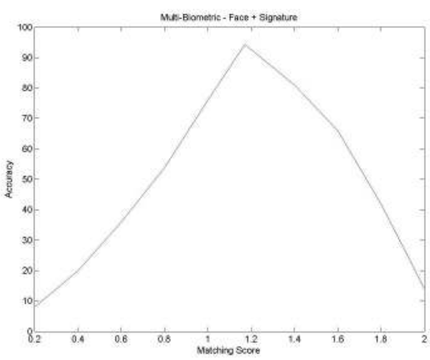
Analysis and Machine Intelligence, 20 (3), pp. 226–239, 1998.
[7] Gonzalez, Woods, Digital Image Processing, Second Edition, Pearson Education.
[8] J. Daugman, “Recognizing Persons by their iris patterns”, Biometric: Personal Identification in Networked Society, Kluwer, pp. 103-121, 1998.
[9] J. J.Brault and R. Plamondon, “Segmenting Handwritten Signatures at Their Perceptually Important Points”, IEEE Transactions on Pattern Analysis and Machine Intelligence, 15 (9), pp. 953-957, 1993.




(a) Matching Score - Face




(b) Matching Score – Signature




(c) Matching Score - Multimodal
Figure 6: Graphs for Matching Score

Matching Score – 1.78
Result – Matched
Case A

Matching Score – 1.62
Result – Matched
Case B


Matching Score – 0.76
Result – Rejected
Case C

Matching Score – 0.24
Result – Rejected
Case D
Figure 7: Experimental Results