IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Issue-10, Oct 2019 E-ISSN: 2347-2693

A Proposed Model of Advanced Security System in ATM: Implementation of Face Recognition and Finger Print Recognition

Jufishan Boksha[1*], Romita Mondal[2], Soumi Mitra[3], Asoke Nath[4]

[1,2,3,4]Department of Computer Science, St. Xavier's College (Autonomous), Kolkata, West Bengal, India

*Corresponding Author: jufishanb@gmail.com, Tel.:8583980490

DOI: https://doi.org/10.26438/ijcse/v7i10.1520 | Available online at: www.ijcseonline.org

Accepted: 09/Oct/2019, Published: 31/Oct/2019

Abstract- ATM is an essential part of every human life as it enables the customer of a bank to perform financial transactions at any time and without the direct interaction with the bank employees. But, with the increase in the use of ATM, the machines are being prone to hacker attacks, fraud, robberies and security breaches. False keypad, hidden cameras are being used to get the account information and PIN of a user which lead to card cloning or skimming. In this paper, the authors introduce a fast and robust method for the advancement of ATM security which applies a combination of face recognition and fingerprint recognition system as biometric customer authentication and thereby obsoletes the use of PIN. In this method, after the user inserts the card in the card reader, his/her face undergoes the detection and matching process using PCA face detection and recognition algorithm with Eigenfaces method. If a match occurs, the user's fingerprint is scanned and matched using Minutiae based matching algorithm. If the result comes positive, the user is allowed to process the usual transaction. The experimental results carried out with a laptop webcam and a commercial fingerprint scanner, illustrates the robustness and efficiency of the approach even in low light environments. The challenges and limitations faced during the research and some suggestions for future research directions are also discussed in this paper.

Keywords-ATM Security, face recognition, fingerprint recognition, biometric, PCA, Minutiae.

I.INTRODUCTION

At the present time, ATM has become a vital part in a majority of human life. By using ATM, any customer of a bank who has a valid ATM card can perform financial transactions such as cash withdrawal, deposit, balance checking etc. at any time in any place. With the 24*7 availability and ease of use, the number of ATM users is increasing day by day. Despite having high security measures, ATM machines are prone to hacker attacks, fraud, robberies and security breaches. Different types of digital attacks such as keyboard attack, shimming, and skimming network based attacks are done in ATMs. Use of fake card reader, keyboard, and hidden cameras to steal user's information has increased. Most of the ATM attacks are done using the PIN of a user. The main objective of this paper is to obsolete the use of PIN. As biometric is the safest method, the authors used two different biometric methods and combined them in order to create a secure method for ATM transaction. In this paper, the authors introduced a fast and robust method for the advancement of ATM security which applies a combination of face recognition and fingerprint recognition system as biometric customer authentication and thereby obsoletes the use of PIN. In this method, after the user inserts the card in the card reader, his/her face is detected and matched with the face detection and recognition algorithm using PCA which is based on Eigenfaces method. If a match occurs, the user's fingerprint is scanned and matched using Minutiae based matching algorithm. If the result comes positive, the user is allowed to process the usual transaction.

Rest of the paper is organized as follows – section I contains introduction, section II contains literature survey, section III contains design, section IV contains proposed methodology, section V contains results and discussion, section VI contains limitations and section VII contains conclusion and future scope.

II. LITERATURE SURVEY

Here some of the advance ATM security methods still in use, across the globe are discussed briefly:
1.PIN (Personal Identification Number): It is a 4-digit security code to verify the user's identity. It is easy to hack.

2.Fingerprint Sensor: It is a biometric process, where the pattern of the user's fingerprint gets scanned and verified with the one stored in the database of the bank. Fraudsters can steal or copy PIN, but they cannot do the same with fingerprint. But there are some disadvantages like a person's finger changes size and form/pattern over time and the fingerprint scanner prevents the user to gain access. Another problem is that if a person's finger contains moisture then the scanner will not detect it correctly.

3.Chip Enabled Cards and EMV Cards: These are smart cards that store their data on an integrated circuit in addition to the magnetic strips.

4.OTP with Fingerprint: The primary step is to verify currently provided fingerprint with the fingerprint which is registered in the bank's database. If the two matches, then an OTP (One Time Password) of 10-digit unique number will be sent to the registered mobile number. The problem with this technique is if any time the network traffic increases, then the OTP will take time to reach the registered mobile number.

5.OTP with Face Recognition: Face recognition helps the machine to identify each and every user uniquely, thus making face as a key, which completely eliminates the chances of fraud due to theft and duplicity of ATM cards. The randomly generated OTP frees the user from remembering PINs as if it acts as a PIN. But here also, as the OTPs are used, the disadvantages remain same.

III.DESIGN

1. Enrollment

In this phase, face image of the user is captured with a visual unit (camera) and processed in a form that can be used in recognition process. It involves:

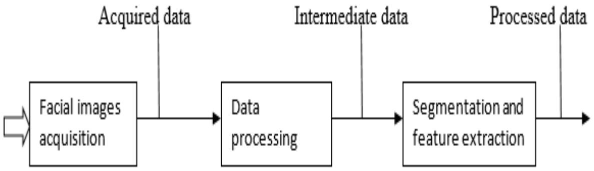

Acquired data
Intermediate data
Processed data
Facial images acquisition
Data processing
Segmentation and feature extraction

Figure 1: Functions of the Face Recognition system

After that user's fingerprint is scanned with a fingerprint scanner and stored in the data container. It involves:

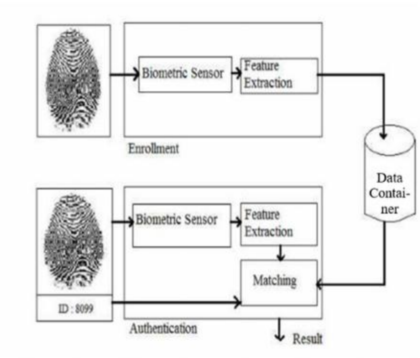


Figure 2: Functions of the Fingerprint Recognition system

2. ATM Transaction

In this phase, the user enters his/her unique id and the retrieved id is sent to software. The image of the user is captured and sent to software to match with the one stored previously. If recognized image's id is matched with the unique id, then the id is sent to the fingerprint module. The template corresponding to that unique id is occupied to match with the scanned fingerprint. If the images match, then the usual transaction takes place. The phase involves:

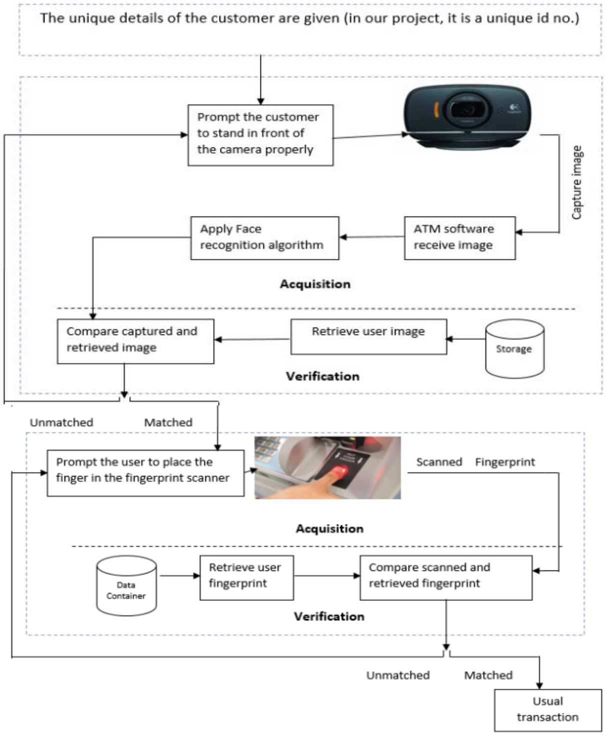

The unique details of the customer are given (in our project, it is a unique id no.)
Prompt the customer to stand in front of the camera properly
Capture image
Apply Face recognition algorithm
ATM software receive image
Acquisition
Compare captured and retrieved image
Retrieve user image
Storage
Verification
Unmatched
Matched
Prompt the user to place the finger in the fingerprint scanner
Scanned Fingerprint
Acquisition
Data Container
Retrieve user fingerprint
Compare scanned and retrieved fingerprint
Verification
Unmatched
Matched
Usual transaction

Figure 3: Different modules with acquisition and verification phases of the system

IV.PROPOSED METHODOLOGY

a) Face Recognition Algorithm

Face detection and recognition using principal component analysis (PCA) is based on the Eigenfaces approach (Holistic matching method) was introduced by Mark and Sirovich in 1987 (Zhao, 2003). Later on, it was successfully demonstrated by Turk and Pentland in 1991 which was also considered to as a great milestone of and automated face recognition technology in its history (Turk & Pentland, 1991).

The face recognition system is broken down into three major modules which are very crucial task to understand for the implementation of the system. The modules are:

- Face Detection & Normalization
- Training
- Face Recognition

Face Normalization And Detection
Step 1: In the normalization process, as the input image is passed through the system, it is first transformed into a grayscale image.

Step 2: Then the noise in the face images is reduced, in each of the face images, using 2-D median filtering.

Step 3: After that, histogram equalization algorithm is applied in each of the face images that will equalize the pixel intensities of each face images.

Step 4: Face detection method is based on the algorithm of Viola and Jones. As the Haar-Like features algorithm tells, hundreds of haar features are applied to an image. Based on the each haar features applied into an image subsection, their sum and difference are calculated and the result is passed to the cascade of classifiers which tells if the image sub-region contains any faces or not. If the face image is found, then the faces in the images are localized based on the image sub-region information. Similarly, if the faces are not found then the system automatically back-propagates the detection process changing the scale size of haar-features by 1.1 and again rechecks the faces with the same algorithm but in different scale of haar features. This allows the system to detect faces of multiple face size.

Step 5: Then the detected faces are cropped from the image, discarding the unnecessary background portion.

Step 6: After this the face images are resized to have same and fixed dimension for easy recognition. These new images will be later trained or projected for the face recognition procedure.

Training
A system is trained using pre-processed face images of the users.
Step 1: A Principle Component Analysis approach has been used in order to extract the face image features.

Step 2: The eigenfaces of the training set are calculated.

Face Recognition
A face recognition task begins after the completion of pre-processing step.
Step 1: A detected and normalized face image is further projected into the eigenspace for the recognition process of detected face.

Step 2: After the projection of detected faces a Euclidean distance is calculated comparing each of the eigenfaces stored in the training set.

Step 3: On the basis of Euclidean distance and a specified threshold, the method makes a decision of face being matched or not with the stored or trained face images.

Detailed explanation of the steps followed in the above-mentioned algorithm:

1. Haar-Like Features Algorithm [1]
2. 2-D median filtering
3. Histogram Equalization
4. Eigenfaces For Recognition [2]
5. Calculating Eigenfaces [2]
6. Recognition Procedure [2]

b) Fingerprint Matching Algorithm
Step 1: The template fingerprint image is read from the dataset using the unique id.

Step 2: The input fingerprint image is scanned using the fingerprint scanner and read.

Step 3: Step 4 to step 7 is repeated for both the template and input image.

Step 4: Binarization of the fingerprint image.

Step 5: Ridge thinning of the binarized image by block filter method.

Step 6: Minutiae data are extracted from the thinned image by considering a region of interest by using an ellipse and stored in a matrix.

Step 7: Post processing i.e. false minutiae are removed and final minutiae data are stored in a matrix.

Step 8: The feature matrices for template and input image is sent to the minutiae matching function and the matching score is calculated.

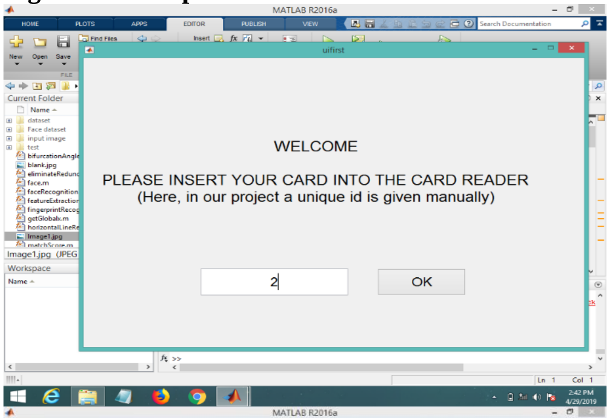
Step 9: If the matching score is greater than a threshold the two fingerprints match, otherwise they do not match.

Detailed explanation of the steps followed in the above-mentioned algorithm:

1. Image Acquisition
2. Image Binarization [3]
3. Ridge Thinning [3]
4. Minutiae Extraction [3]
5. Remove false minutiae [3]
6. Minutiae Matching [3]

V.RESULTS AND DISCUSSION

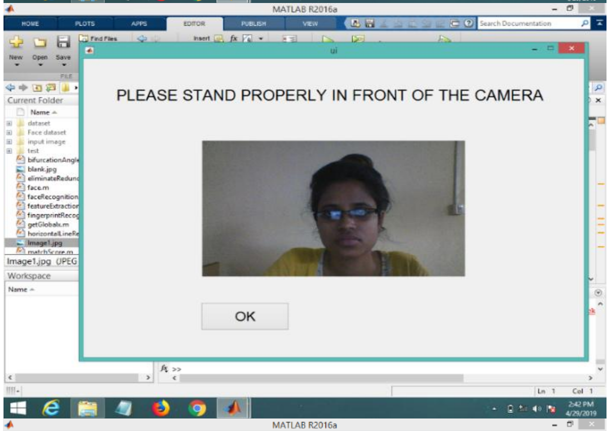
1. For successful face recognition and fingerprint recognition with spectacles on



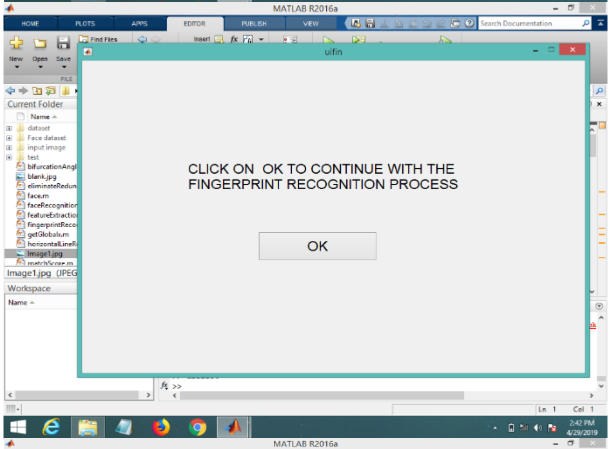
WELCOME

PLEASE INSERT YOUR CARD INTO THE CARD READER
(Here, in our project a unique id is given manually)

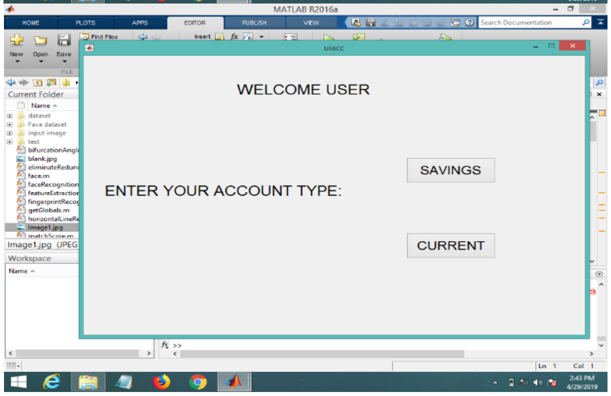
2



PLEASE STAND PROPERLY IN FRONT OF THE CAMERA



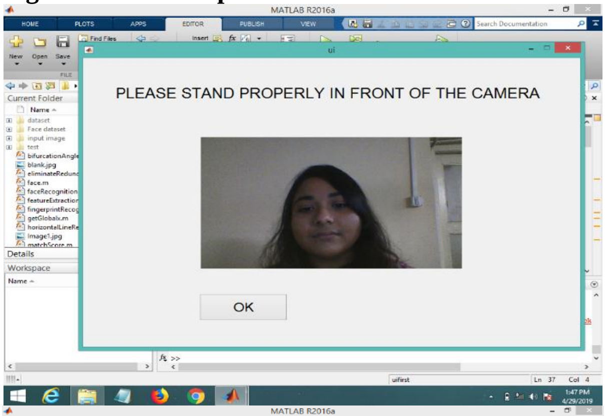
CLICK ON OK TO CONTINUE WITH THE
FINGERPRINT RECOGNITION PROCESS



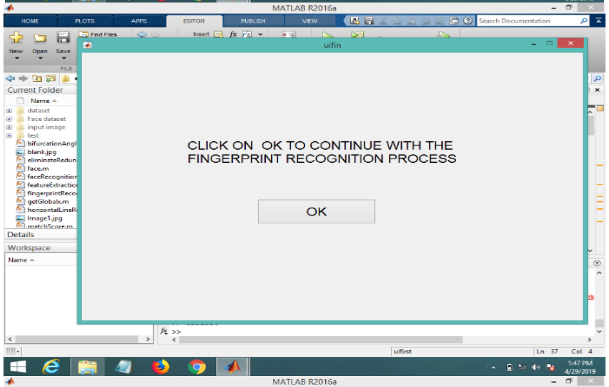
WELCOME USER

ENTER YOUR ACCOUNT TYPE:

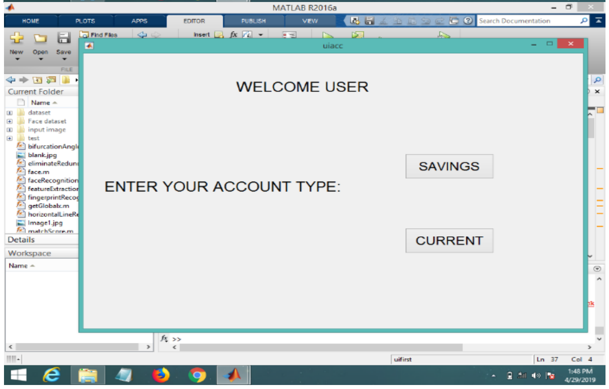
2. For successful face recognition and fingerprint recognition without spectacles on



PLEASE STAND PROPERLY IN FRONT OF THE CAMERA



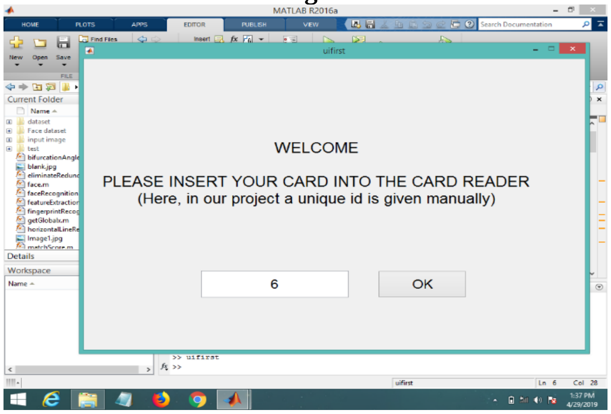
CLICK ON OK TO CONTINUE WITH THE
FINGERPRINT RECOGNITION PROCESS



WELCOME USER

ENTER YOUR ACCOUNT TYPE:

3. For unsuccessful face recognition

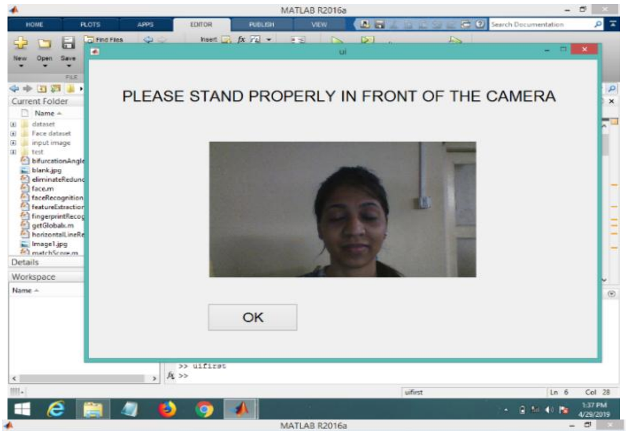


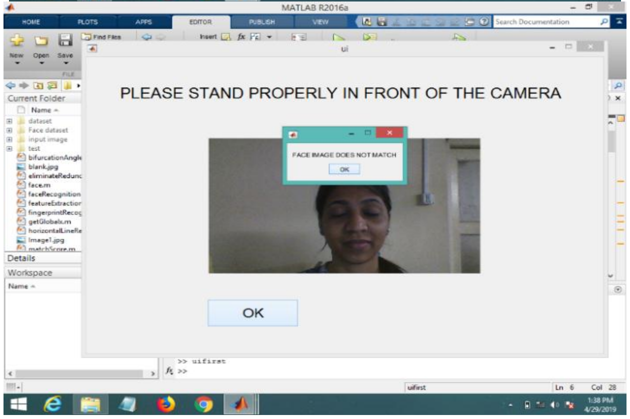
WELCOME

PLEASE INSERT YOUR CARD INTO THE CARD READER
(Here, in our project a unique id is given manually)

6

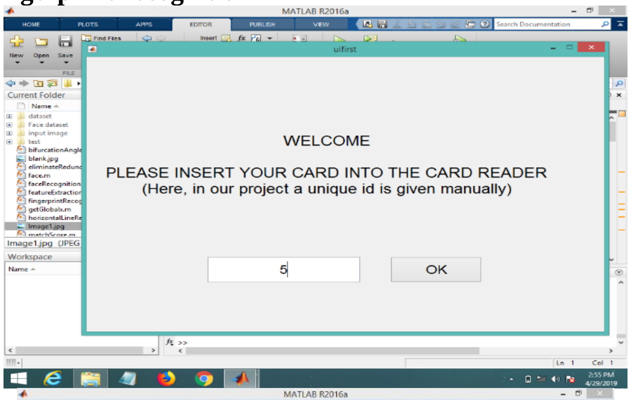
```
>> uifirst
>>
```


PLEASE STAND PROPERLY IN FRONT OF THE CAMERA


PLEASE STAND PROPERLY IN FRONT OF THE CAMERA

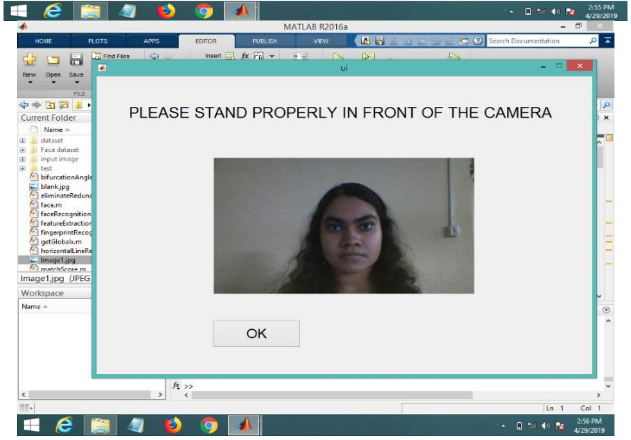
FACE IMAGE DOES NOT MATCH

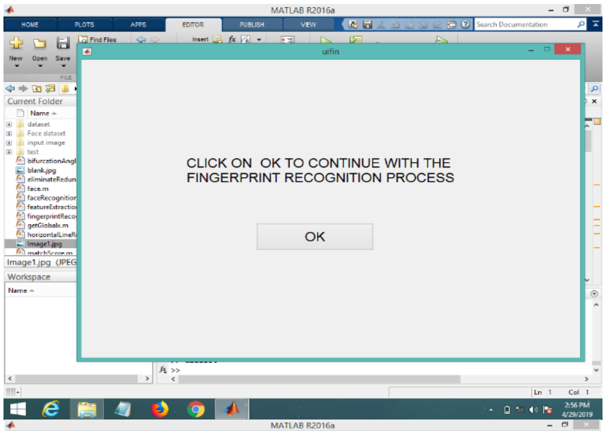
4. For successful face recognition and unsuccessful fingerprint recognition

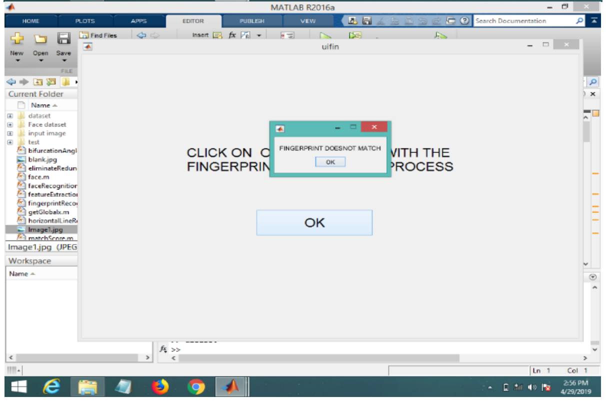

WELCOME

PLEASE INSERT YOUR CARD INTO THE CARD READER
(Here, in our project a unique id is given manually)

5


PLEASE STAND PROPERLY IN FRONT OF THE CAMERA


CLICK ON OK TO CONTINUE WITH THE
FINGERPRINT RECOGNITION PROCESS


CLICK ON C
FINGERPRIN

FINGERPRINT DOESNOT MATCH

VITH THE
PROCESS

VI. LIMITATIONS

1. The image of the user's face will have to be straight and the whole face should be inside the frame.

2. The background should be of a clear monotone colour. Noisy background will create problem in cropping the face of the user from the image.

3. There should be ample light where the pictures of the user's face will be taken in both the time of the enrollment and the transaction.

4. If the user were wearing glasses during enrollment, then he/she will have to wear it during the transaction process also and if not, then will not wear it.

5. If the scanned fingerprint image is too light, then some of the ridges will not be recognizable and the system will not work.

6. If the scanned fingerprint image is too dark, it will not work as well.

7. The moisture or dampness on user's finger can change the surface characteristics of the fingerprint. So, the user will have to ensure that his/her finger is dry before putting it in the scanner.

VII.CONCLUSION AND FUTURE SCOPE

The present study has been made to suggest and develop some tools which will eventually be useful as a base for realizing a scheme to be implemented in other projects of greater level in security enhancement purpose. This project itself can be modified to achieve a home security system, attendance counting system for students and employees, online transaction system and all other projects where biometrics can be used as an identification method.

The project has a very vast scope in future. It can be updated very easily as and when requirement for the same arises, as it is very flexible in terms of expansion. Some of the enhancements that can be made are as follows:

- A provision can be made where the whole hardware and the software of the system gets shut down, if someone tries to remove the camera attached to the machine.
- Some better algorithms can be used for face recognition and fingerprint recognition to overcome the limitations like users having to remove their glasses before taking pictures and problems regarding the too light or too dark fingerprints etc.
- The system can be connected to a formal database where both the face images and the fingerprints of the users will be stored altogether along with their unique ids.
- The corresponding bank authority may want to restrict the number of chances a user is given, in case the face image or the fingerprint taken during the transaction does not match with the previously stored ones.

Finally, it is hoped that the project will serve its purpose for which it is being developed thereby underlining the success of the process.

ACKNOWLEDGEMENT

The authors like to express their special thanks of gratitude to the Head of the Department of Computer Science, **Prof. Shalabh Agarwal**, of St. Xavier’s College, Kolkata, for the thorough guidance and support in completing the project. The authors, Jufishan Boksha, Romita Mondal and Soumi Mitra are greatly indebted to **Mr. Sandip Mitra**, for lending the fingerprint scanning machine. Moreover, they are highly obliged in taking opportunity to sincerely thank the support staff members of the Department of Computer Science, **Mr. Satyabrata Khara** and **Mr. Rana Biswas**, for their generous attitude and friendly behaviour. They would also like to thank **Mr. Sankar Dutta**, **Mr. Amitava Roy Chowdhury**, **Totan Karmakar** of St. Xavier’s College, Kolkata, for providing all the facility that was required. Finally, they would like to express their heartfelt gratitude to fellow student of Postgraduate Department of Computer Science, St. Xavier’s College, Kolkata, **Ms. Bharti Kumari**, for helping in building the test cases.

REFERENCES

[1] Viola, P.; Jones, M.,” Rapid Object Detection Using a Boosted Cascade of Simple Features”, TR2004-043 May 2004.
[2] M. Turk and A. Pentland, “Eigenfaces for Recognition,” J. Cognitive Neuroscience, vol. 3, no. 1, 1991.
[3] Shashi kumar D.R, R.K.Chhotaray, Raja K B & Pattanaik Sabyasachi, “Fingerprint Verification based on fusion of Minutiae and Ridges using Strength factors”, International Journal of Computer Applications, July ,2010.

Authors Profile

Jufishan Boksha has received her M.Sc. degree in Computer Science (2017-2019) from St. Xavier’s College (Autonomous) Kolkata and B.Sc. degree in Computer Science in 2017 from Jogesh Chandra Chaudhuri College under University of Calcutta. She has also done a review paper on “Scope and Challenges in Smart Glasses: A Comprehensive Study on Present Scenario”.

Romita Mondal received M.Sc. degree in Computer Science (2017-2019) from St. Xavier’s College (Autonomous) Kolkata. She has received her B.Sc. degree in Computer Science in 2017 from Narasinha Dutt College under University of Calcutta.

Soumi Mitra received her B.Sc. degree in Computer Science in 2017 from Narasinha Dutt College, Howrah under University of Calcutta and her M.Sc. degree in Computer Science (2017-2019) from St. Xavier’s College (Autonomous), Kolkata.

Asoke Nath is working as lecturer in the Department of Computer Science, St. Xavier’s College (Autonomous), Kolkata. He is engaged in research work in the field of Cryptography and Network Security, Steganography, Green Computing, Big data analytics, Li-Fi Technology, Mathematical modelling of Social Area Networks, MOOCs etc. He has published more than **246** research articles in different Journals and conference proceedings.