Multimodal Biometrics Based System for Efficient Human Recognition

G Vijay Kumar
Research Scholar, CSE
SCSVMV University, Kanchipuram, TN, India
VKR,VNB &AGK College of Engineering, Gudivada
e-mail ID: vijayg.teja@gmail.com,
Cell No:09849748772

Dr G V Raju
Principal,
Sri Sunflower College of Engineering & Technology
Lankapalli-521131, Challapalli, Krishna Dist., AP.
INDIA,e-mail ID:principal@sunflowercet.org,
Cell No:09951344881

ANMV Sri Valli
Asst. Professor, CSE
VKR, VNB & AGK College of Engineering
Gudivada 521301, Krishna Dist. AP
Email ID:sri.valli15@gmail.com

ABSTRACT

This paper proposes the multimodal biometrics system for identity verification using four traits i.e., face, fingerprint, iris and signature. The proposed system is designed for applications where the training database contains a face, iris, two fingerprint images and/or one or two signature image(s) for each individual. The final decision is made by fusion at "matching score level architecture" in which feature vectors are created independently for query images and are then compared to the enrollment templates which are stored during database preparation 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. Multimodal system is developed through fusion of face, fingerprint, iris and signature recognition. This system is tested on IITK database and the overall accuracy of the system is found to be more than 97% accurate with FAR and FRR of 2.46% and 1.23% respectively.

Keywords: Biometrics, Multimodal, Face, Fingerprint, Iris, Signature, Fusion, Matching score

INTRODUCTION

"Biometrics" means "life measurement", but the term is usually associated with the use of unique physiological characteristics to identify an individual. One of the applications which most people associate with biometrics is security. However, biometrics identification has eventually a much broader relevance as computer interface becomes more natural. It is an automated method of recognizing a person based on a physiological or behavioral characteristic. Among the features measured are; face fingerprints, hand geometry, handwriting, iris, retinal, vein, voice etc. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions [1]. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent. 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 till date are facing numerous problems; some of them are 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.

One way to overcome these problems is the use of multi-biometrics. Driven by lower hardware costs, a multi biometric system uses multiple sensors for data acquisition. This allows capturing 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. A unimodal biometric system [2] consists of three major modules: sensor module, feature extraction module and matching module. The performance of a biometric system is largely affected by the reliability of the sensor used and the degrees of freedom offered by the features extracted from the sensed signal.

Further, if the biometric trait being sensed or measured is noisy (a fingerprint with a scar or a voice altered by a cold, for example), the resultant matching score computed by the matching module may not be reliable. This problem can be solved by installing multiple sensors that capture different biometric traits. Such systems, known as multimodal biometric systems [3], are expected to be more reliable due to the presence of multiple pieces of evidence. These systems are also able to meet the stringent performance requirements imposed by various applications. However, multimodal systems address the problem of non-universality: it is possible for a subset of users who do not possess a particular biometric.

This paper proposes an efficient multimodal biometric system which can be used to reduce/remove the above mentioned limitations of unimodal systems. Next section presents an overview of multimodal biometric system. Section 3 presents multimodal biometric system at IITK using face, fingerprint, iris and signature. In order to increase the performance of individual biometric trait, multiple classifiers are combined using matching scores. Finally, the individual traits are fused at matching score level using weighted sum of score technique. Experimental results are given in Section 4. Conclusions are given in the last section.

MULTIMODAL BIOMETRICS SYSTEM

Multimodal biometric systems are those that utilize more than one physiological or behavioral characteristic for enrollment, verification, or identification. In applications such as border entry/exit, access control, civil identification, and network security, multi-modal biometric systems are looked to as a means of reducing false non-match and false match rates, providing a secondary means of enrollment, verification, and identification if sufficient data cannot be acquired from a given biometric sample, and combating attempts to fool biometric systems through fraudulent data sources such as fake fingers.

The levels fusion proposed [2] for multimodal systems are broadly categorized into three system architectures which are according to the strategies used for information fusion as shown in Fig. 1:

- 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. The purpose of the proposed paper is to investigate whether the integration of face and palmprint biometrics can achieve higher performance that may not be possible using a single biometric indicator alone. Both Principal Component Analysis (PCA) and Independent Component Analysis (ICA) are considered in this feature vector fusion context. It is found that the performance improved significantly.

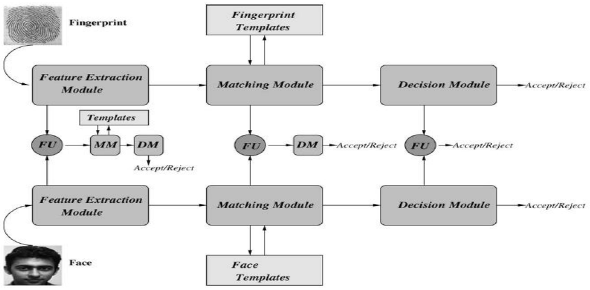

Fig. 1 Multimodal System using three levels of Fusion (taken from Ross & Jain, 2003)

MULTIMODAL BIOMETRICS SYSTEM at IITK

The multimodal biometric system at IITK is developed using four traits i.e., face, fingerprint, iris and signature (as shown in Fig. 2). In Face Recognition, the input face image is recognized using Elastic Bunch Graph matching algorithm. In Fingerprint Verification, the input image is enhanced to bring out obscure information based on Gabor filtering and matching is done by combination of Reference Point and Minutiae matching algorithms. In Iris Recognition, the input image is localized by finding the pupillary and outer iris boundary and is matched using combination of Haar Wavelet and Circular Mellin operator. In Signature Verification, feature vector consists of Global and Local features of signature image and is matched using Euclidean Distance.

The modules based on the individual traits returns an integer value after matching the database and query feature vectors. First of all the fusion is done at classifier level i.e., for face, fingerprint and iris, multiple classifiers are combined at matching score level followed by fusion at multiple modalities level. The final score is generated by using sum of score technique at matching score level which is passed to the decision module. The brief description of various recognition algorithms are presented below:

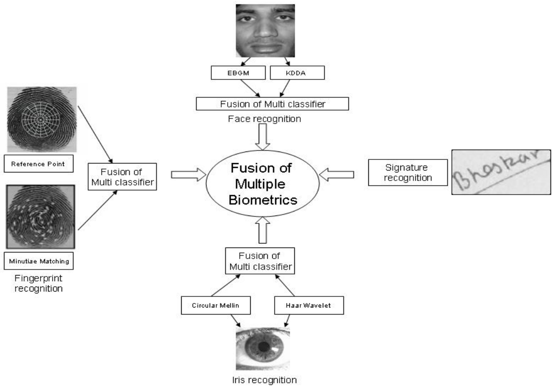

Fig. 2 Multimodal Biometric System at IITK

Face Recognition

Face Recognition is a noninvasive process where a portion of the subject's face is photographed and the resulting image is reduced to a digital code. Facial recognition records the spatial geometry of distinguishing features of the face [2][4][5]. The recognition algorithm takes facial image, measures the unique characteristics and computes the template corresponding to each face. Using templates, the algorithm then compares that image with another image and produces a score that measures how similar the images are to each other.

Feature Extraction using EBGM and KDDA

Elastic Bunch Graph Matching (EBGM)

Face recognition using elastic bunch graph matching [2] is based on recognizing novel faces by estimating a set of novel features using a data structure called a bunch graph. Similarly for each query image, the landmarks are estimated and located using bunch graph. Then the features are extracted by convolution with the number of instances of Gabor filters followed by the creation of face graph. The matching score (MS_{EBGM}) is calculated on the basis of similarity between face graphs of database and query image. The diagrammatic representation of EBGM algorithm is shown in Fig. 3.

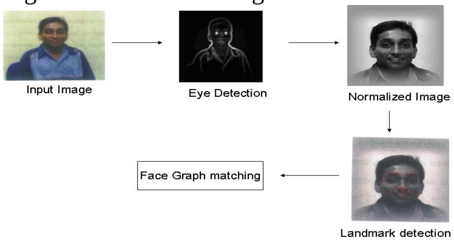

Fig. 3 Steps involved in face recognition

Kernel Direct Discriminant Analysis (KDDA)

Face recognition using KDDA [11] is based on computation of feature space F (from training set) and projection of input pattern into the feature space to calculate significant discriminant features. 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. The matching score for each transformation of database and query feature vectors are calculated with respect to reference feature chosen using bounding box technique. MS_{KDDA} is defined by the maximum of all matching scores divided by the maximum number of features (among the query and the database).

Combination of EBGM and KDDA

The matching scores from the above two classifiers are converted from distance to similarity score and are combined at matching score level using sum of score technique which significantly increases the accuracy of the face recognition system.

3.2 Fingerprint Recognition

The fingerprint recognition system has been developed by the fusion of Reference Point and Minutiae Matching Techniques [3][4]. The key steps involved are fingerprint enhancement, feature extraction using Reference point Algorithm and Minutiae Matching approach and computation of matching score. The goal of fingerprint enhancement [5] is to increase the clarity of ridge structure so that minutiae and the reference points can be easily and correctly extracted.

Feature Extraction using Reference point and Minutiae matching approach

Reference Point Algorithm [4] gracefully handles local noise in a poor quality fingerprint. The detection should necessarily consider a large neighborhood in the fingerprint image. For an accurate localization of the reference point, the input image is segmented to remove any kind of noise present in the image. Further Sobel Operator is applied to obtain gradient of segmented image. The Orientation Field is estimated along with the Y component. A specific pattern in which the value of Y-Component is maximum is Reference point (the point of maximum curvature). The finger code is generated by drawing concentric circles of fixed radius centered at reference point (as shown in Fig. 4). The image is segmented into 5 tracks and 16 sectors from the detected reference point. The size of the feature vector is 512 values. The distance (D_{Ref}) for the database and query feature vectors is calculated using Euclidean distance method.

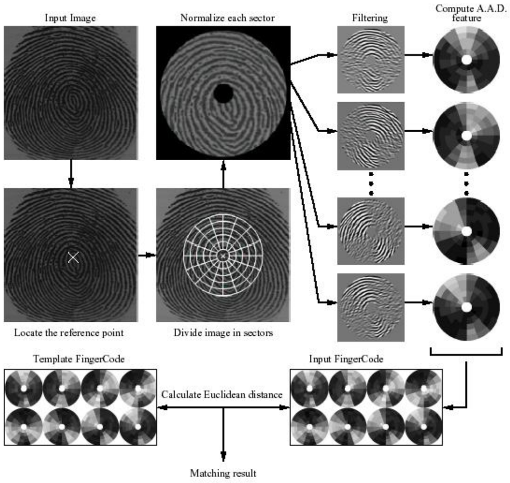

Fig. 4 Diagrammatic representation of Reference point Location algorithm

Minutiae Matching

The input fingerprint image is enhanced using Gabor Filters The enhanced image is further binarized and thinned using a morphological operation that successively erodes away the foreground pixels until they are one pixel wide. The thinned image is used to detect minutiae points [4] by locating ridge ending and bifurcations using Crossing Number (*CN*) method. The matching score MS_{MIN} between the database and query image is computed using Elastic matching approach [3]. Fig. 5 shows various steps involved in minutiae extraction.

Combination of Reference Point and Minutiae Matching Algorithm

The matching scores from the above two classifiers are converted from distance to similarity score and are combined at matching score level using sum of score technique which significantly increases the accuracy of the fingerprint system.

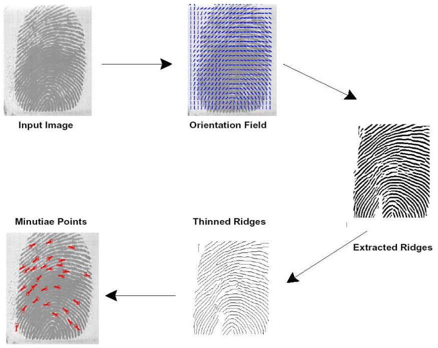

Fig. 5 Steps involved in minutiae extraction

Iris Recognition

The iris image acquired from a 3CCD camera is localized by finding the center of pupil from the spectrum image. The radius of the pupil is the distance between the pupil center and nearest non-zero pixel. The outer iris boundary is detected by drawing concentric circles of different radii from the pupil center and the intensities lying over the perimeter of the circle are summed up. Among the candidate iris circles, the circle having a maximum change in intensity with respect to the previous drawn circle is the outer iris boundary (shown in Fig. 6). The annular region lying between pupil and iris boundary is transformed to polar co-ordinates [6] to take into consideration the possibility of pupil dilation and appearing of different size in different images. From the normalized strip the eyelids are detected and removed.

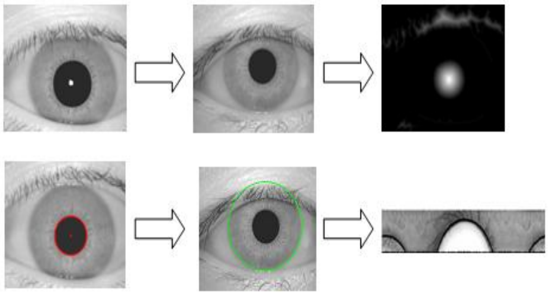

Fig. 6 Steps involved in iris preprocessing and normalization

Feature Extraction using Haar Wavelet and Circular Mellin operator

Haar Wavelet

Haar wavelet is widely used in texture recognition algorithms [7]. The input signal *S* (polarized iris image) is decomposed into approximation, vertical, horizontal and diagonal coefficients using the wavelet transformation and coefficients for the fourth and fifth levels are chosen to reduce space complexity and discard the redundant information. The iris code is generated by assigning one to the positive coefficient values and zero to negative values.

Circular Mellin operators

These "Circular Mellin" operators are invariant to both scale and orientation [18] of the target and represent the spectral decomposition of the image scene in the polar-log coordinate system. Features in iris images are extracted based on the phase of convolution of polarized iris image with mellin operators. The iris code is one for positive phase values and zero for negative phase values.

The iris codes generated using Haar Wavelet and Circular Mellin operators are matched using Hamming Distance approach.

Combination of Haar Wavelet and Circular Mellin operator

The individual matching scores generated by above mentioned classifiers are converted from distance to similarity score and are fused at matching score level for better performance of iris recognition.

Signature Verification

In biometrics terminology, the signature is a behavioral characteristic [8] of a person and can be used to identify/verify a person's identity. The signature recognition algorithm consists of three major modules i.e., preprocessing and noise removal, feature extraction and computation of Euclidean distance. Offline signature acquisition is carried out statically, unlike online signature acquisition, by capturing the signature image using a high resolution scanner. A scanned signature image may require morphological operations (shown in Fig. 7) like normalization, noise removal by eliminating extra dots from the image, conversion to grayscale, thinning and extraction of high pressure region.

Feature Extraction using Global and Local features

The features of the signature images can be classified into two categories - global and local [20]. Global features include the global characteristics of an image. Ismail and Gad have described global features [21] as characteristics which identify or describe the signature as a whole. Examples include: width/height (or length), baseline, area of black pixels etc. They are less responsive to small distortions and hence are less sensitive to noise as well, compared to local features which are confined to a limited portion of the signature. In contrast to global features, they are susceptible to small distortions like dirt but are not influenced by other regions of the signature. Hence, though extraction of local features requires a huge number of computations, they are much more precise. However, the grid size has to be chosen very carefully. It can neither be too gross nor be too detailed. Examples include local gradients, pixel distribution in local segments etc. Many of the global features such as global baseline, center of gravity, and distribution of black pixels have their local counterparts as well.

The difference/distance (D_{Sign}) between the two feature sets are computed using weighted Euclidean distance measure.

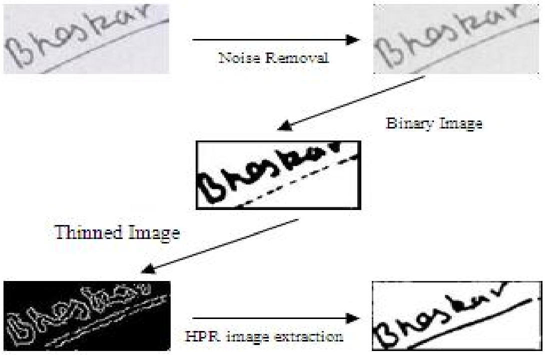

Fig. 7 Preprocessing and noise removal

EXPERIMENTAL RESULTS

The reliability of the proposed multimodal biometric system is described with the help of experimental results. The system has been tested on a database of 250 individuals. The training database contains a face, iris, two fingerprint images and one or two signature image(s) for each individual. The face image has been taken under controlled environment using a digital camera. The face images of frontal view are obtained under different orientations and lightning conditions. The fingerprint images are acquired using optical sensor at a resolution of 500 dpi. The iris image is acquired using 3-CCD Camera and the signature is acquired on a custom made template.

The multimodal system has been designed at multi-classifier and multi-modal level. At multi-classifier level, multiple algorithms/classifiers are combined to generate better results. At first experiment, the individual systems were developed and tested for FAR, FRR and Accuracy. Table 1 and Fig. 8 shows FAR, FRR and accuracy of these systems.

Trait	Algorithm	FAR (%)	FRR (%)	Accuracy (%)
Face	EBGM	0.59	22	88.70
Fingerprint	Reference Point	11	6	91.05
Iris	Haar	3.42	8.45	92.50
Signature	Global and Local Features	10	8	91.00

Table 1 The accuracy, FAR and FRR of individual recognizers

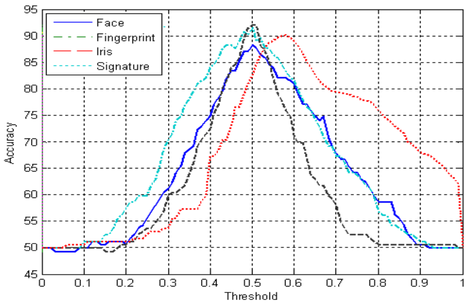

Fig. 8 Accuracy graph for individual trait

In the next experiment, multiple classifiers are combined at matching score level for face, fingerprint and iris traits. For face recognition system, EBGM and Haar algorithms are combined together. Reference point and minutiae matching algorithms are combined for fingerprint recognition system whereas Haar and circular Mellin algorithms are combined for iris recognition.

CONCLUSIONS

Biometrics systems are widely used to overcome the traditional methods of authentication. But the unimodal biometric system fails in case of lack of biometric data for particular trait. Thus the individual scores of four traits (face, fingerprint, iris and signature) are combined at classifier level and trait level to develop a multimodal biometric system. The performance table and accuracy curve shows that multimodal system performs better as compared to unimodal biometrics with accuracy of more than 97%. However, it is worth studying the results by assigning different weightage to different traits. At present equal weightage is assigned to each trait.

REFERENCES

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

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

[3] A.S. Tolba & A. A. Rezq, *Combined Classifier for Invariant Face Recognition*, Pattern Analysis and Applications, 3(4), pp. 289-302, 2000

[4] A. Ross, A. K. Jain & J.A. Riesman, *Hybrid fingerprint matcher*, Pattern Recognition, 36, pp. 1661–1673, 2003

[5] W. Yunhong, T. Tan & A. K. Jain, *Combining Face and Iris Biometrics for Identity Verification*, Proceedings of Fourth International Conference on AVBPA, pp. 805-813, 2003

[6] S. C. Dass, K. Nandakumar & A. K. Jain, *A principal approach to score level fusion in Multimodal Biometrics System*, Proceedings of ABVPA, 2005

[7] J. Kittler, M. Hatef, R. P. W. Duin, & J. Mates, *On combining classifiers*, IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(3), pp. 226–239, 1998

[8] G. Feng, K. Dong, D. Hu & D. Zhang, *When Faces Are Combined with Palmprints: A Novel Biometric Fusion Strategy*, ICBA, pp. 701-707, 2004