Two Factor Authentication System Based On Face Recognition

Bhumika R. Shetty
B.E CMPN, TCET (M.U)

Anita Sinha
B.E CMPN, TCET (M.U)

Ashwini B. Sonar
B.E CMPN, TCET (M.U)

Abstract

Two factor authentication system is a computer based authentication which uses a two way verification mechanism for the person who wants to gain access to the particular system or some confidential information. The two factors which we are using in our project are face recognition and unique Id. This paper focuses on how the face recognition is done and how the unique id is hidden using a special method known as LSB stuffing.

Keywords. Authentication, Face recognition, LSB stuffing, Principal Component Analysis (PCA)

1. Introduction

Two-factor authentication is a security process in which the user provides two means of identification, one of which is a physical token or biometric identification, and the other is the one that can be easily memorized, such as a security code or password. In our project, the two types of user authentication which we are using are what we are and what you know.

The first factor which we are using for authentication is face recognition. Initially, the face of the concerned person will be stored in the database when he enters the system for the first time. Now if the person wants to gain access to the system, his face would be matched with the earlier taken image which is stored in the database and if the face matches, then the person should be ready for second factor authentication.

The second factor which we are using is unique id. Once the person's face is stored in the database, he will be asked to enter his unique id, this unique id will not be stored in the database instead it will be hidden in the image(stored image).Only if both the factor matches, the person will be able to gain access to the system. Before second factor authentication, first factor has to be satisfied.

This system can be used in the places where high degree of security is needed such as banks, lockers, colleges and government organizations.

2. Face recognition

Face recognition is the first authentication factor in the proposed system. Face recognition is identifying a person who is trying to gain access to a system on the basis of various face images that are stored in the system to identify people. Whenever the person tries to gain access an image of his face is taken and is tried to match with a face image from the database. If matched the person is granted access.

The key principle involved in face recognition, is that the system analyzes the characteristics of a person's face images which is given as input through a digital video camera. It measures the overall facial structure, including distances between eyes, nose & mouth and jaw edges. These measurements are retained in a database and used for comparisons when a user stands before the camera.

It is based on the fact that every face has numerous, distinguishable landmarks and the different peaks and valleys- that make up one's facial characteristics unique. Some of these features measured by the Facial Recognition system include distance between the eyes, width of the nose, depth of the eye sockets, shape of the cheekbones and length of the jaw line etc.

2.1. Working

Face recognition system operates in the following four phases which are capture, extraction, comparison and matching.

First phase consists of the capture, in this phase physical or behavioural sample is captured during enrolment. In this phase, person stands in front of camera and his face is captured by the camera which is stored in the database.

Second phase is extraction, in this phase, unique data is extracted from the sample and a template is created.

Third phase is comparison phase, in this phase the original template is compared with a new sample. When the person wants to gain access to the system, his face is captured and matched with the earlier taken image.

Fourth phase consists of matching phase, in this phase system decides whether the features extracted from the new sample match or not and if it matches, the person is granted access to the system.

In our project, we are implementing face recognition using principal component analysis (PCA).We are using Principal Component Analysis (PCA) to perform extraction, comparison and matching for our system.

2.2. Principal Component Analysis

Principal Component Analysis is one of the most successful techniques that have been used in object recognition. PCA is a statistical method under the broad title of factor analysis [1][2].

Principal component analysis (PCA) is a mathematical procedure that uses an orthogonal transformation to convert a set of observations of possibly correlated variables into a set of values of linearly uncorrelated variables called principal components.[4]

The jobs which PCA can do are prediction, redundancy removal, feature extraction, data compression, etc.PCA is a classical technique which can do something in the linear domain, thus applications having linear models are suitable, such as signal processing, image processing, system and control theory, communications, etc. The main idea of using PCA for face recognition is to express the large 1-D vector of pixels constructed from 2-D facial image into the compact principal components of the feature space [3]. This can be called Eigen space projection. Eigen space is calculated by identifying the eigenvectors of the covariance matrix derived from a set of facial images (vectors).

3. Unique Id

Unique Id is the second authentication factor. Initially when the person stores his image for the first time, he will also store his unique Id. In our project instead of storing the unique id in the database, we are hiding the unique Id in the image of the person itself using LSB stuffing.

3.1. LSB stuffing

In our project we are using a technique known as LSB stuffing to hide data into a host image as the plain text and during the extraction process; the system should be able to extract plain text from the image. Thus when the user enters his unique ID, the system extracts the unique ID(which was stored earlier) from the corresponding image of the person stored in the face database in plain text format, the extracted unique id is used for comparison with the text inputted by the user. If both (unique id and input text) matches, then only the person can gain access to the system**.**

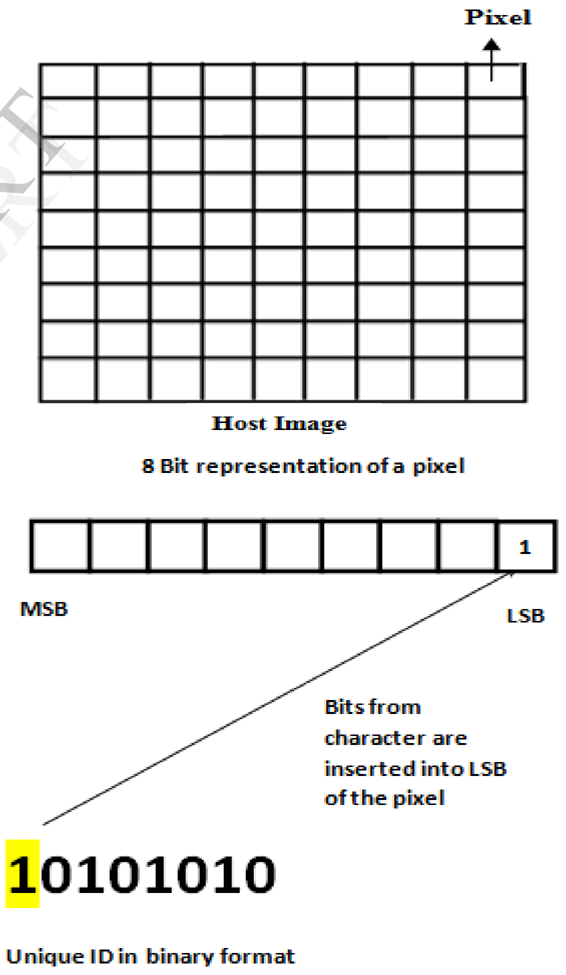
Pixel
Host Image
8 Bit representation of a pixel
1
MSB
LSB
Bits from character are inserted into LSB of the pixel
10101010
Unique ID in binary format

Figure 1. Hiding unique Id in the image

3.1.1. Hiding unique id in the image. The hiding of the unique ID is carried out on LSB or Least Significant Bits of the host image (the faces from the database used for face recognition) In an image the bits representing the MSB carry vital information while the bits representing the LSB carry information which is visually insignificant. Thus the LSB can be used to store bits from the unique ID without affecting the original image. This method does not affect the image to a large extent and also does the job of hiding the unique ID onto the host images. First the unique ID is converted to binary format and is hidden into the host image character by character in different rows. Each character of the ID is converted to binary format and then each bit of this character is hidden into LSB's of corresponding pixels of a particular row of the host image. This procedure is diagrammatically shown in figure1.

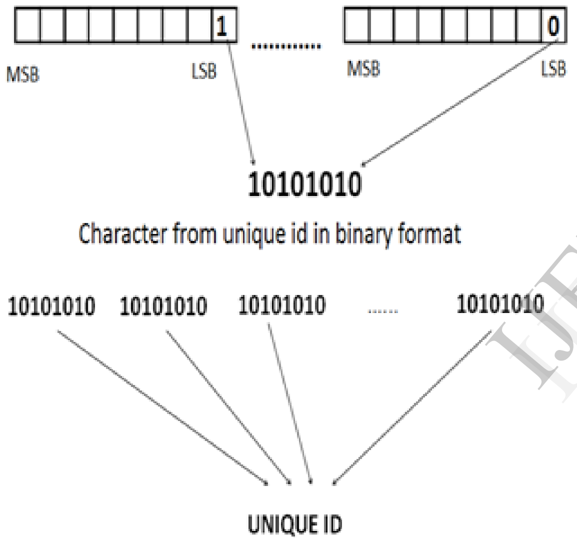

Figure 2. Extracting unique Id from the image

3.1.2. Extracting the unique Id: The extraction procedure is the reverse of the hiding procedure. First the image from which the data is to be extracted is searched and then selected. Then from the rows of the image, characters of the unique ID are extracted in binary format. The data is stored in adjacent pixels of the row in LSB of pixels. These bits are collected together and are then converted to character format. This procedure is repeated for all the characters in the unique ID. Then all the characters are collected together and are then used to compare with the user entered unique ID. This is diagrammatically shown in figure 2.

4. Result

The System is tested under three criteria:

4.1. Recognition under static background

In this scenario, the images of person to be authenticated are taken with a static (white) background with a bright light source in front of him/her evenly illuminating their face. The pie chart showing the data gathered by making legitimate login attempts of 15 users with static background and even illumination is shown in figure 3.

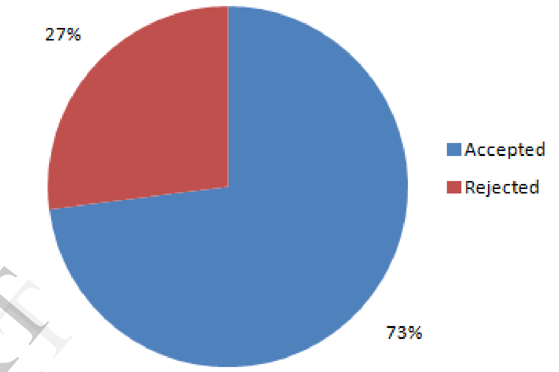

Figure 3. Face recognition done under static background

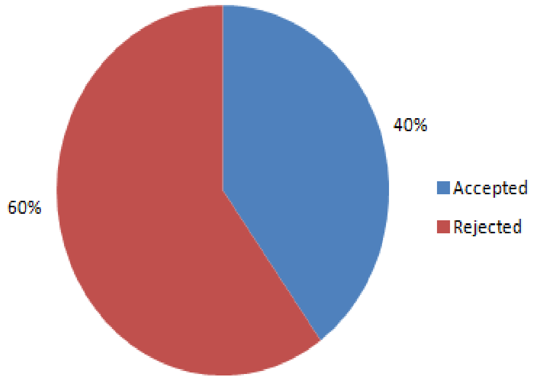

Figure 4. Face recognition done under variable background

4.2. Recognition under Variable Background

In this scenario, the images of person to be authenticated are taken with a variable (natural) background with no light source in front of the person.

Instead ambient light is used to illuminate the face of the person. Also the background is natural background and not a static white background as in previous scenario. The pie chart showing the data gathered by making legitimate login attempts of 15 users variable background and natural illumination is shown in the figure 4.

4.3 Overall authentication process

The whole authentication process consists of two phases that is face recognition phase and if it is cleared by the person then only the person should be ready for the second phase that is password phase. A person in order to pass through the authentication system needs to pass both these phases. Data is gathered by using login data of 15 users.

4.3.1. False login attempt. Here the user tries to login on some other user's login name thus trying to make a false login to the system. However as we are considering the entire system as whole in this case, even though the person bypasses the face recognition phase (Possibly the facial features might be same). The probability of the false user knowing the password of the legitimate user is negligible unless it is compromised by the user himself/herself. The pie chart below in figure 5 shows the data gathered.

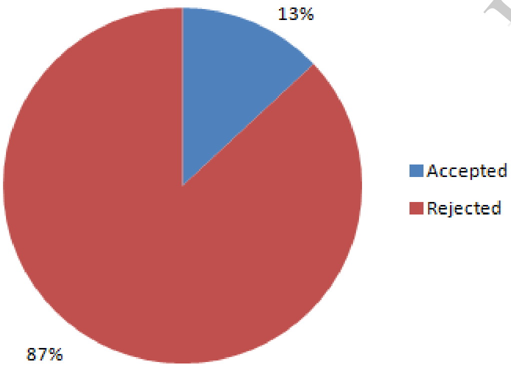

Figure 5. False login attempt

4.3.2. Valid login attempt. Here a legitimate user tries to login into the system. Being a legitimate user the system should accept the user and allow access to him/her. The pie chart below in figure 6 shows the data gathered.

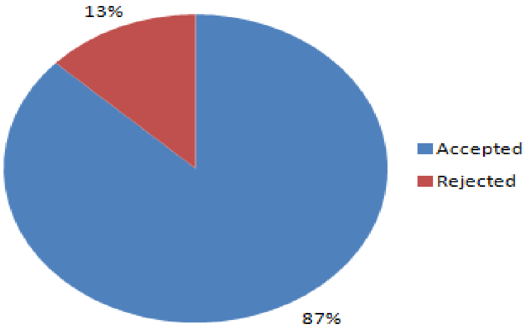

Figure 6. Valid login attempt

5. CONCLUSION

Thus two factor authentication system provides strong authentication as the person will be authenticated twice that is firstly on the basis of face recognition and then on the basis of unique Id. If both the factors are satisfied then only the person can access the system. In our system, we are not storing the unique Id instead we are hiding the unique id using novel method known as LSB stuffing .So there is no chance of unique id being stolen by anyone. This system can be used in the places where high degree of security is needed such as banks, lockers, colleges and government organizations.

6. ACKNOWLEDGEMENT

Sincere thanks to our guide Prof.Ravindra Patil who has immensely supported and encouraged us to complete this paper.

7. REFERENCES

[1] Kyungnam Kim, "Face Recognition using Principle Component Analysis", Department of Computer Science University of Maryland, College Park MD 20742.

[2] Wendy S. Yambor Bruce A. Draper J. Ross Beveridge, "Analyzing PCA-based Face Recognition Algorithms: Eigenvector Selection and Distance Measures", Computer Science Department Colorado State University Fort Collins, CO, U.S.A 80523.

[3] Hyeonjoon Moon and P Jonathan Phillips, "Computational and Performance aspects of PCA-based Face Recognition Algorithms 2001", Department of Electrical and Computer Engineering, State University of New York at Buffalo, Amherst, NY 14260.

[4]http://en.wikipedia.org/wiki/Principal_component_analysis