Secure Face Recognition System based on Eigenface and Fisherface Techniques

Resmi N.G. [#1], Aarya P.S. [*2], K.P.S Sachin [*3], Reshma Gopi [*4], Megha Sara Isacc [*5]

[#1]*Department of Computer Science and Engineering, Muthoot Institute of Technology and Science*
Varikoli, Puthencruz, Ernakulam, India.
[1]resmi.ng@gmail.com

[*2]*ThinkPalm Technologies Pvt. Ltd.*
Infopark, Kochi, India

[*3]*BigBinary*
Infopark Phase 2, Kochi, India

[*4]*HR Solutions*
Kaloor, Kochi, India

[*5]*Zerone Consulting*
Infopark, Kochi, India

[2]aaryaps14@gmail.com
[3]sachinkps1@gmail.com
[4]reshmagopib4u@gmail.com
[5]meghapunnasseril@gmail.com

***Abstract*— Face recognition has been a fast growing, challenging and interesting area in real time applications. Face recognition can serve as a safety feature and can often be used along with surveillance systems to enhance security. In the present pandemic situation, children and old-aged people are often left alone at home and are at high risk of attacks from strangers, burglars or thieves. Crimes against children and the old-aged are increasing day by day and many of these occur within the four walls of their homes. Some of the households do have a surveillance system but it could be used only for verification after the crime has occurred. This paper proposes an efficient method for face recognition using eigenface method based on principal component analysis and fisherface method based on linear discriminant analysis and recognizes a face from live video captured using a CCTV camera. The proposed face recognition system enhances the capability of CCTV to recognize faces of trusted people against attackers. The system takes a series of snapshots using the camera when a person enters into the surveillance region. These snapshots are sent to the software to be analyzed and compared with an existing database of trusted people. Alert messages are sent to the authorized persons' phones if the person is not recognized. The system is very much capable in handling different environmental situations and can recognize the people in a variety of lighting conditions. This approach improves the surveillance efficiency with an addressable margin.**

***Keywords*— Eigenface, fisherface, face recognition, principal component analysis, linear discriminant analysis.**

I. INTRODUCTION

Facial recognition technology can be used as an attractive solution to many contemporary needs such as identification and the verification of identity claims. Facial recognition technology and facial recognition research is a developing area in the field of pattern recognition research and technology. The efficiency of the Face Recognition System (FRS) is determined using its ability to locate or detect a face in a field of vision so that it is only the image pattern of the face (and not the background "noise") that is processed and analyzed.

A general statement of the problem can be formulated as follows: Given still or video images of a scene, identify or verify one or more person in the scene using a stored database of faces [1]. The solution to the problem involves segmentation of the faces from cluttered scenes, feature extraction from the face region, recognition or verification [2].

Crimes against the physically weak category of the population, the children and the old-aged people, are becoming common and such crimes can be very disturbing and very often occur as attacks inside their own residences. The attackers, by careful watching of the movement of persons in and out of the residences and the surroundings, understand the duration of time the weak are left alone at home. An efficient face recognition system used along with a CCTV camera can prevent these problems up to a limit. The proposed FRS helps in figuring out unauthorized persons entering the compound and alerting the trusted people about the same. The system can also be used in various other situations. The system sends alert messages to trusted persons as well as those staying inside the houses if any unfamiliar person enters the compound. Thus, the insider can decide early not to open the door and also the neighbouring or remote trusted person will be alerted early so that appropriate actions can be initiated if necessary.

The proposed face recognition system is implemented using mathematical concepts of principal component analysis and

linear discriminant analysis and is found to produce acceptable results even under different lighting conditions.

The rest of the paper is organized as follows: Section 2 describes the methods used in the proposed system, section 3 gives an overview of the system, section 4 provides the results and discussion and section 5 gives conclusion.

II. Methodology Used

The fig. 1 given below depicts a typical face recognition system that can be used for identification purposes.

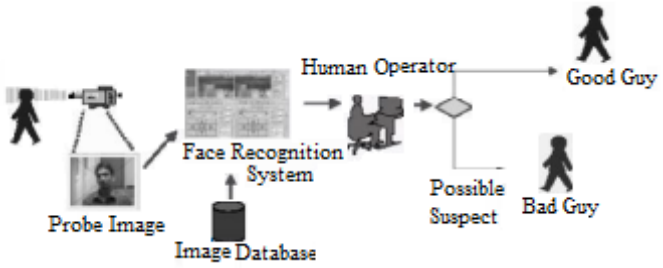

Fig.1. A typical face recognition system

The first step in the facial recognition process is the capturing of a facial image, also known as the probe image. This can be done using a still or a video camera. The system will, "normalize" (or standardize) the probe image so that it is in the same format (size, rotation, etc.) as the images in the database. The normalized face image is then passed to the recognition software. It will then be compared to those available in the reference database. In an identification application, if there is a "match," an alarm solicits an operator's attention to verify the match and initiate the appropriate actions. The match may either be true or it may be false (a "false positive"), meaning the recognition algorithm made a mistake. Facial recognition system can be used for different tasks such as verification, identification etc.

A. Verification

It is the simplest task for a face recognition system. An individual who is already enrolled in the reference database or gallery presents his or her biometric characteristics (face or probe image) to the system, claiming to be in the reference database or gallery [3]. The system must then attempt to match the probe image with the particular, claimed image in the reference database. There are two possible outcomes:

(1) the person is not recognized or

(2) the person is recognized.

B. Identification

It is a more complex task than verification. In this case, the FRS is provided a probe image to attempt to match it with a biometric reference in the gallery[3].

The face recognition process normally has four interrelated phases or steps. The first step is face detection, the second is normalization, the third is feature extraction, and the final cumulative step is face recognition. These steps depend on each other.

1) Face Detection

Detecting a face in a probe image may be a simple task for humans, but it is not so for a computer. The computer has to decide which pixels in the image are part of the face and which are not [4]. Traditionally, methods that focus on facial landmarks (such as eyes), that detect face-like colors in circular regions, or that use standard feature templates, were used to detect faces.

2) Normalization

Once the face has been detected (separated from its background), the face needs to be normalized. This means that the image must be standardized in terms of size, pose, illumination, etc., relative images in the gallery or reference database.

3) Feature Extraction and Recognition

Once the face image has been normalized, the feature extraction and recognition of the face can take place. Facial recognition algorithms differ in the way they translate or transform a face image into a simplified mathematical representation in order to perform the recognition task.

C. Face Recognition Methods

Two of the most significant pattern recognition methods are Principal Components Analysis (PCA) and Linear Discriminant Analysis (LDA). These methods are discussed further.

1) Principal Components Analysis (PCA)

The PCA technique converts each two-dimensional image into a one-dimensional vector. This vector is then decomposed into orthogonal (uncorrelated) principal components (known as eigenfaces) in other words, the technique selects the features of the image (or face) which vary the most from the rest of the image. Each face image is represented as a weighted sum (feature vector) of the principal components (or eigenfaces), which are stored in a one-dimensional array. Each component (eigenface) represents only a certain feature of the face, which may or may not be present in the original image. A probe image is compared against a gallery image by measuring the distance between their respective feature vectors. For PCA to work well, the probe image must be similar to the gallery image in terms of size (or scale), pose, and illumination. It is generally true that PCA is reasonably sensitive to scale variation.

Eigenface Method

Eigenfaces method uses PCA to represent a gray two-dimensional image with a set of correlated variables represented in the form of covariance matrix. Eigenvalues and eigenvectors are calculated and projected over the training samples in a PCA subspace to recognize the facial images [5, 6].

1. Creating the eigenfaces

Prepare a training set of face images. The pictures constituting the training set should have been taken under the same lighting conditions, and must be normalized to have the eyes and mouths aligned across all images. They must also be

all resampled to the same pixel resolution. Each picture has R rows and C columns.

Step 1: Convert each picture in the training set into a vector of length R x C by concatenating the rows of pixels of the original image.

Step 2: If there are N training set images then create a matrix, M where the number of rows = N and the length of each row = R x C. Each row will be represented by one of the image vectors.

Step 3: Calculate the mean image A of the N image vectors. Subtract A from each row of M to obtain the matrix T.

Step 4: The covariance matrix, S is given by

$S = TT^T$ (1)

where T^T represents the transpose matrix of T.

Step 5: Calculate the eigenvectors v_i and eigenvalues λ_i of S.

$Sv_i = (TT^T)v_i = \lambda_i v_i$, i = 1,2, …N. (2)

R x C eigenvectors are obtained but the main idea about the principal components is to store only the eigenvectors corresponding to the higher values. These eigenfaces can now be used to represent both existing and new faces. A new (mean-subtracted) image has been projected on the eigenfaces and thereby record how that new face differs from the mean face. The eigenvalues associated with each eigenface represent how much the images in the training set vary from the mean image in that direction. Information has been lost by projecting the image on a subset of the eigenvectors, but the loss has been minimized by keeping those eigenfaces with the largest eigenvalues.

2. Recognizing a face

Step 1: Obtain a test image I.

Step 2: Subtract the mean image A from the test image.

D=I-A (3)

Step 3: Find its projection on the face space.

P= 'Eigenfaces'xD (4)

Step 4: Find the Euclidean distances of this projection to the projection of the images already in the face space.

Step 5: Find the lowest Euclidean distance. If this distance is lower than a predetermined threshold then it is a successful match. Otherwise, it is a failure.

Step 6: Optionally, if a face image occurs multiple times but is not found within the training database it may be added to the database and the eigenvectors maybe recomputed so that this face can be recognized from the next trial. This process can be automated [7].

2) *Linear Discriminant Analysis(LDA)*

LDA is a statistical approach based on the same statistical principles as PCA. LDA classifies faces of unknown individuals based on a set of training images of known individuals. The technique finds the underlying vectors in the facial feature space (vectors) that would maximize the variance between individuals (or classes) and minimize the variance within a number of samples of the same person (i.e., within a class).

To implement LDA algorithm, an appropriate training set is required. The database should contain several examples of face images for each subject in the training set and at least one example in the test set. These examples should represent different frontal views of subjects with minor variations in view angle. They should also include different facial expressions, different lighting and background conditions etc. Obviously, an increase in the number of varying samples of the same person will allow the algorithm to optimize the variance between classes and therefore become more accurate [4].

Fisherface Method

The fisherface method of face recognition as described by Belhumeur et al. [9] uses both principal component analysis and linear discriminant analysis to produce a subspace projection matrix, similar to that used in the eigenface method. However, the fisherface method is able to minimize variation within each class, yet still maximizing class separation.

Step 1: Take each (N x M) image array and reshape into ((N*M) x1) vector.

Step 2: Using the xk values, calculate both the class mean μk and the mean of all the samples

$$Mean \quad \mu = \frac{1}{N}\sum_{k=1}^{N} x_k \tag{5}$$

$$\mu_k = \frac{1}{N}\sum_{m=1}^{N_k} x_{km} \tag{6}$$

where

N = total number of images

N_k= number of images in class k

x_{km}= image at index m of class k

Step 3: Determine both the between-class scatter matrix (S_B) and the within-class scatter matrix (S_W).

$$S_B = \sum_{k=1}^{c} N_k(\mu_k - \mu)(\mu_k - \mu)^T \tag{7}$$

$$S_W = \sum_{k=1}^{c}\sum_{x\in X_k}(x_k - \mu_k)(x_k - \mu_k)^T \tag{8}$$

where c = Number of classes

Step 4: Find the optimal eigenvectors (U_{opt}) using the equation:

$$U_{opt} = \arg max \frac{|U^T S_B U|}{|U^T S_W U|} = u_1, u_2, \ldots u_m \tag{9}$$

This equation can then be simplified into a generalized eigenvalue equation:

$$S_B u_i = \lambda_i S_W u_i, \; i = 1,2,\ldots,m \tag{10}$$

Step 5: Feature vectors can then be established using the equation

$$Y_k = U^T x_k, k = 1,2,\ldots,m \tag{11}$$

Differing from the eigenface concept, the fisherface method tries to maximize the ratio of the between-class scatter versus the within-class scatter. The result of this shapes the projections so that the distances between the classes are at a maximum, while the distances between samples of the same class are at a minimum. A possible disadvantage is if the between-class scatter is large, then the within-class scatter might also still be of a relatively large value [7]. As for PCA,

LDA works well if the probe image is relatively similar to the gallery image in terms of size, pose, and illumination.

3) Comparison of PCA and LDA

LDA and PCA are the two popular independent feature extraction methods. Both of them extract features by projecting the original parameter vectors into a new feature space through a linear transformation matrix. LDA and PCA optimize the transformation matrix with different intentions. PCA optimizes the transformation matrix by finding the largest variations in the original feature space. LDA pursues the largest ratio of between-class variation and within-class variation when projecting the original feature to a subspace.

PCA has been used in face recognition, handprint recognition, human-made object recognition, industrial robotics, and mobile robotics. LDA has been used in face recognition and mobile robotics. LDA has also been proposed for generic object recognition.

The main differences between these two methods are as follows:

a) LDA is based on a single face image as input. That means, LDA can perform face recognition for a single input image. PCA is based on multiple face images as input.
b) PCA is less sensitive whereas LDA is more sensitive.
c) PCA takes very less computational time whereas LDA takes more computational time [10,11].

III. Proposed System

Fig. 2 shows the flowchart for the proposed system. The system is composed of 2 phases: Enrolment phase and Authentication phase.

In the enrolment phase, the face is detected from an image obtained from the webcam. The image of the face is then converted into gray scale. The image is then aligned and stored in a database along with the details of the person.

In the authentication phase, if a match is not found, then the user is alerted.

A. *Training the Database*

The images are acquired from a webcam and stored in a database. All images are converted to gray-scale, cropped to 100x100 and aligned to match the eye level. From the images captured using camera, detect the face using Haar cascade classifier, convert them into gray-scale, crop them to align the eye-level and save the images for future face detection.

B. *Face detection*

For face detection, Haar Cascade Classifiers can be used. It has high level of accuracy in finding the facial detection with moderate computational requirements than Local Binary Pattern.

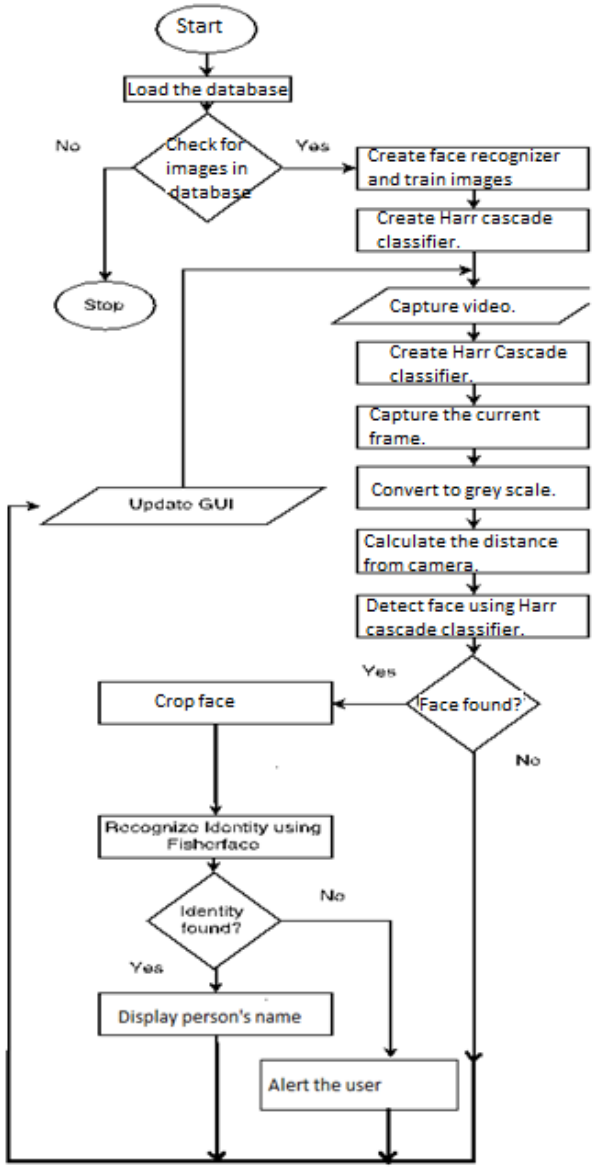

Fig.2. Flowchart of the proposed system

C. *Harr Cascade Classifier*

Haar Cascade Classifier is a famous face detection technique. Haar cascade classifiers is a machine learning approach where the functions of cascades are trained using positive and negative images, where the positive images refer to the image of objects and the negative images refer to the images without the object.

Haar-like features in two dimensions are composed of adjacent light and dark rectangles. They are usually used to detect and recognize objects, and were successfully used for real-time facial detection. To compute the existence of several hundred Haar-like features at different scales and locations in a single image, Viola and Jones (2001) [12, 13] proposed the integral image technique. Each pixel is assigned as the sum of all pixels above it and to its left. Instead of applying all the 6000 features on a window, group the features into different

stages of classifiers and apply one-by-one. The group is called cascade classifier. Harr cascade classifier can be used for detecting face from an image.

D. *Face Recognition*

Eigenface and Fisherface methods have been used for face recognition. Eigenfaces method uses Principal Component Analysis (PCA) [14, 15] to represent a gray two-dimensional image with a set of correlated variables represented in the form of covariance matrix. Eigenvalues and eigenvectors are calculated and projected over the training samples in a PCA subspace to recognize the facial images.

Fisherfaces use Linear Discriminant Analysis (LDA) which find the combination of features by maximizing the ratio of within-classes from between-classes. The clustering of identical classes together and different classes separately are done and is represented in low dimensional space and the face recognition discrimination analysis is done. Fisherfaces methods are best in interpolating and extrapolating the lighting situations and appear to be better for handle the facial expressions.

E. *Alerting system*

Alerting the user about the unidentified person is an important task. For the purpose of communication Twilio package was used. Twilio allows programmatically sent message using its web service API. Using the account number and the authentication number the client program requests the Twilio to send the alert message to the user at state of emergency.

IV. Results and Discussion

The proposed system is tested with a database of multiple facial images of different people in a wide variety of lighting conditions. AT&T database model is used in the experiments. The database contains 25 images (under different lighting conditions) of each person that is to be detected (see Fig.3.).

Fig.3. Subset of images in the image dataset (for a single person).

Fig. 4 shows the image captured and face recognized.

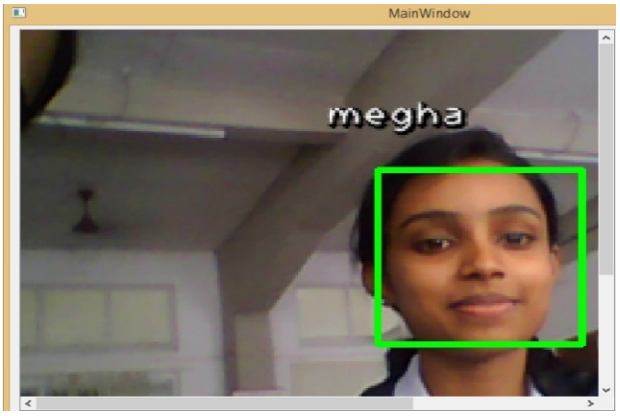

Fig.4. System detects the face from the image and recognizes the person.

Fig. 5 shows the detection of unauthorized person from the image.

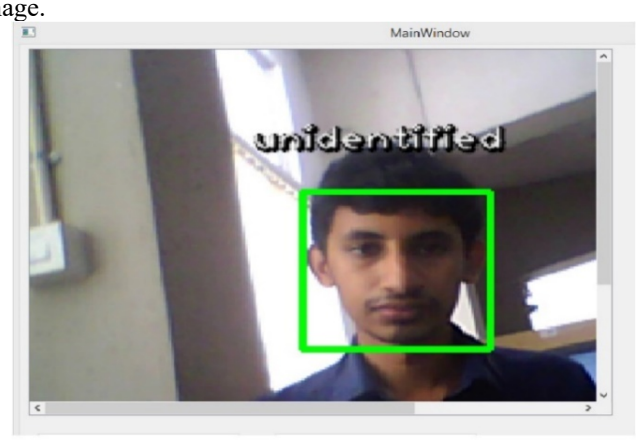

Fig.5. When an unauthorised person is detected

The proposed system sends messages to the user when a face is detected in the image taken by the surveillance camera. The message contains the name of the detected person if he is an authorised person otherwise the person is indicated as unidentified person, time and date of arrival. Fig. 6 shows the message sent to user as an alert.

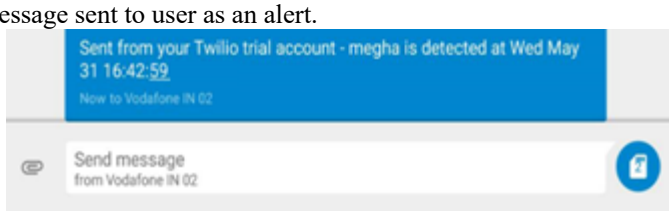

Fig.6. Message sent to the user when an authorized person is detected.

Fig. 7 shows the message sent to user when an unauthorized person is detected.

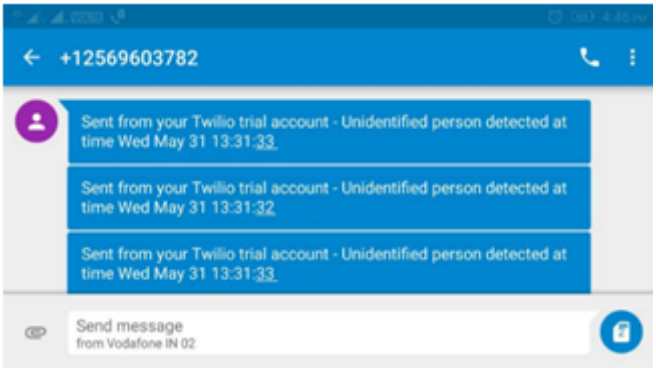

Fig.7. Message sent to user when an unauthorised access is detected.

Figure 8 shows the efficiency of the face recognition system in detecting face under various conditions. The graph shows that under good lighting condition, the system detects all the faces given as input. Under poor lighting condition, the efficiency of the system is less.

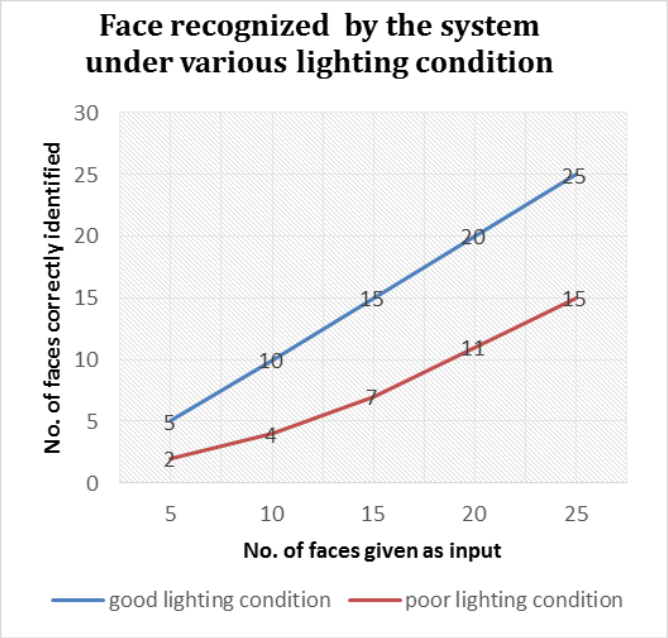

Fig.8. Efficiency of the face recognition system in detecting face under various lighting conditions.

The face detection with Haar Cascade works with great accuracy up to a distance of 5 meters in good lighting condition and up to 3 meters in low light situations. Once the distance exceeds the limit mentioned above, accuracy drops.

Fig. 9 shows the efficiency of the system in identifying the face. Face recognition depends on lighting condition and the number of images in the database; the more images you have, the accurate the results are. The initial test was done with 25 images in the database and it reflects bad recognition rate. To overcome the situation, the system was tested with 200 facial images taken under varying lighting conditions and the performance improved. The system identifies all the faces given as input at good lighting condition. But, under bad lighting condition, the rate of identification of faces is less. For all the identified and unidentified faces, the system sends messages to the phone connected to it.

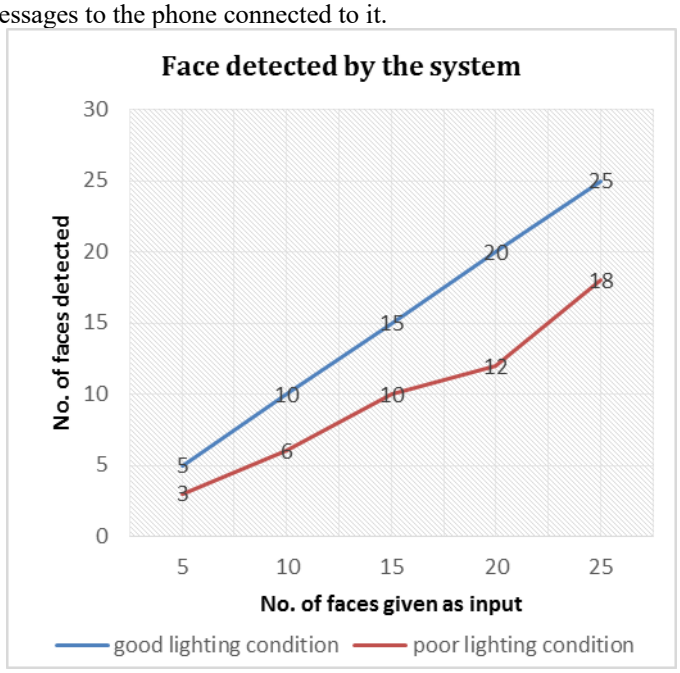

Fig.9. Efficiency of the system in recognizing face under various lighting conditions.

V. Conclusion

The proposed system discussed here is intended to enhance the safety and surveillance of the children and old-aged people confined to home by implementing a visual based system for human motion detection and identification. From the experiments, the system is found to be very capable in handling different environmental situations and can detect the motion and recognize the people in a variety of lighting conditions. It is also capable of sending messages to the phone connected to the system when an unidentified person tries to access the premises. Message will contain the name of the person if the person is an authenticated one. Otherwise, the message will contain the information that an unidentified person is detected. Accuracy of face recognition largely depends on the lighting conditions and the number of images stored in the database. The system developed has great potential to be improved. Training the cascade classifiers for fisherfaces and eigenfaces with more images can improve the accuracy of the system.

References

[1] LH Xuan and S Nitsuwat, “Face recognition in video, a combination of eigenface and adaptive skin-color model”, Proceedings of IEEE International Conference on Intelligent and Advanced Systems, 2007.

[2] Lucas D and I Lancaster, “Facial recognition technology: a survey of policy and implementation issues”, July 2009.

[3] Y Bakhshi , S Kaur and P Verma, “An improvement in face recognition for invariant faces”, International Journal of Current Engineering and Technology, vol. 6(2), 2016.

[4] Rajeshwari J and K Karibasappa, “Face recognition in video streams on homogeneous distributed systems”, International Journal of

Advanced Computer and Mathematical Sciences, vol. 4 (1), pp. 143-147, 2013.

[5] Turk, Matthew e Pentland, Alex, “Face recognition using eigenfaces”, Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, pp. 586-591, 1991.

[6] DN Parmar and BB Mehta, “Face recognition methods and applications”, International Journal of Computer Technology Applications, vol. 4, pp. 84- 86, 2013.

[7] R Saha and D Bhattacharjee, “Face recognition using eigenfaces”, International Journal of Emerging Technology and Advanced Engineering, vol. 3 (5), 2013.

[8] Belhumeur, P.N. Hespanha, J.P. and Kriegman,D.J., “Eigenfaces vs fisherfaces: recognition using class specific linear projection, pattern analysis and machine intelligence”, IEEE Transactions on. vol.19 (7), pp. 711-720, 1997.

[9] S Jaiswal, SS Bhadauria and RS Jadon, “Comparison between face recognition algorithm-eigenfaces, fisherfaces and elastic bunch graph matching”, Journal of Global Research in Computer Science (JGRCS), vol.2 (7), 2011.

[10] TK Kim, J Kittler and R Cipolla, “Discriminative learning and recognition of image set classes using canonical correlations”, July 2007.

[11] ST Gandhe, KT Talele and AG Keskar, “Intelligent face recognition techniques: a comparative study”, Graphics Vision & Image Processing International Journal, vol. 2, pp. 53-60, 2007.

[12] (2021) Face Detection using Haar Cascades, Available at: docs.opencv.org/trunk/d7/d8b/tutorial_py_face_detection.html, accessed July 2021.

[13] (2021) Viola–Jones object detection framework, Available at: https://en.wikipedia.org/wiki/Viola%E2%80%93Jones_object_detection_framework, accessed July 2021.

[14] A Rashad, A Hamdy, MA Saleh and M Eladawy, “3D face recognition using 2D PCA”, Journal of Computer Science and Network Security. vol.9 (12), 2009.

[15] G Kaur, S Kaur and A Walia, “Face recognition using PCA, deep face method”, International Journal Of Computer Science and Mobile Computing, vol.5 (5), pp. 359-366, 2016.