



iJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 Issue: IV Month of publication: April 2018

DOI: <http://doi.org/10.22214/ijraset.2018.4067>

www.ijraset.com

Call: ☎ 08813907089

E-mail ID: ijraset@gmail.com

“Implementation of Biometric Based Authentication System”

Bhagyashri Budhe¹, Prof. Rashmi Jain²

^{1, 2} Computer Science & engineering, Rashtrasant Tukadoji Maharaj Nagpur University.

Abstract: Security is the basic requirement for the today's world. Everything is connected to internet and there is very basic need for the confidentiality of data. If someone stole user's credentials, then he/she will be able to access personal data of user. Traditional way of securing the system is only by using password and it is not so secure in today's world. So now the focus is diverted towards the high secure module for securing the one's credentials that do not rely exclusively on some sequence of characters. So, in this paper we proposed a system based on Biometric authentication where a real time image is captured and compared with our database image and authentication is done on the basis of that only. Biometric authentication provides a secured platform to protect our confidential data. For more security of credentials of user, we are using encryption and decryption algorithm and biometric face authentication. For the detection of image and matching of image with the stored image Viola Jones and Hamming distance algorithm are used respectively.

Keywords: Face detection, Face recognition, Viola Jones, Hamming distance

I. INTRODUCTION

Authentication is a critical part of any trustworthy computing system; it ensures that only individuals with verified identities can log on the system or access system resources. In addition, authentication also serves as the first step for many other security purposes, such as key management and secure group communication. Passwords or smartcards have been the most widely used authentication methods due to easy implementation and replacement; however, memorizing a password or carrying a smartcard, or managing multiple passwords/smartcards for different systems (one for each system), is a significant overhead to users. In addition, they are artificially associated with users and cannot truly identify individuals. More seriously, they can be lost or stolen, resulting in impersonation and other security breaches.

Traditionally based on something that one has (key, magnetic or chip card) or one knows (PIN, password), identity verification has achieved more reliable verification and identification well-known as biometrics [1]– [2]. One of the most natural biometric is face recognition. Mostly developed for surveillance camera in public places, researchers tend to develop biometrics application in order to achieve higher degree of security. Universality, uniqueness, permanence, measurability, and performance are following factors need to be satisfied by biometric identifiers [3]. Face recognition's ability to identify a person without the object's cooperation has made face recognition as one of the most considered biometrics applications despite face recognition lack of uniqueness and performance compared to other biometrics applications.

As a result, biometrics is becoming a promising authentication/identification method because it binds an individual with his identity and overcomes the main shortcomings inherent in the use of passwords and smartcards. Biometrics is a technology which uses physiological or behavioral characteristics to identify or verify a person. Typical characteristics used for authentication include fingerprint, face, and iris. Here in this work we are using Face for the biometric authentication and encryption and decryption is used to encrypt or decrypt the credentials.

A conventional biometric authentication system consists of two phases: enrollment and verification. During the enrollment phase, a biometric feature set is extracted from user's biometric data i.e. image is captured during the registration process and a template is created and stored. During the verification phase, the face is detected using the face detection algorithm and the face is matched with the stored database image using the matching algorithm and the credentials are also encrypted for providing the more security to the system. The query template is matched against the stored template(s) for authentication. Compared to password/smartcard-based authentication approaches, biometrics-based solutions have many desired features such as being resistant to losses incurred by theft of passwords and smartcards, as well as user-friendliness. Biometrics bears a user's identity and it is hard to be forged.

II. LITERATURE REVIEW

Over the years many contributions were done to the field of face detection and recognition. G. Yang came up with Multi resolution rule method. This knowledge based method used the structural nature of the face for detection [4]. Feature based method uses the

facial features [5][6], skin color [7][8] and combined multiple features [9] of the face for better accuracy and detection speed. In order to increase the detection speed, the accuracy is sacrificed. For this, a steady and uniformly scaled images using template matching method was employed. Predefined face templates [10] and deformable templates [11] were incorporated which was completely based on the template (a predefined structure) without using learning. Appearance based methods gives faster detection speeds, more accurate results and adaptive nature that could distinguish a face from a non-face in any environmental conditions. Neural networks [12] is commonly used model for getting the desired results.

A very fast and accurate approach to detect an object was devised by viola and Jones[18] in the year 2001. Nowadays, this method is used in cell phone cameras, security perimeters and also in our paper we are detecting face using viola jones method. Due to the use of Haar features and adaboost machine learning computational speed increased. And within a millisecond a face can be detected in a frame. Further improvements were done by Lienhart and Maydt [19] in the year 2002. In this method, firstly, the value of all pixels in greyscale images which are in black accumulated. Then, they subtracted from the total of white boxes. Finally, the result will be compared to the defined threshold and if the criteria is met, the feature considers a hit.

III. PROPOSED WORK

First we collect user's data at the time of registration and also capture its multiple facial images. This data and images are stored in database in encrypted form. Whenever the user login along with the credentials we again capture the image of user's face and we compare that current image of user with stored database images. If its credentials and image both matched, then the system allows user to login workspace.

In this work we proposed secured authentication for processing and securing our data. Firstly, we took all the user's registration details and then we encrypt the user's credentials using the DES Algorithm so that encrypted data is stored in the database.

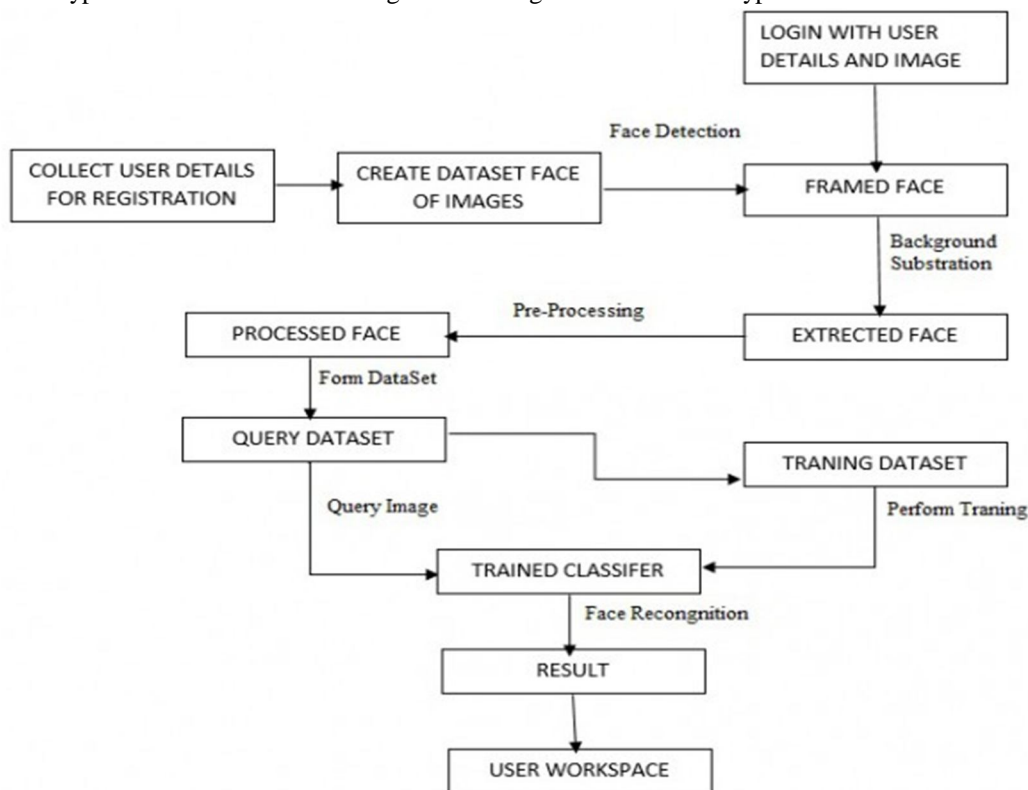


Fig.1 Block Diagram of System

The main parts of the algorithm are as follows:

- 1) Fractioning of the text into 64-bit (8 octet) blocks;
- 2) Initial permutation of blocks;
- 3) Breakdown of the blocks into two parts: left and right, named *L* and *R*;
- 4) Permutation and substitution steps repeated 16 times (called **rounds**);
- 5) Re-joining of the left and right parts then inverse initial permutation

Now, we take the image of user during registration and stored that image in a folder and encrypted folder name and stored in the database. When user login then he/she need to take the current image of face and that image is compared with the image which is taken during the registration. If this image matched with the stored image, then user able to login into the system.

For this detection of face we are using viola jones algorithm. Viola jones algorithm uses the 4 steps for detection of face:

A. First it detects the simple rectangular features, called Haar-like features.

Haar like features are used to detect variation in the black and light portion of the image. This computation forms a single rectangle around the detected face. Based on the color shade near nose or forehead a contour is formed. Some commonly used

Haar features are:

- 1) Two rectangle feature.
- 2) Three rectangle feature.
- 3) Four rectangle feature.

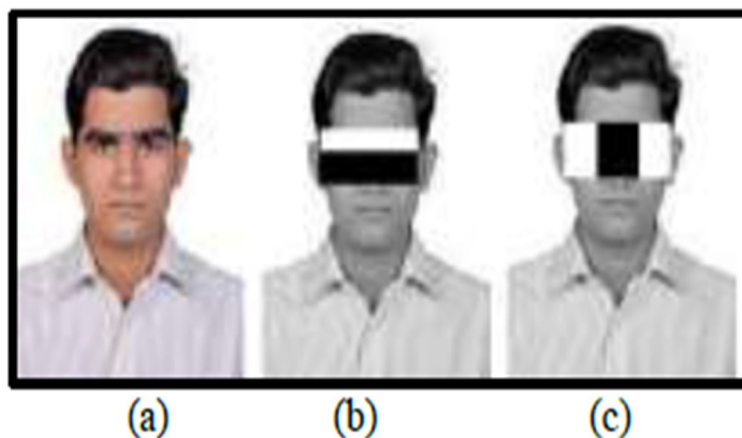


Fig.2 Viola Jones detects features

B. Also uses Integral image for rapid features detection.

C. It uses AdaBoost machine-learning method.

D. Then cascade classifier to combine many features efficiently A. Haar like features Haar like features are used to detect variation in the black and light portion of the image. This computation forms a single rectangle around the detected face. Based on the color shade near nose or forehead a contour is formed.

After the detection of face we need to match the facial image with the stored database image. There is the basic requirement for the matching of image in any biometric authentication. For this matching of image, we are using hamming distance method.

In hamming distance algorithm there are following steps involved in it:

- 1) First we took the current image and stored database image and use resize function to resize our images according to the requirement.
- 2) Then we convert the colored images into black and white images i.e. RGB to gray.
- 3) Now we convert the gray scale images into binary format. Then these binary format images compared with each other.
- 4) Ensure the two strings are of equal length. The Hamming distance can only be calculated between two strings of equal length. String 1: "1001 0010 1101" String 2: "1010 0010 0010"
- 5) Compare the first two bits in each string. If they are the same, record a "0" for that bit. If they are different, record a "1" for that bit. In this case, the first bit of both strings is "1," so record a "0" for the first bit.
- 6) Compare each bit in succession and record either "1" or "0" as appropriate. String 1: "1001 0010 1101" String 2: "1010 0010 0010" Record: "0011 0000 1111"
- 7) Add all the ones and zeros in the record together to obtain the Hamming distance. Hamming distance = $0+0+1+1+0+0+0+0+1+1+1+1 = 6$
- 8) We have set the threshold hamming distance i.e. 20 if the hamming distance is smaller than 20 then the image is matched if it is greater than the 20 then the image is not matched and the login is discarded.

IV.RESULT

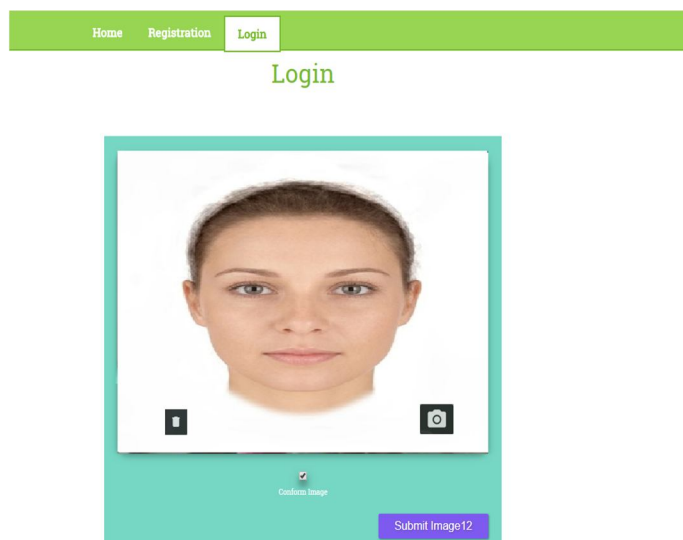
This project consists of two modules registration and login module. Below fig shows Registration module. To use this biometric system first user has to register with its details and image.



The screenshot shows a web browser window with a green navigation bar containing 'Home', 'Registration', and 'Login' links. The 'Registration' page has a teal background and contains the following fields: Name (text input), Gender (radio buttons for Male and Female), EmailId (text input), Password (text input), DOB (text input with placeholder 'dd/mm/yyyy'), and MobileNo (text input). Below these fields is a placeholder for a user image. At the bottom of the form are 'Reset' and 'Submit Form' buttons.

Fig.1- Registration Form

After registration is successful. The system will have to create image dataset of that particular user. For creation of dataset, user will upload 12 real time images.



The screenshot shows the 'Login' page with a green navigation bar. Below the navigation bar is a large image placeholder for a user's face. At the bottom of the image placeholder is a 'Confirm Image' checkbox and a 'Submit Image12' button.

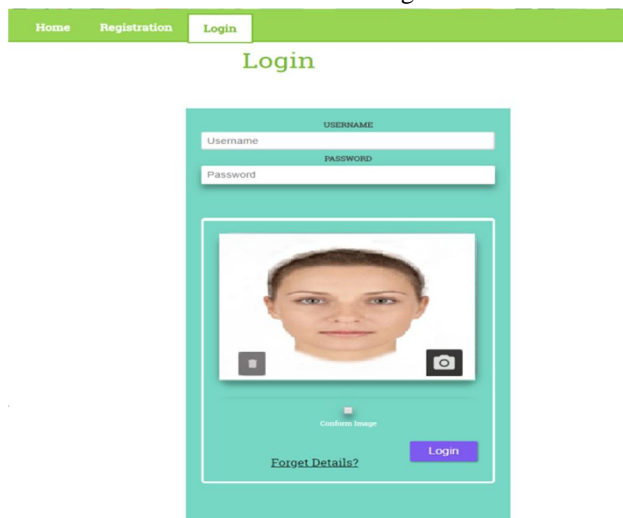
Fig.2-Creating Image Dataset

After uploading images, one by one image will pass to matlab for feature extraction. Each image will have converted to gray scale image and stored in database. Below Figure shows images stored in database.



Fig.3-Image Dataset

Now, user can login through Login module which is shown below. For login user has to enter his/her details and its real time image.



The screenshot shows a web application interface with a green navigation bar containing 'Home', 'Registration', and 'Login' links. Below the navigation bar is a 'Login' heading. The main content area is a light blue box containing a 'USERNAME' field with a 'Username' placeholder, a 'PASSWORD' field with a 'Password' placeholder, a real-time video feed of a person's face, a 'Confirm Image' button, a 'Forget Details?' link, and a 'Login' button.

Fig.4-Login Form

Before passing this real time image for matching we have to extract features and detect face. After feature extraction the image will convert to gray scale image. If the real time image matched with the images stored in database user can login to system.

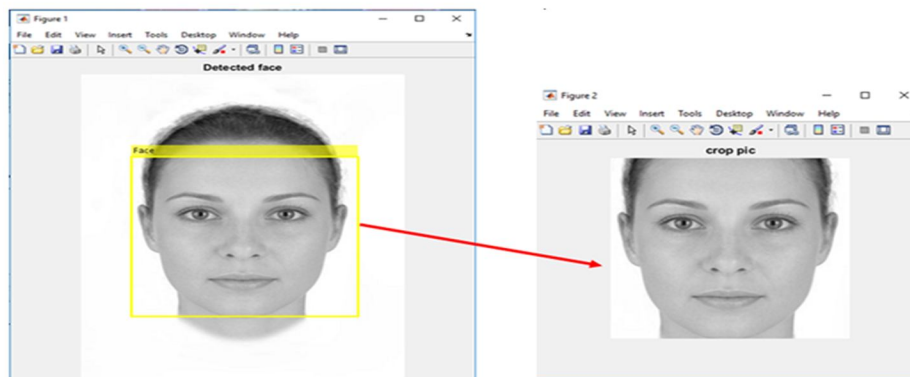


Fig.5 – Face Detection

After login user will see welcome page and there are different options like drive, upload files, update profile as shown in figure.



Welcome to BioMetric Security System

A face recognition system is a computer application capable of identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a face database. It is typically used in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems. Recently, it has also become popular as a commercial identification and marketing tool.



Fig.6 – Welcome Page

Upload file option is used to upload user's confidential data which he/she wants to secure. We can upload MS word documents, PPT's, PDF, Images, Videos, etc.

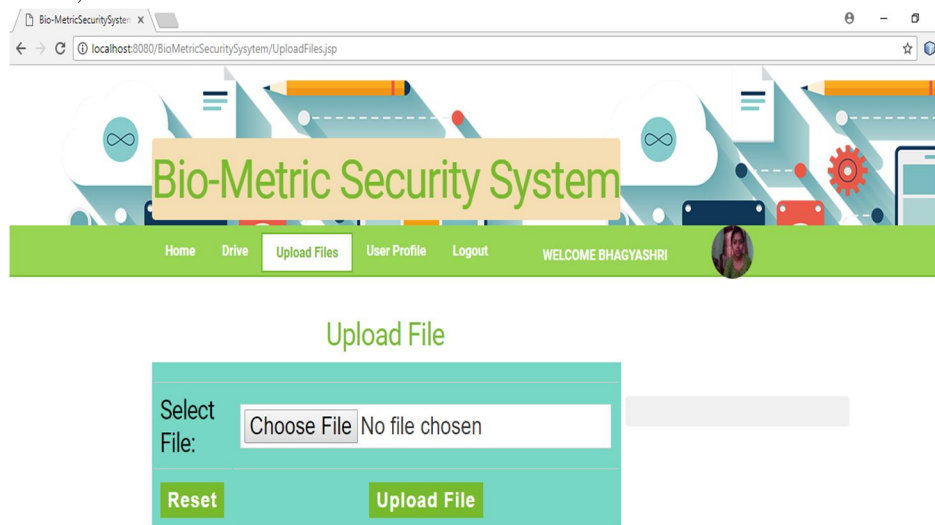


Fig.7 – File Upload Page

The all uploaded data store in Drive and we can access it any time. There are three options in drive view, download and delete.



Fig.8-Stored Files

V. CONCLUSION

In this paper, we developed a system to evaluate the face detection and face recognition methods. This method signifies the importance and utility for different applications. Since this method is progressive, more and more advancements are made every day to achieve accurate and true face detection. For applications such as employee details, member details and criminal record uses the frontal views of the face. This proposed face detection biometric system uses viola jones technique for detection of face and hamming distance algorithm for face recognition is efficient and secure. Also hamming distance algorithm is not affected by the noise, it can handle scaling and it is able to the transform into matrix which the basic need for the matching of any shape.

REFERENCES

- [1] Hsu, Rein-Lien, Mohamed Abdel-Mottaleb, and Anil K. Jain. "Face detection in color images." *Pattern Analysis and Machine Intelligence*, IEEE Transactions on 24.5 (2002): 696-706.
- [2] A.S. Georgiades, P.N. Belhumeur, D.J. Kriegman, From few to many: illumination cone models for face recognition under variable lighting and pose, *IEEE Trans. Pattern Anal. Mach. Intell.* 23 (6) (2001) 643–660.

- [3] MayankChauha and MukeshSakle.—Study & Analysis of Different Face Detection Techniques,| International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014, 1615-1618.
- [4] G. Yang and T. S. Huang, —Human Face Detection in Complex Background,| Pattern Recognition, vol. 27, no. 1, pp. 53-63, 1994.
- [5] T.K. Leung, M.C. Burl, and P. Perona, —Finding Faces in Cluttered Scenes Using Random Labeled Graph Matching,| Proc. Fifth IEEE Int'l Conf. Computer Vision, pp. 637-644, 1995.
- [6] K.C. Yow and R. Cipolla, —Feature-Based Human Face Detection,| Image and Vision Computing, vol. 15, no. 9, pp. 713-735, 1997.
- [7] J. Yang and A. Waibel, —A Real-Time Face Tracker,| Proc. Third Workshop Applications of Computer Vision, pp. 142- 147, 1996.
- [8] S. McKenna, S. Gong, and Y. Raja, —Modelling Facial Colour and Identity with Gaussian Mixtures,| Pattern Recognition, vol. 31, no. 12, pp. 1883-1892, 1998
- [9] R. Kjeldsen and J. Kender, —Finding Skin in Color Images,| Proc. Second Int'l Conf. Automatic Face and Gesture Recognition, pp. 312- 317, 1996.
- [10] I. Craw, D. Tock, and A. Bennett, —Finding Face Features,| Proc. Second European Conf. Computer Vision, pp. 92-96, 1992
- [11] A. Lanitis, C.J. Taylor, and T.F. Cootes, —An Automatic Face Identification System Using Flexible Appearance Models,| Image and Vision Computing, vol. 13, no. 5, pp. 393-401, 1995.
- [12] H. Rowley, S. Baluja, and T. Kanade, —Neural NetworkBased Face Detection,| IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 20, no. 1, pp. 23-38, Jan. 1998.
- [13] Sharifara, Ali, et al. "A general review of human face detection including a study of neural networks and Haar feature-based cascade classifier in face detection." Biometrics and Security Technologies (ISBAST), 2014 International Symposium on.IEEE, 2014.
- [14] Zhengming Li; LijieXue; Fei Tan, "Face detection in complex background based on skin color features and improved AdaBoost algorithms," Progress in Informatics and Computing (PIC), 2010 IEEE International Conference on , vol.2, no., pp.723,727, 10-12 Dec. 2010.
- [15] Campadelli, Paola, RaffaellaLanzarotti, and Chiara Savazzi. "A feature-based face recognition system." Image Analysis International Journal of Computer Trends and Technology (IJCTT) – volume 25 Number 1 – July 2015 ISSN: 2231-2803 <http://www.ijcttjournal.org> Page 61 and Processing, 2003. Proceedings.12th International Conference on.IEEE, 2003.
- [16] Yang, Ming-Hsuan, David J. Kriegman, and Narendra Ahuja. "Detecting faces in images: A survey." Pattern Analysis and Machine Intelligence, IEEE Transactions on 24.1 (2002): 34- 58.
- [17] Xiaowei Zhao, Xiujuan Chai , "Context Constrained Facial Landmark Localization Based on Discontinuous Haar-like Feature" International Conference on Computer Vision (ICCV2013),2013. [18] Paul Viola, Micheal Jones, "Rapid object detection using a Boosted Cascade of Simple features" CONFERENCE ON COMPUTER VISION AND PATTERN RECOGNITION, 2001 .
- [18] Lienhart and J. Maydt. An Extended Set of Haar-like Features for Rapid Object Detection. IEEE ICIP 200



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)