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

CharanGowda S, Adithya S, Jayshree R, Manishri T.L
Computer Science & Engineering Department, Rajiv Gandhi Institute of Technology, Bangalore, India

Abstract- Automated teller machine (ATM) usage has increased over decades and they are susceptible to attacks such as security and accuracy. This paper is alternate to cards and PIN. Such as physiological biometric. Fingerprint recognition is one of the most reliable and promising personal identification technologies. Today, identification and verification of a person are common and important at secured places. The current debit card and signature verification of a person do not provide much perfection and reliability. Fingerprint-based identification is one of the more mature and proven techniques. The proposed system enhances security by combining fingerprint availability, reliability, uniqueness, and high accuracy. The face is computer technologies begin used in a variety of application. In case of emergency if the user is unable to access his account for withdrawing money from ATM his/her nominee can access the account on his/her behalf using mobile technolog**y.**

Keywords-*Authentication, Biometrics, Face detection, Viola-Jones algorithm, Global System for mobile communication (GSM), minutiae-based Algorithm, One-time password (OTP)*

I. INTRODUCTION

A 24x7 self-banking service has made the ATM the heart of banking. The surplus use of ATM 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 with the tradition ATM. The author in [1] built an ATM based on fingerprint verification and incorporated the fingerprints of the user into the database of the respective banks to simulate it for ATM operations. In [2] an algorithm was constructed based on short Message Service verification to enhance the ATM authentication system. The system used for fingerprint and face recognition, along with GSM module to send messages involving three options (yes, no, action) the authorized user's mobile. In [3] a system using face recognition technology was proposed in order to avoid crimes in the ATM transactions. Authors in [4] proposed a system which incorporated facial recognition in the traditional ATM for authentication of the user's. In [5] authors used Hough Transform for face recognition in order to isolate the unique features of particular shape within the image.In [6] a Viola-Jones algorithm was used in order to enhance the security of the ATM transaction. [7] Described a system which used the face as a key. The system performed facial recognition using Principal Component Analysis for facial recognition along with OTP for the security of the transaction. Due to lack of the fingerprint matching algorithm, it proved to be inefficient. [8] Proposed a system which performed authentication by including the fingerprint face recognition and GSM technology into the tradition PIN-based ATM system. The proposed system utilizes minutiae matching algorithm for fingerprint recognition and face recognition. This paper is organized 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 provisions systems.

II. SYSTEM DEVELOPMENT

A. An Overview of the Proposed System

The proposed system presents a frauds detection method using biometrics (fingerprint and face recognition) 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. An ARM7 based LPC2148 controller 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 registration. If the person is valid using the controller with display a message “VALID PERSON” on the LCD. The USB camera is used to capture a face image of the user. A GUI prepared in t Matlab is used for face recognition. After face authentication and matching if the person is valid user the controller displays a message "IMAGE IDENTIFIED" on the LCD.

After the validation, the banking process begins and options 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. For Nominee fingerprint recognition it captures the fingerprint of the person and compares it with the fingerprint of the genuine person stored during registration. After the validation results of the person, a 3 digit code is messaged to the customer's registered mobile number which was saved in the database during enrolment. 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 bank process begins.

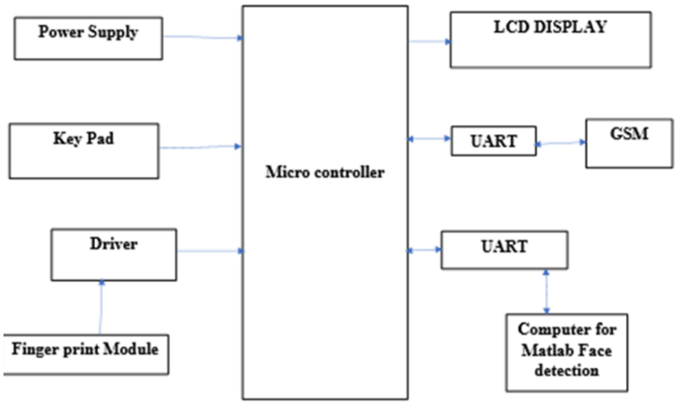


Fig.1: Proposed system block representation

III. PROPOSED BIOMETRIC IDENTIFICATION TECHNIOUES

A. Minutiae-Based Fingerprint Recognition

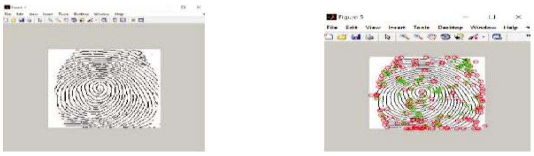
The fingerprint image undergoes pre-processing stages like binarization which user fixed threshold to convert a grayscale Image to binary image a thinning process to reduce the thickness of all ridge edge lines to a single pixel width after which an initial code is generated, prior to the secured final code. The code block consists of five sub-blocks placed within the header and trailer. The fiver 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 counters clockwise (CC). Two bytes are allocated for this parameter. Let gradient x be (gx) and gradient y be (gy) therefore orientation is given by ң

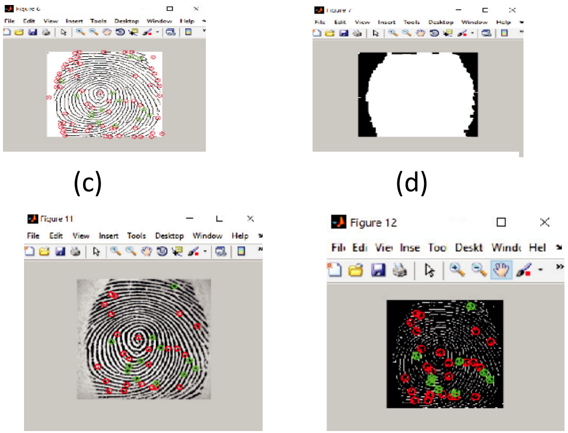
Ң=tan [g(y)/g(x)]... (1)

- 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 minutia matching algorithm is applied to fingerprint image from the Fingerprint Verification Competition (FCV) 2002 database [16][17].



(a) (b)



(c) (d)

(e) (f)

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

B.VIOLA-JONES Face detection

The Viola-Jones face detection method is the first frame based on object detection that provides good detection rates in the real i-time is given by Paul Viola & Michael Jones in the year of 2001. This algorithm has been implemented in software 'Matlab' using the method vision. CascadeObject Detector The Viola-Jones contains 3 techniques for the facial parts detection:

1. The Haar-like features for the feature extraction are of a rectangular type which is determined by an integral image.
2. Ada boost is a machine-learning method for detecting the face. The term 'boosted' determines the classifiers that are complex in itself at each stage, which are built of basic classifiers using any one of the four boosting techniques.
3. Cascade Classifier Used to combine many of the features efficiently. The term 'cascade' in a classifier determines the several filters on a resultant classifier.

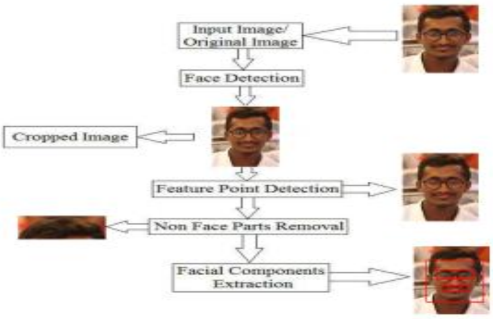


Fig.3: Flowchart

C.Face recognition

The next step in the process is to identify the detected face using Artificial Neural Network. An Artificial neural network can be compared to a human brain system. The concept of Artificial Neural Network is to make the computer think like a human brain. The neural network system has building blocks called as neurons and all the neurons are connected by a path to carry electric current referred to as synapses. An Artificial Neural Network has inputs, outputs and hidden cells shown in Fig.4

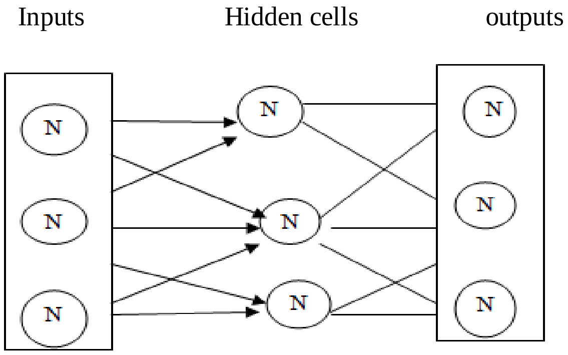


Fig.4: Artificial Neural Networks

The Neural Network finds the connection weights between the inputs, output and hidden cells through backpropagation technique. The Neural Networks learn through the backpropagation technique and determine the connection weights between the inputs, outputs and hidden cells and the desired output is calculated. The backpropagation uses the formula that has weights, inputs, outputs, error and learning rate to minimize the error.

D. Training of Neural Networks

For each individual in the database one, ANN is used. Face descriptors are used as input for the training of ANN. The face descriptors belonging to the same individual are used as positive examples for others. For identifying the individual trained network will be used.

E. Simulation of Neural Networks

All the networks are simulated with face descriptors of the test image calculated from the Eigenfaces as input Maximum output greater than a predefined threshold level confirms that the test image belongs to the recognized person with the maximum output.

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 access for communication and can support 64kbps to 120Mbps of a 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. The commands control the GSM modem

B. OTP Working

The password which is valid only for a single transaction is a One Time Password [11]. Generation of a Random Number: Generates a Pseudo- Random Number Sequence. Let it be (YK)

$$YK+1= (a\times YK +I) \bmod (m)\ldots\ldots\ldots\ldots(2)$$

a- multiplier, I-increment, m-Modulus

V. EXPERIMENTAL RESULTS

A. Results for Fingerprint Module

When a finger was placed on the Biometric fingerprint recognition device it captured a 3D grayscale image after scanning the finger and it will be stored in bitmap format. Key minutiae were extracted using a minutiae based algorithm which converted it into a unique mathematical template. 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 enrolment. 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.

B.Results for Face recognition module

The experiment has been evaluated on several face image database, containing a different collection of photos. A Face database named Bao database contains the image of several faces at various lighting conditions and in various poses which were detected using the algorithm. This gives an accuracy of 92%. And other databases such as AR-Face database, Yale Face database contain straight faces which are not very complex or variant to detect the face on it. So the face with varying parameters in this database and it has done recognition and trained the classifier. So it is a proper database to test the full algorithm. In the algorithm, it can detect the various facial parts of a human and some non-facial regions are removed using thresholding techniques. These experimental results of facial features are as shown in fig 5.

When the image detects some non-textured facial features the merge. The threshold value is increased and tested. The Merge Threshold here is based on the intensity of regions and its defaults value is 4. The Merge Threshold value is also based on the image size and their intensity variations is an image.

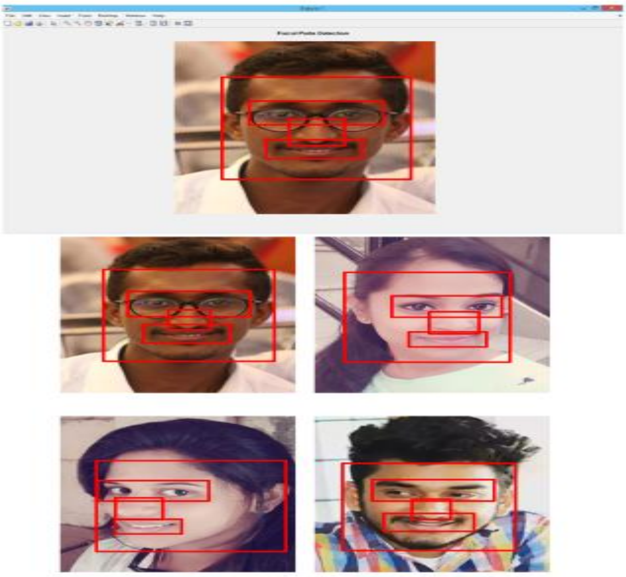
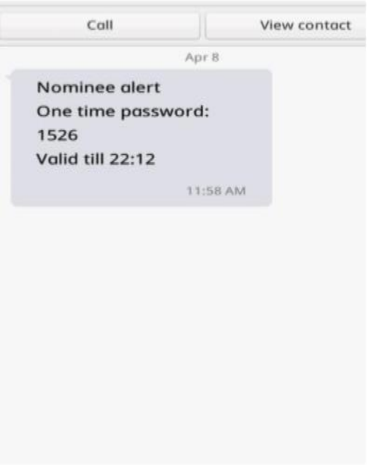


Fig.5: Experimental Results

C.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 to 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.



Apr 8

Nominee alert
One time password:
1526
Valid till 22:12

11:58 AM

Fig.6: OTP message received on the mobile screen

D. Results for Banking process

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

VI. CONCLUSION

The use of the biometric and face recognition 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 remembering 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. The time taken for the overall ATM transaction is less than 10 sec for each user. The proposed system with the previous ATM transaction system and shows the accuracy and security of the proposed system are maximum and reaches up to 95%.

ACKNOWLEDGMENT

The authors Charan Gowda, Jayshree, Adithya, and Manishri would like to thank the Dr. Pamela Vinitha, Head of the Department of Computer Science and Engineering of Rajiv Gandhi Institute of Technology Bangalore and Mrs. Vandana. R Asst. Professor, Dept. of CSE, Rajiv Gandhi Institute of Technology Bangalore and anonymous referees whose help and technical ideas have improved the quality of the paper.

VII. REFERENCES

[1]. AnilK.Jain, JianjiangFeng, Karthik Nandakumar,"Fingerprint Matching", *IEEE* Computer Society2010, pp. 36-44,0018-9162/10.

[2]. KhatmodeRanjit P, KulkarniRamchandra 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.UdayaShree, 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.ShelkarGoud, 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]. Xi Zhao, Emmanuel Dellandrea and Liming Chen, “A People-Counting System based on Face-Detection and Tracking in a Video”, Advanced Video and Signal Based Surveillance, (2009).

[6]. Tsong-Yi Chen, Chao-Ho Chen, Da-Jinn Wang, and Yi-Li Kuo, “A People-Counting System Based on Face-Detection”, Fourth International Conference on Genetic and Evolutionary Computing, (2010).

[7]. J. L. Crowley, T. Cootes, “FGNET, Face and Gesture Recognition Working Group”, http://wwwprima. inrialpes.fr/FGnet/html/home.html, (2009).

[8]. B. Fasel and J. Luettin, “Automatic Facial Expression Analysis: A Survey,” Pattern Recognition, Vol. 36, pp. 259-275, (2003).

[9]. Elena Alionte, Corneliu Lazar, “A Practical Implementation of Face-Detection by Using Matlab Cascade Object Detector”, 19th International Conference on System Theory, Control and Computing (ICSTCC), (2015).

[10]. Abhishek Bansal, Kapil Mehta, Sahil Arora, "Face Recognition using PCA & LDA algorithm", Second International Conference on Advanced Computing and Communication Technologies, (2012).

[11]. MohsinKarovaliya,SaifaliKaredia,SharadOza, Dr.D.R.Kalbande, ”Enhanced Security for ATM machine with OTP and facial recognition features”,InternationalConferenceonAdvancedComputingTechnologiesandApplications(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]. KhatmodeRanjit P, KulkarniRamchandra 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 technology vol.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.