An Enhanced Eigenfaces - based Biometric Forensic Model

Nasser S. Abouzakhar and Praneeth Enjamuri

School of Computer Science, The University of Hertfordshire,
College Lane, Hatfield AL 10 9AB, Hertfordshire, UK
{N.Abouzakhar, P.Enjamuri1}@herts.ac.uk

Abstract

The recent explosive development of the Internet allowed unwelcomed visitors to gain access to private information and various critical - mission resources such as financial institutions, hospitals, airports ... etc. Internet security has become a hot topic and relies on advanced technology. Now, more than ever, there is an increasing need for stronger identification mechanisms such as biometrics, which are in the process of replacing traditional identification solutions. Also, critical - mission systems and applications require mechanisms to detect when legitimate users try to misuse their privileges. Biometrics enables cybercrime forensics specialists to gather evidence whenever needed. This paper aims to introduce a biometric forensic model using facial identification approach. This model is based on the Eigenfaces approach for recognition proposed by Turk and Pentland [1]. Here, an unknown input image is compared with a set of images stored in a database to identify the best match. A freely accessible faces database has been used to develop our model which is based on a mathematical approach, called Principle Component Analysis (PCA). The paper addresses the issue of extracting global features of the images which are stored separately in the database. The features of a test image were compared with a set of images whose features were stored. The distance of the two images was calculated and when was minimum and below a certain threshold, the two images were considered to be the same and belong to a particular person. The calculated distance could be used and / or adjusted by a forensic specialist for deciding whether or not a suspicious user is actually the person who claims to be. The performance of the proposed face identification model was evaluated using standard methods. Distance values were used to express the similarity between any input image and other stored images. The model's performance was evaluated using FAR (False Acceptance Rate), FRR (False Rejection Rate) and EER (Equal Error Rate). In FAR, each user's image was compared with all images present in the database excluding the user's own image. In FRR, each user's image was compared with his own stored in the database. The major findings of the experiments showed promising and interesting results in terms of the model's performance and similarity measures.

1.0 Introduction

Over the last couple of years cybercrime security started playing a significant role in the tremendous development of the modern world. The main sectors which are affected by cybercrime threats are government bodies, military forces, financial institutions, hospitals and private businesses. All these sectors use the internet to gather, store and exchange vital information about their employees, customers, commodities, R & D, economic status ... etc. This information is processed and stored on networked computers and transmitted across various communication links to other networks. Information handled in this way increases efficiency but exposes these organizations to the risk of cybercrime. Therefore, there is an urgent need of increased security against unauthorised access and / or malicious activities.

Among various digital forensic technologies biometrics provides a high level of security and is currently one of the most important security techniques used around the world. Biometrics measures the physiological or behaviour features of an individual and compares these features with relevant material stored in a database for the purpose of confirming the identity of a certain individual. Biometrics technology aims to provide additional security to the traditional security techniques. The main types of biometric techniques are Fingerprint recognition, Hand geometry, Retina scanning, Iris scanning, Face detection, Signature dynamics and Keystroke dynamics. Among these techniques Face detection is one of the most natural means of biometrics identification.

Face detection involves identifying an individual by matching the input image against several images stored in a database and finding the best match. Face characteristics measured include facial shape and facial size. The relation between these characteristics is also technologically possible. The main advantages of the face detection technique are:

- User's permission is not required.
- There is no need for the user to be present physically.
- While enrolling the face image the user does not need to touch the device which is used for enrolling.

Although we can detect faces with little effort, there are certain challenges that are to be faced in identifying the facial characteristics. These challenges include illumination conditions, facial expressions, aging and disguises such as facial glasses or cosmetics ... etc, due to which the system faces a large variation in the visual incentive [2]**.** There are various limitations in biometric technologies as they depend on humans and their activities, as well as their actions, such as [4] [5]:

- Spoofing: the ability to deceive a biometric system when an attacker acts as a legitimate user whose biometric details are stored in a database.

- Mimic: a false person imitates a legitimate person aiming to gain unauthorised access to a victim system or network.

- Skimming: about capturing an unknown legitimate user’s data while submitting his / her details online.

Today person identification using Biometrics is widely used in airports, government institutions such as immigration and law enforcements bodies, private sector like health care, Internet service providers, e - commerce, banks and military services. This paper aims to introduce a human identification model which will identify an individual by matching his / her image against several images stored in a database and finding the best match. In general, the process of face identification has been developed using image capturing, extracting features and storing them in a template form. The extracted features of a test image are compared with those of the stored images templates and the system identifies the best match.

We consider biometric forensics as an approach for identifying and / or analysing forensic evidence using biometric technologies. Biometrics is one of the oldest concepts for any type of security and is about measuring the physiological behaviour of a human being. Based on these measured data the identity of a person can be confirmed. In biometrics, a sample template is compared against several records of enrolled users or cybercrime suspects. If any of the enrolled templates matches with the sample template, then we can say that the match is found. As the level of accuracy increases, the efficiency of biometric forensics increases as well. In order to develop a successful biometric identification system we need to consider the following points [3] [4]:

- The bodily features must not modify during the period of the human`s lifetime.

- The individual must be identified uniquely based on the physical features.

- The features must be stored in such a way that they are easily retrievable.

- The stored data must be accurate to check against valid individuals.

Even though there are various methods in biometrics for identifying face images, there are still challenges to overcome. These challenges include aging, changes in facial expression, lighting, capturing an image from a video ... etc. In order to overcome these challenges, extensive research has been carried out, such as 3D image analysis and multi - model biometrics.

2.0 Method

Humans have their own unique physiological features. Based on these features the biometrics technologies are divided to different categories, such as face, voice, iris, retina ... etc. Several new applications of recognition of unique physiological characteristics, like recognition of vein patterns, DNA, recognition of footprints and foot dynamics are still under research. Face recognition is about identifying an unknown face image from a set of known images based on the facial features. These facial features include eyes, nose, space connecting cheekbones etc. Face identification can be achieved using both 2D and 3D images. There were various methods proposed for implementing face identification for 2D images. However, one of the interesting approaches is the global approach (covered in section 2.1) which is based on the Eigenface technique using Principle Component Analysis (PCA) [1]. In this paper the proposed face identification model has been developed in two phases: Enrolment or Training phase and Identification or Testing phase, as follows [3] [5]:

- Enrolment phase includes:
  - Capturing sample images from a user.
  - Extracting the key features from each sample image.
  - Storing the key features in a database.
- Identification phase includes:
  - Capturing an image from a user.
  - Extracting the key features from the image.
  - Comparing the key features of the image with the key features of all the images stored in the database.
  - Identifying the best match.

Figure 1 shows the proposed Eigenface- based biometric forensic model which includes the Enrolment phase and Identification phase.

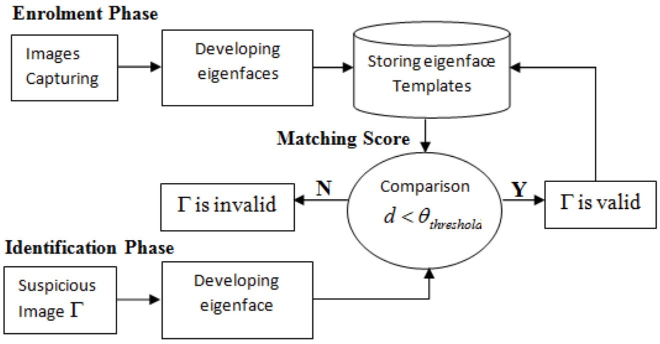


Figure 1: Eigenface - based Biometric Forensic Model.

This diagram shows that identifying a new suspicious face Γ can be achieved by transforming the new image into its Eigenface. The similarity between the input image Eigenface and each of the stored Eigenfaces can be measured using the Euclidean distance. We can confirm whether or not the new face belongs to a known face if the Euclidean distance between the two faces is below some threshold value $\theta_{threshold}$. The details of both phases are covered in section 3.

2.1 Global Approach

There are two different approaches for face identifications, as follows [5] [8]:

i) Feature - based approach.

ii) Global approach.

The feature - based face identification approach uses measurement of certain measuring points on a face including eyes, nose, mouth and some other points surrounding one`s cheekbones ... etc. Based on the geometrical relationship of these points i.e. the distance between these points, a unique geometrical model is built for a certain face. These calculations are then combined to obtain the face's unique features and complete the face identification. The major limitation of this approach is that the features' points are not 100 % accurate.

In the global approach all facial features are considered in order to identify a particular face. Instead of localizing certain points on the face all the features of the face are taken into account. The major advantage of this approach is that it does not destroy any information by processing only certain points of the face and hence more accurate results are achieved. In the global approach face recognition is based on two modes: Identification and Verification, as follows [9] [10]:

- Identification: is about identifying a particular image from a set of images stored in a database. The image is compared with other images stored in a database. In other words, we can say it has 'One-to-many' matching.

- Verification: is about determining whether an individual is who he or she claims to be. An image with certain available data is compared only with an image which is associated with the claimed identity. This refers to as 'One-to-one' matching.

2.2 Eigenfaces Technique

Eigenface is one of the techniques used for the identification of a particular face from a set of faces in a database [1] [2]. The Eigen technique is used to calculate the features of images as a whole. Over the last few years many approaches were introduced in order to solve the overall face recognition problem. The Eigenface technique is a powerful and simple technique for face recognition and represents the most intuitive way to classify the faces. It is considered as one of the most successful techniques in face identification. In this technique there is a usage of a well - built mixture of linear algebra and numerical testing to produce a set of Eigenfaces whose inputs are tested. In Eigenfaces the eyes, nose and mouth together form a high quality collective set of Eigen features. The image data can be extracted by using a mathematical technique called Principle Component Analysis.

2.3 Principle Component Analysis

Principle Component Analysis (PCA) is one of the most common techniques in finding patterns in data of an image [16]. In some fields, such as face identification and image compression, PCA is a useful statistical technique as it transforms each original image of a training dataset into a corresponding Eigenface. The main feature of PCA is reconstructing any original image from a training set by combining the Eigenfaces [16] [17]. An original image can be reconstructed from Eigenfaces by adding all the extracted features. An Eigenface does not represent all the features of the face, but only certain features are represented. These features are not always present in the original image. If the feature's presence is of higher degree, then the share of corresponding Eigenface would be bigger. However, if the feature is not there in the original image, then the corresponding Eigenface contribution to the sum of Eigenfaces is smaller. In order to recover the original image from the Eigenfaces, it is therefore necessary to put up a weighted sum of all Eigenfaces. This means that the recovered original image will be equivalent to the sum of all Eigenfaces, with each Eigenface having a certain weight [7] [16] [17]. It is possible to recover the exact original face images from the Eigenfaces if we use all Eigenfaces extracted from all other original images. This can be achieved by choosing the important feature i.e. the Eigenface. Before we discuss the issue of calculating Eigenfaces, we need to be aware of the following statistical terms [16]:

- **Mean Deviation:** is defined as the mean of pixel values of the deviation of values from average values.

- **Covariance:** is almost similar to standard deviation. Covariance represents a relationship between two matrixes. It is useful in terms of finding how much 2 dimensions vary from the mean with respect to each other.

- **Eigenvectors:** the vectors values which are obtained when the mean image values are subtracted from the original image. Eigenvectors can only be calculated for square matrices (*n x n* matrix); such a matrix would have *n* eigenvectors. These eigenvectors are known as the Eigen images or Eigenfaces.

2.4 Calculating the Eigenface using PCA

To calculate the Eigenfaces there are certain steps that need to be followed. Each step contains some mathematical calculations which help identifying a particular image from a set of images, as follows [1] [2] [18]:

- We have a set of face images used as a dataset and stored in a database. These faces are considered as the training sets (Γ_i) prepared for processing. All faces must have the same size N (in pixels) and use greyscale with values ranging from 0 - 255.

- Calculate the average vector (Ψ) using each face vector (Γ_n), where n is imageheight x imagewidth. Ψ is subtracted from the original faces Γ_i and the results are then stored in the variable Φ_i.

$$\Psi \;=\; \frac{1}{M}\sum_{n\,=\,1}^{M}\Gamma_n \qquad (1)$$

Here *M* is the number of face images in our training set.

$$\Phi_i = \Gamma_i - \Psi \qquad (2)$$

- The Covariance matrix C is calculated as follows:

$$C = \frac{1}{M}\sum_{n=1}^{M}\Phi_n\Phi_n^T \qquad (3)$$

We calculated the eigenvectors (□$_i$) using a particular improved procedure as indicated later.

- In this scenario, we need to choose only M' Eigenfaces that have the highest eigenvalues from M eigenvectors. If the eigenvalue is high, then the eigenvector describes more characteristic features of the relevant face. The Eigenfaces with low eigenvalues are ignored because they do not describe all the characteristic features of their faces. Therefore, we only consider the M' Eigenfaces (□).
- The covariance matrix has a dimension of N^2 x N^2 and hence would have N^2 eigenvectors and eigenfaces. If we take an image of a dimension of 256 x 256, this means that we need to calculate a 65,536 x 65,536 matrix and calculate 65,536 eigenfaces. Computationally, this will not be an efficient way for calculating the eigenfaces. Therefore, we followed the scheme proposed by Turk and Pentland [1]:

$$C = \frac{1}{M}\sum_{n-1}^{M}\Phi_n\Phi_n^T \quad = \mathrm{A}\,\mathrm{A}^T \qquad (4)$$

$$L = A\,A^T \qquad \mathrm{L}_{\mathrm{mn}} = \Phi_m^T\,\Phi_n \qquad (5)$$

$$u_l = \sum_{k=1}^{M} v_{lk}\,\Phi_k \qquad l = 1,2,\; \ldots.\; M \qquad (6)$$

where L is a M × M matrix, $A = (\Phi_1, \Phi_2,\; \ldots..,\; \Phi_{(M-1)}, \Phi_M)$, v_l are M eigenvectors of L and u_l are eigenfaces. The main advantage of this method is that we have to calculate only the *M* number instead of N^2. Using $A\ A^T$ the covariance matrix *C* can be simplified and calculated. Only few principal components (eigenfaces) are relevant as M << N2. The eigenfaces are ranked according to their usefulness using the associated eigenvalues. Therefore, only a subset of M eigenfaces are used, the M' eigenfaces with the largest eigenvalues.

- Identifying a new face Γ_{new} from the set of known faces can be achieved by transforming the new image into its eigenface whose weights are calculated. The similarity between the corresponding images can be measured using the Euclidean distance. We can confirm whether or not the new face belongs to a known face if the Euclidean distance between the two faces below some threshold value. The Euclidean distance can be calculated using the distance equation.

$$d(f_i, f_j) = \sqrt{\sum_{r=1}^{n} (b_r(f_i) - b_r(f_j))^2} \qquad (7)$$

Here $b_r(f)$ is the rth attribute of instance of *f*.

3.0 Experiments and Results

The development of our Eigenface forensics model was achieved in two phases: the Enrolment phase and the Identification phase.

3.1 Enrolment Phase

This phase is about enrolling all the users or suspects' images by extracting their features and then stored in a database. For each image the extracted features were stored with an id that identifies the relevant user or suspect. The implementation of enrolment phase included three steps: Image Capturing, Extracting Image Features and Storing Image Template, as follows [12] [13]:

Image Capturing: a set of images were downloaded from an online AT & T database. This database contains images of forty users, each user having five distinct expressions. All five images of each person were taken in different conditions by changing facial expression (for example, smiling / not smiling). These images are of 92 x 112 pixels with 256 grey levels per pixel. For all images we extracted the features and stored them in a database.

Extracting Image Features: all images in the database had 92 rows and 112 columns. Any coloured images were converted into a grey scale. Each image was divided into a block of cells where each cell represents one pixel value i.e. each image was represented by a matrix. Each image or matrix $I(92,112)$ was converted into a single dimensional matrix $I(92x112,1)$ or $I(10304,1)$, as shown below.

$$\text{Image} = \begin{bmatrix} I_{(1,1)} & I_{(1,2)} & \cdot\ \cdot & I_{(1,111)} & I_{(1,112)} \\ I_{(2,1)} & \cdot & \cdot\ \cdot & \cdot & I_{(2,112)} \\ \cdot & \cdot & \cdot\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot\ \cdot & \cdot & \cdot \\ I_{(91,1)} & \cdot & \cdot\ \cdot & \cdot & I_{(91,112)} \\ I_{(92,1)} & I_{(92,2)} & \cdot\ \cdot & I_{(92,111)} & I_{(92,112)} \end{bmatrix} \longrightarrow \begin{bmatrix} I'_{(1,1)} \\ I'_{(1,2)} \\ \cdot \\ I'_{(1,112)} \\ I'_{(2,1)} \\ \cdot \\ \cdot \\ \cdot \\ I'_{(92,111)} \\ I'_{(92,112)} \end{bmatrix}$$

All $I(92x112,1)$ image matrices were combined in one matrix, as shown below.

$$\begin{array}{c} \begin{array}{ccccc} \textbf{Image1} & \textbf{Image2} & \textbf{..} & \textbf{Image(n-1)} & \textbf{Image(n)} \end{array} \\ \begin{bmatrix} I'_{(1,1)} & I'_{(1,1)} & \cdot\ \cdot & I'_{(1,1)} & I'_{(1,1)} \\ I'_{(1,2)} & I'_{(1,2)} & \cdot\ \cdot & I'_{(1,2)} & I'_{(1,2)} \\ \cdot & \cdot & \cdot\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot\ \cdot & \cdot & \cdot \\ I'_{(92,111)} & I'_{(92,111)} & \cdot\ \cdot & .I'_{(92,111)} & I'_{(92,111)} \\ I'_{(92,112)} & I'_{(92,112)} & \cdot\ \cdot & I'_{(92,112)} & I'_{(92,112)} \end{bmatrix} \end{array}$$

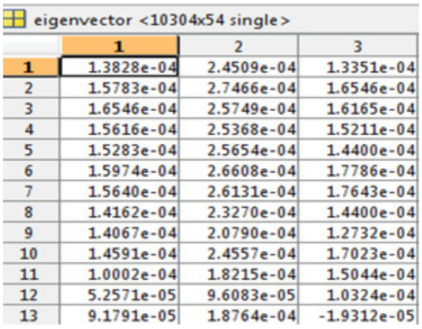
The next step was to calculate the average values for each row. Each image columns were denoted as Γ_1, Γ_2, Γ_3 . . . . . Γ_n and the average matrix was denoted as Ψ, as shown below.

$$\begin{array}{ccc} \begin{array}{ccccc} \Gamma_1 & \Gamma_2 & \cdots\cdots & \Gamma_{(n-1)} & \Gamma_n \end{array} & & (\Psi) \\ \begin{bmatrix} I'_{(1,1)} & I'_{(1,1)} & \cdot\ \cdot & I'_{(1,1)} & I'_{(1,1)} \\ I'_{(1,2)} & I'_{(1,2)} & \cdot\ \cdot & I'_{(1,2)} & I'_{(1,2)} \\ \cdot & \cdot & \cdot\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot\ \cdot & \cdot & \cdot \\ I'_{(92,111)} & I'_{(92,111)} & \cdot\ \cdot & .I'_{(92,111)} & I'_{(92,111)} \\ I'_{(92,112)} & I'_{(92,112)} & \cdot\ \cdot & I'_{(92,112)} & I'_{(92,112)} \end{bmatrix} & \longrightarrow & \begin{bmatrix} A_1 \\ A_2 \\ \cdot \\ \cdot \\ A_{(n-1)} \\ A_n \end{bmatrix} \end{array}$$

A_1, A_2, A_3 .... A_n represent the average values of each row where $A_1 = (I'_{(1,1)} + I'_{(1,1)} + ... + I'_{(1,1)})/n$ and $\Gamma_i = (\Gamma_1, \Gamma_2,\ .....,\ \Gamma_{(n-1)}, \Gamma_n)$. Next, we subtracted the average values (Ψ) matrix from the original values to obtain Φ_i, as shown below.

$$\begin{array}{ccccc} \textbf{Original Images} & & \Psi & & \Phi_i \\ \begin{bmatrix}\Gamma_1\\ \Gamma_2\\ .\\ .\\ \Gamma_{(n-1)}\\ \Gamma_n\end{bmatrix} & - & \begin{bmatrix}A_1\\ A_2\\ .\\ .\\ A_{(n-1)}\\ A_n\end{bmatrix} & = & \begin{bmatrix}X_1\\ X_2\\ .\\ .\\ X_{(n-1)}\\ X_n\end{bmatrix}\end{array}$$

Figure 2 shows a sample display of the calculated eigenvectors of each individual image stored in a database. Figure 3 shows the generated average image and an example of an Eigenface.



eigenvector <10304x54 single>

	1	2	3
1	1.3828e-04	2.4509e-04	1.3351e-04
2	1.5783e-04	2.7466e-04	1.6546e-04
3	1.6546e-04	2.5749e-04	1.6165e-04
4	1.5616e-04	2.5368e-04	1.5211e-04
5	1.5283e-04	2.5654e-04	1.4400e-04
6	1.5974e-04	2.6608e-04	1.7786e-04
7	1.5640e-04	2.6131e-04	1.7643e-04
8	1.4162e-04	2.3270e-04	1.4400e-04
9	1.4067e-04	2.0790e-04	1.2732e-04
10	1.4591e-04	2.4557e-04	1.7023e-04
11	1.0002e-04	1.8215e-04	1.5044e-04
12	5.2571e-05	9.6083e-05	1.0324e-04
13	9.1791e-05	1.8764e-04	-1.9312e-05

Figure 2: A sample of produced eigenvectors

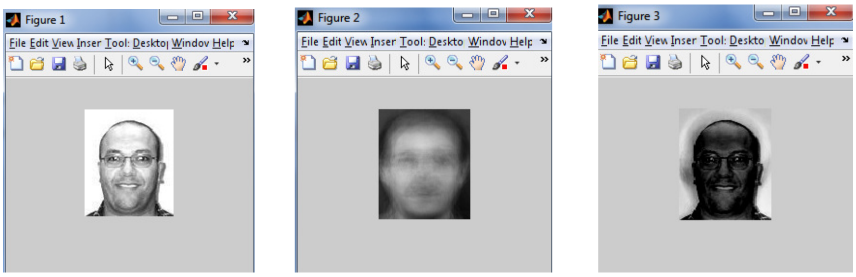


Figure 1
File Edit View Inser Tool: Desktoj Windov Help
Figure 2
File Edit View Inser Tool: Deskto Windov Help
Figure 3
File Edit View Inser Tool: Deskto Windov Help

Original Image Mean Image Eigenface Image

Figure 3: An example of an obtained Eigenface Image

Storing Image Template: after generating the eigenvectors / faces for all users / suspects' images, we stored them in a database. Eigenvectors represent the extracted features of the images presented in the database and were treated as the template images, each with a unique id. To test an unknown image, the features of a template images (or eigenfaces) stored in the database were compared with the unknown image's features. If any of the two compared images were found to be similar, we concluded that both images belonged to the same person.

3.2 Identification Phase

This phase represents the testing stage where we accepted an unknown image as an input and compared it with all images in the database. The Identification phase started with image capturing, followed by extracting image features. This is to produce the Eigenface of the input image. In this phase we needed to test one particular image with a number of images. Therefore, we had to capture only the image which we wanted to identify as an input image and then compare it with each stored image, as follows [13 [14]:

- **Comparison with Stored Images:** in this process we compared the input image's features (or equivalent eigenface) with a set of extracted features of all the images in the database. This comparison was achieved using the Euclidean distance measure.

- **Identification**: this refers to finding out whether or not the unknown input image belongs to a particular known user / suspect. The image was identified based on the values obtained from calculating all the distances. After calculating all distances the stored image with the minimum distance to the input image was identified. Therefore we were able to conclude that the unknown input image belonged to a particular user or suspect.

4.0 Evaluation and Analysis

In this section we analysed the operational characteristics of the developed model in terms of its performance and ability to predict the expected accurate output. In order to achieve that three different evaluation standard methods were used: FAR (False Acceptance Rate), FRR (False Rejection Rate) and EER (Equal Error rate). FAR measured the percentage of times a particular individual user who should be rejected is positively accepted or wrongly matched with a stored image [5] [11]. In other words, it is the case when an unauthorized person is identified as a legitimate person. FAR is calculated as follows:

$$\text{FAR} = \frac{FA}{FAE} \qquad (8)$$

FA = number of false acceptances.
FAE = number of False Acceptance Experiments.

FRR measures the percentage of times a particular individual user who should be positively accepted is rejected [5]. In other words, it represents the user who has been given access permission but is constantly rejected. The FRR is calculated as follows:

$$\text{FRR} = \frac{FR}{FRE} \qquad (9)$$

FR = total number of false rejections.
FRE = number of False Rejection Experiments.

Threshold ($\theta_{threshold}$) is a limiting point which is used to determine the identity of a new test image. Each time we calculated the Euclidian distance (*d*) between the two images, it should be less than the assumed threshold [15]. As a decision threshold, $\theta_{threshold}$ represents the maximum matching value below which a user's image is considered as a match. So, the distance between any two images d should be $< \theta_{threshold}$.

In other words, FAR is the percentage of user images that have values less than or equal to $\theta_{threshold}$, but are not in the database images set. Also, FRR is the percentage of user images that have values greater than $\theta_{threshold}$ and are in the database images set. Equal Error Rate is known as Crossover rate and is the point on the graph where the FAR and FRR intersect [5]. FAR, FRR and EER are evaluated and plotted by varying the threshold value. In FAR, as we increase the threshold value, the FAR value increases. This means that the identification model increases the acceptance of images which belong to illegitimate users as the threshold increases. In order to measure FAR, the user's image tested was compared with all the training users' images, except his / her own, as shown in figure 4a. In FRR, each user's testing image is compared with its own, as shown in figure 4b.

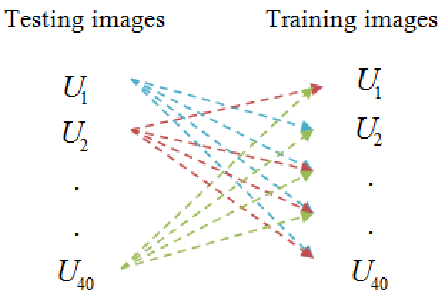


Figure 4(a): FAR measurement

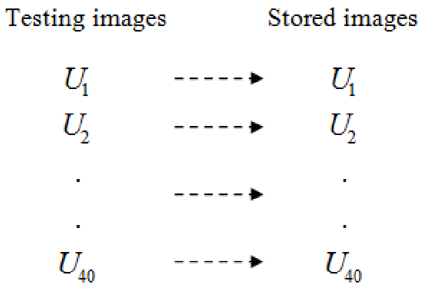


Figure 4(b): FRR measurement

Since we considered testing 40 images, we had to consider the 5 images for each of the other 39 users for each tested image. The FAR equation can be rewritten as follows:

$$\text{FAR} = \frac{FA}{40 \times 39 \times 5} \times 100$$

The FAR's value lies between zero and 100 % and each time we changed the threshold we calculated FAR for each testing image. Figure 4 shows that FAR is decreasing as we decrease the threshold $\theta_{threshold}$.

In FRR, as the threshold value increases, the FRR value decreases. This means that the identification model decreases the rejection of images which belongs to legitimate users as the threshold increases. In FRR, each user's testing image is compared with its own. Since we considered 40 user images, where each user has 5 images, the FRR equation can be rewritten as follows:

$$\text{FRR} = \frac{FR}{40 \times 5} \times 100$$

FRR was calculated for each testing image each time we changed the threshold. In order to obtain the EER, we needed to combine both FAR and FRR curves as both intersect at the EER point, as shown in figure 5. The main reason in evaluating EER is to find out the optimum threshold. The model's highest performance can be achieved with a lower EER. This phenomenon is proven to be true for all identification models.

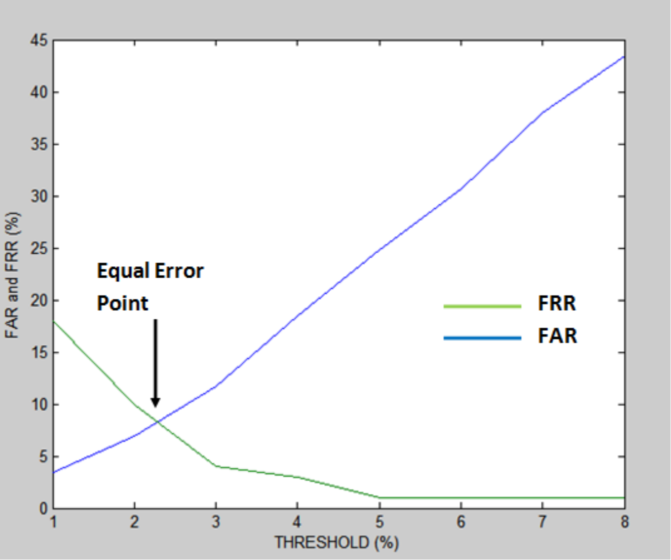


Figure 5: EER for the Eigenface identification model

The EER is an interesting threshold independent performance measure. The lower the EER, the better the model's performance. Figure 4 indicates that the two curves of FAR and FRR intersect at an EER of ~ 2.2 % threshold. The achieved optimum value for both FAR and FRR is ~ 8 %. The total error rate is the sum of the FAR and the FRR at the point of the EER which is ~ 16 %. It is not enough to specify either of the factors FAR or FRR to evaluate a particular identification model. It is possible that an identification model with a lower FAR has an unacceptable high FRR or vice versa. Also, it is not possible to decide whether or not a model with a higher FRR and a lower FAR performs better than a model with a lower FRR and a higher FAR value [6]. Therefore, it is important to consider all factors, FAR, FRR and EER, to evaluate any identification model.

5.0 Conclusion

This paper deals with the problems of designing a biometric forensic model which is used to identify legitimate users and / or suspicious faces. In order to develop this model we have chosen a global approach which considers the facial features as a whole. Based on this global approach, a mathematical technique, known as PCA (Principle Component Analysis), has been used to develop the Eigenface identification model. This model consists of two phases, the Enrolment phase and the Identification phase. In the Enrolment phase, the features of input images are extracted and then stored in a database. In the Identification phase, only the input image is captured, its features are extracted and then compared with all the features of the stored images. A decision threshold $\theta_{threshold}$ is used to represent the maximum matching value below which a user’s image is considered as a match.

By means of evaluation, as well as empirical evidence, we were able to determine the effectiveness of the developed model and assumptions. The performance of the developed model was evaluated using FAR, FRR and EER. Our experiments showed encouraging results and our research indicated a significant eigenface learning power in the application of biometric forensics. The results indicated that the two curves of FAR and FRR intersect at an EER of ~ 8.5 % threshold. The achieved optimum value for both FAR and FRR is ~ 8 %. It is important to consider all factors, FAR, FRR and EER, to evaluate such a biometric forensic model.

References

1 Turk M, and Pentland A, Eigenfaces for recognition, Journal of Cognitive Neuroscience, 3(1), 1991a.

2 Daugman J, Face and Gesture Recognition: overview (1997). IEEE Trans. Pattern Analysis and Machine Intelligence, 19(7), 675-676

3 Biometrics, http://www.globalsecurity.org/security/systems/biometrics.htm (visited April, 2010)

4 Facial Recognition, http://www.globalsecurity.org/security/systems/biometrics.htm (visited April, 2010)

5 Michael P. Down, and Richard J. Sands, Biometrics: An Overview of the Technology, Challenges and Control Considerations

6 Syris Technology Corporation, Technical Document About FAR, FRR and EER, 2004

7 Erum Naz, Umar Farooq, Tabbasum Naz, Analysis of Principal Component Analysis-Based and Fisher Discriminant Analysis-Based Face Recognition Algorithm, 2006

8 Robert Newman, Security and Access Control Using Biometric Technology, 2010

9 http://www.face-rec.org/journals-books/ (visited April, 2010)

10 Image Processing, http://www.mathtools.net/MATLAB/Image_Processing/index.html (visited April, 2010)

11 Biometric Technical Assessment, http://www.bioconsulting.com/Bio_Tech_Assessment.html (visited April, 2010)

12 Face Recognition, http://www.hrsltd.com/biometrics/face-recognition.php (visited May, 2010)

13 Jain A, Wayman J, Maltoni D, Mario D, Biometrics Systems Technology, Design and Performance Evaluation, 2005

14 Stain Z. Li, Anil K. Jain, “Handbook of Face Recognition”, 2004

15 Threshold for Eigenface Recognition, http://cnx.org/content/m12533/latest/ (visited May, 2010)

16 Smith L, A tutorial on principal components analysis, http://www.cs.otago.ac.nz/cosc453/student_tutorials/principal_components.pdf (visited May, 2010)

17 Pissarenko D, Eigenface- based facial recognition, December 1st, 2002

18 Turk M, and Pentland A, Face recognition using eigenfaces. In Proc. of Computer Vision and Pattern Recognition, pages 586–591. IEEE, June 1991b.