Authentication System with Face Recognition Using GSM Technology

[1]Mr. Nikhil Pawar, [2]Mr. Sagar Sale

Department Of Computer Science And Engineering, SVERI's COE Pandharpur.

Abstract- *Authentication systems used today are quite insecure. Generally every person has it's own User_ID and Password for secure login. For authentication password must be known only to the particular person. But it's of no use when same one else hacks ID and Password. Search reranking is one of the effective approaches to refine the text-based image search result. The strategy used in our project is the solution to overcome the above problem. The strategy is to use face recognition system with GSM Tech. Whenever one wants to login. After entering ID and Password & clicking submit button, system will take snap of the user. It try to match the image with the image of the user in database. If it matches with the database image system will complete the authentication and if it doesn't match, system will send E-mail containing the image of invalid user as well as send message to the registered user's mobile number using GSM Tech. The registered user will have privilege to shut down the machine if any such kind of suspect occurs by sending the shutdown' message to the machine.*

Keywords: Authentication, GSM, Face Recognition.

1. INTRODUCTION

The authentication processes we use today are of same kind, but are quite insecure. In order to work in corporate industry security plays vital role. Generally every person has its own User ID and Password for authentication provided password must be known only to the particular person. But it's of no use when same one else hacks ID and Password. The strategy used in our project is the solution to overcome the above problem. The strategy is to use face recognition system with GSM Tech. Whenever one wants to login. After entering ID and Password & clicking submit button, system will take snap of the user. It try to match the image with the image of the user in database. If it matches with the database image system will complete the authentication and if it doesn't match, system will send E-mail containing the image of invalid user as well as send message to the registered user's mobile number using GSM Technology. The registered user will have privilege to shut down the machine if any such kind of suspect occurs by sending the "shutdown' message to the machine. Objective behind this is to protect the organization's business information and any client or customer information within its custody or safekeeping by safeguarding its confidentiality, integrity and availability, to establish safeguards to protect the organization's information resources from theft, abuse, misuse and any form of damage, to establish responsibility and accountability for Information Security in the organization

2. FACE DETECTION AND FEATURE EXTRACTION

2.1 Face Detection

Detecting and tracking of face-like objects in cluttered scenes is an important preprocessing stage of an overall automatic face recognition system. Face region needs to be segmented out from a still image or a video before recognition since most face recognition algorithms assume that the face location is known. The performance of a face recognition algorithm depends on how one controls the area where faces are captured. For applications like mug shot matching, segmentation is relatively easy due to a rather uniform background.

For a video sequence acquired from a surveillance camera, segmentation of a person in motion can be accomplished using motion as a cue. Color information also provides a useful key for face detection while color-based approaches may have difficulties in detecting faces in complex backgrounds and under different lighting conditions. Face detection can be viewed as a special case of face recognition, a two-class (face versus non-face) classification problem. Some face recognition techniques may be directly applicable to detect faces, but they are computationally very demanding and cannot handle large variations in face images. Conventional approaches for face detection include knowledge-based methods, feature invariant approaches, template matching, and appearance-based methods. Knowledge-based methods encode human knowledge to capture the relationships between facial features. Feature invariant approaches find structural features that exist even when the pose, viewpoint, or lighting conditions vary. Both knowledge-based and feature invariant methods are used mainly for face localization. In template matching methods, several standard patterns of a face are stored to describe the face as a whole or the facial features separately. The correlations between an input image and the stored patterns are computed for detection.

The templates are also allowed to translate, scale, and rotate. Appearance-based methods learn the models (or templates) from a set of training images to capture the representative variability of facial appearances. This category of methods includes various machine learning algorithms (e.g. neural networks, support vector machines etc.) that detect upright and frontal views of faces in gray-scale images. The analytic approaches, which concentrate on studying the spatial domain feature extraction, seem to have more practical value than the holistic methods. In these approaches specific facial features are extracted manually or

automatically by an image processing system and stored in a database. A search method is then used to retrieve candidates from the database.

2.2 Feature Extraction for Face Recognition

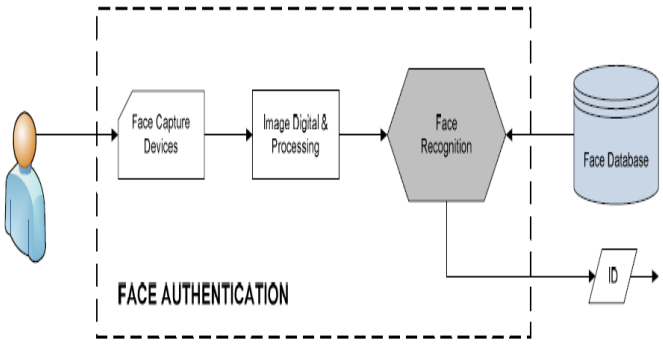
Face recognition involves feature matching through a database using similarity or distance measures. The procedure compares an input image against a database and reports a match. Existing face recognition approaches can be classified into two broad categories: analytic and holistic methods. The *analytic* or feature-based approaches, which concentrate on studying the spatial domain feature extraction, compute a set of geometrical features from the face such as the eyes, the nose, and the mouth. The use of this approach has been popular in the earlier literature.The holistic or appearance-based methods consider the global properties of the human face pattern. The face is recognized as a whole without using only certain fiducial points obtained from different regions of the face. Holistic methods generally operate directly on pixel intensity array representation of faces without the detection of facial features. Since detection of geometric facial features is not required, this class of methods is usually more practical and easier to implement as compared to geometric feature-based methods.

2.3 Access Control System using Face Recognition

Face recognition has been widely used in identification and access management. At the moment, there have been a lot of researches on access control applications and those have been utilized in personal computers' and handheld devices' authentication. They are also integrated into office and home access control systems. We will talk further about applications of face recognition in access control systems and their security drawbacks.

3. FACE AUTHENTICATION

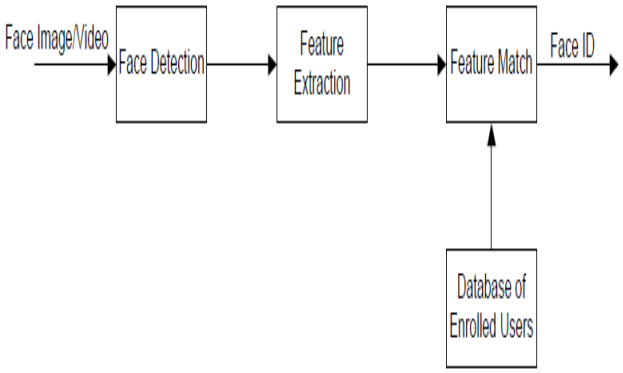
The following figure describes an access control system base on face authentication. In this model, each user has an account and a corresponding ID in the Face database. On a user logging in the system, Face Authentication will use face recognition technologies to analyze and determine his ID as well as his permissions on the system. This model can be applied to access control systems where the number of people is small; for example, user accounts in an operating system, members of an office or a family. When receiving a request, an access control system based on face authentication must find out exactly whether the person requesting is a client.



Access Control System Based on Face Authentication Model

3.1. Face Recognition Model

As you can see from the diagram below, face recognition requires a wide range of technologies.



Face Recognition Processing Flow

Face recognition systems in general, and access control systems based on face authentication in particular, use a "*learning*" mechanism to collect data on facial characteristics if users. Hence, the first important point to care about in a face recognition model is the *Face Database* storing this information. Face Detection: locating the face in the photo or video and removing unnecessary details on the background. Feature Extraction: extracting facial characteristics needed for recognition. Feature Match: comparing scanned information with database to decide if it matches some user's face. If the face matched, the ID of the corresponding is returned.

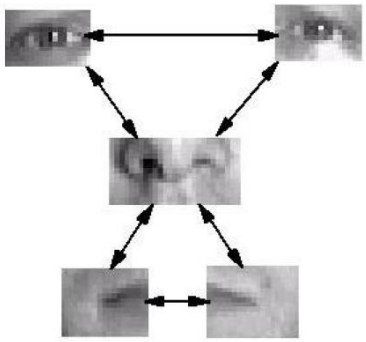
Most of present researches try to create an Automatic Face Recognition model. The hardest part of it is how to get best biometric information on the faces. Therefore, Feature Extraction is the most important module of the system. In the next section, we will focus on basic algorithms used for extracting facial characteristics.

3.2. Face Recognition Algorithm

Geometric feature-based approach

In the 1980s, researches on face recognition were mostly based on the geometric characteristics of faces. Using this approach, parts of human faces such as eyes, nose and mouth are located together with their attributes and their mutual relationships and measurements (distances, angles, areas). The system will distinguish faces based on this information.

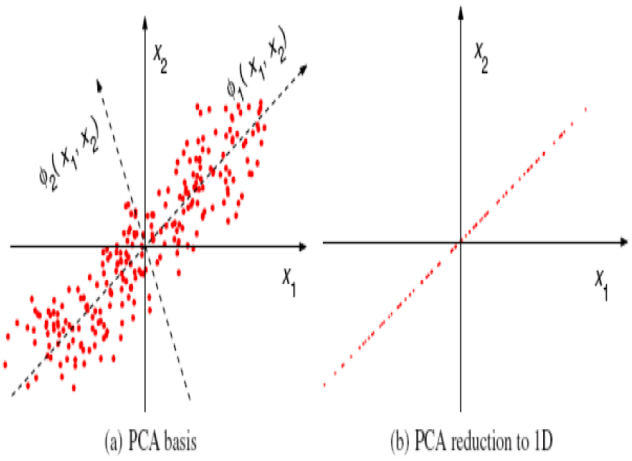
This approach is quite effective for small database, with steady lighting and viewpoint.



Geometric feature-based approach

Appearance-based approach

At the beginning of 1990s, more and more researchers were inspired by a new approach based on human appearance.. This technology transforms the face space into subspaces which have less dimensions but those are the directions that depict the most important parts of the face.



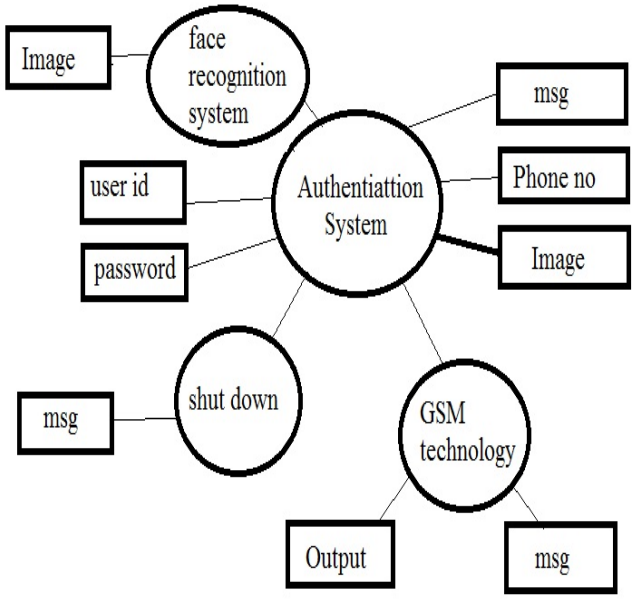
Principal Component Analysis Method

The studies that are talked about the most is Principal Component Analysis (PCA) and KLT – Karhunen-Loève Transform.The above graphs show a typical example of PCA. We can easily spot that the majority of 2D points locate close to the the 1st PC line, which means that we can perform a projection of these points on the 1st PC line without losing essential 2D information.

4. ALGORITHM

Step 1: enter User_id and password.
Step 2: capture image.
Step 3: compare image with database image.
Step 4: if image match found then open valid user application else.
Step 5: send sms to valid user's mobile no.
Step 6: send image through E-mail.
Step 7: read sms.
Step 8: if sms contains shut down then terminate system.
Step 9: stop.

5. DATA FLOW DIAGRAM

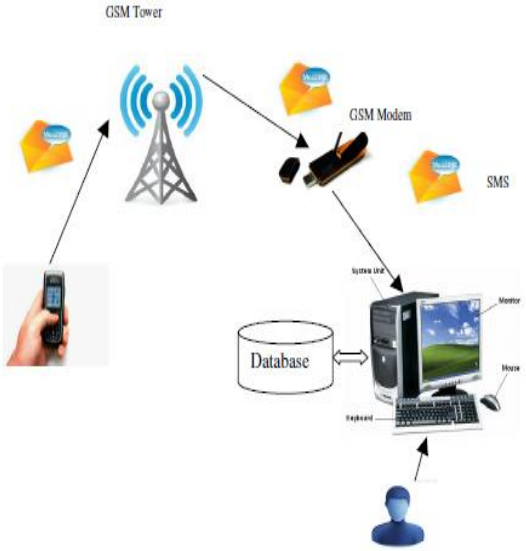


6. GSM AND MODEM

Short Message Service (SMS) is a preferred mode of text communication than using internet as it requires only Mobile Station (mobile phone with SIM) which is available at cheaper rates in the market. Also the SMS packages given by different telecom companies are available at less cost. The research work done by us has achieved two objectives: to develop a SMS repository server that is easy to manage by a teacher for collecting various feedbacks and questions sent from various students via SMS and to access the personal computer or laptop via SMS containing DOS commands.

GSM modem was used to send/ receive SMS. But the system can be expanded by connecting it with microcontrollers and sensors to control and monitor different hardware devices. After receiving SMS, the SMS repository server interprets SMS by extracting the code present in the SMS and takes an appropriate action depending on the code present in SMS Results show that the developed system can meet the requirements of the user.

Below diagram shows the GSM and modem system;



5. CONCLUSIONS

We have introduced new software to authenticate the system using face recognition as well as GSM technology for providing more security for different applications.

REFERENCES

[1] http://en.wikipedia.org/wiki/Facial recognition system. Titaniam group,"comparing face recognition against other types of biometric authentication methods.

[2] Ching-Han CHEN,Chai – Te CHU "Face Authentication System for Information Security".

[3] Anthony Ronald Grue,"Facial Recognition:Limited Application in safety and security".

[4] Stan Z, Li Anil K Jain,"Handbook of Face Recognition".

[5] N. Kumar, Keren Tan , Weiming Chen, Rong Yang," A PCA based feature extraction method for face recognition".

[6] John D Woodward,Christopher Horn,Julius Gatune,Aryn Thomas,"A look at Facial Recognition".

[7] Sebastian Marcel and Yann Rodriguez,"Biometric Face Authentication using Pixel-based week classifiers".

[8] A.J.Goldstein, L.D.Hormon, A.B.Lesk,"Identification of Human Faces".

[9] T. Kanade,"Picture Processing by Computer Complex and Recognition of Human Faces".