Protection of Classified Data through Role based Access Control using Human Authentication

Deepika
Student CSE
Lingaya's University Faridabad

Mamta
Student CSE
NIET Greater Noida

Natasha Soni
Asst. Professor CSE
Lingaya's University

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 etc. If it's being misused then an organizations have to bear a heavy loss. So to protect our data and storage 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 accessing rights, 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 people. 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 security, PCA, face recognition

1. INTRODUCTION

Database security involves the use of wide range of data security controls to protect databases against compromises of their confidentiality and availability. 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 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 analysis and management, 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 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 this is the same person or not. First of all we capture an image 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 or say eigenface. Therefore 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

2. SECURING DATABASE USING ACCESS CONTROL

Access control ensures all communications with the databases and other system objects are according to the policies and controls defined. This ensures that no assumption comes by any attacker neither internally nor externally and thus, protects the databases from potential errors-errors that can make impact as big as stopping firm's operations. Access control also helps in minimizing the risks that may directly impact the security of the database on the main servers. E.g. if a table is unexpectedly deleted or access is modified the results can be roll backed or for certain files, access control can restrict their deletion [6]

Bertino et al. [2] explains a technique for authorization of video databases. In the scheme, the access to a particular stream of the video is granted only after verifying the credentials of that user. The credentials may not just be the user-id but it may be the characteristics that define the user and only after successful verification of the credentials the user is granted the permission to access the database.

Kodali et al. presented a generalized authorization model for multimedia digital libraries [3], [4], [5]. The scheme involves integrating the three most common and widely used access control mechanisms namely: mandatory, discretionary and role-based models into a single framework to allow a unified access to the protected data. The technique also addresses the need of continuous media data while supporting the QoS constraints alongside preserving the operational semantics.

3. FACE RECOGNITION SYSTEM

Automatic face recognition system try to find the identity of a given face image according to the stored data. The data stored in memory of a face recognizer is generally simulated by a training set. The training set comprise of the features extracted from known face images of various persons. The face recognition system is always accepted an image or video stream as an input. The outcome is an identification of the subject or subjects that appear in the image or video. Face recognition is a three step process as shown in figure1.

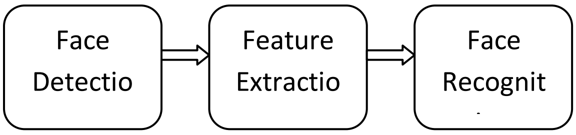

Fig 1: A general face recognition system

Face detection is defined as the process of extracting and identifies human faces in digital images [1]. 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 stored in memory. These features could be positive face sector, deviations, angles or measures, which can be human relevant (e.g. eyes spacing) or may b not. At last, the system does identify the face image. In recognition process, the system would report an identity from a database. This stage includes a comparison form, a classification algorithm and an accuracy measure.

3.1 Face Detection

Face detection can be stated as the process of extracting human faces from picture. So, the system positively identifies a certain image region as a face.

3.1 Pose variation.

The optimal plot for face detection would be one in which only frontal images were involved. But, as says, this is very unlikely in general undisciplined conditions. Moreover, the performance of face detection algorithms drip badly when there are large number of pose variations. Pose variation can happen due to subject’s movements or camera’s angle.

3.2 Feature occlusion.

The presence of elements like beards, glasses or hats introduces high variability. Faces can also be half coated by objects or other faces.

3.3 Facial expression.

Because of different facial gesture, the facial features also vary greatly.

3.4 Imaging conditions.

Various cameras quality and surroundings conditions can affect the picture quality, affecting the display of a face. There are some problems closely related to face detection besides feature extraction. For example, location of face is a simplified approach of face detection. The main aim is to determine the location of a face in an image where there’s only one face.

3.2 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 context of use of memory and computational time. There should me an optimal solution for the classification step. Feature extraction includes various steps - dimensionality reduction, feature extraction and feature selection. These steps may overlap, and dimensionality reduction could be seen as a consequence of the feature extraction and selection algorithms.

It converts or combines the data in order to select a proper subspace in the original feature space. Secondly, a feature selection algorithm used to selects the best subset of the input feature set. It eliminates non-relevant features. Feature selection process is often implemented after feature extraction. Therefore, facial features are extracted from the images, and then a capital subset of these features is found.

3.3 Face Recognition

In figure 2 Automatic face recognition system tries to find the identity of a given face image according to their stored data. A face recognizer’s memory is generally simulated by a training set. These training set contain the features extracted from known face images of different persons. Hence the process of face recognizer is to obtain the most identical feature vector among the training set to the feature vector of a given test image. In the learning phase it learns all the images and stores in the database. The features templates come into actions like the facial markers etc. and this all work are 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.

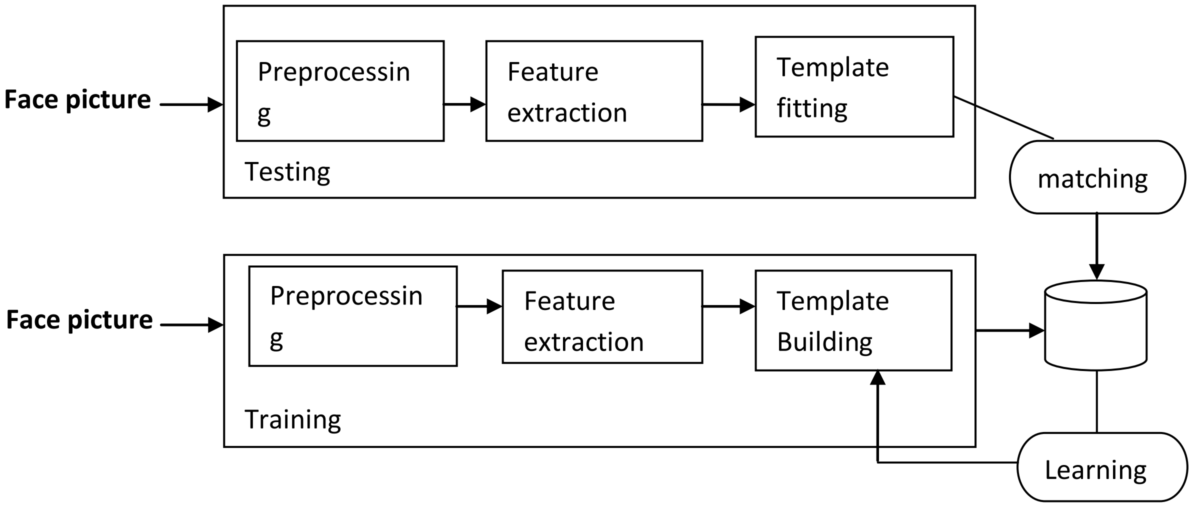

Fig 2: A general face recognition system

4. EIGENFACE USING PCA

A set of eigenfaces can be generated by performing a mathematical process called principal component analysis (PCA) on a large set of images depicting different faces of human. Casually, eigenfaces can be taken as a set of "standardized face ingredients", received from statistical analysis of large number of human face images. Any human face can be considered to be a combination of these standard faces. As an instance, one's face might be composed of the average face plus 10% from eigenface 1, 55% from eigenface 2, and even -3% from eigenface 3. Main thing is, it does not take many eigenfaces combined together to achieve a fair approximation of most faces. Also, because a person's face is not recorded by a digital photograph, but instead as just a list of values (one value for each eigenface in the database used), much less space is taken for each person's face.

Sirovich and Kirby [7] 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 eigenfacebased algorithm for recognition. The main task of this is to distinguish input signals or Image sets from noisy signals that corrupt 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) Bring training set of sample pictures. Training set should be taken under the same lighting conditions. They must be resampling to the same pixel resolution. Every image must be taken 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, label a new image.

5. PCA

PCA stands for principal component analysis. The input data are very 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. The highest eigenvalues of an Eigenvectors 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. One of the important features 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 of eigenface specifies to what extent the specific feature is present in the original image. Let Ω be a training image of person A. concerning to extract PCA features of Ω, first convert the image into a pixel vector$^{\varphi}$ by concatenating each row 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[7].In the testing phase we will be given a test image of a 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=1, 2……….p. For each training image, we should form pixel vector$^{\varphi}$. For applying PCA to a training set, 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 ω as ω=¥$^{\varphi tt}$ where these are the transpose of the matrix. Therefore it can transform each eigenvector to an image by reversing the concatenation operation.

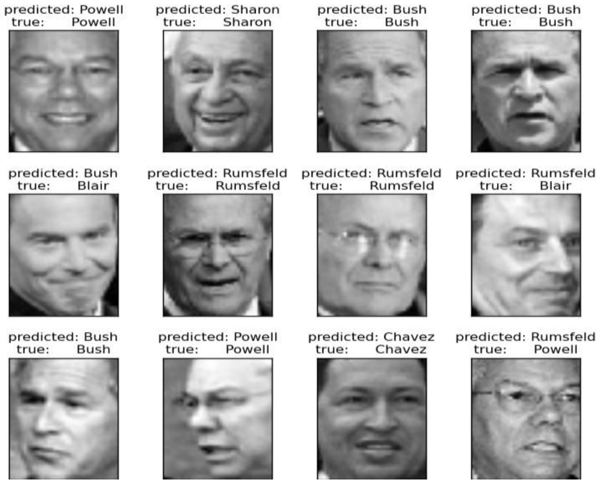

Figure.3 Sample faces

In this way we can have eigenfaces using principal component analysis

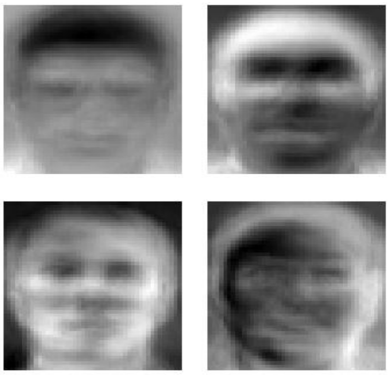

Figure 4 Average face of sample faces

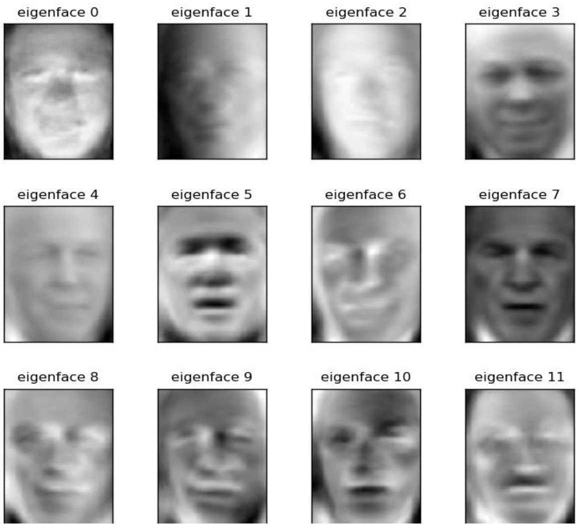

Figure 5 Average face of sample faces

6. EXPERIMENTAL SETUP AND RESULTS

The proposed system is designed to operate with a single static camera which is inbuilt within the system location. HP static camera is used for image acquisition which captures images at a spatial resolution of 640 x 480 pixels having a frame rate of 25 frames per second. To capture image a low cost camera is used because main aim of this research work was to design an economical system. The distance between the camera and the persons is approx 6 to 8 meters

7. RESULT

The performance of the proposed Face Recognition System is tested on different images in different poses recorded in different conditions. Some of the images include one person, and some includes more than that. In some images lighting varies, pose variation and expression also vary. In case of huge crowd encapsulating in image, the rate for correct recognition is little low as compared to the images with fewer persons where the false recognition rate goes pretty below around 1 to 2% resulting the correct recognition in the range of around 98 to 99% which shows excellent results.

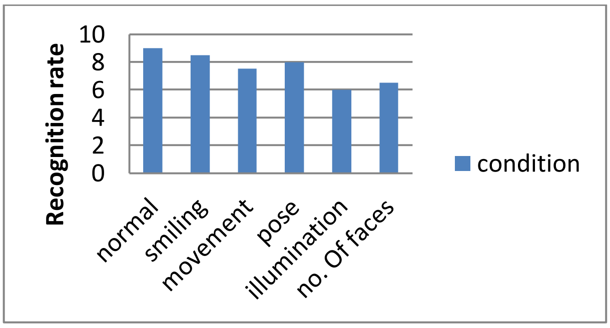

Figure 4 Output for different conditions

8. CONCLUSION

Keeping this application into context, we can safely conclude that: It can be effectively used in all the business verticals where secured access of database records is an essential. This application associates the ability of database role-mapping with human verification for the security of records. From this application, not only the records will be protected but data definition and manipulation procedures will also be effectively enforced .This application will effectively allow the new users to safely access the data through minimal roles assigned to them which can be duly changed at any point of time in future.

During the second layer of multi-layered security mechanism which is human authentication, this application shall not allow the user to keep his/her face before the camera for a long time. There is a time-based human verification which will be implemented and this new concept shall surely strengthen the security during accessibility of the database records.

Table 1 comparison of different condition

	Normal	**Smiling**	**Movement**	**Pose**	**Illumination**	**No. of faces**
Image1	Y	Y	N	Y	Y	Y
Image2	Y	Y	Y	Y	Y	Y
Image3	Y	Y	Y	N	N	N
Image4	N	Y	Y	Y	Similar	Y
Image5	Y	Y	Y	Similar	N	N
Image6	Y	Similar	Y	Y	Y	Similar
Image7	Y	Y	N	Y	N	N
Image8	Y	Y	Y	Similar	Y	Y
Image9	Y	Y	Similar	Y	Y	Y
Image10	Y	Y	Y	Y	Similar	Y

9. REFERENCES

[1] https://en.wikipedia.org/?title=Face_detection

[2] Elisa Bertino, Moustafa A. Hammad, Walid G. Aref , Ahmed K. Elmagarmid, “An Access Control Model for Video Database Systems”, Proceedings of the ninth international conference on Information and knowledge management, 2000, pp. 336 – 343.

[3] Naren Kodali, Csilla Farkas, Duminda Wijesekera, “An authorization model for multimedia digital libraries”, International Journal on Digital Libraries, vol. 4, no. 3, 2004, pp. 139-155

[4] Béchara Al Bouna, Richard Chbeir, “Multimedia-based authorization and access control policy specification”, Proceedings of the 3rd ACM workshop on Secure Web Services, 2006, pp. 61–68.

[5] Shermann S.M. Chan, Qing Li, José A. Pino, “Access Control Mechanism for Collaborative Video Database Production Applications”, Proceedings of IEEE Sixth International Symposium on Multimedia Software Engineering, 13-15 Dec. 2004, pp. 396- 402.

[6] Iqra Basharat,” Database Security and Encryption: A Survey Study “, International Journal of Computer Applications (0975 – 888) Volume 47– No.12, June 2012

[7] Sneha Arora, Rajiv Munjal, “Database Security Based on Human Authentication Using Facial Recognition”, IJARCSSE, Volume 4, Issue 7, July 2014 , ISSN: 2277 128X.