IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321- 5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

NFTPCOS-18

National Conference on Future Technologies in Power Control and Communication Systems

College of Engineering Perumon, Kollam, Kerala

Vol. 1, Special Issue 2, March 2018

Face Recognition and Finger Print Based Enhanced Security System for ATM Transaction

Surjith S[1], Akshaya Mohan[2] Akhila Alexander[3], Ayana Mohanan[4]

Asst. Prof, Dept of Electronics and Communication,College of Engineering,Perumon,Kollam,India[1]

UG student, Dept of Electronics and Communication, College of Engineering, Perumon, Kollam, India[2,3,4]

Abstract: Access control has been a great concern in the information and communication era. In this proposed system we try to reinforce the security of conventional ATM models by using password authentication method combined with biometric identification technology. Biometric refers to automatic identification of a person based on his/her physiological characteristics. Biometric introduces its own challenges such as being irreplaceable once compromised. Biometric authentication is achieved by capturing the fingerprint and facial features of the client. Then the system will check for user's identity. If it finds valid, the ATM machine will ask the customer for 4 digit code. The 4 digit code is automatically generated by the system as OTP which is sent to the customer's registered mobile number. Here the customer has to enter this code. The system checks for the validity of the code. If it is found valid bank transaction starts and the customer is able to access his account. Provisions are also included for securing the ATM terminal from fire and theft attacks

Keywords: ATM machine, Authentication, OTP, Biometric

I. INTRODUCTION

Nowadays ATM has become the heart of banking processes. With the increase in number of banking services and ATMs the number of fraudulent attacks on them is also on increase. Many systems has been proposed to avoid such attacks. Biometrics introduces safer and newer technologies for preventing ATM thefts and attacks. Biometric character of a person will be different from that of other .Therefore biometrics can be incorporated into traditional ATMs.

The author in [1] proposed an ATM that includes fingerprint verification in which fingerprints of the users are incorporated into the database of the respective banks. It proved to be inefficient due to the lack of fingerprint matching algorithm. [2] Proposed a traditional PIN based ATM system which performed authentication using finger print and GSM technology. As finger print matching alone provides lesser security, the system was proved to be not much efficient. Authors in [3] secured the system using finger print and iris along with RFID reader. [8] Described a system using facial recognition methods for user identification. Our proposed system provides multi security using finger print matching, facial recognition and OTP which enhances the security of ATMs. Implementation of this card less system swipes away the problems like stolen PINs, lost cards and difficulty in memorizing the password .Biometric authentication introduces certain challenges in situations when the user is not able to access the ATM terminal himself due to illness or other domestic issues .To avoid such cases our proposed system has provided an additional facility for the user to authorize a second person whom he trust to access his account. This proposed system uses a finger print sensor for storing the databases during enrolment and provides access to the valid users account if the scanned fingerprint matches with that in the database. .It also uses Hog algorithm to identify the facial features of the valid user. The later parts of this paper are as follows: Overview of the proposed system is discussed in section 2. The different biometric techniques which are employed in this system are discussed in section 3. The technique used in generating the OTP is discussed in section 4.Experimental results will be described in section 5. Conclusions and future scope in section 6.

II. PROPOSED SYSTEM

In our proposed system we introduce an ATM which is purely based on biometrics. The use of multiple biometrics adds more security to the system. The illegal access to the account can be prevented by the use of biometrics. Our prime objective is to reduce the effort of carrying smart cards and memorizing the PINs and to enhance the security of ATMs. In this system ARM7 based microcontroller is used. This is the core of the system. The finger print module attached to the controller captures the finger print images of the user and compares that image with that stored during the enrolment process. If the person is a valid user ie if the finger print matches, then a message "VALID PERSON' is

IJIREEICE
ISSN (Online) 2321-2004
ISSN (Print) 2321- 5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
NFTPCOS-18
National Conference on Future Technologies in Power Control and Communication Systems
College of Engineering Perumon, Kollam, Kerala
Vol. 1, Special Issue 2, March 2018

displayed on the interfaced LCD screen. Otherwise "INVALID PERSON" will be displayed. USB cam in the PC captures the facial image of the user and compares with the image in the database. It is based on hog algorithm. If the person is a true user, then message "IMAGE IDENTIFIED" is displayed on the LCD. After matching of both finger print and facial feature and OTP will be sent to the user's registered mobile number The transaction will be started by entering the 3 digit OTP. This process is performed by GSM Module. If the entered OTP is found correct, the transaction begins or else the message" RE-ENTER PIN" will be displayed on the screen. At the same time there will be monitoring of temperature and position of the ATM terminal and message "TEMP "and "POSITION" will be displayed on the screen. If the position of the banking machine changes, i.e in case of theft attacks, the electric buzzer associated with it sounds and the shutter of the terminal will be automatically closed. If the temperature inside the terminal increases above the threshold value , ie in case of fire attacks water sprayer is turned on. After the transaction "TRANSACTION COMPLETED" message will be displayed on the screen

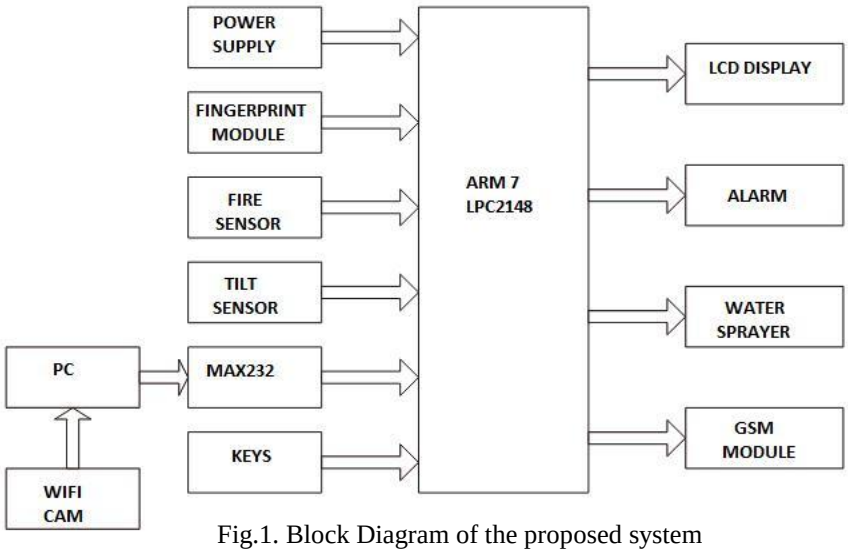


Fig.1. Block Diagram of the proposed system

III. PROPOSED BIOMETRICS

A. Finger Print Module

In our proposed system we use R30X series fingerprint identification module. The power consumption of this module is about 3.6 to 6 volt. Its image acquiring time is less than 0.5 seconds average searching time is less than a single second.

Fig.2. Fingerprint Module

1) Fingerprint overview: Fingerprinting utilizes distinctive features of the fingerprint to identify or verify the identity of individuals. All fingerprints have unique characteristics and patterns. A normal finger print pattern is made up of lines and spaces. These lines are called ridges while the spaces between the ridges are called valleys. It is through the pattern of these ridges and valleys that a unique fingerprint is matched for verification and authorization. These unique fingerprint traits are termed "Minutiae" and comparisons are made based on these traits. On average a typical live scan produces 40 minutiae. The Federal Bureau of Investigation (FBI) has reported that no more than 8 common minutiae can be shared by two individuals.

IJIREEICE
ISSN (Online) 2321-2004
ISSN (Print) 2321- 5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
NFTPCOS-18
National Conference on Future Technologies in Power Control and Communication Systems
College of Engineering Perumon, Kollam, Kerala
Vol. 1, Special Issue 2, March 2018

2) Operation principle: There are two parts for this finger print processing: fingerprint enrollment and finger print matching. During fingerprint enrollment the user needs to scan his fingerprint image twice. The system will process both the images based on the processing results and generate template of the finger. During the matching process, user enters his/her fingerprint through the sensor and the system will generate a template of his/her fingerprint. The system will search the whole library for the matching fingerprint

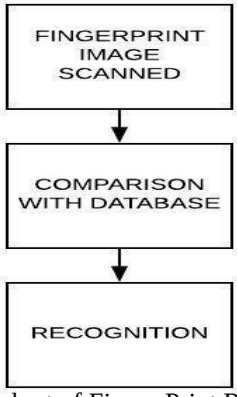
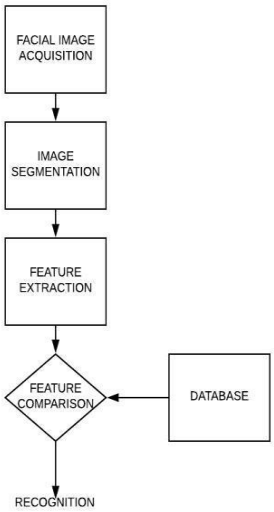


Fig. 3 Flow chart of Finger Print Recognition

B. Facial Recognition: A high quality image of the face is captured with good contrast and sufficient illumination. The captured image is pre-processed and the required facial region is isolated from it. Images of constant dimensions are produced so that number of images being captured will have same features under different conditions. The features are extracted with the help of HOG, LBP and wavelet transform. HOG stands for histogram of orientation of gradience.



HOG stands for histogram of oriented gradients. This descriptor in used mainly in real time applications of facial recognition since it is less complex compared to others. It takes into account the image gradients and its statistical properties of its orientations. The idea conveyed by the descriptor is that the object's appearance and shape is characterized by the distribution of local intensity gradients or edge directions.LBP stands for local binary pattern. It takes into account the neighboring pixels of an image while computing the histogram of the image. It is highly sensitive to noise. In wavelet transform the transformation values are the wavelet coefficients which are interpreted as the objects for classification. The next step after feature extraction is classification. The classifier used is the Random Forest classifier. It is a decision tree type classifier. The classified data is then subjected to training and testing to obtain the output of facial recognition. GSM is a mobile communication modem. It stands for global system for mobile communication. The idea of GSM was developed at Bell Laboratories in 1970. It is widely used mobile communication system in the world. GSM is an open and digital cellular technology used for transmitting mobile voice and data services operates at the 850MHz, 900MHz, 1800MHz and 1900MHz frequency bands. A GSM digitizes and reduces the data, then sends it down through a channel with two different streams of client data, each in its own particular time slots.

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321- 5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

NFTPCOS-18

National Conference on Future Technologies in Power Control and Communication Systems

College of Engineering Perumon, Kollam, Kerala

Vol. 1, Special Issue 2, March 2018

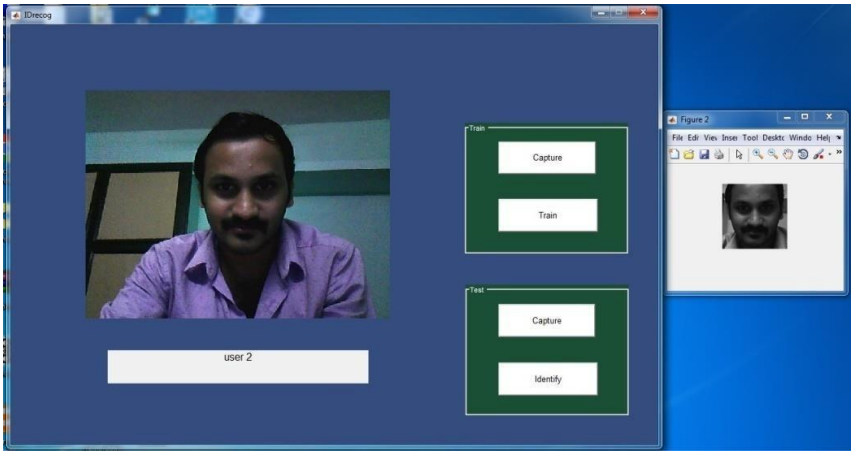


Fig. 5 Graphical user interface of facial recognition

IV. GSM TECHNOLOGY FOR OTP GENERATION

A. GSM Module Working

A SIM card will be mounted on the GSM module. When both the biometrics are matched an OTP will be generated and is sent to the user's registered mobile number.

V.EXPERIMENTAL RESULTS

A. Flame Sensor: A flame sensor is used in the system for the protection of ATM terminal against fire. When there is a flame detected by the sensor, buzzer is sounded and water sprayer is turned ON and water was sprayed to the flame.

B. Shake Sensor: The shake sensor ADXL is used to identify any theft attacks in the ATM terminal. In case of shaking of the terminal the buzzer was sounded.

C. Results for Finger Print Module: When a fingerprint was placed on the fingerprint module , it captured the image and converted into a template and was stored in the database. When the same user's new fingerprint image was captured during transaction process a new template of that 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.

D. Results for Facial Recognition: The facial image of a person was captured using a WI-FI camera and the three features viz local binary pattern, hog(histogram of orientation of gradients),wavelet transform were extracted and combined as a single feature and stored in the database as a feature vector. When the same user's new facial image was captured during transaction process a new feature of that image was created in the same manner as it was done 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 a message "MATCH" will be displayed on the monitor, else a message " NO MATCH FOUND" is displayed.

E. OTP: After the valid biometric identification of the account holder a message "ACCESS CODE" SMS was received on the user's registered mobile number. Also a message "ENTER THE CODE" was displayed on the LCD screen simultaneously. After the valid code was entered the transaction starts. But when the wrong code was entered an SMS "UNKNOWN PERSON TRYING TO ACCESS" was received on the user's registered mobile number.

VI. CONCLUSION

User having accounts in more than one bank needs to carry more smart cards and memorize the PINs .Use of biometric says" you be your own password". The use of the biometric as a password has made the ATM transaction system more reliable and secured. The OTP concept added more security and reliability to the system and avoids the need for us to remember passwords. Also there is no need to carry the smart cards with us. 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 time taken for the overall ATM transaction is less than 10 sec for each user .By implementing this system 'YOU BECOME YOUR OWN PASSWORD'

ACKNOWLEDGMENT

We, **Akshaya Mohan, Akhila Alexander, Gopika S Nair and Ayana Mohanan** would like to thank our guide **Surjith S** for his constructive suggestions in improving the quality of this paper. We also thank the anonymous referees for their technical support in completing this 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]. 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
[4]. 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.
[5]. 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.
[6]. Deepa Malviya, "Face Recognition Technique : Enhanced Safety Approach for ATM", International Journal of Scientific and Research Publications, Volume 4, Issue 12, December 2014.
[7]. Matsoso Samuel Monaheng, Padmaja Kuruba, "Iris Recognition Using Circular Hough Transform", International Journal of 413 Innovative Research in Science,Engineering and Technology,Vol.2, Issue 8, Aug.2013.
[8]. Mohsin Karovaliya,Saifali Karedia,Sharad Oza, Dr.D.R.Kalbande, "Enhanced Security for ATM machine with OTP and facial recognition features",International.
[9]. 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.
[10]. 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
[11]. S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," IEEE Security Privacy M ag., vol. 1, no. 2,pp. 33–42, 2003.
[12]. S. Sai Kumar et al, "Fingerprint Minutia Match Using Bifurcation Technique", International Journal of Computer Science & Communication Networks, Vol 2(4), 478-486.
[13]. Ravi.J. et al, "Fingerprint Recognition using Minutiae Score matching", International Journal of Engineering Science and TechnologyVol.1(2), 2009, 35-42.
[14]. 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