Intensifying Security Using Multifactor Authentication for Mobile Banking

[1]P.Rajalakshmi, [2]R.Sangeetha, [3]Dr.B.Vanathi, [4]K.Shanmugam, [5]S.celin sindhya
[1]UG Scholar, [2]UG Scholar , [3]Professor&Head,[4]Assisstant Professor,[5]PG Scholar
Department of Computer Science and Engineering, Valliammai Engineering College
Kattankulathur, Chennai, India

***Abstract*—Authentication is a significant issue in system control in computer based communication. Human Finger/Face Recognition is an important branch of biometric verification. It has been widely used in many applications, such as video monitor system, human-computer interaction, and door control system and network security. This proposed project aims for providing security to systems using both finger and face recognition by extracting images. The proposed system deals with security issues in mobile commerce applications and provides ways to enhance secure authentication as mobile commerce applications involve high level of confidential information. The proposed system invokes finger recognition, face recognition, One Time Password (OTP), Quick Response (QR) code for user authentication and secure transaction. OTP is encrypted using an Advanced Encryption Standard (AES) 256 bit-Encryption algorithm and then converted into QR code.**

***Index Terms*—finger recognition, one time password, face recognition, quick response, Advanced Encryption Standard**

I. Introduction

Mobile commerce has exploded in the last five years. In fact, Bank of America predicts US$67.1 billion in purchases will be made from mobile devices by European and US shoppers in 2015.1 Several factors are driving this rapid growth of mobile commerce. Another driving factor is consumer demand for applications for buying and selling goods and services, as well as for online banking and bill payment. Nowadays, most banks and brokerage firms provide mobile apps for their customers to support online banking and trading.

The final factor is the rapid adoption of online commerce due to stronger security practices. For example, authentication techniques that use multiple factors or out-of-band verification are common practices now. A variety of m-commerce products and services have thus emerged. These include mobile money transfer, mobile Automated Teller Machine (ATM), mobile ticketing, content (video and audio) purchase and delivery, and location-based services (local discount offers). New applications are also developing quickly. Mobile payments can be made directly inside of a mobile app running on a Smartphone. Such in-app purchases can be a recurring revenue stream for developers.

M-commerce defined as "the delivery of electronic commerce capabilities directly into the hands, anywhere, via wireless technology" and "putting a retail outlet in the customer's hands anywhere." M-Commerce users expect immediate response and provide the exact result based on context. M-Commerce occurs through the use of wireless devices such as cell phones, pocket Personal Computer (PC's), and Personal Digital Assistant (PDAs). It allows a user to purchase goods and services on the move, anytime, and anywhere. This project enhances the security of the trusted device and minimizes the possibility of security breach in Authentication scheme.

II. LITERATURE SURVEY

A. *Improved principal components analysis (PCA)*

Face recognition has become a very challenging problem in presence of clutter and variability of the background, noise and occlusion, and finally speed requirements. This paper focuses on developing a face recognition system using an extended PCA algorithm. The proposed algorithm uses the concept of PCA and represents an improved version of PCA to deal with the problem of orientation and lightening conditions present in the original PCA. The preprocessing phases of the proposed algorithm emphasize the efficiency of the algorithm even when number of images per person or the orientation is very different [13].

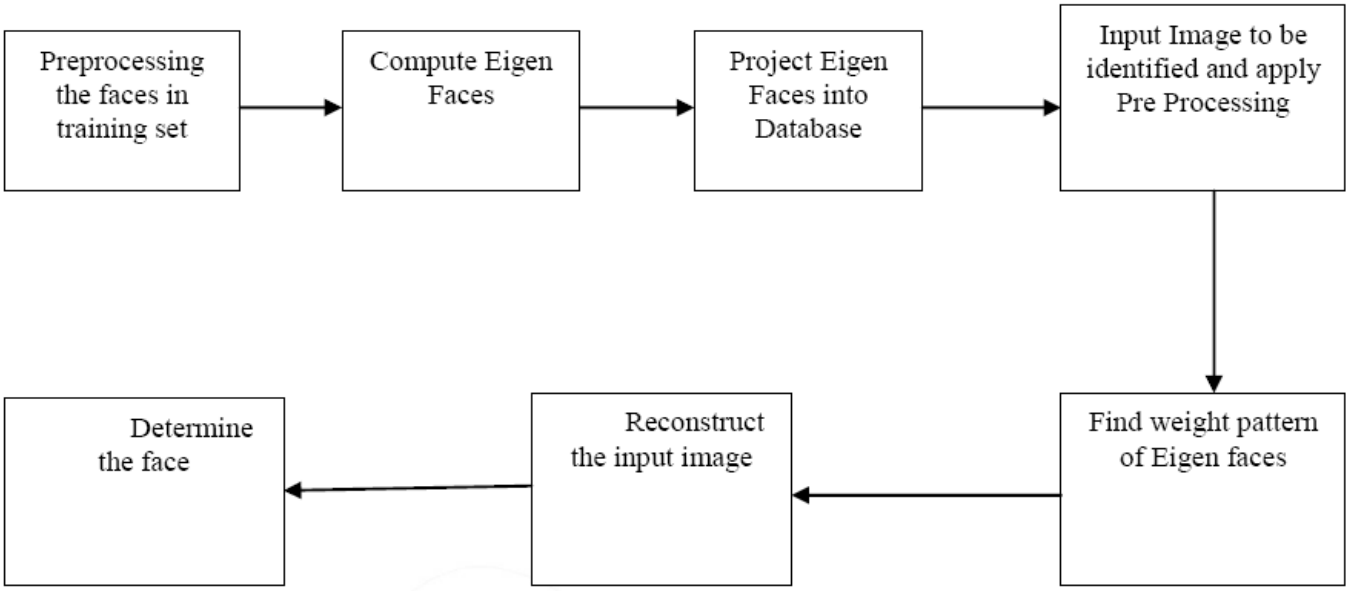


Figure 1: The main steps of Improved PCA Algorithm [1]

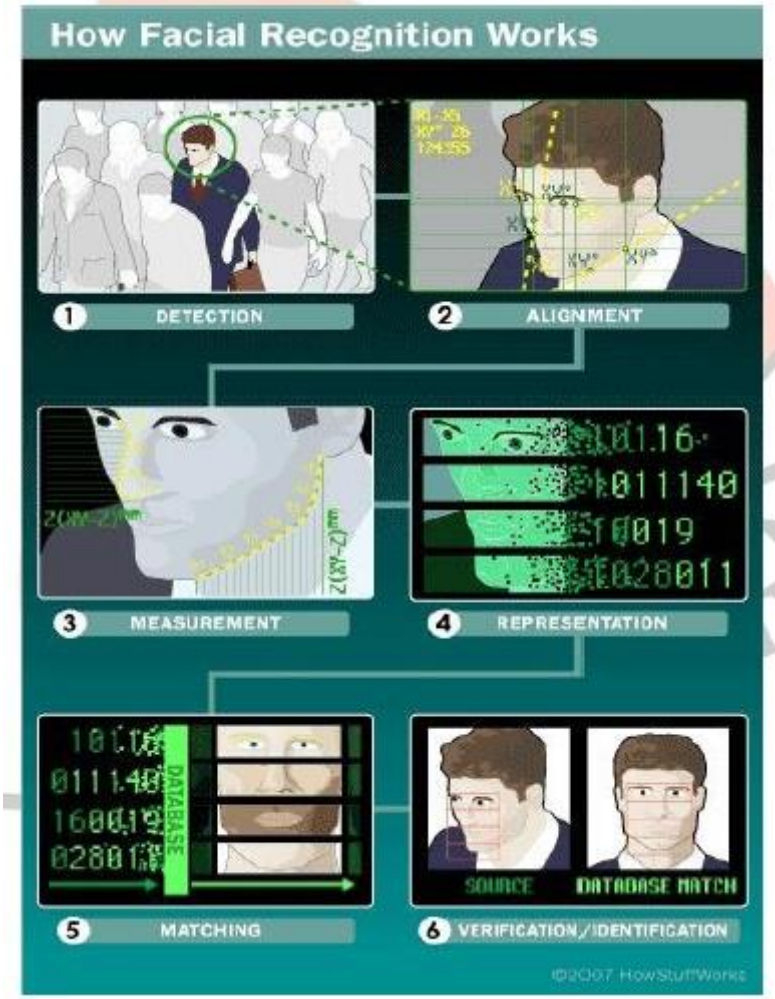


Figure 2: The face recognition process [1]

Advantages

• In IPCA method, the preprocessing of training images has been done to remove the background, lightening conditions and the orientation factor.

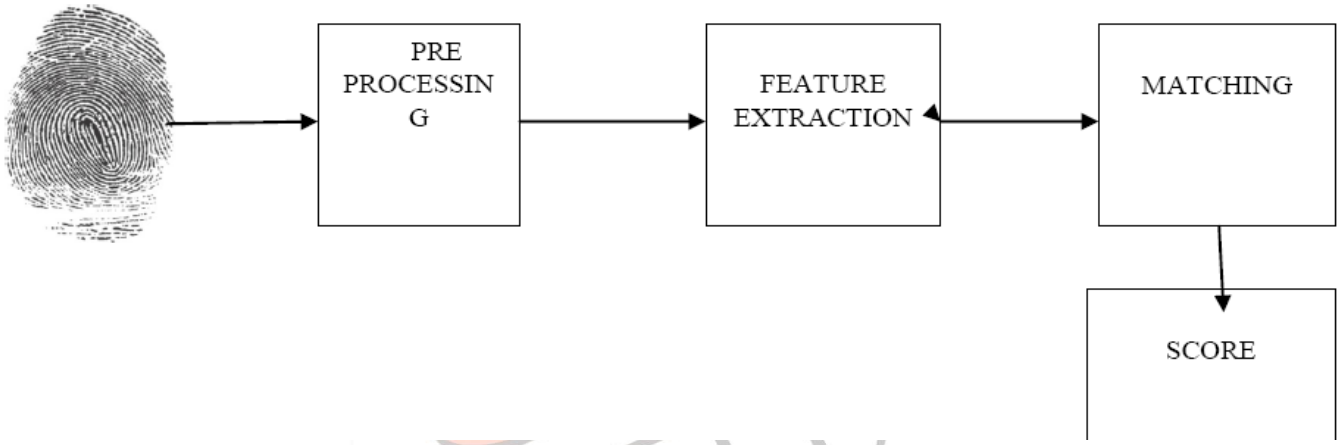
• The IPCA algorithm work well when the orientation of the images was very large that is around 90 degrees

Disadvantages

• The IPCA-PCA algorithm gives lower performance when the training set size becomes larger because the lower the sample to dimension ratio the harder a statistical estimation problem.

B. Performance improvements using rank-level fusion

Fingerprint classification represents an important preprocessing step in fingerprint identification, which can be very helpful in reducing the cost of searching large fingerprint databases. Over the past years, several different approaches have been proposed for extracting distinguishable features and improving classification performance. This paper presents a comparative study involving four different feature extraction methods for fingerprint classification and proposes a rank-based fusion scheme for improving classification performance. Specifically, the paper compared two well-known feature extraction methods based on Orientation Maps (OMs) and Gabor filters with two new methods based on ‘‘minutiae maps” and ‘‘orientation collinearity’’. Each feature extraction method was compared with each other using the NIST-4 **(**National Institute for Standards and Technology**)** database in terms of accuracy and time. Moreover, the issue of improving classification performance using rank-level fusion has been investigated. Gabor features fell behind OMs mainly because their computation is sensitive to errors in localizing the registration point [2] [3].



Advantages

• The distribution on the fingerprint provides a unique signature for an individual

• In MM (Minutiae Mapping) Method Preprocessing steps are carried out for fingerprint feature extraction like thinning, binarizing, and finding minutiae points

Disadvantages

• Pressure and Skin Condition-Pressure, dryness, disease, sweat, dirt, grease, humidity

• Noise- Dirt on the sensor

• Distortion (Non-Linear)-stretches when pushed down

C. STUDY OF ENCRYPTION ALGORITHM FOR SECURITY

In recent years network security has become an important issue. Encryption has come up as a solution, and plays an important role in information security system. Many techniques are needed to protect the shared data. This paper focuses on cryptography to secure the data while transmitting in the network. Firstly the data which is to be transmitted from sender to receiver in the network must be encrypted using the encryption algorithm in cryptography. Secondly, by using decryption technique the receiver can view the original data. In this paper, three encryption techniques like AES, DES and RSA algorithms are compared based on the

analysis of its stimulated time at the time of encryption and decryption. Experiments results are given to analyze the effectiveness of each algorithm [4].

Advantages

• AES is more secure and faster in both hardware and software-when you use it with its most secure 256-bit key length, it would take about a billion years to guess the key through a brute force attack.

• AES supports large key sizes.

Disadvantages

• Sharing the key-The problem with symmetric key Encryption is that you need to have a way to get the key to the party with whom you are sharing the data.

• More damage if compromised-when someone gets their hands on a symmetric key, they can decrypt everything with that key.

D. A SURVEY ON QR CODES: IN CONTEXT OF RESEARCH AND APPLICATION

QR code stands for Quick Response Code, which is the trademark for the type of matrix barcode which was invented by the Japanese corporation Denso Wave. QR Code has a number of features such as large capacity data encoding, dirt and damage resistant, high speed reading, small printout size, 360 degree reading and structural flexibility of application.
Statistically QR codes are capable of symbolizing same amount of data in approximately one tenth the space of a traditional barcode. Information such as URL, SMS, contact information and plain text can be embedded into the two dimensional matrix. Moreover, with the explosive of the trend to use smart phones has also played an important role in the popularity of QR Codes [5][7].

Figure 4: Scanning QR Code in the Smart Phones [5] [7].

Advantages

• QR Code contains unique details and it can be easily integrated with mobile devices

• The Code itself stores huge amount of information that is easily scanned and stored onto the mobile device.

• QR Codes are easy to use and versatile.

Disadvantages

• A disadvantage of QR Code is that smart phones are far more expensive compared to the conventional phone.

• Users must be equipped with camera phone and the correct reader software that can scan the image of the QR Code.

III. EXISTING SYSTEM

The Existing system consists of user login, password and normal OTP Generation. Users login with their ID and Password. The Server side of M-banking verifies the validation of user ID & password, generates an OTP and then transfer it to the receiving equipment i.e., Mobile phone of the user. It requests the user for valid OTP in Specified Time period. If the input OTP is correct, the user will be requested to provide the biometric data. It will compare &verify the uploaded biometric data with the user

Disadvantages
The disadvantages of the existing system are:

• Less effective and possesses high risk of interception via Internet or telecommunication

• Does not focus on the fingerprint feature extraction level

• It is not secure as the user detail can be hacked by session hacking & phishing attacks

Thetemplateisusedtoformatyourpaperandstylethetext.Allmargins,columnwidths,linespaces,andtextfontsareprescribed;pleasedonotalterthem.Youmaynotepeculiarities.Forexample,theheadmargininthistemplatemeasuresproportionatelymorethaniscustomary.Thismeasurementandothersaredeliberate,usingspecificationsthatanticipateyourpaperasonepartoftheentireproceedings,andnotasanindependentdocument.Pleasedonotreviseanyofthecurrentdesignations.

IV. PROPOSED SYSTEM

In the proposed system, the client login into the system by providing user name and password. If the username and password are correct, the system provides fingerprint authentication using Minutiae Mapping (MM) algorithm**.** If fingerprint matching value is lesser than the threshold value (> 90 %), the user is requested to provide face recognition authentication. Face recognition is done by IPCA (Improved Principle Component Analysis) algorithm. If the face authentication is complete, then the server generates OTP (One Time Password). Security is increased by integrating QR (Quick Response) Code for data hiding. OTP is encrypted using an AES 256 bit-Encryption algorithm and then converted into QR code. The proposed work provides comparison between different fingerprint feature extraction algorithms, face recognition algorithms and Encryption algorithms.

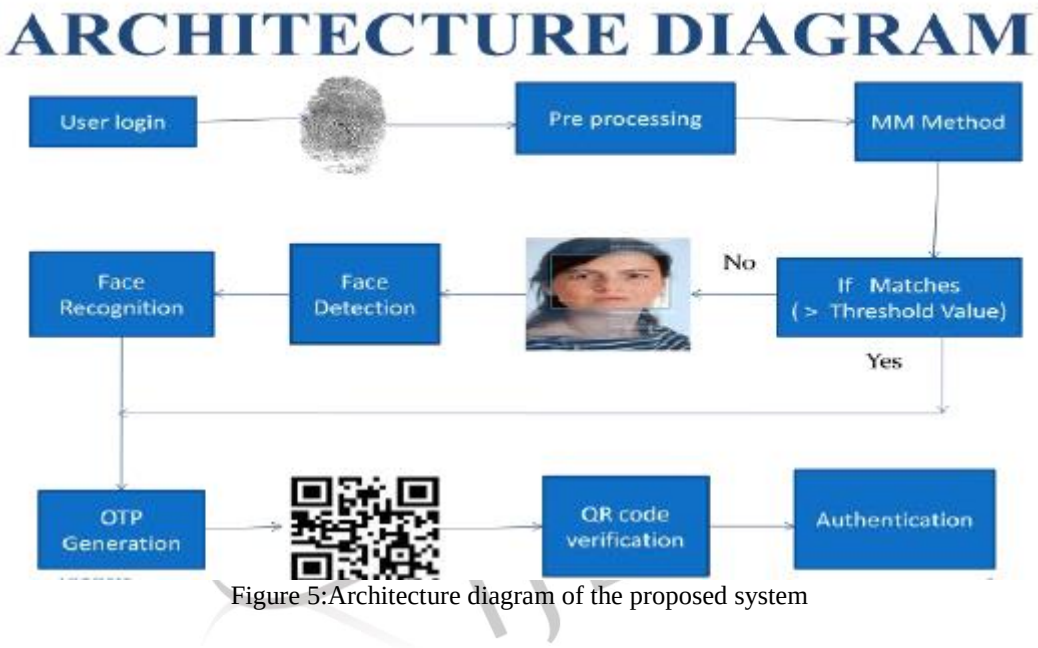


Figure 5:Architecture diagram of the proposed system

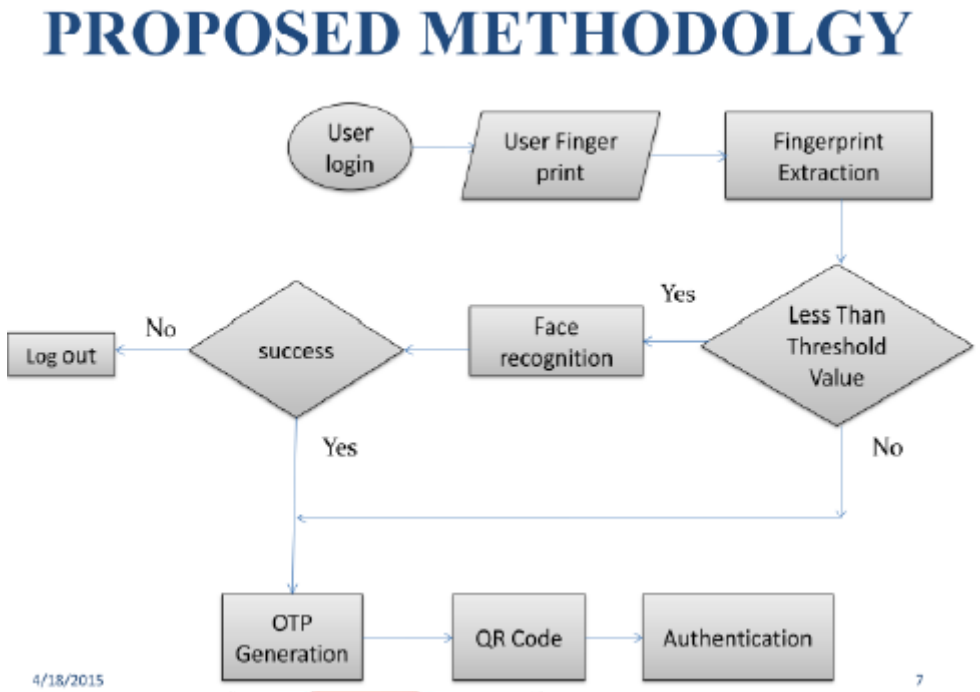


Figure 6:Proposed methodology for mobile banking

Advantages

The advantages of the existing system are:

- Intensifies security by restricting access to unauthorized users
- More effective and accurate
- Faster encryption and decryption using AES-256 algorithm
- Multiple factors are considered for authentication

V. EXPERIMENTAL RESULTS

Shown in figure is the filling information of the user for performing the initial process. The user requests to login the details with the login id and the password

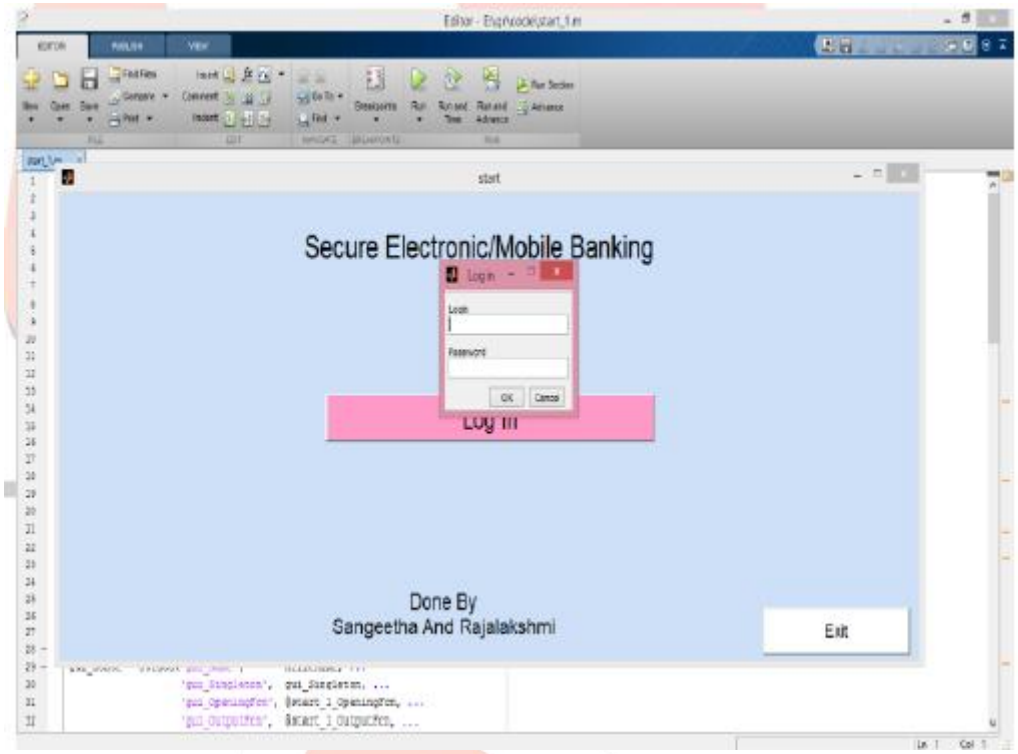


Figure 7:login page with login Id and password

Shown in Figure 8 Finger Print recognition with the matching percentage. The preprocessing steps such as thinning and binarizing is carried out using MM method

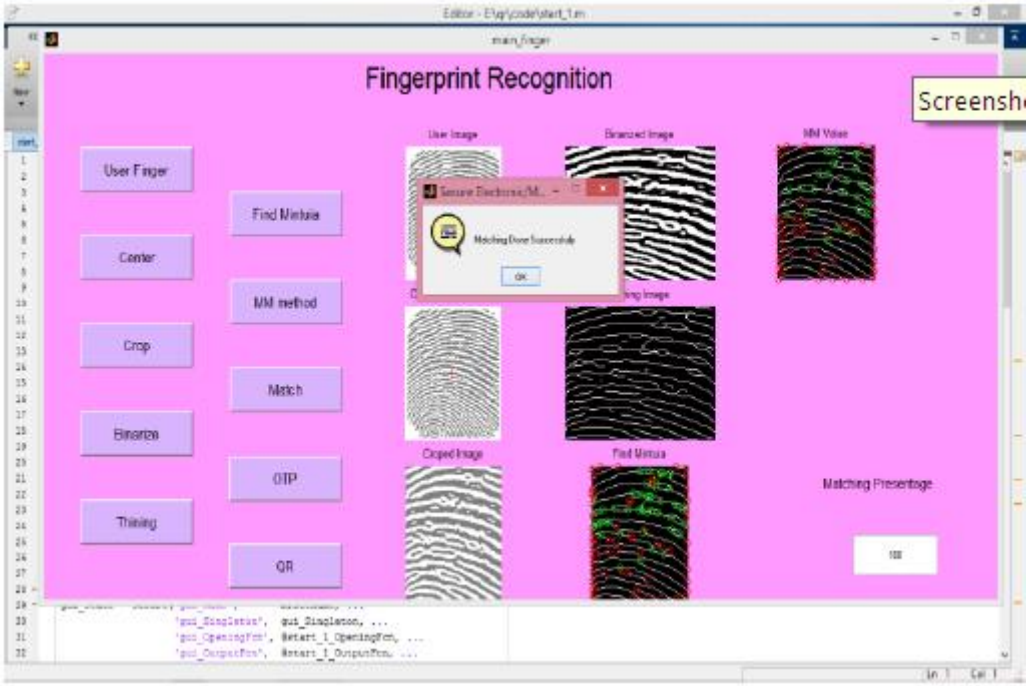


Figure 7:Finger Print recognition with the pre processing steps

Shown in figure 8 is the detected faces and recognized faces. The faces are recognized using IPCA (Improved Principal Component Analysis) Algorithm

Figure 8: Face detection and recognition process.

Shown in figure 9 the comparison and verification of the OTP (One Time Password).The encrypted and the decrypted OTP are compared

Figure 9: The entered OTP is encrypted and decrypted for the verification

VI. CONCLUSION AND FUTURE WORK

The existing system deals with providing security for mobile banking applications based on an ordinary OTP generation. This OTP may be accessed by session hackers as it does not use any encryption standard. As mobile banking applications involve highly confidential information, this existing system is not secure enough. The proposed system uses multiple authentication factors like fingerprint authentication, face authentication and OTP generation. Fingerprint authentications is done by using MM algorithm which has the least average processing time. Face authentication involves IPCA algorithm with preprocessing procedures for removing background, lighting and orientation problems. OTP is encrypted using AES-256 bit algorithm which makes it difficult to hack. Also, AES-256 has the least encryption and decryption time. Altogether, the proposed system is designed to be secure as well as time efficient.

The proposed system has been implemented in simulation using MATLAB. In future, the proposed system can be implemented in real time. Also, the proposed system involves two biometric authentication i.e., face and fingerprint authentication. Another biometric authentication using voice recognition can be added so as to increase security.

REFERENCES

[1] Vinay Rishiwal ,Ashutosh Gupta, "Improved PCA Algorithm for Face Recognition", World Applied Programming, Vol (2), Issue (1), January 2012. 55-59.
[2] UdayRajanna, Ali Erol, George Bebis, "A Comparative study on feature extraction for fingerprint classification and performance improvements using rank-level fusion" 28 April 2009,Pattern Anal Applic,DOI 10.1007/s10044-009-0160-3.
[3] Ayodeji S. Makinde, Yaw NkansahGyekye, Loserian S. Laizer "Enhancing the Accuracy of Biometric Feature Extraction Fusion Using Gabor Filter and Mahalanobis Distance Algorithm ",International Journal of Computer Science and Information Security, Vol. 12, No. 7, July 2014.
[4] Dr. Prerna Mahajan & Abhishek Sachdeva "A Study of Encryption Algorithms AES, DES and RSA for Security "Global Journal of Computer Science and Technology Network, Web & Security ", Volume 1 3 Issue 15 Version 1.0 Year 2013.
[5] Deepak R.Thorat, ShetalS.Sonawane, "Risk Based Multilevel and Multifactor Authentication using Device Registration and Dynamic QR code based OTP Generation", International Journal of Advanced Research in Computer and Communication Engineering, Volume 3,Issue 10,October 2013.
[6] Dr.P.K.Suri, Dr.Ekta Walla ,"Face recognition techniques using PCA,LDA,Histogram".
[7] Kinjal H.Pandya, Hiren J. Galiyawala, "A Survey on QR codes: in context of research and application "International Journal of Emerging Technology and Advanced Engineering,website:www.ijetae.com (ISSN 2250-2459,ISO 9001:2008 Certified Journal volume 4,Issue 3,March 2014).
[8] Ms. Varsha Gupta, Mr. Dipesh Sharma. "A Study of Various Face Detection Methods ",International Journal of Advanced Research in Computer and Communication Engineering, Volume 3,Issue 5,may 2014.
[9] Nikita Gupta, Nagesh Mokashe, Mangesh Parihar, "QR code: A safe and secure method of authenticating legal documents",International Journal of Engineering Research and General Science,volume 3,Issue 1,jan-feb 2015
[10]". Aruni Singh, Sanjay Kumar Singh, Shrikant Tiwari, "Comparison of face Recognition Algorithms on Dummy faces"International Journal of Multimedia and its Applications(IJMA) Vol 4,Issue 4,August 2012.
[11] Simon Gangl, Domen Mongus "Comparison of face recognition algorithms in terms of the learning set selection
[12] Uma Shankar Kumari,Dheeraj Agarwal, R.K.Baghel, "Study of different face recognition algorithms and challenges", International Journal of Engineering Research,Volume 3,Issue 2,pp :112-115.
[13] Abhishek Singh, Saurabh Kumar, "Face Recognition Using PCA and Eigen Face Approach".
[14] W.Zhao R.Chellappa, A.Rosenfeld, P.J.Phillips, "Face Recognition: A Literature Survey".
[15] Yongzhong Lu, Jingli Zhou, Shengsheng Yu, "A survey of face detection, Extraction and Recognition".