Real Time Enrollment System Using Two Way Authentication

Yash Sangani\textsuperscript{1}, Shraddha Yadav\textsuperscript{2}, Namaswi Chandarana\textsuperscript{3}, Veena Kulkarni\textsuperscript{4}

\textsuperscript{1}(BE student, Computer Engineering, Thakur College of Engineering of Technology/ Mumbai University, India)
\textsuperscript{2}(BE student, Computer Engineering, Thakur College of Engineering of Technology / Mumbai University, India)
\textsuperscript{3}(BE student, Computer Engineering, Thakur College of Engineering of Technology/ Mumbai University, India)
\textsuperscript{4}(Associate Professor, Computer Engineering, Thakur College of Engineering of Technology/ Mumbai University, India)

Abstract: Security is the primary requirement of every system and with the increasing organisation and the necessity of the secrecy of the information, level of security can be increased by having a powerful login system. The paper proposes design of Real time enrolment system using two way authentication which is a system in the form of desktop application. It is a system which can be used to enroll users to the organization with the help of biometric recognition and passwords. Two way authentication will use, first, face recognition technique to capture the image of the user and will store it as primary password and will also take in a keyboard based password as the secondary password. These passwords will be stored in a cloud database using LSB stuffing. Now, when the user will login to the system, the system will recapture his/her image and take the password. If the passwords match, user will gain access to the system.

1. Introduction

System and data security is the most important aspect people look into these days. Multinational firms are spending millions to make sure that their data is secured and doesn’t go into wrong hands. And these days, even individuals are worried about their privacy. Our project mainly focuses on providing individual’s the privacy they need using two-factor authentication which will protect the data of the user as well as the organization providing the services. Two-factor authentication is a security process in which the user provides two means of identification, one of which is a biometric identification or physical token you can say, and the other as a security code or password which can be easily memorized. In our project, the two types of user authentication which the system is using are what we are and what you know. Two Factor Authentication (2FA or TFA), also known as “multi factor authentication” gives you an extra layer of security, that doesn’t only requires a password and username but also something that only, that particular user has on them, that is, a piece of information(such as a physical token) only they should know or provide immediately at that time. When we use a username and password along with a piece of information that only the user knows makes it harder for potential intruders to gain access of the system and steal that user’s identity or personal data. Historically, two-factor authentication isn’t a very new concept but with the digital age we live in now, it is now widely accepted. Using a TFA process, we can help to reduce the number of cases related to identity theft on the Internet because the intruder would need more than just the username and the password.

2. Face Recognition

Biometric Recognition, i.e. face recognition, is the first authentication stage in this system. When a user tries to access the system first, its facial features are analyzed, only if the features of the person are matched with the one present in the database, the user will gain access to the next stage of the authentication. During the registration of the user, multiple images of user are captured of the user, in order to increase the efficiency of the recognition as well as increase the efficiency of the system. Humans usually use facial features to recognize a person as each and every person is gifted with different characteristics which can be easily used to identify a person. There various parameters which are looked into to perform the comparison with the image stored in the database and the image captured at the runtime of the user, who is trying to gain access. Parameters such as size of the face and the
distance between jaw, nose and eyes are majorly compared. In this system, to maintain a consistent size of the image, a predefined size is already provided to the system, for easy processing of the recognition in different computer systems.

We are using four steps to perform the face recognition. The four steps are capture, extraction, comparison and matching. In the capture stage, the images of the user are input using a webcam and stored in the format which the system requires to perform operation. In the extraction stages, the features of the face such as eyes noses and mouth are extracted from the captured image. In the extraction stage, the extracted features are compared with the features stored in the computer of the desired user. In the matching stage, the system makes a decision whether the user, trying to gain access to the system is a genuine user. Some facial recognition algorithms identify facial features by extracting landmarks, or features, from an image of the subject's face. For example, an algorithm may analyze the relative position, size, and/or shape of the eyes, nose, cheekbones, and jaw. These features are then used to search for other images with matching features. These steps have been performed in the system using principal component analysis. PCA is the simplest of the true Eigen vector based multivariate analysis. Mathematically, it is an orthogonal linear transformation that transforms the data to a new coordinate system. The use of Eigen faces and vectors is commonly called as Principal Component Analysis. With PCA, the image must be used of same size and they are normalized to a particular size for the usage. In PCA, dimension of data is reduced and decomposes the face structure into orthogonal and uncorrelated components which are the Eigen faces. The face image can be represented as a weighted sum of the Eigen faces. Mathematically, principal component analysis approach converts a set of correlated variables into a set of linearly uncorrelated variables. Each face image in the training set contributes to the eigenvectors. This can be displayed as an Eigen face expresses the data in such a way as to highlight the similarities and differences. Eigen faces are look like ghostly faces and each of them has some variations which deviate from the original image. If an Eigen face with small Eigen values are neglected, then the image will be a linear combination of reduced number of that faces[1][4].

3. Password

The second stage of authentication uses the ideology of what the user knows. The user will have to enter password which was set during its registration. We are using a technique known as LSB stuffing to hide data into a host image in the form of plain text. 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 from the corresponding image of the person stored in the face database. 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.

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. The figures below shows the idea of how the LSB stuffing is carried out. Fig.1 shows an example of the complete image and password which will result into an image with password hidden in the last column of the captured image. Fig.2 gives similar representation of the process of hiding the password in the image.

![Image](Image1.png)

**Fig.1**

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

![Image](Image2.png)

**Fig.2**
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.[2][5].

4. Conclusion and Future Scope

The proposed project i.e. ‘Real Time Enrolment System Using Two Way Authentication’ is intended towards providing strong security to the system and facilities where it will be implemented and thus safeguards the data which is to be secured more efficiently.

The face recognition part of the system uses the persons face to authenticate him and grant access to the system which is an asset that cannot be replicated and thus making it difficult for the attacker to enter the system. More over the unique ID of the user which is stored in a quiet new and novel way into the images of the person also makes the system more secure from attackers as it is difficult to extract the ID from images without the knowledge of where it is stored.

Such a system can be implemented to provide authentication based security in places such as Airports, Military bases, Government offices, Banks and even colleges and other organizations where there are some rooms. The proposed project can be extended with future scope being implementation of more rigorous authentication mechanism with multiple checks performed on the face before authenticating the person. Complex algorithms can also be used for face recognition. It can be further extended on the method of storing Unique ID in more random manner so that the work of the attacker in extracting the Unique ID becomes even more difficult.

Moreover, a feature can be added to the system which can store the images of the user on cloud or cloud platform storage. As the system stores all the data locally, we can add an extended feature which will upload the image files on cloud so that incase of failure or data loss, the backup of the files are already present on cloud.[4]

5. Acknowledgements

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

6. References