2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT)
International Institute of Information Technology (I²IT), Pune

Fingerprint and Iris Biometric Controlled Smart Banking Machine Embedded with GSM Technology for OTP

Joyce Soares
Electronics & Telecommunication Department
Zeal College of Engineering &Research, Nahre,
Pune,India
joycejas@rediffmail.com

A.N.Gaikwad
Electronics & Telecommunication Department,
Zeal College of Engineering &Research, Nahre,
Pune ,India
arun.gwkd47@gmail.com

***Abstract*—Frauds attacking the automated teller machine has increased over the decade which has motivated us to use the biometrics for personal identification to procure high level of security and accuracy This paper describes a system that replaces the ATM cards and PINs by the physiological biometric fingerprint and iris authentication. Moreover, the feature of one time password (OTP) imparts privacy to the users and emancipates him/her from recalling PINs. Additionally the system provides protection to the ATM terminal from fire and thief attacks by making provisions of pump motor and a DC motor for rolling the shutter. In this system during enrollment the genuine user's fingerprint and iris samples of are retained in the database. The process of transaction begins by capturing and matching fingerprints and iris patterns. The system will automatically distinguish between real legitimate trait and fake samples. A GSM module connected to the ARM7 LPC2148 will message a 3-digit code generated by the system to the registered mobile number. After the valid OTP is entered the user can either withdraw or deposit cash or check his/her balance. In any kind of fake access attempts the account is blocked .In this paper the experimental results are obtained on the data set of fingerprint and iris in real time using fingerprint module with a minutiae matching algorithm and a GUI based of Circular Hough Transform respectively**.

Keywords— Authentication, Biometrics, Circular Hough Transform, Enrollment, Global System for Mobile Communication (GSM), Minutiae Based Algorithm, One Time Password (OTP).

I. INTRODUCTION

A 24 x7 self banking service has made the ATM the heart of banking. The surplus use of ATMs, has not only lead to an increase in their number but has also increased fraudulent attacks on the ATMs. This calls for the biometric systems to be integrated in the traditional ATM. The author in [1] Built an ATM based on fingerprint verification and incorporated the fingerprints of the users into the database of the respective banks to simulate it for ATM operations. Due to the lack of the fingerprint matching algorithm it proved to be inefficient. [2] Proposed a system which performed authentication by including both the fingerprint and GSM technology into the traditional PIN based ATM system. In [3] an algorithm was constructed based on Short Message Service (SMS) verification to enhance the ATM authentication system. Authors in [4] secured the system using fingerprint and iris, along with this the system used RFID reader module. [5] developed a RFID card as input to the microcontroller for identification and a GSM module to send messages involving three options (yes, no, action) to the authorized user's mobile. Authors in [6] proposed an efficient system which used the method of analyzing iris patterns for user identification In [7] a system using iris recognition and palm vein recognition technology was proposed in order to avoid crimes in the ATM transactions. Authors in [8] proposed a system which incorporated facial recognition in the traditional ATM for authentication of users. In [9] authors used Hough Transform for iris recognition in order to isolate the unique features of particular shape within an image. In [10] an Advanced Encryption Standard (AES) algorithm was used in order to enhance the security of the ATM transaction. [11] described a system which used face as a key. The system performed facial recognition using Principal Component Analysis for facial recognition along with OTP for security of transaction.

This proposed system utilizes minutiae matching algorithm for fingerprint recognition and Circular Hough Transform for iris recognition. The later part of this paper is designed as follows: The system development is furnished in Section II .Proposed Biometric identification techniques are described in Section III. GSM technology for OTP generation is explained in Section IV. Experimental results are focused upon in Section V. In Section VI finally conclusion are drawn with the help of comparisons with the previous systems.

II. SYSTEM DEVELOPMENT

A. An Overview of the Proposed System

In the proposed system we present a fraud detection method using two biometrics (fingerprint and iris) to detect various types of illegal access attempts during the ATM transaction. The objective of the proposed system is to

enhance the security of the ATM transaction using biometric recognition frameworks. In this system ARM7 based LPC2148 controlling is used for smart ATM access. The fingerprint module utilizes the minutiae based algorithm for fingerprint recognition it captures the fingerprint of the person and compares it with the fingerprint of the genuine person stored during enrollment. If the person is a valid user the controller will display a message "VALID PERSON" on the LCD. The USB camera is used to capture the eye image of the user. A GUI prepared in Matlab based on Circular Hough Transform is used for iris recognition. After iris authentication and matching if the person is a true user then the controller displays a message "IMAGE IDENTIFIED" on the LCD. During this process there will be continuous monitoring of the position and temperature and a message will be displayed on the LCD which includes "POSITION:" and "TEMP:".After the validation result of the person is true a 3 digit code is messaged to the customer's registered mobile number which was saved in the database during enrollment. This process is done through the GSM module which is interfaced to the ARM board. Depending on whether the OTP entered is correct or wrong messages like" CORRECT CODE "or "REENTER CODE" is displayed on the LCD. After the entered code is found valid the banking process begins and a message "BAL, DEP, WTD" for entering the option for the task to be performed is displayed on the LCD.After the task is performed finally a message "TRANSACTION COMPLETED" is displayed on the LCD.

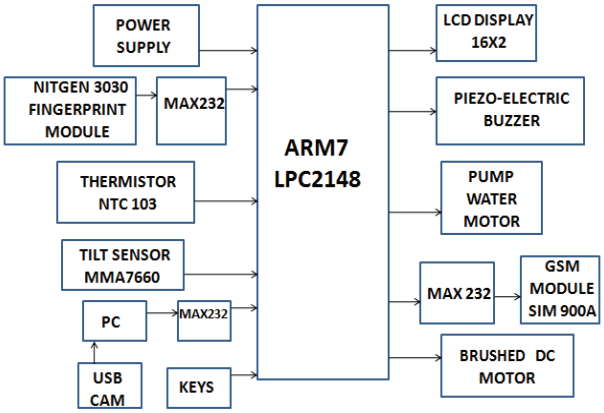


Fig. 1. Proposed system block representation

III. Proposed Biometric Identification Techniques

A. Minutiae Based Fingerprint Recognition

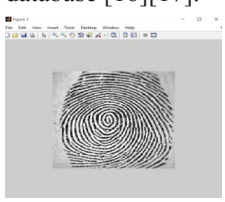
The fingerprint image undergoes preprocessing stages like binarization which uses fixed threshold to convert a grayscale image to a binary image and then proceeds to thinning process to reduce the thickness of all ridge edge lines to a single pixel width after which an initial code is generated, prior to the secured final code. The code block consists of five sub-blocks placed within the header and trailer. The five sub-block patterns are five minutiae characteristics which are chosen of suitable length for example consider 14 bytes:

- Type: It specifies the termination and bifurcation points. Three bytes are allocated for this parameter.

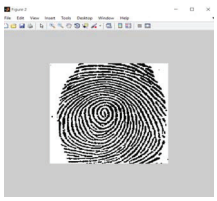
- Orientation: Each minutia point faces a particular direction. It is either clockwise (CW) or counter clockwise (CC). Two bytes are allocated for this parameter. Let gradient x be(gx) and gradient y be (gy) therefore orientation estimation is given by ɵ

$$ɵ = \tan^{-1}[g(y)/g(x)] \quad \ldots\ldots(1)$$

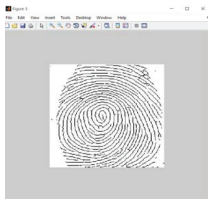
- Spatial Frequency: indicates the distance of the ridges in the neighborhood of the minutia point. It's measured in pixels and only one byte is allocated for this parameter.
- Curvature: Is the rate of change of ridge orientation. It is also measured in pixels and one byte is allocated for this parameter.
- Position: indicates its x, y location. It is calculated in relative to the core or delta points One byte is allocated for this parameter. An initial code string of 14 bytes is generated depending on these features and it is saved in the database. Later this code is passed through the one way hash MD5 algorithm to generate a secured multipurpose code. The Fig.2 gives the matlab results when a minutiae matching algorithm is applied to a fingerprint image from the Fingerprint Verification Competition (FVC) 2002 database [16][17].



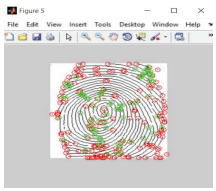
(a)



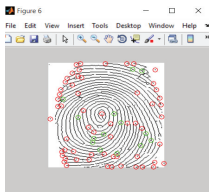
(b)



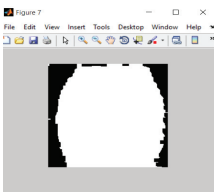
(c)



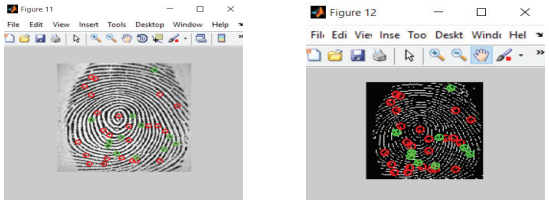
(d)



(e)



(f)



(g) (h)

Fig. 2. (a) Original image (b)Binarized image (c) Thinned image (d) Minutiae Terminations points (e) Minutiae Bifurcations marked (f) ROC (g) Extreme Minutiae Suppressed (h) Orientations

B. 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 pre-processed 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.

$$I(x(\rho, \theta),y(\rho, \theta))=>I(\rho, \theta)\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

The value of θ ranges within [0 2π], ρ covers [0 1]

- Feature Extraction: canny detection is used for detecting the edges after applying circular Hough Transform for calculating radius and center co-ordinates. The characteristic equation of a circle of radius r and center (m, n) is given by

$$(x-m)^2+(y-n)^2= r^2\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3)$$

This circle can be described by the two following equations:

$$x=m+r\cos(\theta)\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(4)$$
$$y=n+r\sin(\theta)\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(5)$$

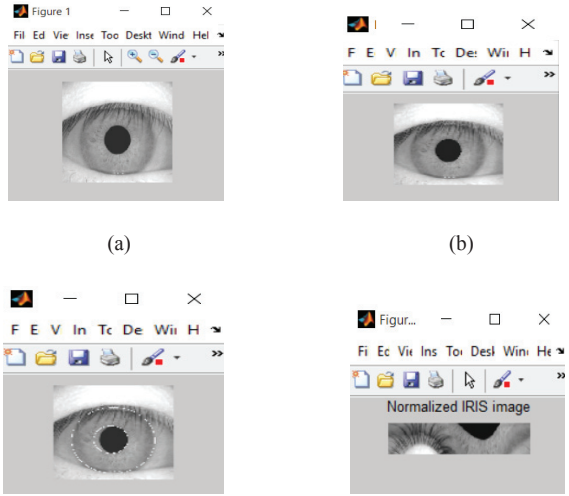
the Hough transform thus searches for the triplet of parameters (m, n, r) which determines the points (x_i,y_i)[9].

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

$$HD=1/N\sum (Pi \oplus Ri)\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(6)$$

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

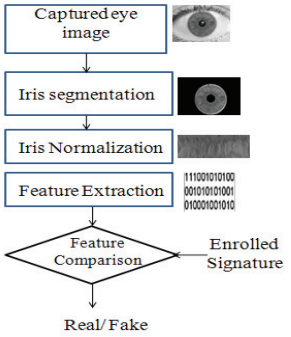


Fig .4. Flow of Iris recognition process

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[11].

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

$$Y_{K+1}=(a\times Y_K +I)\text{mod } (m)\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(7)$$

a- multiplier
I-increment
m- modulus

V. Experimental Results

A. Results for Thermistor

The thermistor NTC 103 which is used in the system will continuously monitor the temperature and display it on the 16 X 2 LCD .A thershold of 49 ^{0} C is set while programing, when the temperature inside the ATM terminal increased above this limit the permisible water pump motor turned on and the buzzing sound was heard, indicating a fire atttack on the ATM terminal.

B. Results for Tilt Sensor

The MMA7660 tilt sensor interfaced in the system is a free scale accelerometer. It is set in Shake mode. ASIC uses the technique of switched capacitors to measure the g-cell capacitor and from the difference between the two capacitor the acceleration data is extracted. The ASIC also signal conditions and filters the signal providing the digital output that is proportional to acceleration. When we shook the tilt sensor the fan 12V DC motor turned on and a buzzing sound was heard.

C. Results for Fingerprint module

When a fingerprint was placed on the NITGEN 3030 fingerprint recognition device it captured a 3D grayscale image after scanning the fingerprint and a 256×288 pixels image was stored in bitmap format. Key minutiae were extracted using a minutiae based algorithm which converted it into a unique mathematical template that could be compared to a 60 digit password. This template was stored in the database after encryption. When the same user's new fingerprint image was captured a new template of that query image was created in the same manner as it was done during enrollment. This new template was compared with the templates in the database and a message "VALID PERSON" was displayed on the LCD but when another fake user went through the same process a message "PERSON NOT IDENTIFIED" was displayed and the buzzer turned on. The minutiae matching algorithm within the module provides about 75-80% accuracy[17].

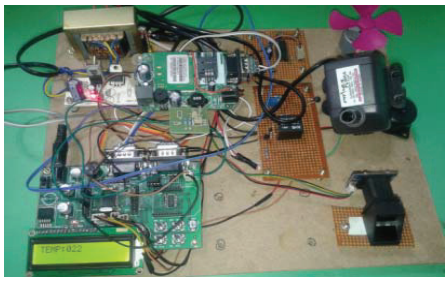
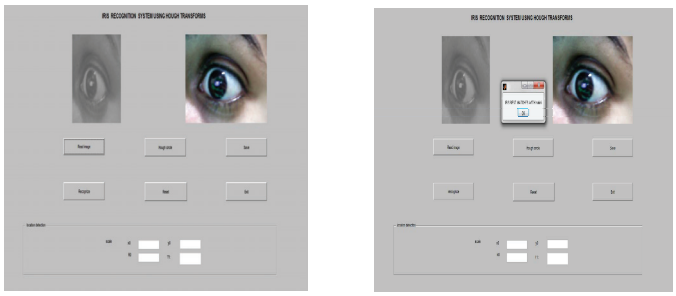


Fig.5. Hardware for fingerprint recognition, temperature sensing & position sensing

D. 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.



(a) (b)

Fig.6. GUI for Iris recognition (a) Iris enrollment (b) Iris Authentication

Table 1:Analysis of the proposed system

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

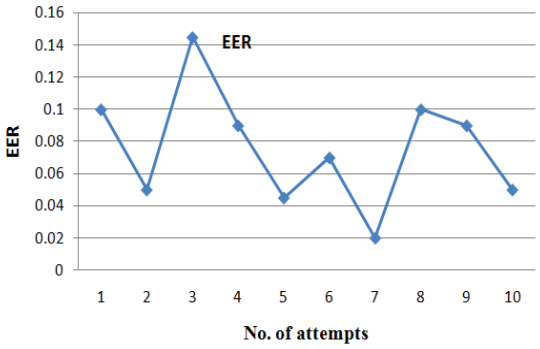


Fig.7. Graph for the equal error rate (EER) of the proposed system

E. 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 vaild 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.

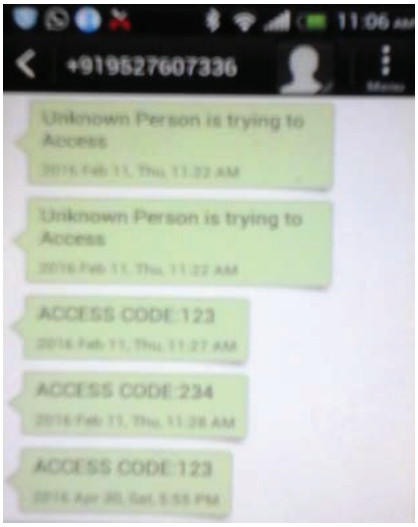


Fig.8. OTP messages received on the mobile screen

F. 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%.

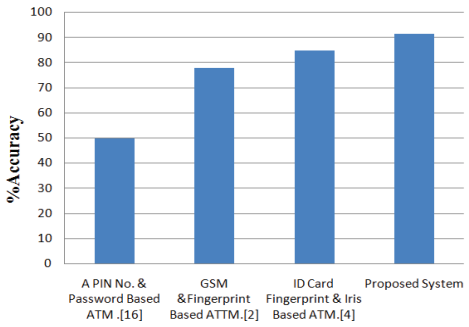


Fig.9: A graph on the survey of the security in the ATM transaction

Acknowledgement

Both the authors Joyce Soares and Arun Gaikwad would like to thank the anonymous referees whose help and technical ideas have improved the quality of the paper.

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,"SecuredATMtransaction system using micro-controller", 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 of

Innovative 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 ConferenceonAdvancedComputingTechnologiesandApplications(ICATA-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.