ENHANCING ATM SECURITY USING BIOMETRIC AND GSM TECHNOLOGY

[1]**Mala K**
PG Student,
Computer Science and Engineering,
SSIT, Tumkuru, Karnataka.

***Abstract:**The main aim of this system is, to propose the system which is used for ATM security application .The usage of the ATM has increased over the decades which has motivated us to use biometric for personal identification to procure high level security and accuracy.This paper describes the replacement of ATM cards and pins by biometric authentication.Moreover the feature one time password imparts privacy to users and emancipates user from recalling pins. In this system, the genuine user's biometric are enrolled and are retained in databases, the transaction begin and the biometric are cross checked and thus distinguish from legitimate user and the fake ones. A GSM module connected to ARM7L2128 will send the 3 digit code that is generated by system to the legitimate user's mobile number. After the valid OTP is entered the user can do the transaction that he wants to do. If incase there is any fake access attempts then the account is blocked. In this the biometric that are used are fingerprint and irisrecognition. In this paperthe experimental results are obtained on the data set of fingerprint and iris in real time using fingerprint module with minutiae matching algorithmand iris with GUI based Circular Hough transform.*

***Index terms** – Authentication, Biometrics, Circular Hough transformation, Minutiae matching algorithm, Global system for mobile communication (GSM), one time password (OTP).*

I.INTRODUCTION

ATMis the electronic banking machine that is located in differentplaces, which helps the customerto do transaction without the help of bank staffs. With the help of the ATM one can do many banking operation like withdrawal of money, deposition of money, online payments etc. The surplus of ATM not only increased in their number but also increased in the fraudulent attacks on it. This call for the biometric system to be integrated into traditional ATM. In this paper we discuss some of the biometric measures as the means to enhance the security for both customer and bankers.

Biometric authentication can be Fingerprint scanning, Face recognition, Iris scanning etc. But here we are introducing new technology which works the technology fingerprint recognition system and nominee for the main user and GSM technology. Biometric technology provides strong and indisputable authentication. Because biometrics data are unique, cannot be shared, cannot be copied and cannot be lost. The fingerprint based identification is one of the most mature and proven technique. So we use the fingerprint for the identification purpose. Biometrics technologies are a secure means of authentication,the fingerprint of the card and nominee will be stored in the database of the bank when the cardholder or the nominee tries to access the account; they will have to enter the pin and need to enroll the fingerprint. In case of the iris recognition the user iris is captured by camera and matched with that stored in the database. After the authentication by biometric the GSM comes into picture .The GSM technology is cellular network which means that mobile phone connect to it by searching for cells in the immediate vicinity. The GSM modem connected to the microcontroller generates the 3 digit code to the main user mobile number. The user can access the account after he/she enter one time password, after they can begin the transactions.

II.SYSTEM DEVELOPMENT

In the proposed system we present a fraud detection method using two biometrics (fingerprint and iris) to detectvarious types of illegal access attempts during the ATMtransaction. The objective of the proposed system is toenhance the security of the ATM transaction using biometricrecognition frameworks. In this system ARM7 basedLPC2148 controlling is used for smart ATM access. The fingerprint module utilizes the minutiae based algorithm forfingerprint recognition it captures the fingerprint of the personand compares it with the fingerprint of the legitimate user that stored in the database. If the person is a valid user thecontroller will display a message "VALID PERSON" on theLCD. The USB camera is used to capture the eye image of theuser. A GUI prepared in Mat lab based on Circular HoughTransform is used for iris recognition. After iris authenticationand matching if the person is a true user then the controllerdisplays a message "IMAGE IDENTIFIED" on the LCD.Afterthe validation result of the person is true a 3 digit code ismessaged to the customer's registered mobile number whichwas saved in the database during enrollment. This process isdone through the GSM module which is interfaced to theARM board. Depending on whether the OTP entered is corrector wrong messages like" CORRECT CODE "or "REENTERCODE" is displayed on the LCD. After the entered code isfound valid the banking process begins and a message "BAL,DEP, WTD" for entering the option for the task to beperformed is displayed on the LCD.After the task is performedfinally a message "TRANSACTION COMPLETED" is displayed on the LCD.

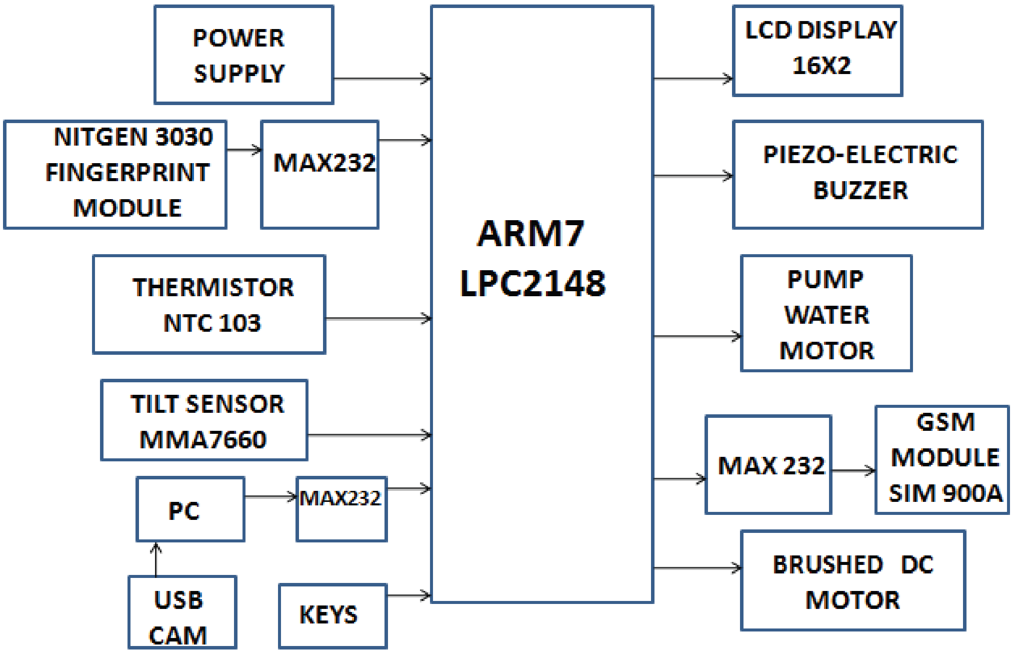


Fig 1:Proposed systems block representation.

III.PROPOSED BIOMETRIC IDENTIFICATION TECHNIQUES

3.1. Minutiae Based Fingerprint Recognition

The fingerprint image undergoes preprocessing stages like binarization which uses fixed threshold to convert a gray scaleimage to a binary image and then proceeds to thinningprocess to reduce the thickness of all ridge edge lines to asingle pixel width after which an initial code is generated,prior to the secured final code. The code block consists of fivesub-blocks placed within the header and trailer.The fingerprint image recognition act as first level of bio-metric authentication.

3.2.Circular Hough Transform Based Iris Recognition

The Circle Hough transform is basic technique used in digital image processing for or detecting circular objects in a digital image. The software of the application is based on detecting the circles surrounding the exterior iris pattern. The flow of iris recognition process is as shown in the fig 2.This iris recognition act as the second level of authentication after the finger print recognition.

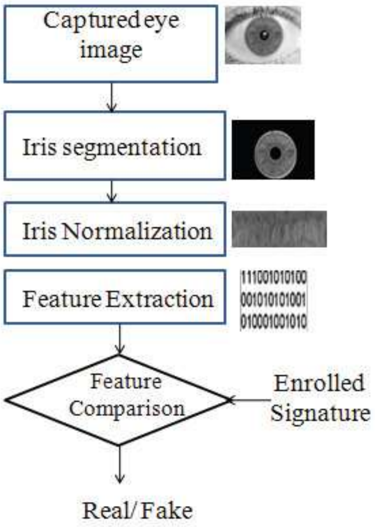


Fig 2:Flow of iris recognition process

IV. USING GSM TECHNOLOGY FOR GENERATION OF OTP

Global System for Mobile Communication is a digital cellular technology with the help of which we are able to transmit both voice and data services operating at 800MHz, 900 MHz,1800 MHz and 1900MHz frequency bands. It uses Time division multiple for communication and can carry 64kbps to 120Mbps of data rate.With the fingerprint and iris reorganization method we also embedded the GSM technique. That the GSM modem connects to microcontroller. That will send the 3 digit code to the user.After enter the 3 digit number the transaction will begin.

4.1. GSM Module Working

The SIM card mounted on the GSM modem on receivingSMS from some other mobile delivers the data to themicrocontroller through serial communication.AT commandscontrol the GSM modem.

4.2. OTP Working

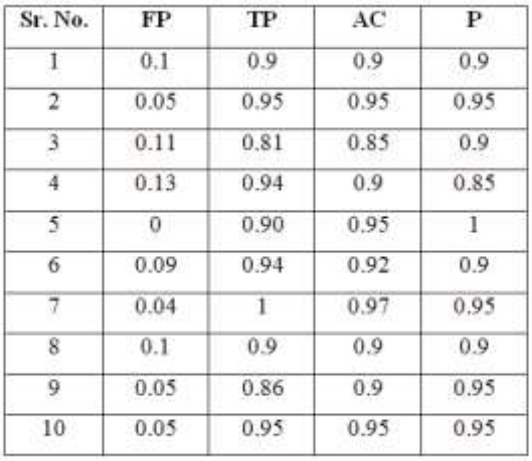
A password which is valid only for a single transaction is a One Time Password.

Generation of a Random Number:
Generates a Pseudo- Random Number Sequence. Let it be (YK)
YK+1= (a× YK +I) mod (m)……………..……....….(1)
a- multiplier, I-increment, m- modulus.

V. RESULTS AND DISSCUSSION

5.1. Results for Fingerprint module

When a fingerprint was placed on the NITGEN 3030 fingerprint recognition device it captured a 3D grayscaleimage after scanning the fingerprint and a 256×288 pixelsimage was stored in bitmap format. Key minutiae wereextracted using a minutiae based algorithm which converted itinto a unique mathematical template that could be compared toa 60 digit password. This template was stored in the databaseafter encryption. When the same user’s new fingerprint imagewas captured a new template of that query image was createdin the same manner as it was done during enrollment. Thisnew template was compared with the templates in the databaseand a message “VALID PERSON” was displayed on the LCDbut when another fake user went through the same process amessage “PERSON NOT IDENTIFIED” was displayed andthe buzzer turned on. The minutiae matching algorithm withinthe module provides about 75-80% accuracy.



Sr. No.	FP	TP	AC	P
1	0.1	0.9	0.9	0.9
2	0.05	0.95	0.95	0.95
3	0.11	0.81	0.85	0.9
4	0.13	0.94	0.9	0.85
5	0	0.90	0.95	1
6	0.09	0.94	0.92	0.9
7	0.04	1	0.97	0.95
8	0.1	0.9	0.9	0.9
9	0.05	0.86	0.9	0.95
10	0.05	0.95	0.95	0.95

Table 1: Analysis of the proposed system.

5.2. Results for Iris Recognition

The eye image of a person was captured using a QHMPLPC camera and was stored in 640×480 pixels in bitmapformat. The Hough Transform detected the iris and pupilboundaries. After capturing the query eye image a featurevector of the input pattern was obtained in the same manner asit was determined during enrollment. This feature vector wascompared with those feature vectors present in the database ifthe person was a valid person then after running the GUIbased on Circular Hough Transform a message “MATCH”will be displayed on the monitor, else a message “ NOMATCH FOUND” is displayed. Investigations show that theiris recognition system used in this work provides about95.6% accuracy.

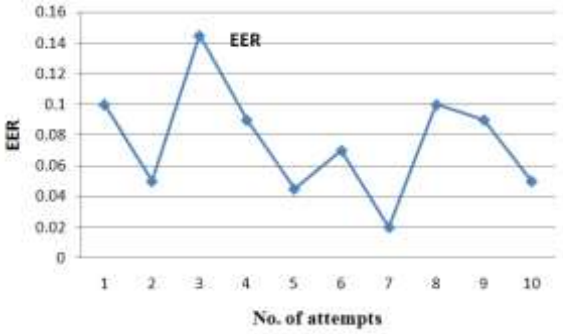


Fig 3:Graph for the equal error rate of the proposed system.

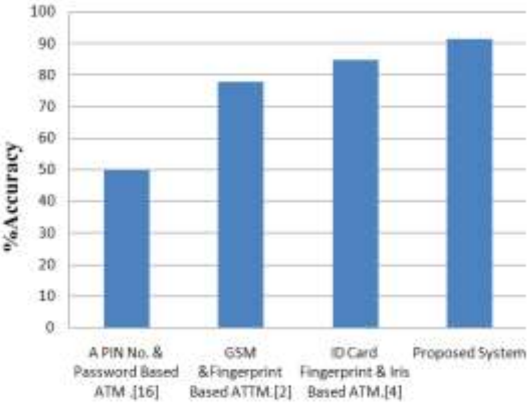
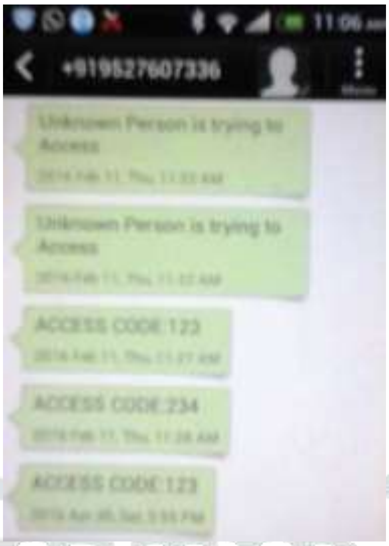


Fig 4: The graph of survey of security in ATM system

5.3.Results for OTP generation

After the valid biometric identification a message “ACCESS CODE” SMS was received on the user’s registered mobile number simultaneously a message“ENTER THE CODE” was displayed on the LCD. After the valid code was entered the system proceeded towards the banking process. But when the wrong code was entered an SMS “UNKNOWN PERSON TRYING TO ACCESS” was received on the user’s registered mobile number.



11:06 am

+919527607336

Unknown Person is trying to Access
2014 Feb 11, Thu 11:33 AM

Unknown Person is trying to Access
2014 Feb 11, Thu 11:32 AM

ACCESS CODE:123
2014 Feb 11, Thu 11:27 AM

ACCESS CODE:234
2014 Feb 11, Thu 11:28 AM

ACCESS CODE:123
2014 Apr 05, Sat 3:55 PM

Fig 5: OTP message received on the mobile screen

5.4. Results for Banking Process

The system is fed with a default amount 999. So when awithdrawal of 100 was done the balance amount showed 899.

VI.CONCLUSION

The use of the biometric as a password has made theATM transaction system more reliable and secured. The OTP concept added to the system further enhances the security andavoids the need for us to remember passwords. Moreover the system is built on embedded technology which makes it userfriendly and non-invasive. Using this system the ATM terminal is secured from thief attacks. The Fig 3andTable.1 shows that the average accuracy of the overall systemis 91.6% and the average equal error rate is 0.076. The timetaken for the overall ATM transaction is less than 10 sec foreach user. The Fig. 4 compares the proposed system with theprevious ATM transaction systems and shows that theaccuracy and security of the proposed system is maximum andreaches up to 95%.

VII. ACKNOWLEDGEMENT

The authors Mala K would like to thank the anonymous referees whose help and technicalideas have improved the quality of the paper.

REFERENCES

[1] Anil K. Jain, Jianjiang Feng, Karthik Nandakuma, “FingerprintMatching”, *IEEE* Computer Society2010, pp. 36-44, 0018-9162/10.

[2] Khatmode Ranjit P, Kulkarni Ram Chandra V,”ARM7 Based Smart ATM Access and Security System Using Fingerprint Recognition and GSM Technology”, International Journal of Emerging Technology and Advanced Engineering, Vol.4, Issue 2,Feb. 2014.

[3] G.Udaya Shree, M. Vinusha”Real Time SMS-Based HashingScheme for Securing Financial Transactions on ATM terminals”, International Journal of Scientific Engineering and Technology Research, Vol.2 Issue 12. Sep.2013.

[4] D.Shelkar Goud, IshaqMd, P.J.Saritha,”A Secured Approach forAuthentication system using fingerprint and Iris”, Global journal of Advanced Engineering Technology, Vol, Issue3-2012.

[5] Kriti Sharma, Hinanshu Monga, “Efficient Biometric IrisRecognition Using Hough Transform with Secret Key”,International Journal of Advanced Research in Computer Science and Software Engineering. Vol.4, Issue 7, July 2014.

[6] Ritu Jindal, Gagandeep Kaur, “Biometric Identification SystemBased on Iris, palm and Fingerprint for Security Enhancements”, International Journal of Engineering Research and Technology, Vol.1, Issue 4, June 2012.

[7] Deepa Malviya, “Face Recognition Technique: Enhanced SafetyApproach for ATM”, International Journal of Scientific and Research Publications, Volume 4, Issue 12, December 2014.

[8] Matsoso Samuel Monaheng, Padmaja Kuruba, “Iris RecognitionUsing Circular Hough Transform”, International Journal of Innovative Research in Science, Engineering and Technology, Vol.2, Issue 8, Aug.2013.

[9] Fakir Sharif Hossian, Ali Nawaz, Khan Md. Grihan,”BiometricAuthentication Scheme for ATM Banking System using AES Processor”, International Journal of Information and Computer Science Volume 2 Issue 4, May 2013.

[10] R. Wildes, J. Asmuth, G. Green, S. Hsu, R. Kolczynski, J. Mateyand S. McBride, “A system for automated iris recognition”, Proceedings *IEEE* Workshop on Applications of Computer Vision, Sarasota, FL, pp. 121-128, 2011.