Investigation of Facial Artifacts on Face Biometrics using Eigenface based Single and Multiple Neural Networks

K. Sundaraj
University Malaysia Perlis (UniMAP)
School of Mechatronics Engineering
02600 Jejawi - Perlis
MALAYSIA
kenneth@unimap.edu.my

Abstract: - Biometrics has been an important issue pertaining to security in the last few decades. Departments or agencies entrusted with national security are increasingly installing surveillance cameras in strategic or critical areas to monitor the identities of the general public. Upon locating suspicious characters in the video feed, they are compared with existing databases to find a match. These databases are generally compiled from the National Registration Department (NRD), Immigration, intelligence agencies, etc. Unfortunately, as mentioned in most reports of tragic events, suspicious characters do not resemble anything like what has been stored in the databases. There is a high chance that the face biometric identification software will miss these culprits. In this paper we propose to investigate the effects of facial artifacts on the recognition rate of eigenface based neural networks. It has been found that eigenfaces coupled with Euclidean distance can be successfully used to recognize the human face in almost real-time. However, facial artifacts can cause the features that characterize a face to be distorted. Hence, it is desirable to identify problematic facial artifacts that can cause false identification or no identification. The main focus of this paper is the investigation of common facial artifacts on the performance of recognition and the proposition of modification to existing databases to improve the positive rate of identification. A professional graphic artist was used to modify the images used in the experiments. We use a single and multiple eigenface based neural network as the classifier in our experiments.

Key-Words: - Face Biometrics, Face Recognition, Eigenfaces, Facial Artifacts.

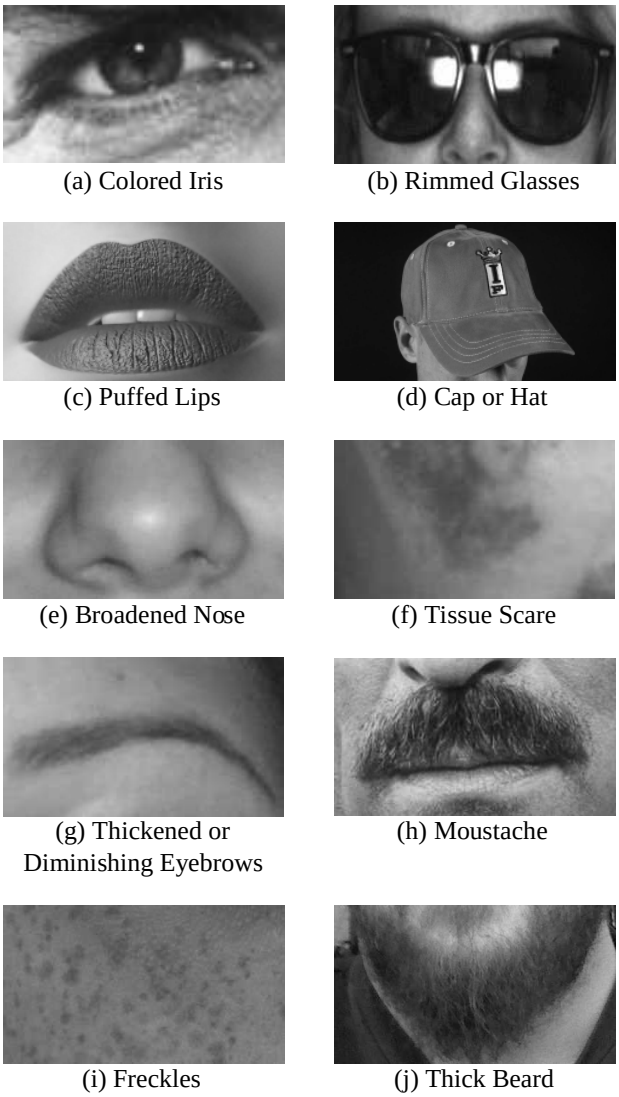
1 Introduction

Biometrics consists of automated methods of recognizing a person based on a physiological or behavioral characteristic. Among the features that are measured are face recognition, fingerprint, hand geometry, handwriting, irises and voice patterns. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent. Biometric based solutions are able to provide for confidential financial transactions and personal data privacy. The need for biometrics can be found in federal, state and local governments, in the military and in commercial applications. Enterprise-wide network security infrastructures, government IDs, secure electronic banking, investing and other financial transactions, retail sales, law enforcement and health, social services are already benefiting from these technologies.

Face recognition for biometric identification or face biometrics is a fairly young technology compared to other biometrics. Research in this field has been going on for decades, but it has been in the last 10 to 15 years that the greatest advances have taken place. Reviews of face recognition methods can be easily found in the literature such as [1] [2] and [3]. Owing to the growing number of applications, especially in the security domain, various research groups have devoted their work to face biometrics. In the past two decades or so, various methods (2D and 3D) have been applied and benchmarked for face biometrics. Some of the most important results are found in 2D face biometrics. [4] and [5] used principle component analysis (PCA) to recognize faces. In [6], [7] and [8] artificial neural networks (ANN) have been used. A local autocorrelation coefficient (LAC) method was found to be computationally efficient, invariant to translation and suitable for pattern recognition in [9]. This approach was applied by the authors in [10] and [11]

for pattern recognition and found to produce good results. In [12] the authors applied a linear discriminant analysis (LDA) to process human faces. This method was extended by the inclusion of LAC to perform face recognition with a high successful rate. There was an improvement in performance but at the cost of memory space. In [13] and [14], the Support Vector Machine (SVM) technique was applied to face recognition and [15] applied a method called Elastic Graph Matching (EGM) to face biometrics. PCA couple with autocorrelation feature vector (AFV) was used by [16] to speed up the recognition process. 3D face biometrics is relatively new. Very few researchers have been involved in this area. By 3D face biometrics, we mean the combination of a 2D face image plus a 3D disparity image. The disparity image is usually derived from the use of stereovision images. According to [17], adding 3D face biometrics can overcome some of the shortcomings of 2D face biometrics and improve recognition rate. Some of the recent works on 3D face biometrics using stereovision images comes from [18], [19] and [20].

However, face biometrics for security can be a complicated issue. We are not talking anymore about how accurate a face biometric system is but we wish to know how much foolproof it can be. Security agents responsible for national security rely heavily on face biometric softwares to identify culprits. Very often, as it was reported in the 911 terrorist attacks, had the responsible culprits been identified earlier at the airports, that tragic incident could have been avoided altogether [21]. 28 countries in the European Union (EU) have agreed to put in place a face reading security system by the end of 2007. In fact, the United Kingdom (UK) is already testing its face biometric system at some airports [22]. The fact that face biometric systems could be used to save lives has made the notion of a foolproof system all the more relevant. A foolproof system is one that cannot be fooled or one that knows when it is fooled [23]. Face images of perpetrators in the database can be considered as the standard image without facial artifacts. An individual who wishes to carry out a plan undetected and who is aware of the presence of any face biometric system (most of them are) would naturally opt to mask himself/herself with an aid of facial artifacts [24]. Some common facial artifacts are shown in Fig. 1. The previously mentioned 2D and 3D face biometric systems do not consider the problem of how much the system can be fooled but rather how accurate is the system in matching. Most of these systems insist conditions such as high resolution, full-frontal perspective, sufficient contrast and good lighting. Other acquisition conditions are also required, such as a neutral facial expression and the removal of any glasses, headgear or hair that obscures facial landmarks [25] [26].



(a) Colored Iris (b) Rimmed Glasses

(c) Puffed Lips (d) Cap or Hat

(e) Broadened Nose (f) Tissue Scare

(g) Thickened or Diminishing Eyebrows (h) Moustache

(i) Freckles (j) Thick Beard

Figure 1. Some common facial artifacts.

This paper presents an investigation into the problems posed by facial artifacts in a face biometric system. We limit ourselves to systems that perform face recognition using eigenface based neural networks. The method of using eigenfaces is not new. In [27] and [28], a near real-time system for face biometrics was developed using such a method. We

employ such a system in our analysis. Experiments were done to obtain the fool rate when facial artifacts were added to or removed from the standard face image. In the case, when the facial artifacts could not be removed or added easily onto a person in real, a professional graphic artist was used to touch up the standard image accordingly. We compare results obtained by using eigenfaces coupled with minimum distance and eigenface based back-propagation neural network.

2 The Eigenface Method

The basic idea of eigenfaces is that all face images are similar in certain aspects. There is a common pattern in all faces; for example, a face has two eyes, one nose, one mouth, etc. These characteristic features are called eigenfaces or the principle components in the facial recognition domain. They can be extracted out of the original image data by means of a mathematical tool called Principal Component Analysis (PCA). With this tool, an image of a human face can be transformed into eigenfaces. It is interesting to note that the original image can be obtained by combining all the eigenfaces. Therefore one could say that the original face image can be reconstructed from eigenfaces if one adds up all the eigenfaces. Each eigenface represents only certain features of the face. If the feature is present in the original image very often, the weight of the corresponding eigenface should be greater. On the contrary, if the particular feature is not (or almost not) found in the original image, then the corresponding eigenface should have a smaller (or zero) weight. So, in order to reconstruct the original image from the eigenfaces, one has to build a weighted sum of all eigenfaces. That is, the reconstructed original image is equal to a sum of all eigenfaces, with each eigenface having a certain weight. This weight specifies, to what degree the specific feature (eigenface) is present in the original image.

The procedure of applying the eigenface method to the face biometric problem is as follows [29] :

a) We start with the training sets of images Λ_1, Λ_2, …, Λ_m with each image denoted as *I(x,y)* where *x* and *y* are the size of the image in rows and columns.

b) Convert each image into its gray scale values and crop them into an image of size $n \times n$. Ensure that all faces in these cropped images are located at the same position of the image, for example, in the center of the image. Also, *n* has to be fixed for all images.

c) Form a set of vector $[n^2 \times 1]$. Combine the ensemble of vectors into a new full-size matrix $[n^2 \times 1 \times m]$ (row × column × depth) where *m* is the number of training images.

d) Find the mean of the training set by,

$$\psi = \frac{1}{m}\sum_{i=1}^{m} \Lambda_i \qquad (1)$$

e) Compute the mean subtracted face in the training set using,

$$\Theta_i = \Lambda_i - \Psi \quad \forall \quad i = 1, 2, \ldots, m \qquad (2)$$

f) Form the mean subtracted matrix $A = [\Theta_1, \Theta_2, \ldots, \Theta_m]$ of size $[n^2 \times m]$,

g) Compute the covariance matrix from *A* and its transpose A^T using,

$$C_{mm} = A^T_{mn^2} \times A_{n^2 m} \qquad (3)$$

h) Find the eigenvectors Γ_{mm} and the eigenvalues λ_m from the *C* matrix using any standard numerical method [30].

i) The eigenfaces *U*, can now be obtained using,

$$U_k = \sum_{n=1}^{m} \Theta_n \Gamma_{kn} \quad \forall \quad k = 1, 2, \ldots, m \qquad (4)$$

j) Order the eigenvectors in decreasing eigenvalues and normalize *U*. Instead of using all *m* eigenfaces, a subset of them *m'*, can be selected to represent the characteristic features of that particular training

set. This subset contains the strong features (highest eigenvalues) of the person. Based on this subset, the weights that describe the characteristics of the training class is given by,

$$W_k = U_k^T \Theta_k \quad \forall \quad k = 1, 2, \ldots, m' \tag{5}$$

k) The weights form a feature vector given as,

$$\Omega^T = [W_1, W_2, \ldots, W_{m'}] \tag{6}$$

l) An approximated face can be reconstructed by using its feature vector Ω, and its eigenfaces *U* using,

$$\Lambda_k = \Psi + \sum_{k=1}^{m'} \Omega_k U_k \quad \forall \quad k = 1, 2, \ldots, m' \tag{7}$$

m) Train the single or multiple neural networks with the feature vector, Ω.

n) Perform classification with unknown feature vector, Ω′. Tabulate the recognition rate.

3 Classification and Recognition

The feature vector Ω obtained from the previous section is used as inputs through a back-propagation neural network for classification and recognition. The proposed procedure for this study is shown in Fig. 2. In order to determine the value of *m'* used in Fig. 2, the *m* eigenvectors are firstly ordered according to their eigenvalues. The eigenvectors with the largest *m'* eigenvalues are chosen among the *m* eigenvectors. The value of *m'* is determined by the following,

$$\frac{\sum_{i=1}^{m'} \lambda_i}{\sum_{i=1}^{m} \lambda_i} > \varepsilon \tag{10}$$

where = [λ_1, λ_2, …, λ_m] are the eigenvalues of the *m* eigenvectors and ε is a used defined threshold that represents the maximum percentage of variation allowed in the *m'* eigenvectors.

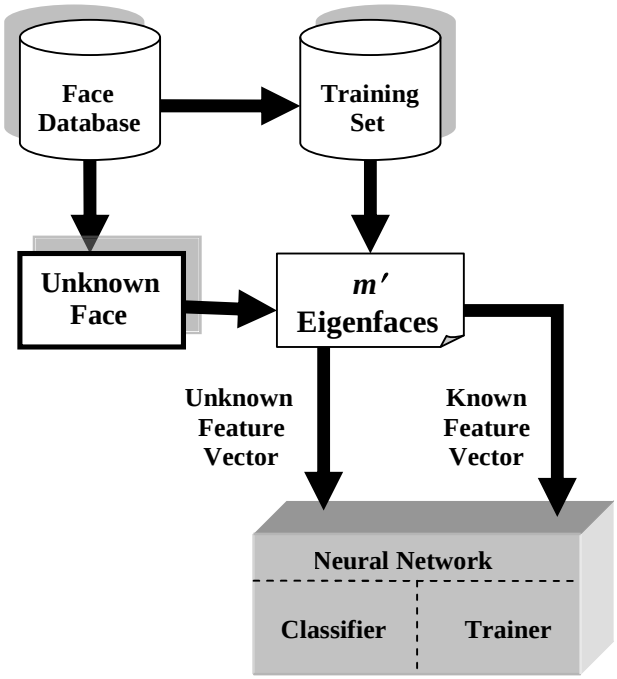


Figure 2. Proposed experimental process.

In our experiments, a back-propagation neural network for face biometrics was implemented and trained. A back propagation neural network consists of an input layer of nodes to accept input variables, an output layer of nodes to output results. The number of nodes on both ends depends on the number of input and output variables. There exists also one or several layers of nodes in between the input and output layers called hidden nodes. These nodes help capture the nonlinearity of the data. They can be fully or partially connected between layers through the weights between nodes. In the application of this back-propagation network for face recognition, parameters such as learning rate, types of transfer functions, momentum, number of hidden layers, number of hidden nodes, etc. have to be determined in advance. In our implementation as shown in Fig. 3, a combination of *Tansig* and *Logsig* functions has been used to obtain a nonlinear sigmoid function. This most commonly used transfer function was chosen in the hidden and output layers. The nonlinear sigmoid function is given as,

$$f(x) = \frac{1}{1 + e^{-x}} \tag{8}$$

In the single and multiple architecture neural networks, the number of input nodes is a function of the

dimension of the feature vector, Ω. On the other hand, the number of output nodes in the single architecture neural network is equal to the number of individuals (or classes) in the face data base whilst in the multiple architecture neural network, the number of output nodes is always equal to one. The number of hidden layers was arbitrary; one was used in our experiment for simplicity and efficiency. The number of nodes in the hidden layer was set according to,

$$\#\frac{Hidden}{Nodes} = \frac{1}{2}\left(\#\frac{Input}{Nodes} + \#\frac{Output}{Nodes}\right) \qquad (9)$$

However, the final parameters of the network and the number of hidden neurons were adjusted during the learning phase based on the performance of the network. Basically, this was a trial and error process. We also set the termination criteria of our network to be 1000 epochs or when the sum of squared error (SSE) reached 0.1.

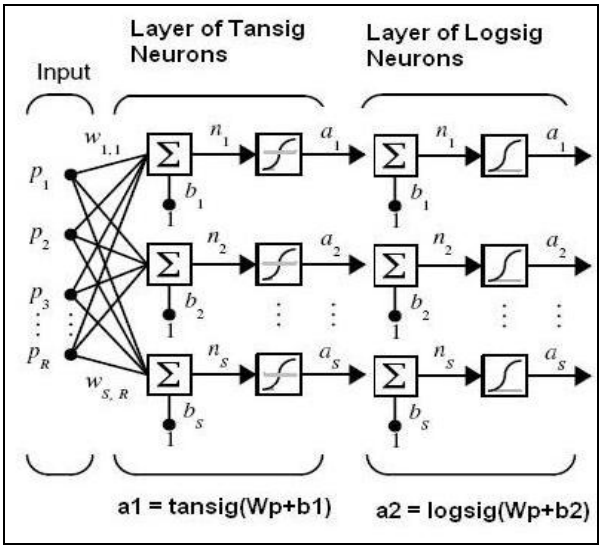


Figure 3. The architecture of the proposed neural network comprised of Tansig and Logsig neurons.

4 Implementation and Results

The proposed method was implemented on a personal computer with Pentium Core 2 Duo 2.8 GHz and 1GB SDRAM. Fig. 4 shows the software that was developed to capture the region of interest of a human face. This software was developed using Visual Basic 6.0 under the Windows XP platform. A Marlin FO33C ½″ progressive scan color CCD firewire camera with a maximum resolution of 640 × 480 pixels was used to capture the image of the subject in various orientation. All images were converted to gray scale values using the internal driver of the hardware provided by the manufacturer. The distance of the subject from the camera during the process of capturing face image was adjusted such that a complete face (including hair and beard) plus some background would fit into a window size of about 400 × 400 pixels. This choice is actually arbitrary and differs from one author to another in the literature.

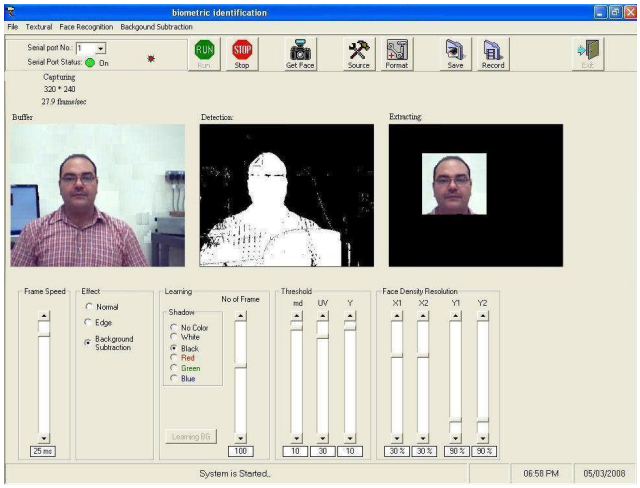


Figure 4. Software developed for the face acquisition and face recognition using neural networks.

A total of 15 individuals or classes were used as subjects in the experiment. Each individual's face image was captured 12 times. In each set of 12 images, 3 images were adjusted with facial artifacts by either touching up by a professional graphic artist, manual inclusion of artifacts before image capture or by face morphing using a dedicated software. These 3 images were only used in the recognition phase. In the remaining 9 images, 1 image was captured as a standard image (full frontal view), 5 more images were normal face images in various orientation and finally 3 more images of various expressions of emotion. These 9 images were used as the source of data in the training phase. Fig. 5 shows a sample of subjects that can be considered to have faces with artifacts. Fig. 6 shows a sample of subjects that were used in the training process.

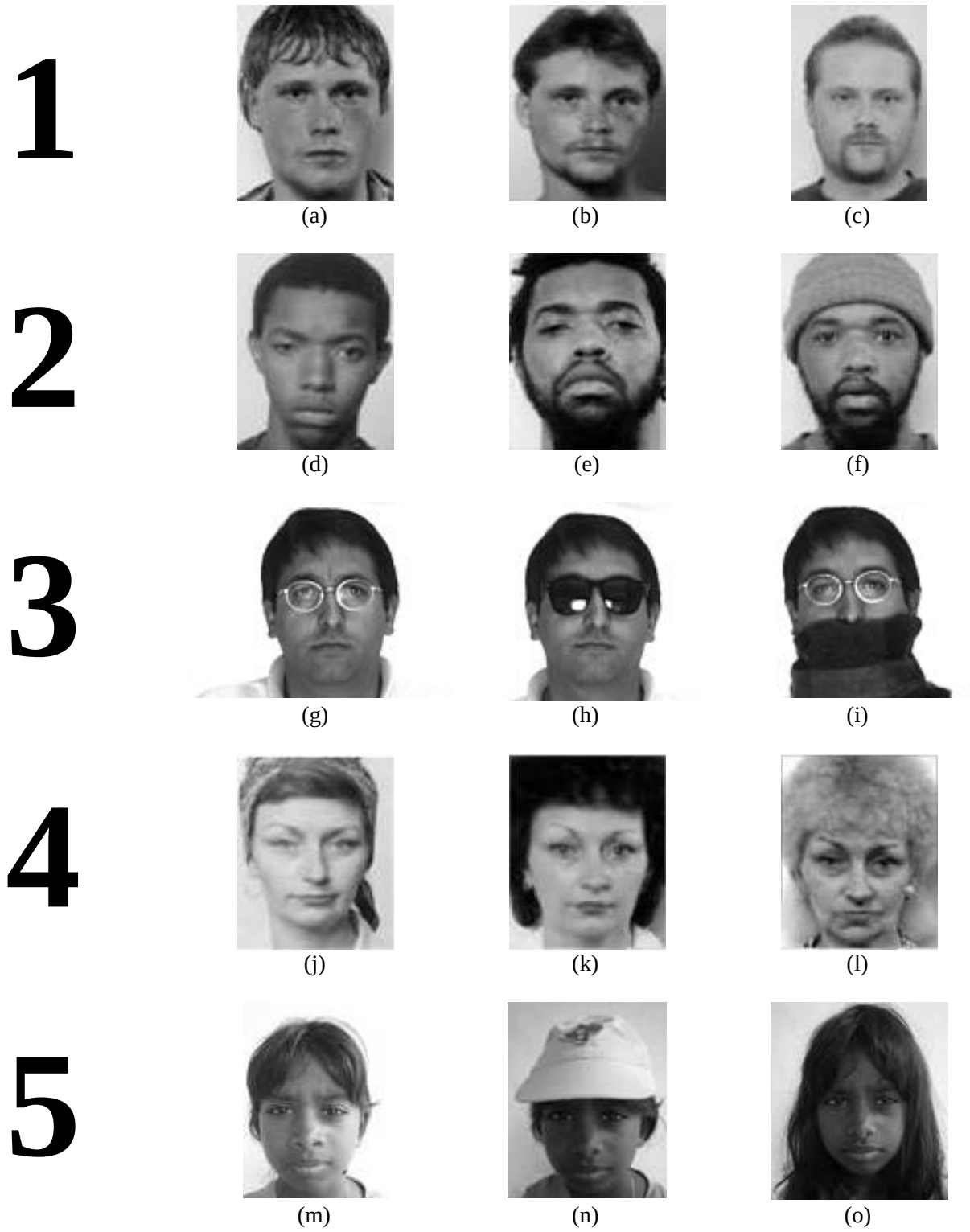


Figure 5. Five sample of subjects with various types of facial artifacts that were obtained using touching up by a professional graphic artist, manual inclusion of artifacts before image capture or by face morphing using a dedicated software.

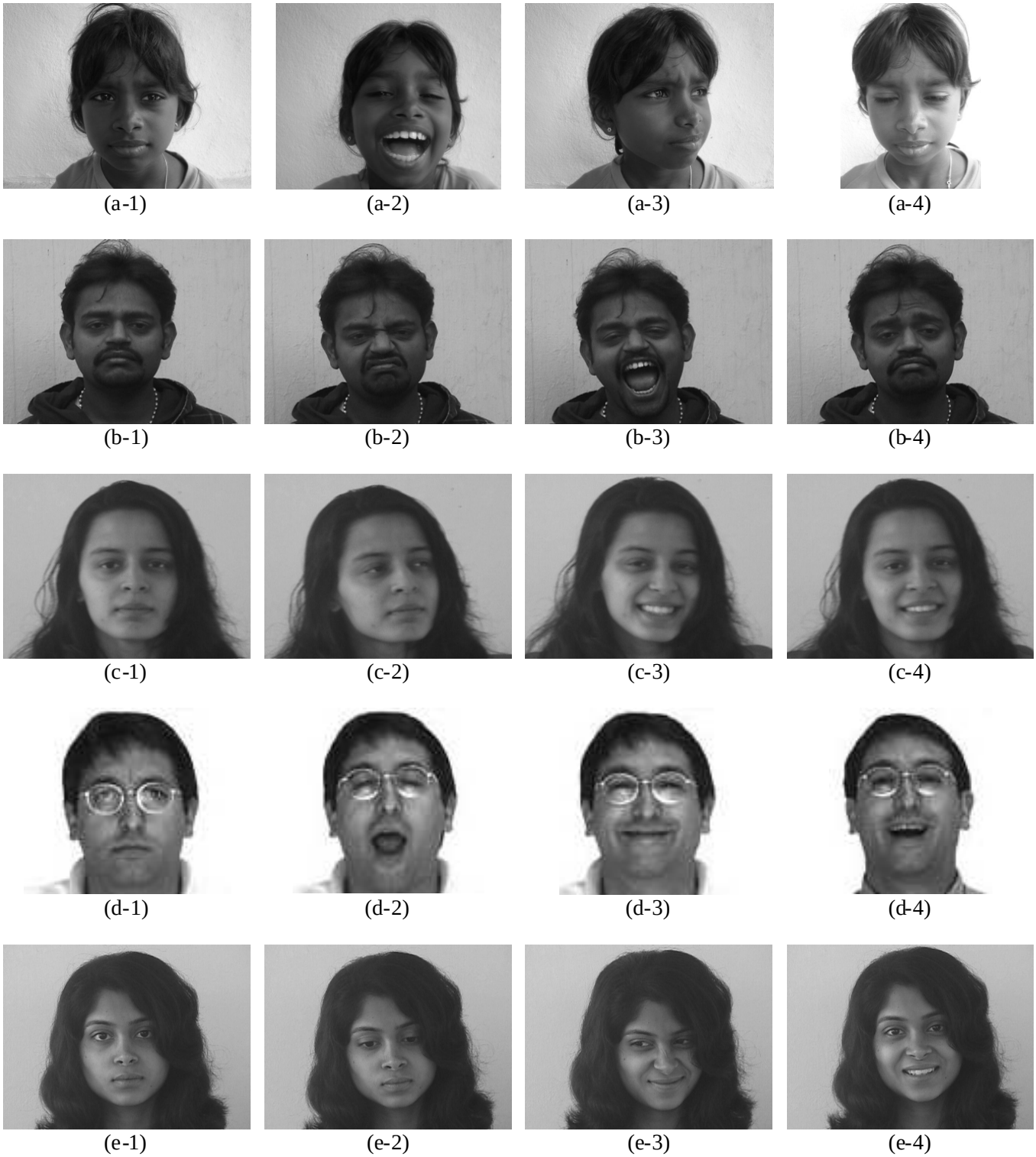


Figure 6. Sample of subjects that were used in the learning phase of the back propagation neural network. The left most images are the standard image of each subject. Also included are images of various face orientation and images of faces of various emotions. Taken from [31].

To setup of the network, the eigenface method was firstly applied to the training set of images of each subject to find the best *m'* eigenfaces. Table 1 summarizes the result of this procedure. Then, in the learning phase of the back propagation neural network, the corresponding feature vectors Ω of the best *m'* eigenfaces of all subjects are used as inputs to train the single and multiple networks. The data is fed from the input layer, through the hidden layer to the output layer without feedback. The network then uses the feed forward error back propagation scheme to search for a surface with minimum error using gradient descent. The process of feeding the input layer with data is repeated until the network is self-adjusted with a set of weight that gives minimum error. These weights are stored and are used later in the recognition process. Table 2 shows the network parameters for both the single and multiple architectures used in our experiments at the end of the training phase. The network parameters were adjusted until the performance of the network was acceptable.

Table 1. Determination of the best *m'* eigenfaces.

Parameter	Value
# Database	15 subjects
# Training Images (*m*)	random 5 out of 9 per subject
ε	0.8 (fixed)
m' (per subject)	4 (final choice)

Table 2. Final parameters of the back propagation neural network after adjustment during training.

Architecture	Parameter	Value
Single (one for all)	# input nodes	4
	# output nodes	15
	# hidden nodes	12
	Momentum	0.8
	r, Learning Rate	0.9
	SSE	0.1
Multiple (per individual)	# input nodes	4
	# output nodes	1
	# hidden nodes	3
	Momentum	0.7
	r, Learning Rate	0.9
	# of Hidden Nodes	50
	SSE	0.1

After the feature vector was obtained for various combinations of training images, the proposed network was set up and trained. The proposed method was then validated for the recognition of faces with facial artifacts with different sizes of trained data (various combinations of trained faces). Recognition was done using 3 methods; eigenfaces with Euclidean minimum distance (EEMD), eigenface based single neural network (ESNN) and eigenface based multiple neural networks (EMNN). Fig. 7 shows the experimental results of these experiments. Fig. 8 shows the false acceptance rate (FAR) which is the probability that the wrong person is accepted (fraud) and the false rejection rate (FRR) which is the probability that the right person is rejected using these methods. These two parameters can serve as a measure of how foolproof the face biometric system is.

From the results, we can see that the EEMD method gives most than 78% recognition rate for a very small size of data. But this gradually decreases as the size of the database increases. A similar pattern can be observed for both the neural networks; ESNN and EMNN. The recognition rates for all tested methods are not as high as reported in the literature due to the fact that in the conducted experiments, facial artifacts were added. Facial artifacts were added one by one as the database size was increased. This amounts to reducing the contribution of the feature vectors that was originally determined from the database. It is clear that facial artifacts are capable of fooling a face biometric system especially when the database size becomes large. On average, all the experimented methods gave a recognition rate of more than 75%. With the use of a single neural network, there is an increase of about 5–10% in recognition rate. When multiple neural networks are used, there is a further increase of about 3–5% in recognition rate when compared to a single network.

5 Conclusions

This paper presents a study to investigate the effects of facial artifacts on the recognition rate of face biometric systems that are based on eigenfaces. The proposed study is based on the implementation of a fast and efficient method to extract the eigenfaces from a set of face images that belong to an individual. These images are expected not to contain any facial artifacts. In the recognition phase, facial artifacts were added to the images of an individual with the help of a professional graphic artist, manual inclusion or image morphing by

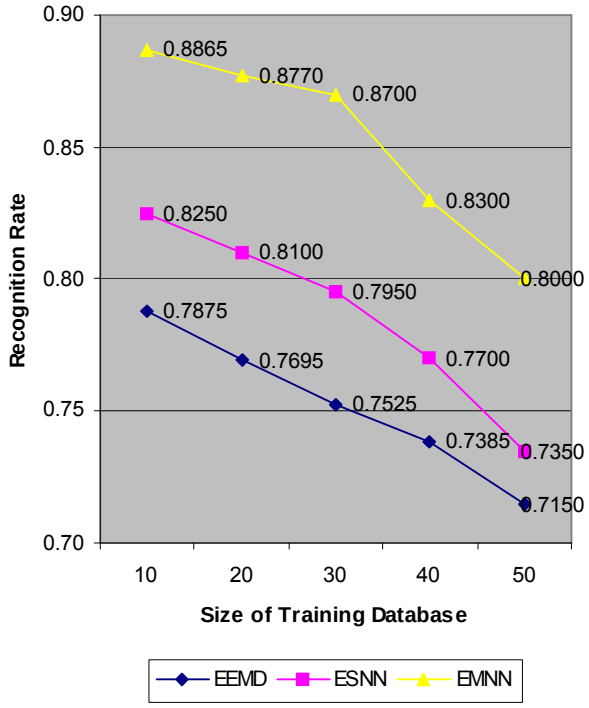


Figure 7. Recognition rate of proposed study.

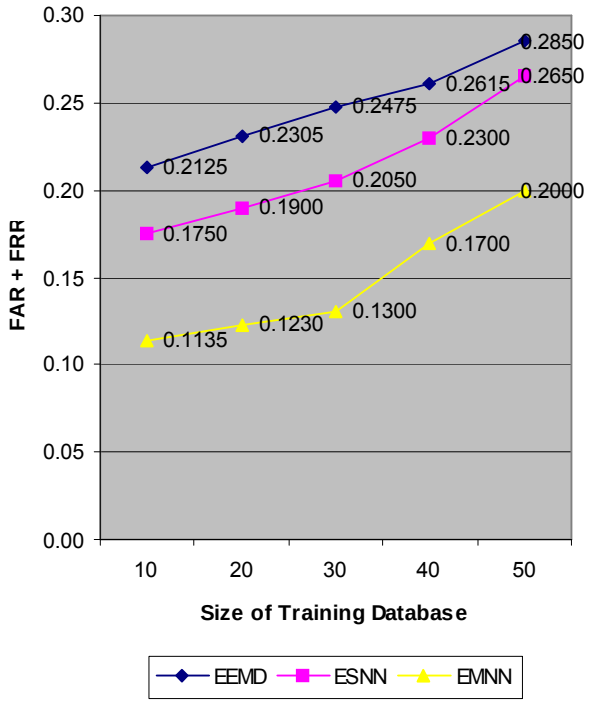


Figure 8. Foolproof rate of the proposed methods.

a dedicated software. The amount of facial artifacts added was slowly increased as the database size was increased. According to our experiments, it was found that all methods could be fooled by the inclusion of facial artifacts especially when the database size increases. We also found that eigenface based multiple neural networks produced a good recognition rate even with the presence of facial artifacts. The foolproof rate which has been presented is a combination of FAR and FRR. It is hoped that these rates can help security agents that are in charge of national security decide the type of method chosen as the discrimination basis of the face biometric system. A limitation in the proposed study is the size of the training database in terms of individuals. This is partly due to the fact that modifying images with facial artifacts can be time consuming to produce realistic images. It is hoped that a specific database will be created and available online for this purpose in our future work.

References:

[1] R. Chellappa, C. L. Wilson, and S. Sirohey, "Human and machine recognition of faces: A survey," *Proceedings of the IEEE*, vol. 83, no. 5, pp. 705–741, 1995.

[2] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, "Face recognition: A literature survey," *ACM Computing Surveys*, vol. 35, no. 4, pp. 399–458, 2003.

[3] A. F. Abate, M. Nappi, D. Riccio, and G. Sabatino, "2D and 3D face recognition: A survey," *Pattern Recognition Letters*, vol. 28, no. 14, pp. 1885–1906, 2007.

[4] M. A. Turk and A. L. Pentland, "Eigenfaces for Recognition," *Cognitive Neuroscience*, vol. 3, no. 1, pp. 71–86, 1991.

[5] M. Kirby and L. Sirovich, "Application of the Karhunen Loeve Procedure for the Characterization of Human Faces," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 12, no. 1, pp 103–108, 1990.

[6] D. Valentine, H. Abdi, A. J. O`Toole and G. W. Cottrell, "Connectionist models of face processing: A survey," *Pattern Recognition*, vol. 27, no. 9, pp. 1209–1230, 1994.

[7] J. Zhang, Y. Yan and M. Lades, "Face recognition: eigenface, elastic matching and neural nets," *Proceedings of IEEE*, vol. 85, no. 9, pp. 1423–1435, 1997.

[8] M. Hazem, M. El-Bakry and Q. Zhao, "A New Technique for Fast Pattern Recognition Using Normalized Neural Networks," *WSEAS Transactions on Information Science and Applications*, vol. 2, no. 11, pp. 1816–1835, 2005.

[9] J. E. Keogh and M. J. Pazzani, "An enhanced representation of time series which allows fast and accurate classification," *Clustering and Relevance Feedback in Knowledge Discovery and Data Mining*, 1998, pp. 239–243.

[10] K. Hotta, T. Kurita and T. Mishima, "Scale invariant face detection method using higher order autocorrelation features extracted from log-polar image," in *IEEE International Conference on Automatic Face and Gesture Recognition*, 1998, pp. 70–75.

[11] H. Hotteling, "Analysis of complex statistics variables into principle components," *Educational Physiology*, vol. 24, pp. 498–520, 1993.

[12] G. Goudail, E. Lange, T. Iwamoto, K. Kyuma and N. Otsu, "Face recognition system using local autocorrelations and multiscale integration," *Pattern Analysis and Machine Intelligence*, vol.18, no. 10, pp. 1024–1028, 1996.

[13] Y. Wang, C. Chua and Y. Ho, "Facial feature detection and face recognition from 3D images," *Pattern Recognition Letters*, vol. 23, pp. 1191–1202, 2002.

[14] L. Chiunhsiun, "Using Lighting Normalization and SVM for Face Recognition with Uneven Illumination," *WSEAS Transactions on Information Science and Applications*, vol. 4, no. 5, 2007.

[15] L. Wiskott, J. Fellous, N. Kruger and C. Malsburg, "Face recognition by elastic bunch graph matching," *Pattern Analysis and Machine Intelligence*, vol. 19, no. 7, pp. 775–779, 1997.

[16] V. Popovici and J. P. Thiran, "Pattern recognition using higher order local autocorrelation coefficients," in *International Conference on Image Processing*, 2002, pp. 229–238.

[17] F. Tsalakanidou, D. Tzovaras and M. G. Strintzis, "Use of depth and color eigenfaces for face recognition," *Pattern Recognition Letters*, vol. 24, pp. 1427–1435, 2003.

[18] S. Lao, Y. Sumi, M. Kawade and F. Tomita, "3D template matching for pose invariant face recognition using 3D facial model built with iso-liminance line based stereo vision," in *International Conference on Computer Vision*, 2000, pp. 911–916.

[19] A. Samani, J. Winkler and M. Niranjan, "Automatic face recognition using stereo image," in *International Conference on Acoustics, Speech and Signal Processing*, vol. 5, 2006, pp. 913–916.

[20] C. Beumier and M. Acheroy, "Face verification from 3D and gray level cues," *Pattern Recognition Letters*, vol. 22, pp. 1321–1329, 2001.

[21] "The 911 Commission Report," *The National Commission on Terrorist Attacks upon the United States*, 2004.

[22] Council of the European Union, "Standards for security features and biometrics in passports and travel documents issued by Member States," *Council Regulation (EC) No 2252/2004*, 2004.

[23] Bruce Schneier, "Sensible Authentication," *Queue*, vol. 1, no. 10, pp. 74 – 78, 2004.

[24] Christopher Lukasik, "The Physiognomy of Biometrics: The face of counterterrorism," *www.common-place.org*, vol. 5, no. 1, 2004.

[25] W. Funk, M. Arnold, C. Busch, A. Munde, "Evaluation of image compression algorithms for fingerprint and face recognition systems," in *Sixth IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop*, pp. 72–78. West Point, NY, USA: IEEE Computer Society, 2005.

[26] B. Christoph, "Facing the future of biometrics," *European Molecular Biology Organization*, vol. 7, Special Issue, pp. 23–25, 2006.

[27] Y. Zhujie and L. Yu, "Face recognition with eigenfaces," in *International Conference on Industrial Technology*, 1994, pp. 434–438.

[28] Yan Ma and Shunbao Li, "The Eigenface Method Combined with the Reordered DCT Coefficient Subbands," *WSEAS Transactions on Information Science and Applications*, vol. 3, no. 9, pp. 1669–1673, 2006.

[29] M. A. Turk and A. L. Pentland, "Face Recognition using Eigenfaces," in *International Conference on Computer Vision and Pattern Recognition*, 1991, pp. 586–591.

[30] J. H. Matthew, "Eigenvalues and Eigenvectors," *Technical Report – Department of Mathematics, University of California*, 2003.

[31] Vidit Jain, Amitabha Mukherjee. "The Indian Face Database," *http://vis-www.cs.umass.edu/~vidit/IndianFaceDatabase*, 2002.