ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

A Haar casecade based Biometric Approach for Ensuring Secured Authentication.

Vijayapriya V, Bala Krishnan R*, Rajesh Kumar N, Raajan NR, Meganathan S.

Department of CSE, SASTRA University, Tamil Nadu, India

ABSTRACT

In order to avoid fraudulent activities, face recognition method is used widely now-a-days. The proposed method deals with real time human face detection using Haar casecade. It is an automated system model for human face recognition in a real time background. It reads the features from the human face and performs the comparison in the background using the Haar casecade features to decide the user authentication. From the experimental observations, it is established that this biometric approach assures accuracy in terms of detecting the human face through the biological features and grants access for the eligible users.

Keywords: Haar casecade, Face Detection, Authentication, Data accuracy.

**Corresponding author*

INTRODUCTION

The terminology 'Authentication' plays the lead role in restricting the resources access from authorized and unauthorized users. Existing authentication systems deals from password based model to biometric authentication models [1- 4]. Passwords are simply the collection of characters from keyboard. They authenticate the users on the systems to access the available resources on the basis of the user rights. In order to get access over the resources, the user needs to prove our identity through a confidential data possibly the secret key. To ensure our privacy over the data, the users need to keep the secret key. They also implement non- renunciation, keeping the users from later refusing the cogency of transactions attested with the secret key. The username identifies the name of the user and the password decides the access rights of the user over the environment. The major drawback over the existing model is that the secret keys (password) have some weaknesses: more than one person can use the password at a time to access the resources. Moreover, there is a incessant threat of missing the secret key because of the malicious intent. Secret key stealing can be done regularly by the hackers. Hence the protection of the secret key plays the lead role in restricting the unauthorized access of the resources [5-6]. Some of the existing systems deal with multiple keys and random keys also [4-5]. The proposed system deals with offering a secured learning system through biometric signatures of the users. The biometric signature is the face based features of the users; it decides the access rights of the users for accomplishing the secured authentication. The rest of the paper is organized as follows: Section 2 presents the proposed model, section 3 presents the experimental outcomes and conclusion is presented in Section 4.

Proposed System

Even though it is easy to follow traditional approaches like text based mechanisms for authentication systems, there is a possibility for the occurrence of fraudulent behaviour in authentication. (i.e) An intrusive attack by an intruder by simply guessing the password of an authorized user. To identify and to avoid the illegal penetration the proposed model is introduced with biometric authentication mechanisms.

The proposed mechanism introduces three modules for the implementation of this secured authentication system. The first module deals with human face registration along with text based secret key registration for accessing the E-Learning portal. The devised E-Learning portal is a learning facilitator which includes study materials for the courses. In order to access the benefits of the portal the students / users need to login into the system. The available data inside the portal has been classed into various categories. The categories are Admin User and Student User. The functionalities of the users are as follows:

Admin User: Add the new user details and upload the necessary course related learning materials along with the user type. The Admin user also having the provision / rights to approve the registered user and they can delete the user.

Student User : Needs to register their face along with the registration details such as name, registration number, class, course etc., and for accessing the documents from their corresponding login they need to login through their user name, password and their face input. The haar cascade features get extracted from the received face input to decide the user authentication. The authorized users along can login to the portal and access their respective materials. The registration procedure has been stated in the Figure 1.

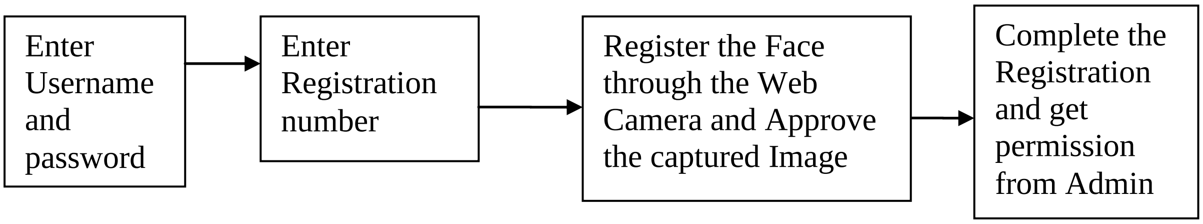
Enter Username and password
Enter Registration number
Register the Face through the Web Camera and Approve the captured Image
Complete the Registration and get permission from Admin

Figure 1: Steps involved in the Registration Procedure

The groups of the users and the Sample set of the Portal data along with the users' access rights are stated in the Table 1.

Table 1. Details of the E-Learning Portal User with available resources

S.No	Users	Materials Category
1	Administrator	All
2	Student User (Arts)	Access All Arts Course Materials
3	Student User (Engineering)	Access All Engineering Course Materials
4	Student Arts + Engineering	All Training and Placement Materials

The Procedure of the proposed model is stated below:

Step 1: Webcam is turned on.
Step 2: Detect the facial features using Haar-like features.
Step 3: Sum of the pixels in white area is subtracted from the sum of the pixels in black area.
Step 4: This gives a single value as output.
Step 5: It is stored in the database.
Step 6: Recognize the new face which is given through webcam as input.
Step 7: Then the images are matched with the image in database with reference to username and password.
Step 8: If the image matches user is allowed to enter into the portal and can access the corresponding materials.

Haar casecade:

It is a series of "Haar like features" that are combined to form a classifiers. Each feature is a single value obtained by subtracting sum of pixels under white rectangle from sum of pixels under black rectangle and is stated in Figure 2 and the Haar needs two features to form a classifier. It is a mathematical function that actually produces square wave output and it works by Picks a scale for each feature, Slide it across the image and compute the average pixel values under the white area and black area. If the difference between these areas satisfies the threshold, the feature matches with the captured content.

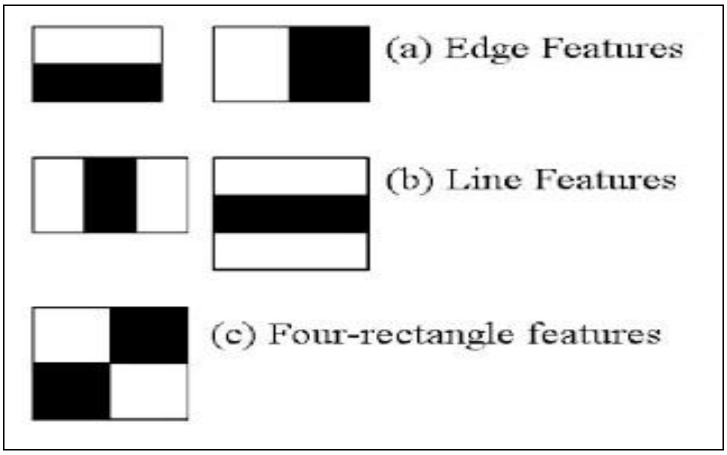

Figure 2: Representation of Haar Like Features

EXPERIMENTAL RESULTS

The proposed server application has been implemented in Windows platform and runs the Server using Apache Tomcat version 7 and the client application is implemented using Java Server Pages. The Login Screen for the Student user is depicted in the Figure 3.

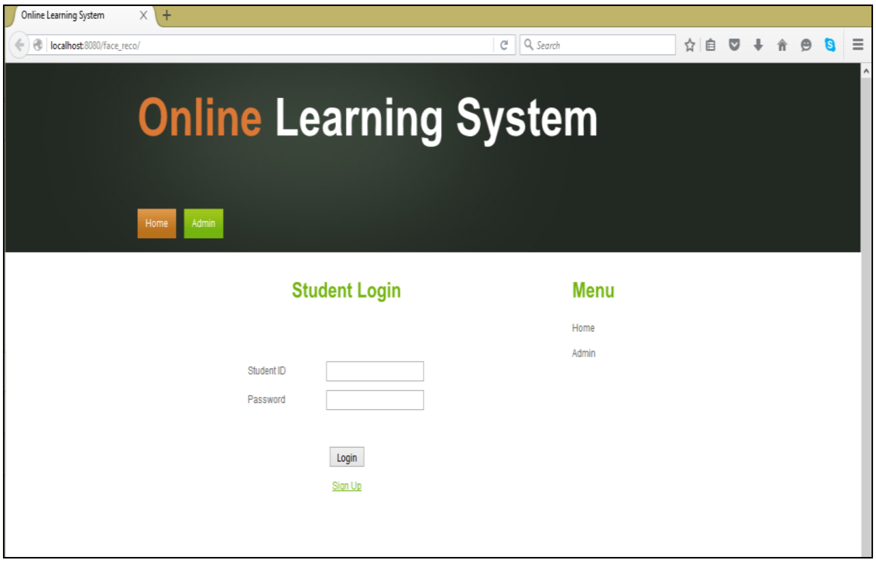

Figure 3: Login Screen for the Student User

The Face Detection module reads the user face and password and matches the face with the available images and password in the database and the similarity between the images are identified and on the basis of the similarity the application either permits or rejects the user. The face detection screen is stated in Figure 4.

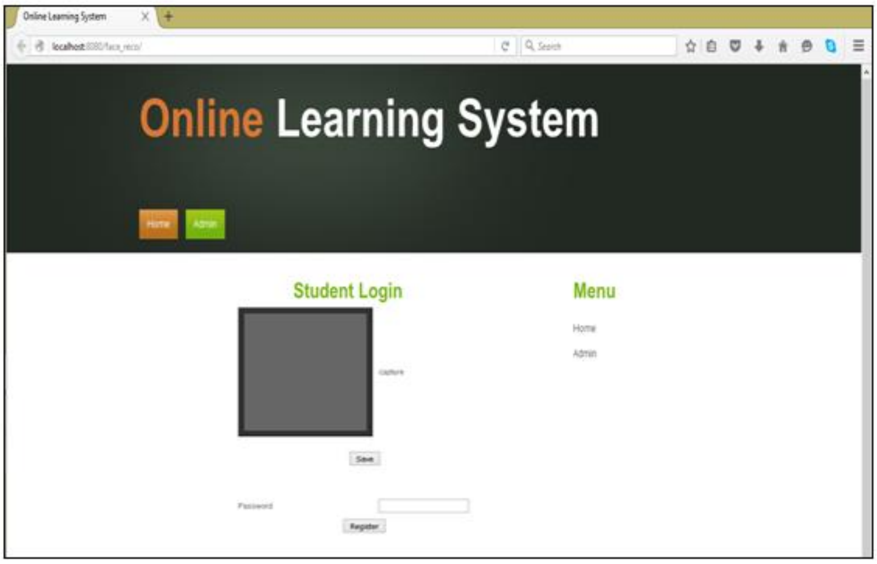

Figure 4: Face Capturing Module Screen for the Student User

CONCLUSION

The proposed system here is a Secured Biometric based Login System for achieving privacy in an E-Learning Portal. The proposed model classes the users' on the basis of their access rights and offers the exact right document or material to the right user by verifying the text based identity along with the strong biometric identify. Hence through this model the illegal access over the E-Learning portal and Intrusion would be avoided. Hence the performance of the system would be improved. In future this approach can be used to detect the users with other biological features.

REFERENCES

[1] Raajan NR, Shiva G, Vijayabhaskar PVM, Mithun P. And Raj PJ. Research Journal of Information Technology 2013; 5(3): 462-467.

[2] M Turk and A Pentland. Journal of Cognitive Neuroscience 1991; 3(1): 71-86.

[3] R Bala Krishnan and NR Raajan. Far East Journal of Electronics and Communications 2016 Special Issue; I:121 – 131.

[4] D Narasimhan et al. IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT-2015) IEEE Xplore Digital library 2015:1-5.

[5] R Bala Krishnan et. al., Far East Journal of Electronics and Communications, Special Issue; I: 179 - 187.

[6] Sung-Hoon Hong, Jae-Won Lee, Ramesh Kumar Lama and Goo-Rak Kwon. Multimedia Tools and applications 2016; 75(12): 6717-6735.