Face Recognition in Securing Optical Telecom Network Equipment

Nadeem[1], M. Ali[2]

[1,2]Electrical Engineering Department, University of Engineering & Technology (UET), Lahore, Pakistan
[1]nadeemengineer@yahoo.com

***Abstract*-**In this paper, face recognition is used with a microcontroller based hardware module to secure the telecommunication equipments like ONU (optical network units) or any other telecommunication equipment. The face recognition classifier value optimization adaption is deployed and in this scheme by increasing or decreasing the number of images in the database will automatically generate and adopt the classifier value for recognition of known and unknown persons. On recognizing an unknown person, the hardware module will send an SMS to the concerned security personnel for security preventive measures.

***Keywords*-**Optical Fiber Access Networks (OFAN), Optical Line Terminal (OLT), Optical Network Unit (ONU), Principal Analysis Components (PCA)

I. Introduction

The start of fiber optics in 1980 brought a revolution in the telecom industry [i]. It replaced the earlier transmitting media with the optical medium. It fulfilled the ever increasing demand of bandwidth. Now, the networks have moved to optical communication to utilize its huge bandwidth to satisfy their customers' requirements.

Optical networks have increased the revenue of the providers owing to less maintenance expenses and high performance. However, the risk of the theft of outdoor costly optical fiber equipment installed in mini-exchanges has increased. PTCL is the leading network provider in Pakistan and facing the critical issue of theft of costly equipment from the outdoor access networks. The need of the time is to develop and design security mechanism to stop this stealing. In this paper, face recognition is used to detect unauthorized access to optical network unit (ONU) in an optical network and an instant message is sent to the security personnel with a hardware module. The currently different security techniques such as door sensors, biometrics and CCTV presently available are based on hardwired alarms system which deployed wiring cables between alarm monitoring panels and devices. Those systems cannot deliver instant messaging alarms on malicious activities to different location at a time. All techniques are not flexible and independent from each other, they provide alarms on certain spots whereas our proposed hardware module is low cost, dynamic and flexible and can deliver different types of alarms simultaneously everywhere required for the alarms monitoring [ii]. This system is based on instant messaging on the mobile in the event of theft through GSM modem. The proposed security hardware module easily can be integrated in the existing networks and having its own independent low power consumption source. The module will continuously work successfully under different scenario such as completely isolated from other devices by power break down or by fiber cut. In this paper face recognition is utilized to authenticate the security personnel

The rest of the paper is divided into following sections: Section-II describes the architecture of OFAN; Section-III is about the security hardware module; Section-IV presents the face recognition mechanism; Section V provides the results and Section-VI concludes the paper.

II. Optical Fiber Access Network

The access network that employs OFAN [iii-iv]. OFAN bandwidth is up to several Giga bits per second (Gbps). The fundamentals parts of OFAN are shown in Fig. 1 and summarized below:

A. Optical Line Terminal (OLT) Unit

OLT is mounted at evidences of service provider [v]. Such places are the buildings of the Telephone Company or local area exchange, near the switching centre of a company and cable TV network provider ends. Various types of interfaces are available like E1/V5 interface that are used to attach the OLT and main telephone local exchange or digital distribution frame (DDF).

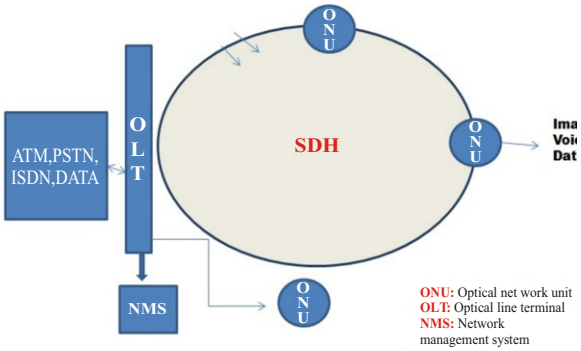

Fig. 1. OFAN Architecture for Access Networks

B. Optical Network Unit (ONU)

ONU's are installed at customer premises to execute the services to client, most probably neighborhood, within the office building, apartments or near residential home area [vi-vii]. The users of telephone, broadband services and smart TV etc., are connected to customer sides of ONU's directly by the drop wire or cable of twisted pair of different category to accomplish their demands.

As per planning and designing of the services and network, various hierarchies of structure of the ONU's formation in the geographical area can be employed like mesh topology, star, tree and ring, which provide the basis of communication between ONUs and OLT.

The transmission technology like Plesiochronious hierarchy, DWDM and SONET or SDH can be imposed for the communication in networking of the ONU typology [viii].

III. Hardware Security Module

This section presents a low cost valuable hardware module [ii] for generating instant message in the event of theft. The system will be supportive under the situations when network managing system totally fails to deliver alarms at monitoring terminals of the fiber system due to power failure, fiber cable cut or some other malicious action.

The proposed model shown in Fig. 2 which consists of the following components:

1. *Detector circuits for the unauthorized removal of equipment*
2. *Microcontroller for controlling the operations*
3. *GSM module for interfacing and communicating theft messages to the concerned security personnel for preventing thefts of costly equipment*
4. *Mobile phone to which the theft message is sent*

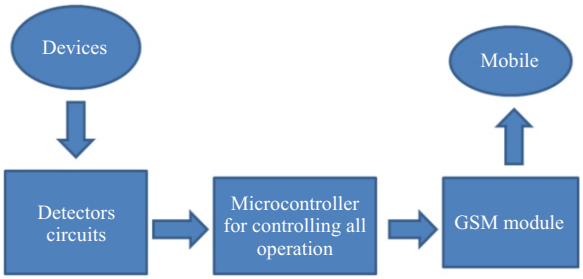

Fig. 2. Proposed model

The major hardware components of the security module are 89C51 microcontroller, GSM Module and MAX232. The interfacing of all components is shown in the schematic diagram in Fig. 3. The core part is 89C51 microcontroller in which the Hex file of C-program is burned for interconnecting the commands coming from PC/Laptop. After identification of unauthorized person, an alert message is sent through serial port reserved for GSM modem to the concerned security personnel.

The option of SPDT switches is also fabricated in the design and devices like cards, batteries and other devices can also be connected through these switches. This can provide a mechanism of alarm generation on the activation of these switches.

The complete hardware for the security protection is shown in Fig. 4. The hardware start functions on recognition of unauthorized access. The status of the hardware can be visualized with the help of different LEDs mounted on the board. LEDs give the indication of different types of communication and certain action or response by the microcontroller. Some of them represent the serial communication take place between microcontroller and PC and other represent the instant message delivery status to the concerned security personnel through the GSM modem.

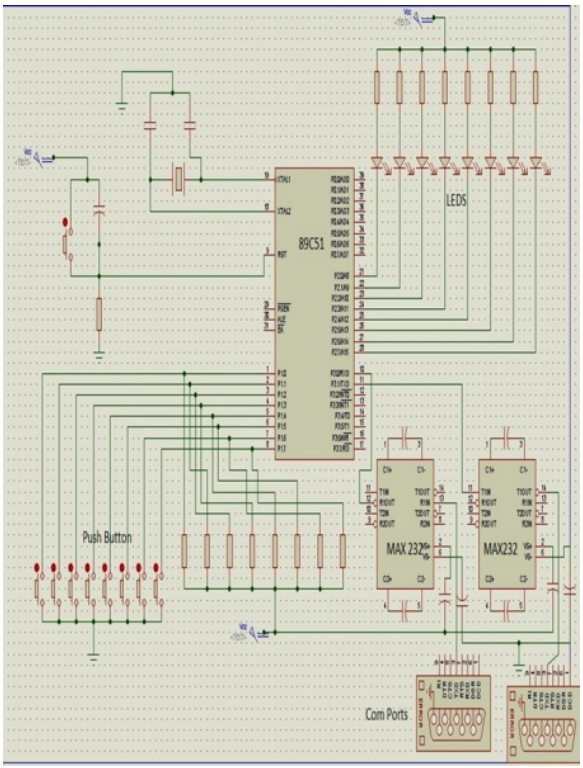

Fig. 3. Schematic diagram showing interfacing of different components

IV. Face Recognition With Threshold Optimization

After identifying an unauthorized access, a critical message is sent to the concerned authority for the preventive measures. This section demonstrates the complete development of the software based on Principal Components Analysis (PCA) [ix].

A face is a complicated multi-array visual space model and forming a computational model for face

identification is always a difficult task. The PCA is solitary of the mainly thriving techniques which were developed and used in recognition of image and works based on a statistical procedure Eigen method. The core aim of this technique is to minimize the huge dimensions of the vector space into small numbers of variables which are independent and not correlated.

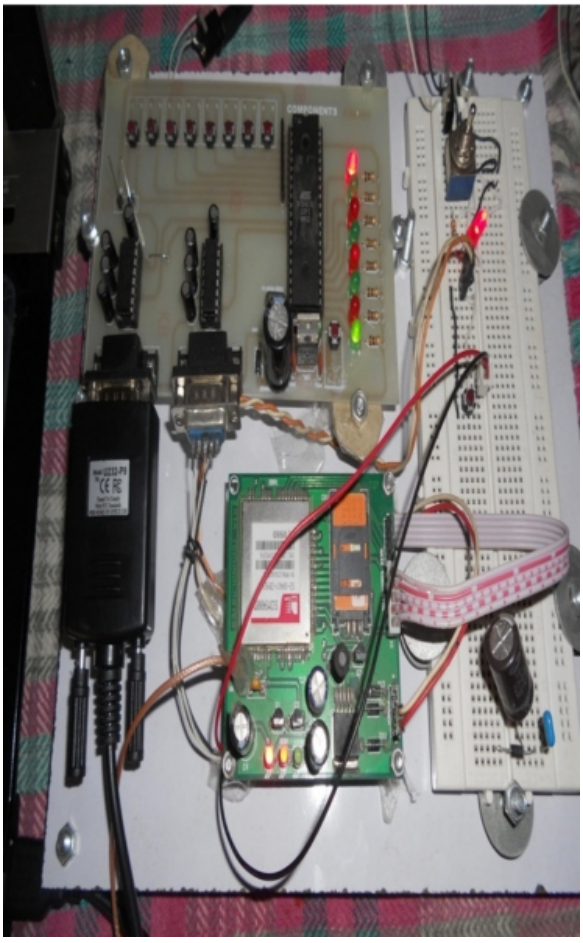

Fig. 4. Hardware module for sending SMS on unauthorized access

A. Principal Component Analysis

A mathematical procedure of principal components analysis [x] based on Eigen vector techniques that imposed an orthogonal transformation to translate the set of values of probably correlated M faces images into a set of values uncorrelated K variable called Eigen faces. The number of images in Eigen faces is always less than or equal in amount to number of original face images, i.e. $K < M$.

Since the principal components always present for the most leading direction or features of the dataset correlated variable and each preceding component shows less direction and more unwanted noise. So only the first few K-Eigen faces have been selected and discarded the remaining ones due to their less importance.

These selected K components are fully representing the whole original dataset (face images) because they illustrate major facial features or direction that makes up the dataset.

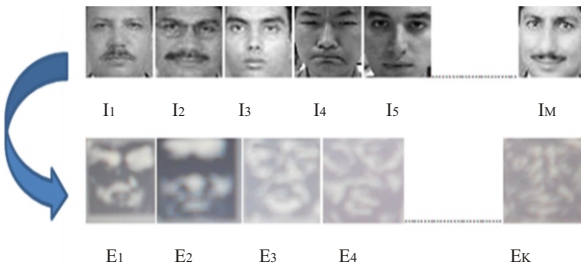

Fig. 5. Images and associated Eigen faces

So every face image in the original training databases or problem image can be reconstructed in term of these K parts of principal components. It is illustrated by the under mentioned figure.

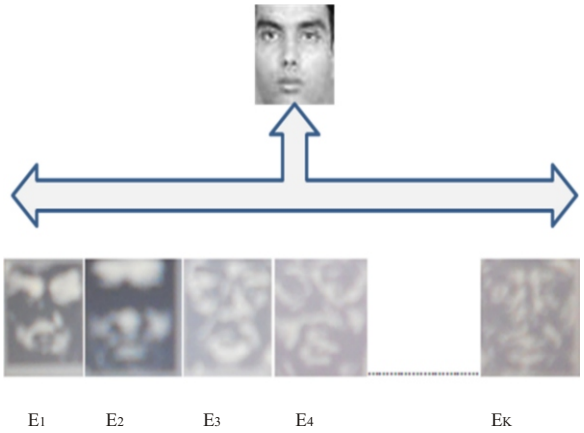

Fig. 6. Image reconstructed from Eigen faces

B. Eigen face Method

Eigen face technique used to be a satisfactory approach for implementing in face recognition due to its ease, enhancement and erudition competence. Eigenvectors are composed of the Eigen face vector sets used in the computer vision problem of human face unique pattern recognition. This technique is known as an appearance-based methodology for getting identical features of face and variation of features is to be used for comparison and coding. Huge multidimensional space is to be converted in less space by the calculation of Eigen vectors.

The procedures of the face recognition based on Eigen method [ix-xii] and adaption of classifying value algorithm consists of the following steps

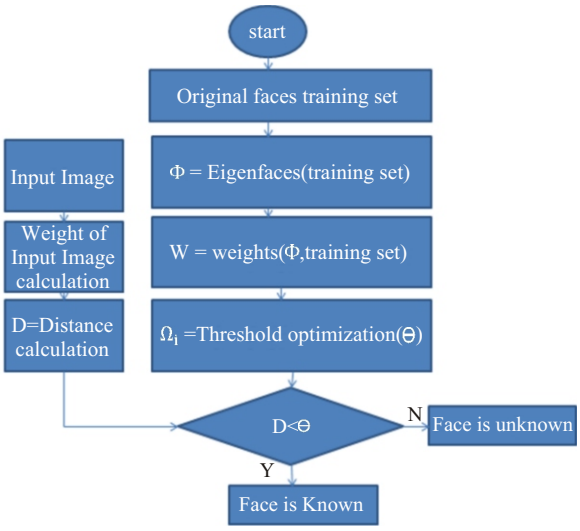

Fig. 7. Flow chart for threshold optimization

Every face image which is basically 2 dimension vector set is transformed into a column vector for the simplicity of manipulation operation [ix].

$$(\mathrm{Im})_i = \begin{bmatrix} y_{11} & y_{12} & \cdots & y_{1N} \\ y_{21} & y_{22} & \cdots & y_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ y_{N1} & y_{N2} & \cdots & y_{NN} \end{bmatrix}_{N*N} \quad (1)$$

$$T_i = \begin{bmatrix} y_{11} \\ \vdots \\ y_{1N} \\ \vdots \\ y_{2N} \\ \vdots \\ y_{NN} \end{bmatrix}_{N^2*1} \quad (2)$$

The all images data are concatenating into a big matrix whose number of columns are equals to the number of images used for in face recognition data set. Then calculating the mean or average face vector of the big all image matrix [ix].

$$\mathrm{Averagefacevector}\,(\Psi) = \frac{1}{M}\sum_{i=1}^{M} T_i \quad (3)$$

The mean face is subtracted from each face columns vector for getting a set of vectors. The purpose of subtracting the average image from each image vector is to get only the distinguishing characteristics from each face and discarding common one for simplicity [ix].

$$\Phi_i = T_i - \Psi \quad (4)$$

The covariance matrix is essential for the further manipulation and selection of the best *K* eigenvectors [ix].

$$\text{Covariance matrix} = L^T L \quad (5)$$

$$\text{Where } L = [\Phi_1\ \Phi_2 \ldots\ldots\ldots\ldots\ldots\ldots \Phi_M\ ] \quad (6)$$

The next step is to calculate the weight of every Eigenvector [ix].

$$\Phi_i = \sum_{j=1}^{k} w_j\ u_j \quad (7)$$

Each normalized training image is shown on the basis of a vector. This give the direction to find out such a vector corresponding to each image in the training set and store it for calculation.

The Eigenvectors are calculated for the training set of images and their related weights [ix].

$$w_j = u_j^T \Phi_i \quad (8)$$

$$\Omega_i = \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_k \end{bmatrix} \quad (9)$$

C. Problem Image Recognition Task

The problem image face for its reorganization is projected into the vector space (the collection of Eigenvectors/faces) and find out the corresponding weights [ix]. The problem images can then simply be classified for recognition purpose.

$$\Omega = \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_k \end{bmatrix} \quad (10)$$

The distance of the unknown face is calculated on the basis of the above calculation, and then the weight vector of the problem image and its distance with the weight vectors associated with each of the training image [ix].

$$D = \min\|\Omega - \Omega_i\| \quad (11)$$

D. Algorithm for Threshold Optimization

The threshold value is calculated from the distance of each image on the vector space. If the distance of the input problem image with vector space is greater than the threshold value then the image is not recognized.

Algorithm. Threshold Optimization by using histogram

Required: M A list of images
for images in M **do**
    histogram (images)
    threshold = max (histogram)
end for

V. RESULTS

The adaption of the threshold classifier value for face recognition process is critical one and calculated on the basis of linear distances of each face image from the vector space database training set of all images. The execution time of the algorithm for finding the classifier value and instant message to the particular cell phone is mentioned in the following table

TABLE 1
EXECUTION TIME OF CODE

Execution Time for code	
Event	**Execution Time**
Algorithm code for adaption	5 s
Message sending time	30-60 second

The execution time is recorded from MATLAB and microcontroller 89C51 and Figure 8-11 provide comparison between the number of images and their associated threshold values on the basis of which the face is recognized. Fig. 8 shows the scenario in which 6 images are in the database and their corresponding threshold value is 928.The image distance less than this threshold value will be considered as recognized image. Similarly, Fig. 9-11 show the scenario of 10, 20 and 25images and their corresponding thresholds respectively. These results illustrate that the threshold value is optimized automatically as the number of images in database changes.

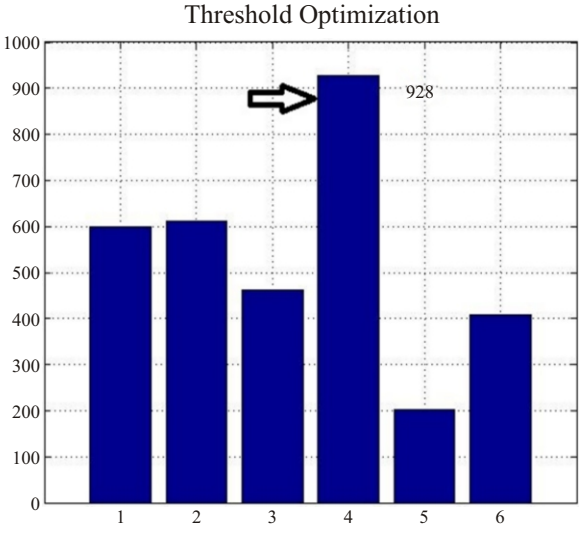

Fig. 8. Threshold value for 6 images

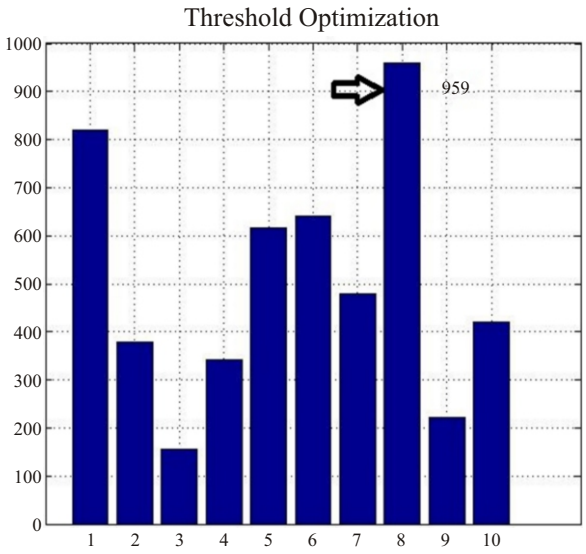

Fig. 9. Threshold value for 10 images

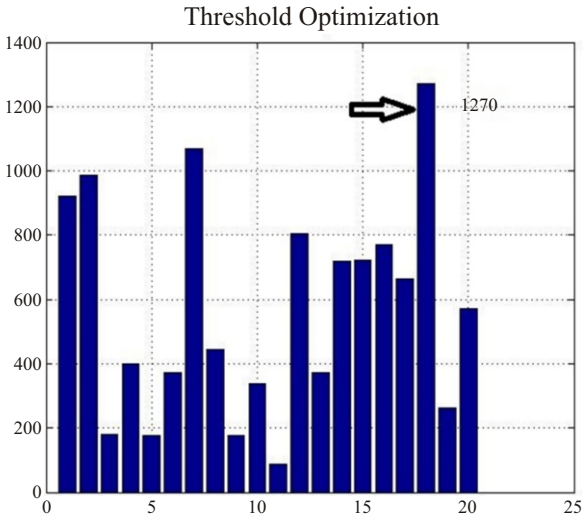

Fig.10. Threshold value for 20 images

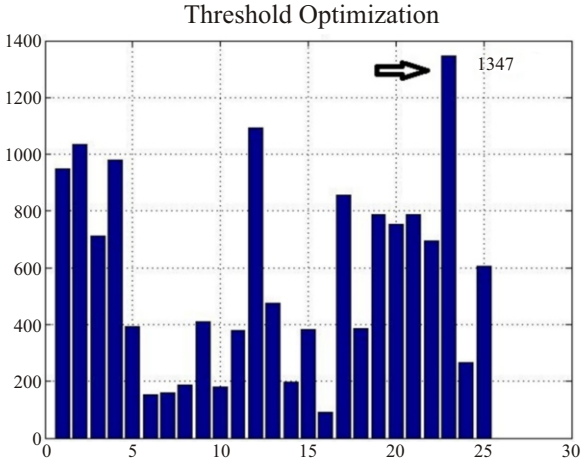

Fig.11. Threshold value for 25 images

VI. CONCLUSION

Face recognition is a biometric technique which is implemented to detect unauthorized access in the costly optical network equipment. Automatically threshold optimization of face classifier value is determined in the research and its results by increasing number of images are presented. On detection, an instant message will be sent to the security personnel, hence, minimizing the risk in security of network equipment.

REFERENCES

[i] Y. Su, "All-optical virtual-private-network in access networks," in *Proc. LEOS*, 2007, pp. 802-803.

[ii] Nadeem and M. Ali, "Hardware Module for the Security Enhancement of Optical Telecom Network Equipment", Vol 52 (1), PP. 40-44, The Nucleus Journal,2015

[iii] I. P. Kaminow, T. Li, and A. E. Willner, Eds., Optical Fiber Telecommunications V. San Diego, CA: Academic, Feb. 2008.

[iv] P. Morin, Optical Fiber Commun. Conf., 2009, Plenary Session.

[v] John M Senior, "Optical Fiber Communications", Pearson publication,2010.

[vi] G. Kramer, "The problem of upstream traffic synchronization in Passive Optical Networks" Davis, CA 95616

[vii] Y. Chen, W. Tang, "Concurrent DWDM Multi-Mode Switching: Architecture and Research Directions," IEEE Communications Magazine, vol. 48, no. 5, May 2010.

[viii] J. Yu and X. Zhou, BUltra-high-capacity DWDM transmission system for 100G and beyond, [IEEE Commun. Mag., vol. 48, no. 3, pp. S56-S64, Mar. 2010.

[ix] Papia Banerjee, Pradipta K. Banerjee "Phase-Eigen Subspace based Illumination Invariant Face Recognition using Associative Memory",2012 National Conference on Computing and Communication Systems (NCCCS)

[x] Chunjing Li, Jinwu Liu "Matrix reduction based on generalized PCA methodin face recognition"2014 International Conference on Digital Home

[xi] P. K. Banerjee, J. K. Chandra, and A. K. Datta, "Class dependent 2dcorrelation filter for illumination tolerant face recognition," in *Proceedings of the First Indo-Japan conference on Perception and Machine Intelligence*, ser. PerMIn'12. Berlin, Heidelberg: Springer-Verlag, 2012,pp. 338-345.

[xii] Prof. V. P. Kshirsagar, M. R.Baviskar, M. E. Gaikwad," Face Recognition Using Eigenfaces" Dept. of CSE, Govt. Engineering College, Aurangabad (MS), India.