Volume 4, Issue 7, July 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Database Security Based on Human Authentication Using Facial Recognition

Sneha Arora
M.TECH Scholar
Cbs group of institutions
Jhajjar, India

Rajiv Munjal
A.P CSE
Cbs group of institutions
Jhajjar, India

Abstract-Data is the most significant and essential entity to every organization. Companies invest millions of dollars in order to protect and manage the access to their data. The privacy and confidentiality of any data could be easily determined from the fact that the sensitivity of organizational data is because of its profit figures,business revenues, client details etc. If this falls into wrong hand or rivals and is being misused organizations have to bear a heavy loss and pay a penalty for that. So in order to protect our data and database we take the precautionary measures to the next level. We validate and restrict the access to the database according to the roles assigned to the human beings for records accessibility, on the basis of their facial features by using Eigenface algorithm Face recognition is a pattern recognition task performed specifically face either "known" or "unknown", after comparing it with stored known individuals. It is also desirable to have a system that has the ability of learning to recognize unknown faces. So when administrator inhibit details of employee then it will save in our database and the program will be asked to capture the image of the employee it takes 100 images per person and trained them and then store in training set after validation of image only then employee can further do work according to the roles assigned by administrator . In this way our database is secured using facial recognition.

Keywords- database, eigenfaces, PCA, facial recognition, training set

I. INTRODUCTION

Database security concerns the use of broad range of information security controls to protect databases against compromises of their confidentiality, integrity,availability. Data is the most significant and essential entity to every organization. Companies invest millions of dollars in order to protect their databases. Traditionally databases have been largely secured against hackers through network security measures such as firewall, network based intrusion system etc. we prefer to design databases in such a way that they are assigned different roles which govern the access to records. In the very first place databases are normalized and then different tables are accessed according to the role of the user. The security design for specific databases systems typically specify further security administration and reporting of user access rights, log management and analysis, database replication and protecting our database programs. So we develop an application for let say rural bank where there are less number of employees and we want to secure the database so we will use facial recognition technique called eigenface to validate the identity of the user. In this paper we will tell how we use facial recognition technique called eigenface algorithm is used for human authentication in order ensure the validation of the person and to check that the person is same or not. Firstly we take picture of any person. Then using eigenface algorithm it takes 100 images of the person and stores in its database and put them in the training set. Then when the person again comes in front of the camera it will go on training phase first and then it checks the person image from the images stored in the database of the training set and if it matchs then it is a known face otherwise unknown and the ghost appearance image will be shown which are called eigenfaces. Hence we want to recognize the identity of a person where an image of that person is given to the system we will use PCA as feature extraction algorithm in our paper.

II. FACE RECOGNITION SYSTEM

Automatic face recognition system try to find the identity of a given face image according to their memory. The memory of a face recognizer is generally simulated by a training set. The training set consists of the features extracted from known face images of different persons. The input of a face recognition system is always an image or video stream. The output is an identification or verification of the subject or subjects that appear in the image or video. Face recognition is a three step process as shown in figure.

Figure 1.1: A general face recognition system.

Face detection is defined as the process of extracting faces from scenes. So, the system positively identifies a certain image region as a face. The next step -feature extraction- involves obtaining relevant facial features from the data. These features could be certain face regions, variations, angles or measures, which can be human relevant (e.g. eyes spacing) or not. Finally, the system does recognize the face. In an identification task, the system would report an identity from a database. This phase involves a comparison method, a classification algorithm and an accuracy measure.

2.1 Face Detection

Face detection is defined as the process of extracting faces from scenes. So, the system positively identifies a certain image region as a face.

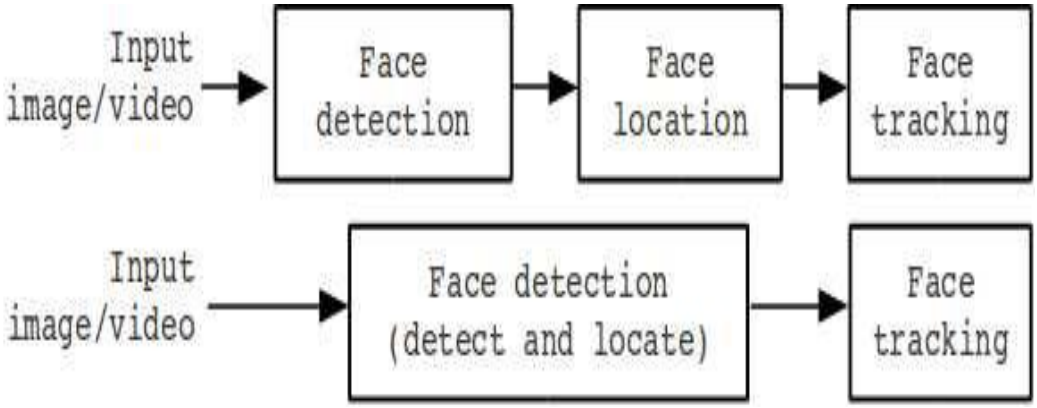

Figure 2.1 Face Detection process

a)Pose variation. The ideal scenario for face detection would be one in which only frontal images were involved. But, as stated, this is very unlikely in general uncontrolled conditions. Moreover, the performance of face detection algorithms drops severely when there are large pose variations. It's a major research issue. Pose variation can happen due to subject's movements or camera's angle.

b)Feature occlusion. The presence of elements like beards, glasses or hats introduces high variability. Faces can also be partially covered by objects or other faces.

c)Facial expression. Facial features also vary greatly because of different facial gestures.

d)Imaging conditions. Different cameras and ambiental conditions can affect the quality of an image, affecting the appearance of a face. There are some problems closely related to face detection besides feature extraction and face classification. For instance, face location is a simplified approach of face detection. It's goal is to determine the location of a face in an image where there's only one face.

2.2 Feature Extraction

Feature extraction process can be defined as the procedure of extracting relevant information from a face image. This information must be valuable to the later step of identifying the subject with an acceptable error rate. The feature extraction process must be efficient in terms of computing time and memory usage. The output should also be optimized for the classification step. Feature extraction involves several steps - dimensionality reduction, feature extraction and feature selection. This steps may overlap, and dimensionality reduction could be seen as a consequence of the feature extraction and selection algorithms.

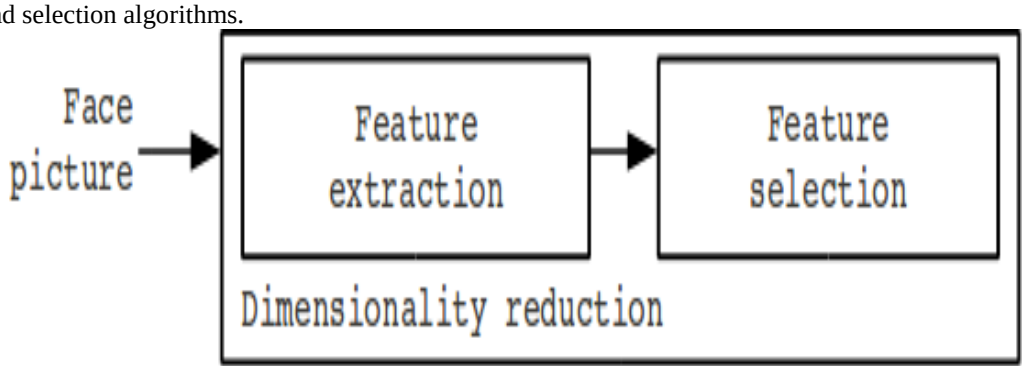

Fig2.2 Feature extraction process

It transforms or combines the data in order to select a proper subspace in the original feature space. On the other hand, a feature selection algorithm selects the best subset of the input feature set. It discards non-relevant features. Feature selection is often performed after feature extraction. So, features are extracted from the face images, then a optimum subset of these features is obtained.

2.3Face Recognition

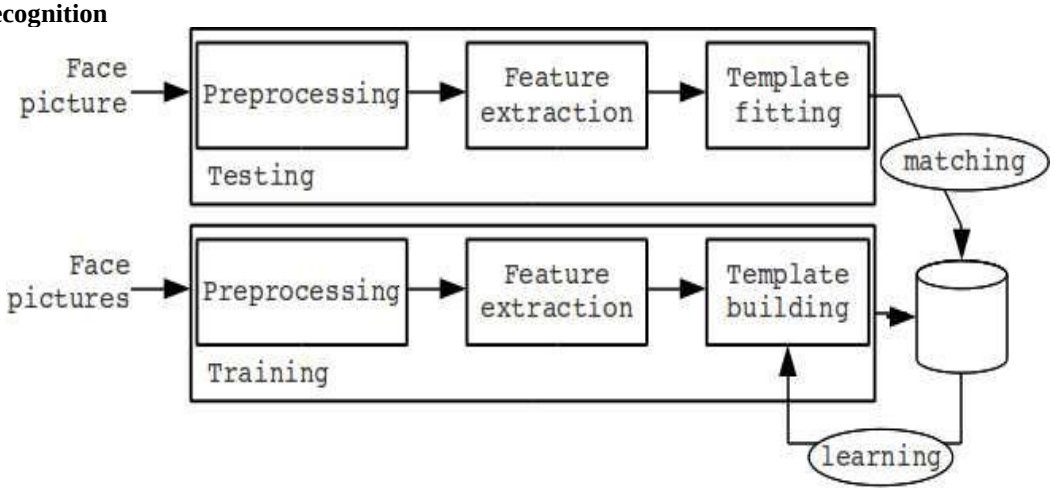

Fig 2.3Face Recognition process

Automatic face recognition system tries to find the identity of a given face image according to their memory. The memory of a face recognizer is generally simulated by a training set. The training set consists of the features extracted from known face images of different persons. Thus the task of face recognizer is to find the most similar feature vector among the training set to the feature vector of a given test image. Then in the learning phase it learns all the images and stores in the database. All the features templates come into account like the facial markers etc. and this all work is done under training phase and then the image is recognized as known or unknown face of image. In the training phase we extract feature vectors for each image in the training set.

III. EIGENFACE USING PCA

Sirovich and Kirby [101, 56] developed a method for efficiently representing faces using PCA (Principal Component Analysis).Their goal of this approach is to represent a face as a coordinate system. The vectors that make up this coordinate system were referred to as eigen pictures. Later, Turk and Pentland used this approach to develop a eigenface-based algorithm for recognition. The main task of this is to distinguish input signals or Image sets from noisy signals that corrupts the data .It uses an approach in which it transforms face images into a set of basis faces called principal component of face images. Basic working of eigenface is as follows:

a) Firstly get sample images or pictures of people you want to recognise.

b) Get training set of these images . Training set should be taken under the same lighting conditions. They must be resampled to the same pixel resolution. Each image must be treated as one vector.

c) Subtract the mean: The average image has to be calculated and then subtracted from each original image.

d) Calculate the eigenvectors and eigenvalues of covariance matrix.

e) Choose the principal components

f) Now from these sample images or pictures, classify new image

3.1 PCA

PCA stands for principal component analysis. The input signals are highly noisy to calculate eigenvectors and values we need to have training sets of images which then differentiate input signals from noisy signals. After calculating eigenvectors we chose component and form a feature vector. Eigenvectors with highest eigenvalues is chosen as principal component of data set and then we get ghost like images which we called as eigenfaces. Features can be extracted out of original image data by means of a mathematical tool called Principal Component Analysis. By means of PCA one can transform each original image from the training set into a corresponding eigenface. An important feature of PCA is that one can reconstruct any original image from the training set by combining the eigenfaces. Therefore the original face image can be reconstructed from eigenfaces if one adds up all the eigenfaces in the right proportion.So in order to reconstruct the original image from the eigenfaces one has to build a kind of weighted sum of all eigenfaces. That is the reconstructed original image is equal to sum of all eigenfaces with each eigenface having a certain weight. This weight specifies to what degree the specific feature is present in the original image.

Let Ω be a training image of person A. In order to extract PCA features of Ω,you will first convert the image into a pixel vector$^{\varphi}$ by concatenating each rows into a pixel vector.The length of the vector will be m*n. For each training image Ω we should calculate and store these feature vectors ω.In the recognition phase or testing phase we will be given a test image of a known person. Let α be the identity of the person. And then we compute feature vector of the person using PCA and obtain ω.

Assume we have p training images.Ω=1,2…….p. For each training image , we should form pixel vector ᵠ .In order to apply PCA to a training set we should first form a training data matrix of A. Then the eigenvalues and vectors are calculated and the one which has highest value would be considered the best among all we will calculate ɷ as ɷ=¥ᵠᵗᵗ where these are the transpose of the matrix. Thus we can convert each eigenvector to an image by reversing the concatenation operation**.**

Fig 3.1sample faces

In this way we can have eigenfaces using principal component analysis

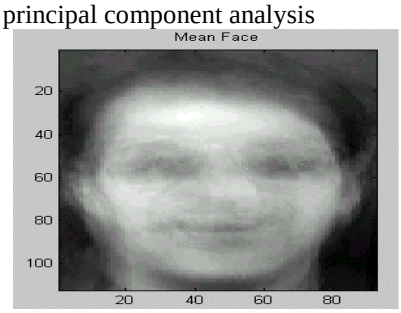

Fig 3.2 Average face of sample faces

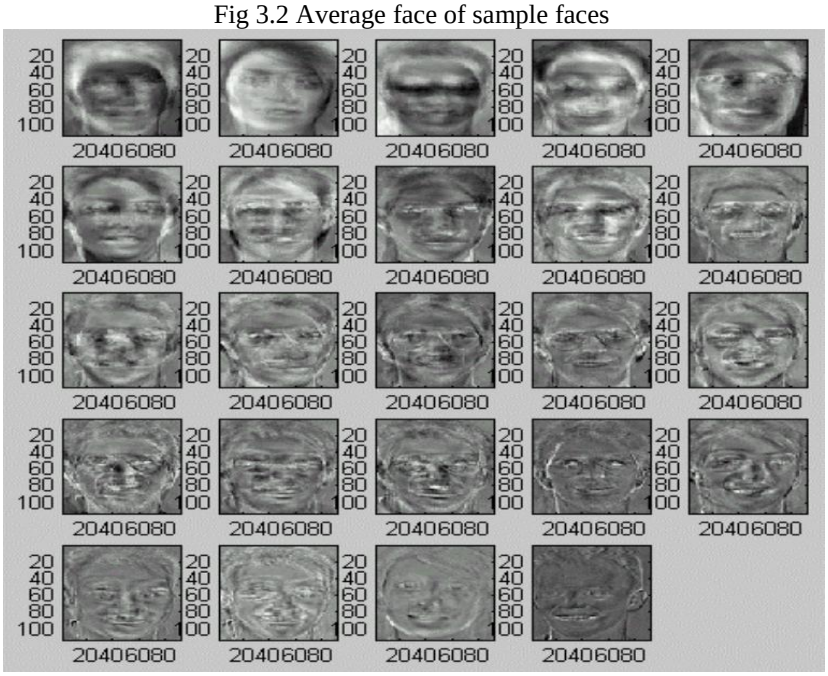

Fig 3.3eigenface of sample faces

IV. CONCLUSION

We can safely conclude that It can be effectively used in all the business verticals where secured access of database records is a necessity. This application combines the power of database role-mapping with human verification for the security of records. Through this application, not only the records will be secured but data definition and manipulation procedures will also be effectively enforced The main problems found in the implementation of the application were originated from memory leaks, caused by some images being incorrectly unloaded after use. An-other problem was the noise on the images that worsened the accuracy of the recognition. There are many factors that can improve the performance of the program. Good pre-processing of the images is very important for getting adequate results. To improve the face recognition accuracy, it would be necessary to have more input images. This could be achieved by taking at least 50 photos of each person, particularly from different angles and in various lighting conditions, or by obtaining more training images, or by generating new images from the existing ones (mirroring, resizing, rotating or adding noise). In conclusion, a robust face recognition system should be insensitive to:

- Changes in illumination
- Changes in head orientation and scale
- Presence of facial details such as glasses, beards or other artefacts
- Background
- Noise

However, the application created was quite effective to detect and recognize faces in controlled environment.

REFERENCES

[1] M.Turk and A.pentland. “Eigenfaces for recognition”. Journal of cognititive neuroscience,3, 71-86,1991
[2] Eigenface based facial recognition by Dimitri PISSARENKO december1,2002
[3] Face recognition using Principal Component Analysis by Shervin Emani
[4] Face recognition using eigenface and neural networks by Volkan Akalin
[5] Face Recognition Algorithm by Jon Marynes.

