International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 1, January- 2013

Tracking of Unauthorized Access Using Face Recognition

Chanchal S. Khandelwal, Shilpa R. More
Computer Department
Modern Education Society's College of Engineering
Pune, India

Sai S. Phalke, Prachi J. Kamble
Computer Department
Modern Education Society's College of Engineering
Pune, India

***Abstract*— Computer Security involves protecting the computing resources, restricting access to computer for unauthorized firms, maintaining data confidentiality, and to ensure data integrity. An Effective Security within organization has become mandatory so that credentials of the organization are not exposed. This paper proposes a technique for safeguarding organization's crucial asset like servers, and other computing resources. Various Biometric Techniques are in practice today like finger print, iris scan etc. In this paper we extend the detection of unauthorized access using Face Recognition. This paper clearly states the action that will be forced when an unauthorized access is detected, which allows a legitimate firm to track the unauthorized action that compromised the organization's security.**

***Keywords*—ComputerSecurity,Eigen Face Recognition, Principle Component Analysis.**

INTRODUCTION

Physically protecting computer equipment and data against illegitimate access or loss is a large concern of computer security. In order to accomplish this we need to restrict the access to the confidential data only to the authorized users. Following are the different ways to distinguish between authorized and unauthorized firm:

- Using a piece of information such as a password, this is known only to an individual.
- Using a physical token such as a credit or ID card, possessed by an individual.
- Using a biometric characteristic of the individual (for example their signature, finger print, DNA, retinal scan).

Effective security needs employment of any two approaches mentioned above. For example, to withdraw money from a bank cash machine both ATM card and PIN (Personal Identification Number) is required. In order to analyze legitimate and illegitimate firms, a biometric technique 'Face Recognition' is applied. Among various biometric authentication schemes available, face recognition is the most promising and flexible authenticating scheme as the object is unaware of being scanned. Facial Features like width of nose, distance between eyes, jaw line etc are taken into account while recognition. In this paper, a detail description of how face recognition along with two system feature like sms and email, is employed to track unauthorized access is illustrated. In this field of face recognition, work was carried out on various algorithms to increase its effectiveness and accuracy in recognition of faces.

I. BACKGROUND AND RELATED WORK

Face Detection consists of precise location of facial features where there are many lightening variations and large poses, which presents a biggest challenge in this biometric system. Without accurate localization of important features, accurate and robust face recognition is to be achieved. Various techniques were surveyed each had its advantages and disadvantages which are as follows:

A. Geometric Technique

This technique uses the Geometric information present in the template image as the primary feature for matching. This includes the mouth, nose and eyes. Face geometry is used to locate the features like mouth, nose, and eyes. To locate the boundaries of face features, the detected face undergoes edge detection. It's Simple to implement and efficient. But requires a manual locating of facial features and works on the assumption that the shape of the pattern in the template can be reliably represented by a set of geometric features.*[8]*

B. Neural Network

A Back propagation neural network, when trained can be easily used to recognize face image. In a typical image recognition network large number of input neurons are required, one for each of the pixels in an image. In this, Face Features are recognized in static way.
To reduce the difficulty of training network, back-propagation net, Auto association net and classification net is used to train the network and gather matching information. Basic aim of this approach is to train the

network to respond correctly to the input pattern that is being used for training and inputs that are similar. During face recognition dimensionality of face image is reduced by the Principal component analysis (PCA) and the recognition is done by the Back propagation Neural Network (BPNN).when BPNN technique is combined with PCA non linear images can be recognized easily. However, even a simple network is very complex and difficult to train.*[1]*

C. Template Matching

A simple version of template matching is that a test image represented as a two-dimensional array of intensity values is compared using a suitable metric, such as the Euclidean distance, with a single template representing the whole face. In general, template-based approaches compared to feature matching are a more logical approach. It is effective face recognition in exact same conditions in which the templates were store. Change in surroundings or features of the user drastically affect the accuracy of face recognition.*[7]*

II. APPLICATION DEVELOPMENT

A. System Requirement

The Desktop application can run on any Windows Operating system and need a GSM/GPRS modem or a GSM supported cell.

B. Application Architecture

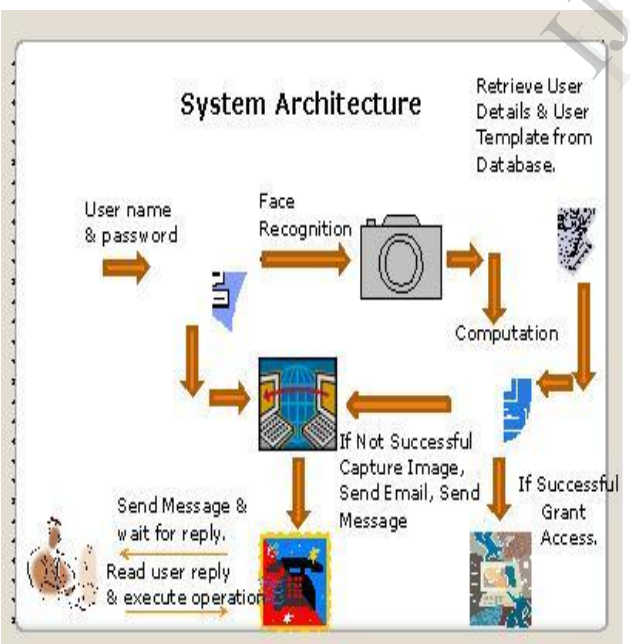

Fig 1: System Architecture

The above figure displays features of application. The architecture specifies the major responsibility the system will undertake. The system architecture has following functions which will take during execution. The flow of the process is as follows

1. Faces of authorized firms has to be stored within database during registration. Initially, an unidentified person is authorized by scrutinizing username and password provided by him.
2. After the validation is successful in first step, then the Second level of authentication begins with face recognition of the user. Here database image is compared with the real time image of the firm who desires to get an access to system.
3. If the unidentified image matches a known template within database, a successfully login is done within system. As the focus of this paper is to track an unauthentic person, actions are therefore taken to accomplish the Moto of tracking the illegitimate person.
4. If the user is unauthorized, then actions like capturing image of an unauthorized person and sending the same as mail, at the same time generating random password for system and sending the same onto authorized person mobile phone.

Following the above two level authentication approaches, unauthorized person who attempted to hack can be tracked and security can be guaranteed to some extent.

EIGEN FACE APPROACH

A. Feature Extraction

The integral part of any recognition system is the extraction of feature matrix. Feature extraction approach tends to build computational model through transformation of data so that the extracted feature is as representative as possible. Feature extraction algorithms mainly fall into two categories: geometrical features extraction and statistical (algebraic) features extraction. The geometric approach, represent the face in terms of structural measurements and distinctive facial features that include distances and angles between the most characteristic face components such as eyes, nose, mouth or facial templates such as nose length and width, mouth position. These features are used to recognize an unknown face by matching it to the nearest neighbor in the stored database. Whereas, Statistical features extraction is usually driven by algebraic methods such as principal component analysis (PCA).These methods find a mapping between the original feature spaces to a lower dimensional feature space. In this paper eigenface method is considered for extracting features of face which are eyes, nose, lips, forehead and cheeks.

Emphasizing on the significance of the features of the person and enabling the recognition, the Eigen face approach focuses on important phases and aspects required for recognition. These aspects include:

B. Principle Component Analysis(PCA)

The features can be extracted out of original image data by means of a mathematical tool called *Principal Component Analysis* (PCA). It decomposes face images into a small set of characteristic feature images called 'eigenfaces', which are actually the principal components of the initial training set of face images. . In PCA, one can transform each original image of the training set into a corresponding eigenface. Therefore, one important feature of PCA is that the reconstruction of any original image from the training set by combining the eigenfaces is possible.*[3]*

C. EIGEN FACE

The presence of some objects (eyes, nose, and mouth) in any face as well as relative distances between these objects. These characteristic features are called *eigenfaces* in the facial recognition domain.

- Creation of Eigen face
  Step 1: Prepare a training set T={t1,t2…Tm}
  Step 2: Subtract the mean

$$\Psi = \frac{1}{M}\sum_{n=1}^{M} \Gamma_n$$

Equation 1

$$\Phi_i = \Gamma_i - \Psi$$

Equation 2

Step 3: Calculate The Covariance matrix S
Step 4: Choose the Highest principle Component and a D*D Matrix is formed with D Eigen vectors. *[4]*

Eigen face is the crucial part of the algorithm considered in this paper. There are various aspects of Eigen faces include Eigen vector which is the matrix consisting of Eigen values of each image in the training set of different users. They posses following properties that they can be determined only for square matrices and there are n eigenvectors (and corresponding Eigen values) in an n * n matrix. Co jointly other decisive aspect are the Eigen values. They are the values calculated for the images of training set which consists of calculation of features of faces. Eigen values together form Eigen vector.

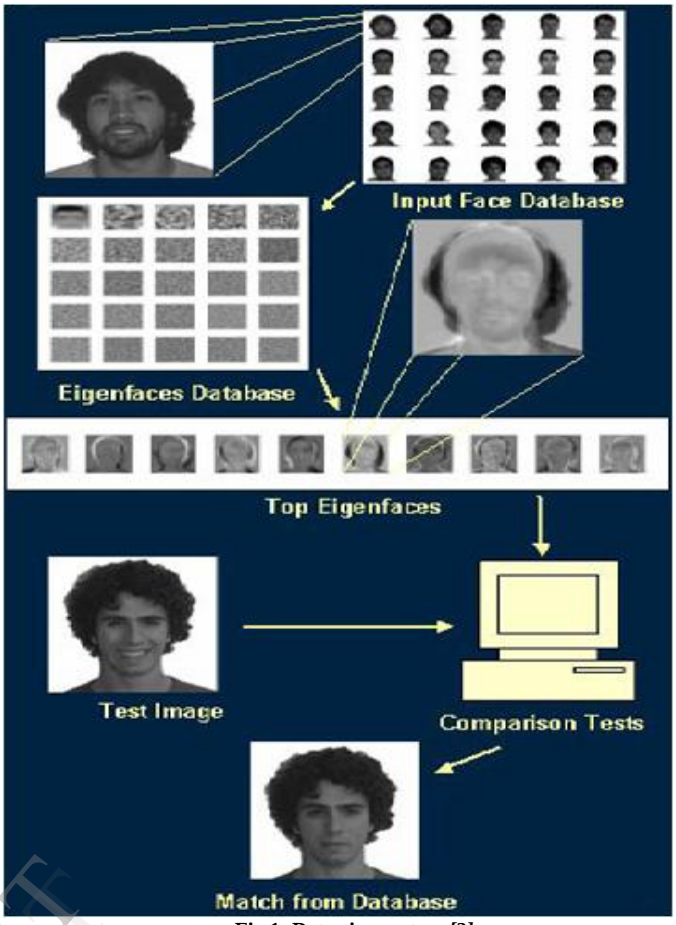

Fig 1: Detection system *[3]*

ALGORITHM

The algorithm for recognition of authorized used is divided in two parts. The first part describes about the checking whether the image is face or not. And the second part provides description about the recognition whether it is authorized or non authorized user.

- PART 1

a) Acquire initial set of face images. (training set)
b) Transform training set to Eigen faces (E).
c) Calculate the weight for each image in the training set and store it in set W.
d) Consider the unknown image and calculate weight for it and store it in vector Wx.
e) Compare Wx with W. Calculate distance between them using Euclidian distance.
f) If the average distance exceeds the threshold value then it is not a face.

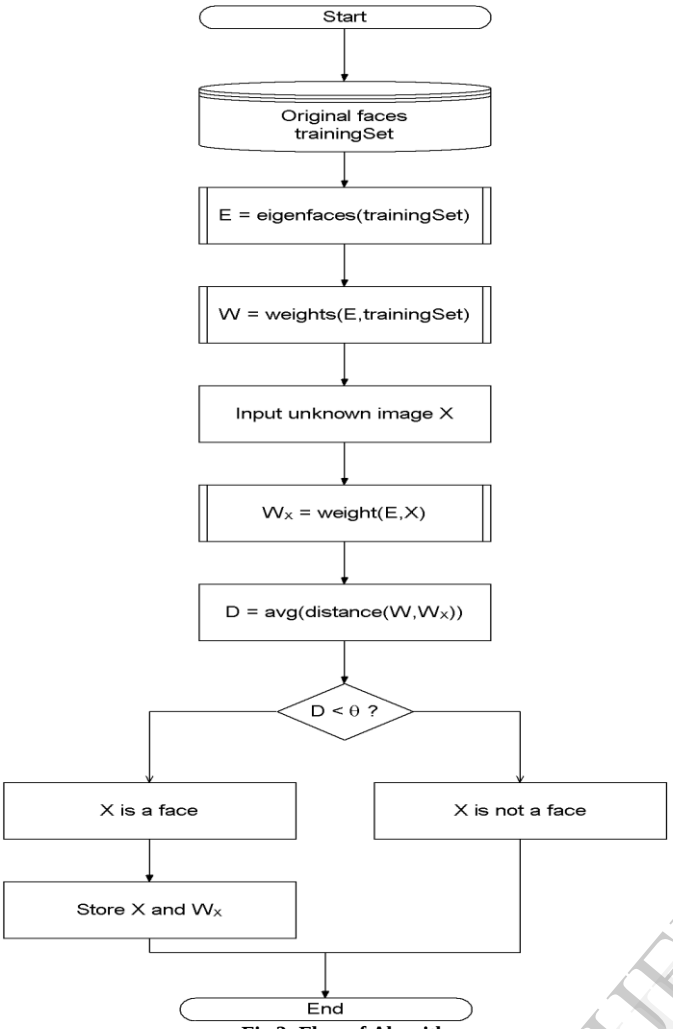

Fig 3: Flow of Algorithm

- PART 2

a) Compare the distance between the input image and the images of the training set.

b) If the distance is minimum and the weight is maximum then the input image is a known face else it is an unknown face

OTHER FUNCTIONALITY

- SMS - SMS is a salient feature added to our system enhancing the privacy and security of the user's desktop and preventing unauthorized access intruding the system.

The prime concern behind sending an sms to an authorized person is to alert him about the access to the system by an unauthorized user by dropping an SMS onto any restored authorized mobile number. The message content is appended with a random password that is generated. This system presents an approach to send SMS without the need of a mobile phone and internet using a GSM modem. It uses a GPRS modem and a SIM card to send messages to any mobile network. The message cost is based on the message tariff subscribed with the SIM card of the corresponding network. There are many kind of sms applications available in market, and many others are being developed. The instructions used to control, the GPRS mobile are called THE AT COMMANDS.

- Email – Email is another functionality provided for our system. This is a crucial step which is forced on an unauthorized access, which sends an email embedding the image of the unknown firm, which provides flexibility to authorized user to have visual glimpse of unauthorized firm.

ADVANTAGES

- Our system overcomes the traditional approach of authenticating user thus saves time, money and effort.
- Manual Monitoring is eliminated thus man power is saved.
- High level security maintained in the client server network through face recognition and tracking of unauthorized access.
- The valid user can keep track of his account by receiving SMS and email about unauthorized access to his system

DISADVANTAGES

- Ageing

It is one of the disadvantages in face recognition in which the features of the employee differs with their age. Due to this there are errors in authentication if the features do not match with the face templates stored in the database.

Fig 4: Ageing*]*

- OCCLUSION

Occlusion may cause error in authentication if the captured image has certain features that are hidden or are blocked and are different from the face templates stored in the database.
For example: Spectacles, scarf, cap, etc.

Fig 5: Occlusion/Blockage/Hiding of some features

APPLICATION

Our system can have many applications in various areas with very little or modification. Few of these applications are as follows.

- Organization/Institutions can use this system for Providing security and marking attendance of users.
- Government office VIP entry can be authenticated using facial recognition.
- Crime branch to identify criminal records.
- General home security.

CONCLUSION

We plan to develop a system that is very flexible and can be applied with little modifications for various purposes in many areas requiring security. We have chosen the Eigen face approach for face recognition as it is more accurate and feasible according to our survey. We have also added the SMS and email sending functionality to our system for reporting unauthorized access and thus added more security.

REFERENCES

[1] Barrett W (1998),"A Survey of Face Recognition Algorithms and Testing Results", Proc. IEEE 1998 pp. 301-305.

[2]Utkarsh Goel, Kanika Shah, Mohammed Abdul Qadeer, "The Personal SMS Gateway", Proc.IEEE 2011

[3]P. Aishwarya1 and Karnan Marcus2, "Face recognition using multiple eigenface subspaces", Journal of Engineering and Technology Research Vol. 2(8), pp. 139-143, August 2010*

[4]Matthew Turk and Alex Pentland ,"Eigenfaces for recognition", in journal of cognitive Neuroscience, vol. 3, No. 1, 1991, pp 71-81.

[5]L. Sirovich and M. kirby, "Low-dimensional procedure for the characterization of human faces", journal of the Optical Society of America A, Vol. 4, page 519, March 1987

[6]P.Latha, Dr.L.Ganesan & Dr.S.Annadurai "FACE RECOGNITION USING NEURAL NETWORK" An International Journal (SPIJ) Volume (3) : Issue (5) 2010

[7] R. Brunelli, Template Matching Techniques in Computer Vision: Theory and Practice,Wiley, ISBN 978-0-470-51706-2, 2009

[8] V. Starovoitov and D. Samal "A GEOMETRIC APPROACH TO FACE RECOGNITION" Institute of Engineering Cybernetics, 2010