A Novel Methodology of Integrated ATM Security

Mr.S.Vijay sarathi[1], S.Akash[2], I.Nihilkumar[3], M.Nirmal[4], M.Muthukumaran[5]
[1]*Assistant Professor/Department of EEE, Panimalar institute of technology, Chennai 600123*
[2,3,4,5] *UG Student/ Department of EEE, Panimalar institute of technology, Chennai 600123*

Abstract- **In the past few years robbery of ATM card is increasing, in the present system pin number is used for ATM transaction security. which can be easily stolen, guessed or misused by many ways with this one can lose his money. This motivated us to increase user security by adding the biometric and OTP to the existing system. It also put forward some issues which include sensor durability and time consumption. And some queries like "user lose how much if his card is misused?" and "to withdraw a low amount is it really admirable to go through the entire biometric process?". As a solution we introduce a constraint on transactions by ATM involving biometric (finger print) to improve the system performance and to solve the issues. We are adding a limit on amount of cash, if the entered amount is more than the limit, it is necessary to present biometric. If one need to withdraw the minimum cash, biometric scanning is not mandatory only will enter the OTP for user authentication. It help users to save time and maintain sensor performance by not furnishing their biometric for few hundred apart from maintaining security.**

Index Terms- biometric, fingerprint, OTP, GSM, Security.

I. INTRODUCTION

Security has always been a major concern and securing the integrity of it is the major goal of all organization. When talking about ATM machines we are mainly concerned with Physical security which aims at ensuring Access control, Identification and Authentication. Access control is another consideration of Information System security to confirm the identity of individual so that only authorized entity is accessible to the system. With the development of banking technology the way of banking has changed. On one hand where it has freed us from standing in long queues to carry out cash withdrawal, on the other it has also increased the risks of theft. ATM (Automatic Teller Machine) has proved to be an easy and convenient way to carry out all our banking tasks in just few minutes. An ATM card or debit card authenticates person after verification of card number, Expiry date, card holders name and the PIN. But what in case when the card is stolen, or PIN is known to an unauthorized person. For this we require a higher level of security which coined up an idea of adding Biometric to the current technology. Biometric has emerged as a measure for highly secure identification and personal verification. Biometric system, to conduct the verification requires sensor every time to collect the biometric sample. This sensor is exposed to dusty, sweaty and oily hands depending on person to person thus effects the sensitivity of sensor to gather the accurate sample for verification. There can be a chances that sometime a person needs to withdraw only a little amount, behind him is a long queue. So, just to debit a little cash he has to wait for long time and upon it time consumption for biometric identification is simply irritating and causes much delay than needed. To skip this problem we propose a concept of setting cash limit, where one has to present one's biometric only if one wants to withdraw above the predefined cash limit condition is found to be true else cash withdrawal without biometric is permitted only he just need to enter the OTP. It also guarantees security as each ATM has its cash limit and bank has its transaction limit. So, in case of card misuse, this embedded system developed will prevent withdrawal of large cash. Low amount transaction is secured by the OTP in order to increase sensor durability and to save the user time. It will also limit the maximum amount that can be withdrawn by unauthorized person in case of card misuse. Along with this enven we are securing the ATM machine itself from fraud attacks by using tilt sensor and buzzer.

II. LITERATURE SURVEY

A Novel Method to Enhance the Security of ATM using Biometrics. Nowadays we are using the pin number for security in ATMs, which replaced signature based system. The pin based security is the simplest level of security. The pin number is a unique number which is encrypted and decrypted during transaction. Nowadays the pin number can be extracted through many ways, for fraudulent activity. So, as a solution the pin number can be replaced with biometric security. The biometric security may be fingerprint, retina and so on. Nowadays, the system is used to compare the input image with the image in the database and if they are verified, the bank staff would disperse the cash. But the proposal model would completely replace the pin number with biometric system and the machine would disperse the cash when the comparison gets satisfied. Thus the security of the transaction is improved to a greater extent.

Biometrics to Control ATM Scams: A Study

In the current scenario the way banking and transaction system is changing in the world, the validation, authentication and confirmation of a person is very important and should be of more concern. Authentication and verification has always been the part to worry about the security and confidentiality of the consumers. In the rapid changing environment it's not easy to maintain integrity and authenticity of persons. There is a lot of risk to losing money and identity if we lose our ATM PIN. If it is hacked by someone then we can lose entire money. To prevent all these frauds we need some foolproof security solution which we can use along with the current available technology. Biometric is one of the technologies which we can combine with the current technology. We can use fingerprints, iris scan, palm scanning along with the PIN authentication and verifications. Even we can use voice recognition also. Combination of such technologies may help in reducing the ATM frauds and hence can improve the security level of other financial transactions.

SMART ATM SECURITY SYSTEM USING FPR, GSM, GPS

This paper gives the description of the new approach towards the security of ATM (Automatic Teller Machine) systems. The objective of the paper is to know the Enhanced smart ATM security system which is developed using the Embedded system and advanced technologies. In our proposed system RFID card is used as ATM card, IR sensor in order to sense the presence of the card holders and to turn on Fan and Light, if ATM is tampered then SMS is sent to two main stations via GSM. GPS is used to track the location in case the cash box is robbed. Finger print is used to identify and verify authorized bank personnel. Hence the proposed system is the highly secured system for ATMs. Fingerprint and Iris Biometric Controlled Smart Banking Machine This paper describes a system that replaces the ATM cards and PINs by the physiological biometric fingerprint and iris authentication. system provides protection to the ATM terminal from fire and thief attacks by making provisions of pump motor and a DCmotor for rolling the shutter.

III. PROPOSED SYSTEM

In this proposed system we are securing the atm user transaction by using OTP and biometric. Here we are using RFID card as ATM card, amount and OTP is entered by number pad, OTP is sent to the registered mobile number by using GSM, a finger print scanner is used for biometric security, the output of the overall system is displayed on the lcd. In addition with this a tilt sensor is used for the security of the atm machine, if anybody try to steal the machine then there will be tilting which is sensed by tilt sensor interfaced to the atm machine and is indicated by the buzzer alert. All these sensors are connected to the ATMEGA 328 microcontroller, which is shown in the below block diagram.

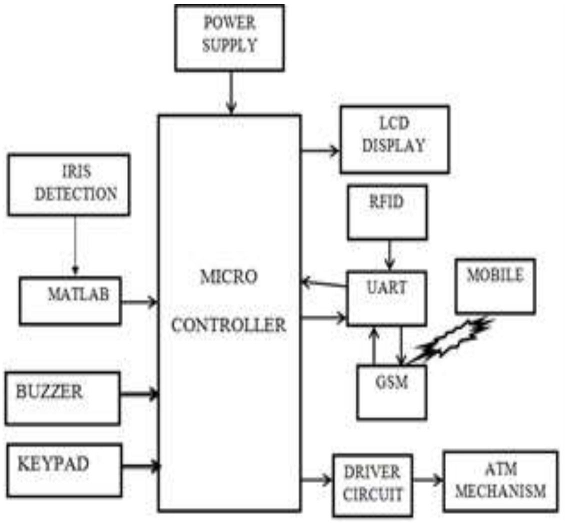


Figure: Proposed Block Diagram

First we will initialize all the components start the procedure by scanning the RFID, we will ask to enter the amount if it is below the permissible limit then will move to A point and we need to enter only OTP no need of scanning the biometric.

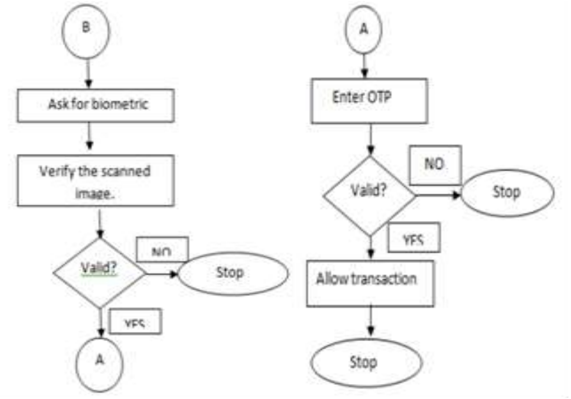


Fig inputting OTP and scanning biometric

If the entered amount is more than permissible limit we need to scan biometric and also we need to enter the OTP if it is matched then only we will allow the transaction. Otherwise transaction ends we need to start it again.

Circular Hough Transform Based Iris Recognition

Image Acquisition: Captures high quality image of the iris with good contrast and sufficient illumination.

- Iris localization: the captured eye image is preprocessed and the iris region is isolated from it which consists of iris/sclera boundary and iris/pupil boundary.
- Iris Normalization: It produces iris images of constant dimensions so that number of iris images being captured will have same features under different conditions.

Feature Extraction: canny detection is used for detecting the edges after applying circular Hough Transform for calculating radius and center coordinates

(x-m)2 +(y-n)2 = r2

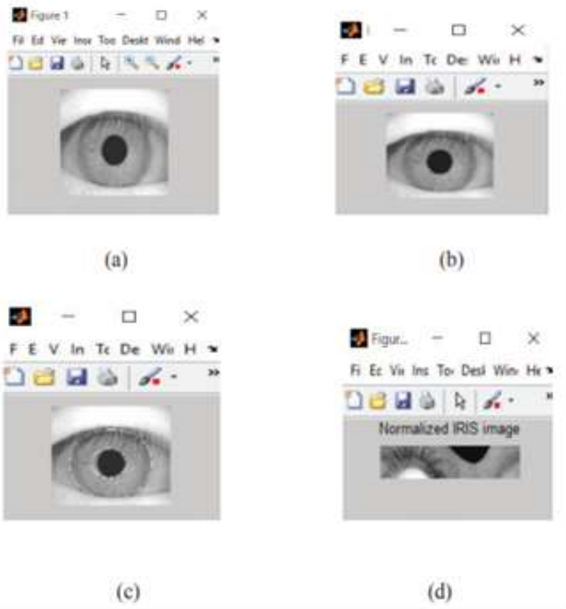
Storage and Matching: stores iris codes in the database where hamming distance algorithm is used for the recognition of the two samples.

N-dimension of feature vector

Pi-ith component of present feature vector\

Ri–ith component of referenced feature vector

After comparison if the two bit patterns are totally random then the hamming distance between them will be close to 1, but if they are similar then it will be cose to 0



(a) (b) (c) (d)

Fig. Original Eye image (b) Grayscale image (c) Iris Segmentation (d) Nornalized image

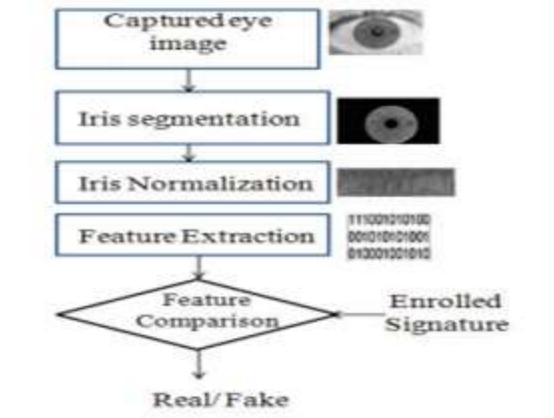


Fig .4. Flow of Iris recognition process

IV. USING GSM TECHNOLOGY FOR OTP GENERATION

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.

A. GSM Module Working

The SIM card mounted on the GSM modem on receiving SMS from some other mobile delivers the data to the microcontroller through serial communication .AT commands control the GSM modem

B. OTP Working

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

a) Generation of a Random Number: Generates a Pseudo- Random Number Sequence. Let it be (YK)

V. EXPERIMENTAL RESULTS

Results for Iris Recognition

The eye image of a person was captured using a QHMPL PC camera and was stored in 640×480 pixels in bitmap format. The Hough Transform detected the iris and pupil boundaries. After capturing the query eye image a feature vector of the input pattern was obtained in the same manner as it was determined during enrollment. This feature vector was compared with those feature vectors present in the database if the person was a valid person then after running the GUI based on Circular Hough Transform a message "MATCH" will be displayed on the monitor, else a message " NO MATCH FOUND" is displayed. Investigations show that the iris recognition system used in this work provides about 95.6% accuracy [9].Table 1 gives an idea of accuracy of the system output for the overall system.

Results for OTP

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 was entered an SMS "UNKNOWN PERSON TRYING TO ACCESS" was received on the user's registered mobile number.

Results for Banking Process

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

VI. CONCLUSION

The use of the biometric as a password has made the ATM transaction system more reliable and secured. The OTP concept added to the system further enhances the security and avoids the need for us to remember passwords. Moreover the system is built on embedded technology which makes it user friendly and non-invasive. Using this system the ATM terminal is secured from fire and thief attacks. The Fig.7and Table.1 shows that the average accuracy of the overall system is 91.6% and the average equal error rate is 0.076. The time taken for the overall ATM transaction is less than 10 sec for each user. The Fig.9 compares the proposed system with the previous ATM transaction systems and shows that the accuracy and security of the proposed system is maximum and reaches upto 95%.

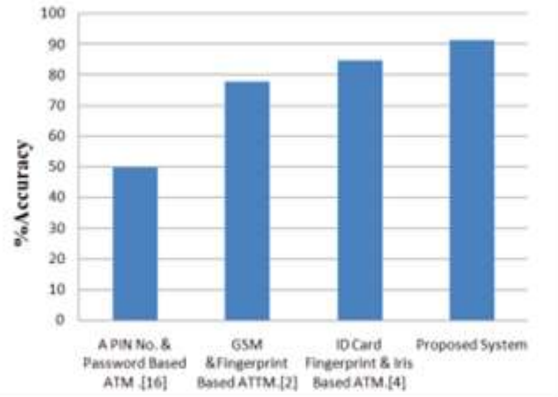


Figure: A graph on the survey of the security in the ATM transaction

REFERENCES

[1] Anil K. Jain, Jianjiang Feng, Karthik Nandakuma,"Fingerprint Matching", IEEE Computer Society2010, pp. 36-44,0018-9162/10.

[2] Khatmode Ranjit P, Kulkarni Ramchandra V,"ARM7 Based Smart ATM Acess 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 Hashing Scheme 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, Ishaq Md,P.J.Saritha,"A Secured Approach for Authentication system using fingerprint and iris", Global journal of

Advanced Engineering Technology,Vol,Issue3-2012.

[5] Mrs.S.P.Balwir, Ms.K.Katole, Mr.R.D.Thakare, Mr.N.S.Panchbudhe, Mr.P.K.Balwir,"Secured ATMtransaction system using microcontroller", International Journal of Advanced Research in computer science and software engineering ",Vol.4,Issue4,April 2014.

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

[7] Ritu Jindal, Gagandeep Kaur, "Biometric Identification System Based on Iris, palm and Fingerprint for Security Enhancements", International Journal of Engineering Research and Technology,Vol.1, Issue 4, June 2012.

[8] Deepa Malviya, "Face Recognition Technique: Enhanced Safety Approach for ATM", International Journal of Scientific and Research Publications, Volume 4, Issue 12, December 2014.

[9] Matsoso Samuel Monaheng, Padmaja Kuruba, "Iris Recognition Using Circular Hough Transform", International Journal ofInnovative Research in Science,Engineering and Technology,Vol.2, Issue 8, Aug.2013.

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

[11] Mohsin Karovaliya,Saifali Karedia,Sharad Oza, Dr.D.R.Kalbande, "Enhanced Security for ATM machine with OTP and facial recognition features", International Conference on Advanced Computing Technologies and Applications (I CATA-2015).

[12] R. Wildes, J. Asmuth, G. Green, S. Hsu, R. Kolczynski, J. Matey and S. McBride, "A system for automated iris recognition", Proceedings IEEE Workshop on Applications of Computer Vision, Sarasota, FL, pp. 121-128, 2011

[13] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," IEEE Security Privacy Mag., vol. 1, no. 2,pp. 33–42, 2003.

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

[15] S. Sai Kumar et al, "Fingerprint Minutia Match Using Bifurcation Technique", International Journal of Computer Science & Communication Networks, Vol 2(4), 478-486.

[16] Ravi.J. et al, "Fingerprint Recognition using Minutiae Score matching", International Journal of Engineering Science and TechnologyVol.1(2), 2009, 35-42.

[17] Bashar Ne'ma and Hamza Ali,"Multi Purpose Code Generation Using Fingerprint Images", The International Arab Journal of Information Technology,Vol.6,No.4,Oct. 2009.