International Journal of Soft Computing 9 (4): 246-254, 2014
ISSN: 1816-9503

Multimodal Biometric Authentication System Based Performance Scrutiny

[1]R. Manju, [1]A. Shajin Nargunam and [2]A. Rajendran
[1]Department of EIE, Noorul Islam University, [2]Department of ECE,
Sun College of Engineering and Technology, Kanyakumari, India

Abstract: In many real-world applications, Unimodal Biometric Systems often face significant limitations due to sensitivity to noise, intraclass variability, data quality, non-universality and other factors. Multibiometric Systems seek to alleviate some of these problems by providing multiple pieces of evidence of the same identity. This study presents an effective fusion scheme that combines information presented by multiple domain experts based on the Rank-Level Fusion Integration Method. The developed Multimodal Biometric System possesses a number of unique qualities, starting from utilizing principal component analysis and Fisher's Linear Discriminant Methods for individual matchers (face, iris and fingerprint) identity authentication and utilizing the Novel Rank-Level Fusion Method in order to consolidate the results obtained from different biometric matchers.The results indicate that fusion of individual modalities can improve the overall performance of the Biometric System, even in the presence of low quality data.

Key words: Biometric identification system, Fisher's Linear Discriminant Methods (FLD), Multibiometric System, Principal Component Analysis (PCA), rank-level fusion

INTRODUCTION

Software and computer systems are recognized as a subset of simulated intelligent behaviours of human beings described by programmed instructive information. Biometric Information System is one of the finest examples of computer system that tries to imitate the decisions that humans make in their everyday life, specifically concerning people identification and matching tasks.

A Biometric Identification (matching) System is an automatic pattern recognition system that recognizes a person by determining the authenticity of a specific physiological and/or behavioural characteristic (biometric) possessed by that person. Multibiometric is a relatively new approach to biometric knowledge representation that strives to overcome the problems by consolidating the evidence presented by multiple biometric traits/sources. Multibiometric systems can significantly improve the recognition performance in addition to improving population coverage, deterring spoof attacks, increasing the degrees of freedom and reducing the failure to enrol rate.

Although, the storage requirements, processing time and computational demands of a Multibiometric System can be higher than that for a Unimodal Biometric System, the aforementioned advantages present a compelling case for deploying Multibiometric Systems in real-world large-scale authentication systems. The key to successful Multibiometric System is in an effective fusion scheme which is necessary to combine the information presented by multiple domain experts. The goal of fusion is to determine the best set of experts in a given problem domain and devise an appropriate function that can optimally combine the decisions rendered by the individual experts (Faundez-Zanuy, 2006).

In this study, researchers provide the first application of fusion at the rank level for consolidating the rank information produced by three separate unimodal biometric systems and discuss its efficiency. The developed Multimodal Biometric System possesses a number of unique qualities such as utilization of Principal Component Analysis (PCA) and Fisher's Linear Discriminant (FLD) Methods for individual matchers (face, iris and fingerprint) in combination with the novel rank-level fusion mechanism. The ranks of individual matchers are combined using the Highest Rank Method. In the rest of this study, researchers will focus on the performance issues and parameters of a Biometric System (Fig. 1).

Corresponding Author: R. Manju, Department of EIE, Noorul Islam University, Kanyakumari, India

Fig. 1: Three traits used in the system

PERFORMANCES OF A BIOMETRIC SYSTEM

The main goal of this study is to improve the recognition performance of a Biometric System by incorporating multiple biometric traits. Usually, the performance of a Biometric System is expressed by some parameters. There are a total of four possible outcomes: a genuine individual is accepted, a genuine individual is rejected an impostor is rejected and an impostor is accepted. Outcomes 1 and 3 are correct whereas outcomes 2 and 4 are incorrect. The confidence associated with different decisions may be characterized by the genuine distribution and the impostor distribution which are used to establish the following two error rates.

False Acceptance Rate (FAR): It is defined as the probability of an impostor being accepted as a genuine individual. It is measured as the fraction of impostor score exceeding the predefined threshold.

False Rejection Rate (FRR): It is defined as the probability of a genuine individual being rejected as an impostor. A small FRR usually leads to a larger FAR while a smaller FAR usually implies a larger FRR. Generally, the system performance requirement is specified in terms of FAR. A FAR of zero means that no impostor is accepted as a genuine individual. Sometimes, another term, Genuine Accept Rate (GAR) is used to measure the accuracy of a Biometric System. It is measured as the fraction of genuine score exceeding the predefined threshold: GAR = 1-FRR.

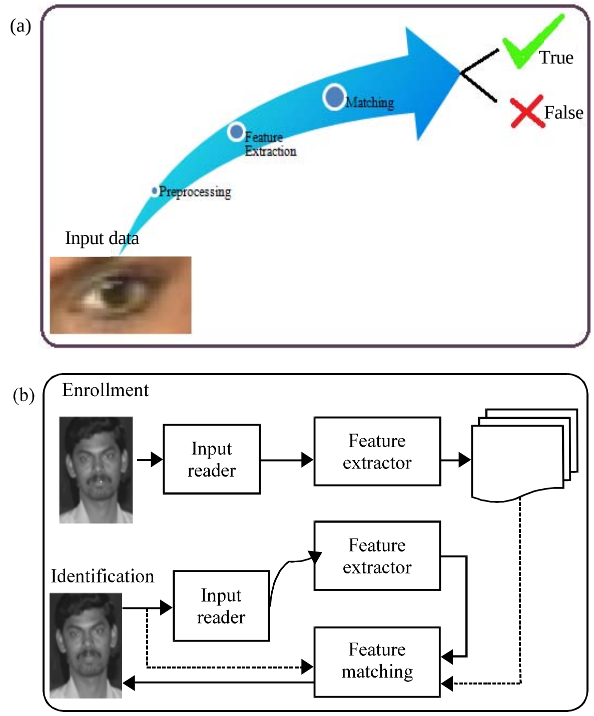

Fig. 2: a) Block diagram of the Unimodal Biometric System; b) Generic Biometric System architecture

In this context, researchers develop a Multibiometric System which makes personal identification by integrating faces, iris and fingerprint of individuals. Researchers develop three unimodal biometric systems for face, iris and fingerprint using PCA and FLD Methods. These systems produce ranking of individuals which will then be consolidated by the Rank-Level Fusion approach to achieve the consensus rank of individuals. The use of PCA and FLD Methods for Unimodal Biometric Systems results in rank determination of individuals very precisely. Thus, utilizing rank-level fusion to consolidate the results produced by these unimodal experts results in a much higher recognition rate. The simple block diagrams of a Unimodal System and the proposed Multibiometric System are shown in Fig. 2a and b, respectively. The proposed system integrates three different biometric matchers of face, iris and fingerprint and incorporates a rank-level fusion module to improve the recognition performance.

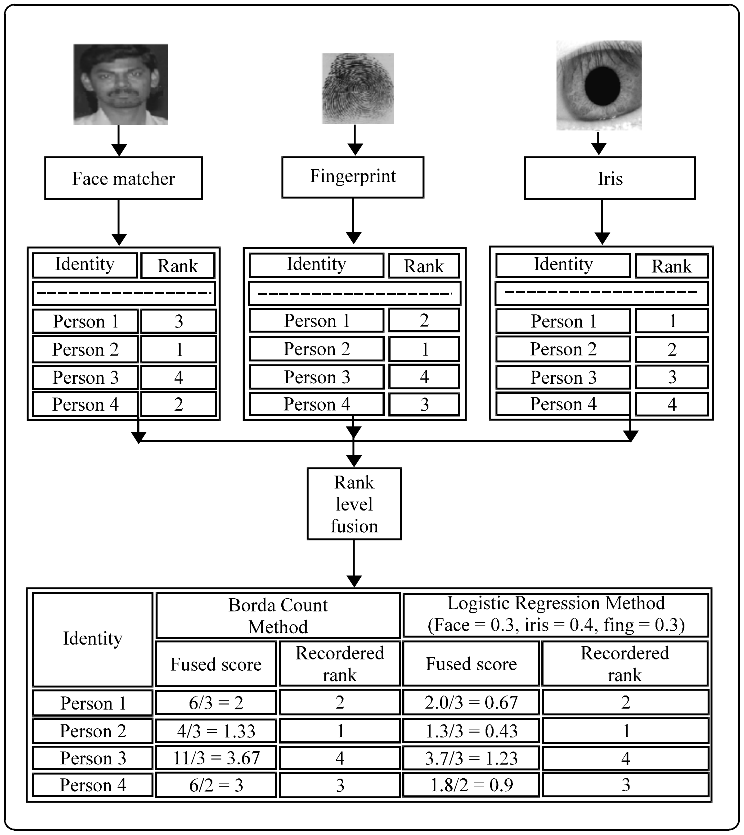

Fig. 3: Example of rank-level fusion

RANK-LEVEL FUSION

The goal of rank-level fusion is to consolidate the rank output by individual biometric subsystems (matchers) in order to derive a consensus rank for each identity. Daugman (2006) describe three methods to combine the ranks assigned by different matchers. Those are the Highest Rank Method, the Borda Count Method and the Logistic Regression Method. In the Highest Rank Method each possible match is assigned the highest (minimum) rank as computed by different matchers. Ties are broken randomly to arrive at a strict ranking order and the final decision is made based on the combined ranks.

The Borda Count Method uses the sum of the ranks assigned by individual matchers to calculate the final rank. This method assumes that the ranks assigned to the users by the matchers are statistically independent and that the performances of all the modules are equally. On the other hand, in the Logistic Regression Method, a weighted sum of the individual ranks is calculated. The weight to be assigned to different matchers is determined by logistic regression. Researchers propose to use all three matchers (face, iris and fingerprint) and have considered only those identities which appear in the results of at least two matchers. The identities which appear in the result of only one matcher have been discarded or not considered for the final rank in this system. Figure 3 shows an example of rank-level fusion. The less the value of the rank, the more accurate the result.

MULTIMODAL BIOMETRIC SYSTEM DEVELOPMENT

This study deals with the development procedures of the proposed Multimodal Biometric System through the Rank-Level Fusion Method. Eigen image and Fisherface techniques are used in this system for enrollment and recognition of biometric traits. A more detailed representation of the proposed system is shown in Fig. 4.

PCA is a statistical method which involves analysis of n-dimensional data. PCA observes correspondence between different dimensions and determines principal dimensions along which the variation of the data is high. The basis dimensions or vectors computed by PCA are in the direction of the largest variance of the training vectors. These basis vectors are computed by solution of

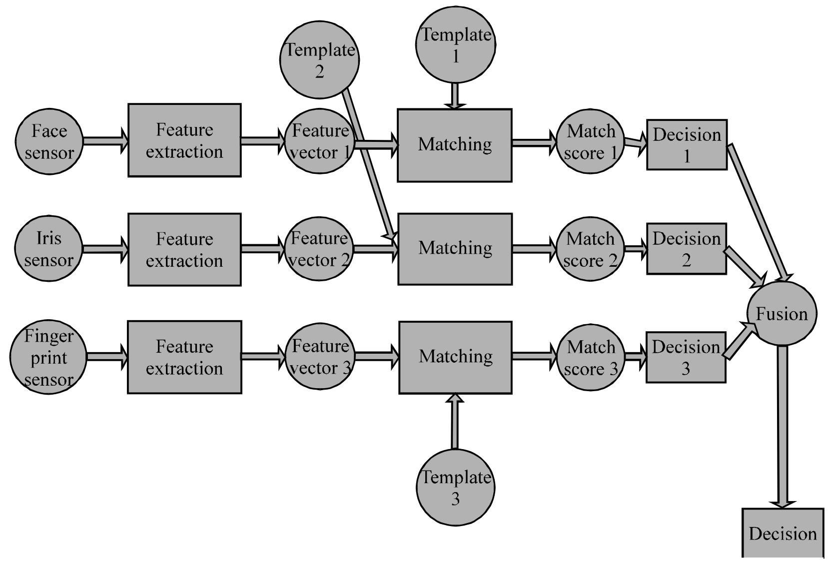

Fig. 4: Block diagram of the Multimodal Biometric System

an "eigen" problem and as such the basis vectors are eigenvectors. These eigenvectors are defined in the image space. They can be viewed as images. Hence, they are usually referred to as eigenimage. The first eigenimage is the average image while the rest of the eigenimage represent variations from this average image. Each eigenimage can be viewed as a feature. When a particular image is projected onto the image space, its vector (made up of its weight values with respect to each eigenimage) into the image space describes the importance of each of those features in the image. The eigenimage approach has a compact representation an image of a face, iris or fingerprint can be concisely represented by a feature vector with a few elements.

The eigenimage technique has some limitations too. This method is very sensitive to image conditions such as background noise, image shift, occlusion of objects, scaling of the image and illumination change. When substantial changes in illumination and expression are present in the face image much of the variation in the data is due to these changes. For the aforementioned reasons, researchers also use the Fisherface approach introduced by Bowyer *et al.* (2008) in order to achieve higher recognition rate. The Fisherface Method uses both PCA and LDA to produce a subspace projection matrix, similar to that used in the Eigenface Method. As the iris and fingerprint databases used for the system have very limited illumination change, so researchers use the FLD Method only for face. The following two studies describe eigenimage and Fisherface techniques as unimodal experts.

Recognition using PCA: Eigenimage feature extraction is based on the wavelet transform and is used to obtain the most important features from the face, iris and fingerprint subimages in the system. These features are obtained by projecting the original subimages into the corresponding subspaces. Researchers create three image subspaces one for the face subimages, one for the fingerprint subimages and one for the iris subimages. The system is first initialized with a set of training images. Eigenvectors and eigen values are computed on the covariance matrix of these images according to the standard procedure described by Zuo *et al.* (2007) for face, iris and fingerprint, respectively. From the eigenvectors (eigenimages) that are created, researchers only choose a subset which has the highest eigen values. The higher the eigen value, the more characteristic features of an image the particular eigenvector describes. Eigenimage with low eigen values can be omitted as they explain only a small part of the characteristic features of the images.

Finally, the known images are projected onto the image space and their weights are stored. This process is repeated as necessary. After defining the eigenspace, researchers project any test image into the eigenspace. An acceptance (the two images match) or rejection (the two images do not match) is determined by applying a threshold. Any comparison producing a distance below the threshold is a match (Daugman, 2007). The steps for the recognition process can be summarized as follows:

- Project the test image into the eigenspace and measure the distance between the unknown image's position in the eigenspace and all the known image's positions in the eigenspace

- Select the image closest to the unknown image in the eigenspace as the match. Researchers define the image with the lowest distance as rank-1 image, the image with the second lowest distance as rank-2 image and so on. This same technique is applied for ranking of face, iris and fingerprint

Algorithm:
1. Consider a training set of face images $T_1, T_2, ..., T_L$ where, L is the total number of training images. Let, 'M' be the dimension of the training images. The mean of these face images is given by:

$$\mu = \frac{1}{L}\sum_{i=1}^{L} T_i$$

2. Let's consider the difference image from the mean value is given by the vector as:

$$X_i = T_i - \mu, \quad i = 1, ..., L$$

3. Covariance matrix which is given by:

$$C = \frac{1}{L}\sum_{i=1}^{L} X_i X_i' = AA'$$

Where, $A = [X_1 X_2, ..., X_L]$
4. Vectors 'u_n' and scalars 'λ_n' are the eigenvectors and eigen values, respectively of the covariance matrix C and the eigen values are given by:

$$\lambda_n = \frac{1}{L}\sum_{i=1}^{L}\left(u_n^t X_i\right)^2$$

Recognition using Fisherface (FLD): Eigenspace representation is very sensitive to image conditions such as background noise, image shift, occlusion of objects, scaling of the image and illumination change. Due to certain illumination changes in the face images of the database used in this research, a fisherface based face recognition method (Daugman, 2007) is developed to compare with the eigenface technique. The Fisherface Method uses both PCA and LDA to produce a subspace projection matrix, similar to that used in the Eigenface Method. However, the Fisherface Method is able to take advantage of within-class information, minimizing variation within each class yet still maximizing class separation (Fernandez-Saavedra *et al.*, 2007).

Researchers define the training set shown where Γ_i is a facial image and the training set is partitioned into c classes such that all the images in each class X_i are of the same person and that no single person is present in more than one class. Then, researchers compute two scatter matrices representing the within-class (SW), between-class (SB) and total (ST) distributions of the training set through the image space:

$$\text{Training set} = \left\{\underbrace{\Gamma_1\Gamma_2\Gamma_3\Gamma_4\Gamma_5}_{X_1}\underbrace{\Gamma_6\Gamma_7\Gamma_8\Gamma_9\Gamma_{10}}_{X_2}\underbrace{\Gamma_{11}\Gamma_{12}\Gamma_{13}\Gamma_{14}\Gamma_{15}}_{X_3}\underbrace{\Gamma_{16}\Gamma_{17}}_{X_4}\cdots\cdots\underbrace{\Gamma_M}_{X_c}\right\}$$

$$S_W = \sum_{i=1}^{C}\sum_{\Gamma_k \in X_i}(\Gamma_k - \Psi_i)(\Gamma_k - \Psi_i)^T$$

$$S_B = \sum_{i=1}^{C}|X_i|(\Psi_i - \Psi)(\Psi_i - \Psi)^T$$

$$S_T = \sum_{n=1}^{M}(\Gamma_n - \Psi)(\Gamma_n - \Psi)^T$$

where, Ψ = (1/M). The variables are getting datas from Eigen value and the threshold value. Like the Eigenface System, the components of the projection matrix can be viewed as images, referred to as Fisherfaces in Fig. 5.

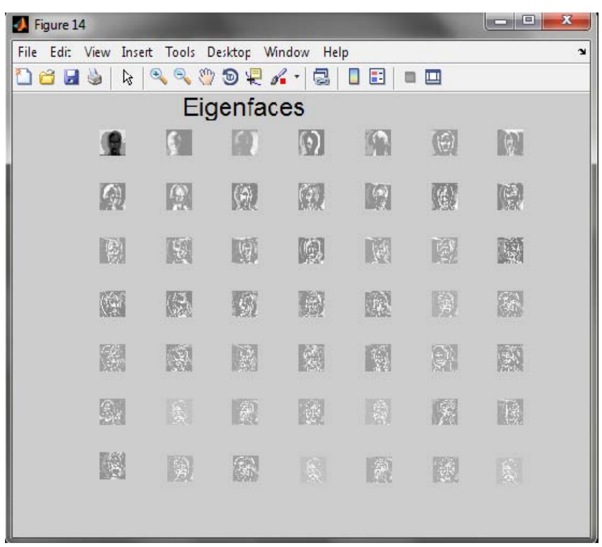

Fig. 5: Fisherfaces generated from the training set

EXPERIMENT AND RESULTS

Experimental data: In Multibiometric System, it is quite often that the database used is the true database which contains records. In this research, researchers have used a true database which contains three unimodal databases for face, iris and finger print, respectively.

Here, researchers have used different sensor for capturing images in face, iris and finger print like camera, scanner, etc. The face training set is given in the following Fig. 6-9.

For the input data, researchers can use virtual or real time data by using the sensors or directly from the database training set also. For face, researchers have used Olivetti Research Lab database which contains 49 images, 7 for every 7 different persons.

For iris recognition, there are several public databases (e.g., UBIRIS data base, Casia database, Upol database, NIST ICE database) are available for testing. Among that NIST ICE database is the largest public database and was proposed by NIST for the Iris Challenge Evaluation in 2005. It is consist of nearby 3000 infrared images from 244 different users.

Results: Researchers have compared various eigenimage techniques and the Fisherface technique in terms of FAR and GAR. From the results shown in Fig. 10, it is clear that Fisherface works more efficiently than eigenface (Fig. 10a). Therefore, in this system, researchers obtained better recognition performance by the Fisherface Method.

Figure 10b shows the performance rate of three different kinds of Rank-Level Fusion approaches in terms of GAR (Genuine Acceptance Rate) and FAR (False Acceptance Rate). From this, it is clear that the Equal Error Rate (EER) would be reasonably high without incorporating any fusion method. Significant performance gain can be achieved with the combination of rank information of different unimodal experts.

Considering wavelet transformation, several tests have been performed according to the different data input lengths for the filters and the number of bits dedicated to the binary point values has been modified. Researchers have considered three values: 10, 13 and 16 bits, fixing the integer part to 10 bits. In biometrics, the most common parameters used for evaluating system performance include the False Acceptance Rate (FAR) this is a measure of the number of potential intruders that access the system and the False Rejection Rate (FRR) which measures the number of authorized users who will be rejected by the system. These two parameters are usually expressed in a single curve called the Receiver Operating Characteristic (ROC). Figure 10b depicts the obtained ROC curve for the proposed system.

Accuracy: An ideal Biometric System should always provide the correct identity decision when a biometric sample is presented. However, a Biometric System seldom encounters an rank (m). Rank-m identification rate (%) the Cumulative Match Characteristic (CMC) curve for the Face-G matcher in the NIST BSSR1 database which plots the rank-m identification rate for various values of m. In this example, the rank-1 identification rate is ¼ 78% which means that for ¼ 78% of the queries, the true identity of the query user is selected as the best matching identity. Sample of a user's biometric trait that is exactly the same as the template. This results in limits the system accuracy.

The main factors affecting the accuracy of a Biometric System are noisy biometric data:

- A noisy fingerprint image due to smearing, residual deposits, etc.
- A blurred iris image due to loss of focus

Non-universality of a biometric trait: Figure 11 shows three impressions of a user's finger in which the ridge details are worn-out.

Noisy sensor data: Noise can be present in the acquired biometric data mainly due to defective or improperly maintained sensors. For example, accumulation of dirt or the residual remains on a fingerprint sensor can result in a noisy fingerprint image is failure to focus the camera appro-privately can lead to blurring in face and iris images recognition accuracy of a Biometric System is highly sensitive to the quality of the biometric input and noisy data can result in a significant reduction in the GAR of a Biometric System.

Non-universality: If every individual in the target population is able to present the biometric trait for recognition then the trait is said to be universal. Universality is one of the basic requirements for a biometric indenter. However, not all biometric traits are truly universal. The National Institute of Standards and Technology (NIST) has reported that it is not possible to obtain a good quality fingerprint from approximately two percent of the population (people with hand-related disabilities, manual workers with many cuts and bruises on their fingertips and people with very oily or dry

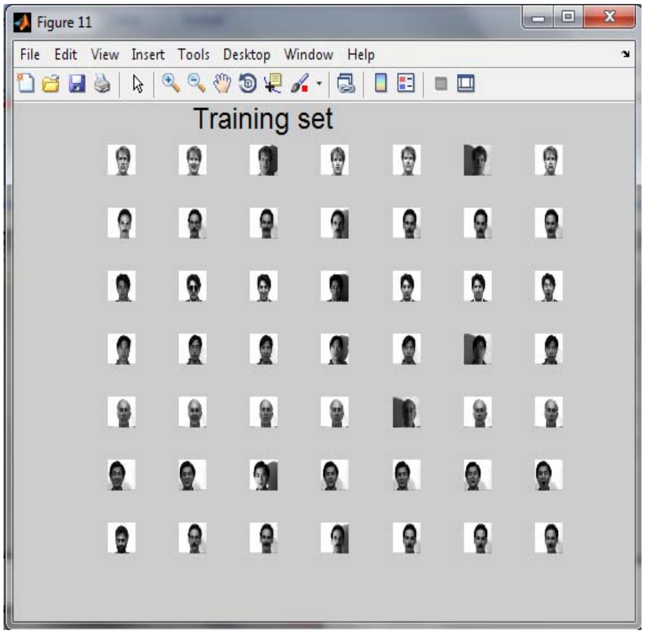

Fig. 6: Databases of face

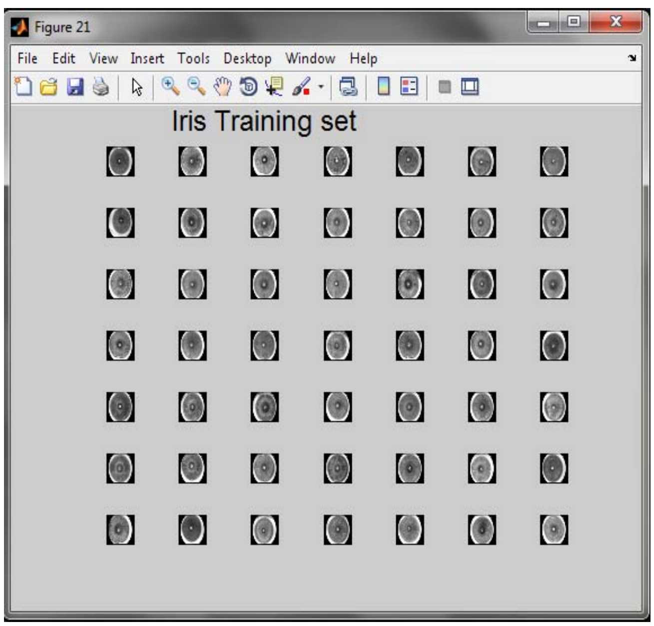

Fig. 7: Databases of iris

fingers). Hence, such people cannot be enrolled in a fingerprint verication system. Similarly, persons having longeye-lashes and those suffering from eye abnormalities or diseases like glaucoma, cataract, aniridia and nystagmus cannot provide good quality iris images for automatic recognition. Non-universality leads to high FTER and FTCR in a Biometric System (Table 1).

Security analysis: The security of biometric cryptosystems in terms of the min-entropy of the helper data. Min-entropy of a random variable A is need as:

$$H1(A) = ¡log (maxaP(A = a)): (5.5)$$

Note that all the logarithms in this study are of base 2. Suppose the security of a system relies on

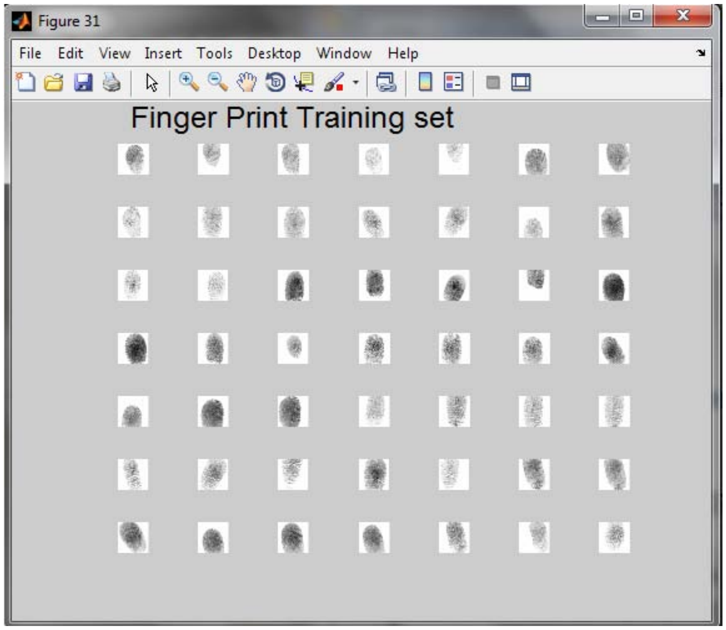

Fig. 8: Databases of fingerprint

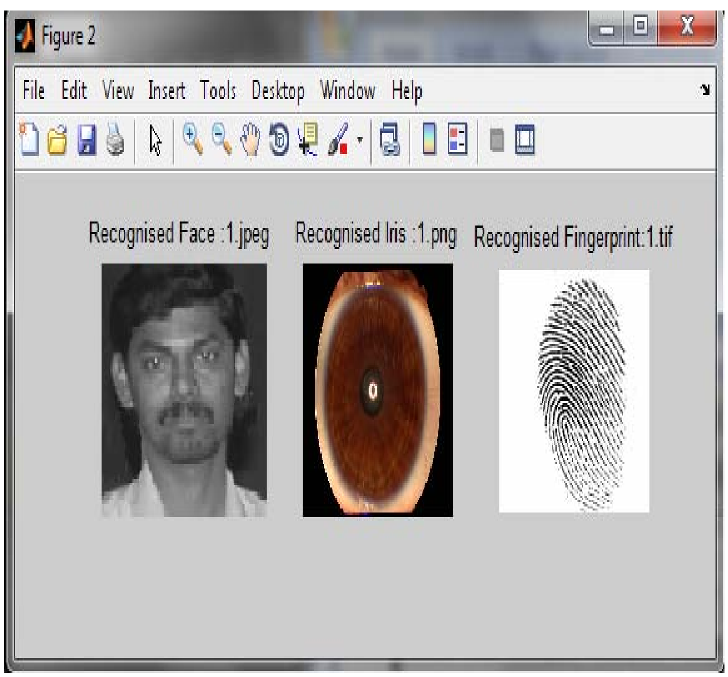

Fig. 9: Recognized output

the diculty in guessing A. The best strategy for an adversary to circumvent this system is to start with the most likely value of A and the min-entropy measures the security of the system in this scenario. Now consider a pair of random variables A and B. In entropy of A given B as:

H1(AjB) = ¡log (maxaP(A = ajB = b))

and the average min-entropy of A given B as:

H1(AjB) = ¡log (EbÃB [maxaP(A = ajB = b)])
= ¡log³EbÃBh2¡H1(AjB)i

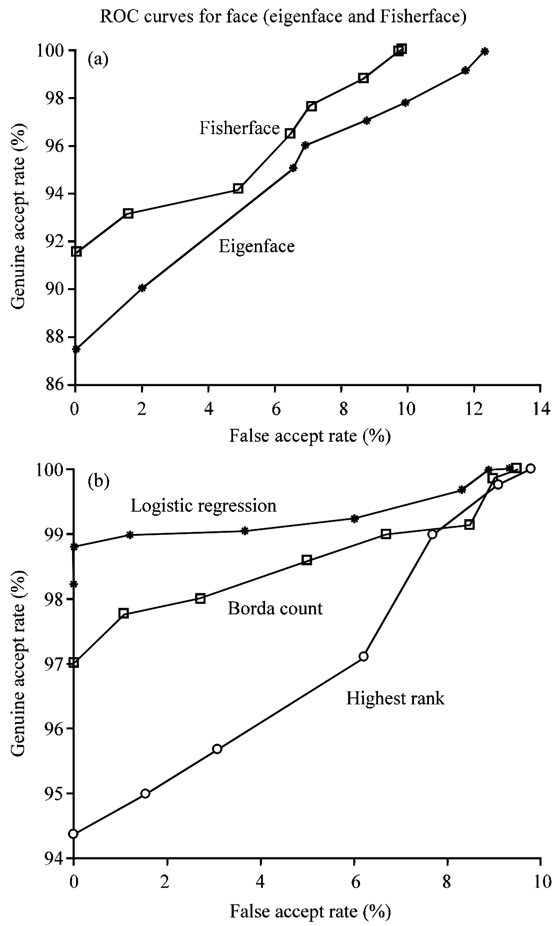

Fig. 10: a) Output response comparison; b) ROC curve for different rank Fusion Method

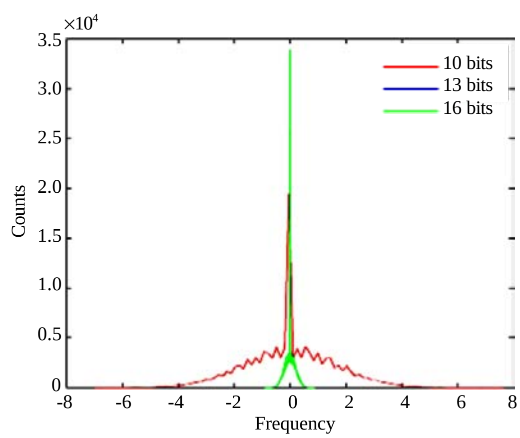

Fig. 11: Histogram of the values obtained in different simulation with PC computation

Table 1: Response time comparison

Approaches	Training time (min)	Recognition time (min)
Eigenface	1.87±0.29	0.50±0.19
Fisherface	2.64±0.09	0.53±0.16

Researchers can analyze the security of the fuzzy vault framework by measuring the average min-entropy of the biometric template given in the system.

CONCLUSION

This study is specifically focused on understanding the complex mechanisms employed to find a good combination of multiple biometric traits and various fusion methods to get the optimal identification results. In this study, researchers present a comparison between various PCA and FLD-based Multimodal Biometric Systems and differences between the results obtained before and after using rank-level fusion. Following extensive experimentation, some of the suggestions for the choice of the most appropriate technique (PCA or FLD) were drawn. For instance, on the studies' databases, the Fisherface Method demonstrated better recognition performance, although the training time was slightly higher than that of the eigenimage technique.

REFERENCES

Bowyer, K.W., K. Hollingsworth and P.J. Flynn, 2008. Image understanding for iris biometrics: A survey. Comput. Vision Image Understanding, 110: 281-307.

Daugman, J., 2006. Probing the uniqueness and randomness of IrisCodes: Results from 200 billion iris pair comparisons. Proc. IEEE, 94: 1927-1935.

Daugman, J., 2007. New methods in iris recognition. IEEE Trans. Syst. Man Cybern. B: Cybern., 37: 1167-1175.

Faundez-Zanuy, M., 2006. Biometric security technology. IEEE Aerospace Electr. Syst. Mag., 21: 15-26.

Fernandez-Saavedra, B., J. Liu-Jimenez and C. Sanchez-Avila, 2007. Quality measurements for iris images for biometrics. Proceedings of the IEEE International Conference on Computer as a Tool, September 9-12, 2007, Warsaw, Poland, pp: 759-764.

Zuo, J., N.A. Schmid and X. Chen, 2007. On generation and analysis of synthetic iris images. IEEE Trans. Inform. Forens. Secur., 2: 77-90.