Volume 6, Issue 5, May 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Biometric Based Novel Automatic Teller Machine (ATM)

Anil Kumar C[1], Shiva Prasad K M[2], Asha Rani H[3], Gowthami N[3], Impana R[3], Nalina R[3]
[1]Assistant Professor, Dept. of ECE, R.L Jalappa Institute of Technology, Bangalore, India
[2] Associate Professor, Dept. of ECE, R.L Jalappa Institute of Technology, Bangalore, India
[3] Final year UG scholar, Dept. of ECE, R.L Jalappa Institute of Technology, Bangalore, India

Abstract- This paper presents the Biometric-based access system in automatic teller machine (ATM). The access will be authorized simply by means of the biometric authentication attached to the automatic teller machine to perform the transactions by providing inputs. A person, who wishes to draw money from owner account, first should verify with their finger print whether he is the authorized user or not and then the face of the person will be recognized, if the face does not match then an OTP will be sent to owner through SMS, Owner should response back to give permission to withdraw.Once verification done then ATM automatically draw amount depends owner response. If the person is not verified in biometric authentication the alarm unit will be on, SMS will be sent to the owner. It provides second level security.

Keywords: ATM, Biometric, GSM, Microcontroller

I. INTRODUCTION

The advance security system in Automatic Teller Machine, which consists of a biometric authentication subsystem, a GSM module and a control platform. The biometric authentication subsystem bases on finger print algorithm and can detect person in Automatic Teller Machine room during the period of withdrawing money, and make an alarm loudly. The GSM module sends necessary OTP information to owner and help to keep eyes on owner account all the time. This system prototype is built on the base of microcontroller based embedded system. Experimental results illuminate the Authentication of person in Automatic Teller Machine [4].

It consists of PC memory unit it stores the different driver fingerprint images. Fingerprint sensor is used to detect the fingerprints of the predefined users and compare it with the predefined image. If the image doesn't match then the information is send to the owner through SMS. Owner can identify the theft, can take further actions [5] [12].

The biometric fingerprint sensor takes a digital picture of a fingerprint. The fingerprint scan detects the ridges and fingerprint is considered and verified. If the person is not verified in the fingerprint the alarm unit will be on, SMS will be sent to the owner [6].

II. METHODOLOGY

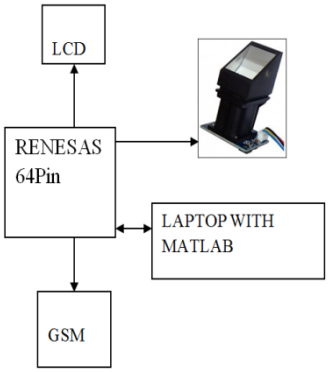

Fig 1: Block diagram of the proposed system.

Many embedded systems have substantially different designs according to their functions and utilities. In this project design, structured modular design concept is adopted and the system is mainly composed of Renesas microcontroller, Finger print module, gsm module, finger print Recognizer[14].

This proposed system consist of a finger print recognizer in the ATM unit whenever a person enter into the ATM he needs to impress his finger prints in this device and the device signals this information to the microcontroller and the controller compares it with the authorized finger prints of that particular account if matches then the face image will be captured and compared with the available data. If he is not authorized user he has to select a friend user in the beginning then GSM sends an OTP to owner then after the owner has to send response about confirmation of permission to withdrawal. If not matches it sends a message to the authorized Account owner [14] [15].

The Renesas microcontroller is programmed so that whenever the finger print recognizer sends a scanned image of the finger print. Whenever the microcontroller gets this signal it compares with the default image stored in microcontroller in terms of 0'sand 1's and when the captured image matches with the default.[7]

Here the GSM is used in order to alert the prior person through a text message and which is also included to the text message. Here the serial communication interface UART is used for the communication between the Microcontrollers, GSM module.[9]

Components Used:

- Renesas (64 pin) microcontroller.
- LCD.
- GSM module.
- Finger print recognizer.

Software Used:

- Cube suite+ IDE tool.
- Renesas flash tool.
- MATLAB

III. OBJECTIVE

[i] To research scope of biometric authentication techniques in ATMs. [3]

[ii] Fingerprint recognition: The masters' fingerprint information was used as the standards of identification. It must certify the feature of the human fingerprint before using ATM system.[11]

[iii] Remote authentication: System can compare current client's fingerprint & finger print information with remote data server.

[iv] To generate module this helps for simple operation of ATMs with full proof secure authentication.

IV. REVIEW OF LITERATURE

1. Mr. Wang et al. Expresses his view like that now a day ATM with magnetic strip authenticated only by inserting password on the ATM machine. But according to today's scenario, cases of fraud are another problem. So they provided fingerprint for more security. Now a days we are directing towards the pile of new powerful, intelligent, auto rated system, which will give us easy to do the work smoothly, Thus systems are not dependent on human support, one of these „ATM SECURITY SYSTEM‟ which we have evolved [7].

2. Mr. Aru et al. Suggests that Today, ATM systems use PIN & access card for identity verification. The recent advance in biometric identification techniques, retina scanning, including fingerprinting, and facial recognition has made a great effort to rescue the unsafe situation at the ATM. This research investigated the development of a scheme that integrates facial recognition technology into the verification process used in ATMs. An ATM system that is reliable in providing more security by using facial recognition is proposed. The development of such a scheme would help to protect clients & financial institutions alike from intruders and identity thieves. This paper concentrates on an ATM security system that would combine a physical access card, a Personal Identification Number, & electronic facial recognition that will go as far as withholding the fraudster‟s card [8].

3. Nevertheless, it's obvious that man's biometric features cannot be replicated, this proposal will go a long way to solve the problem of Account safety making it possible for the actual account owner alone have access to his accounts. The combined biometric features approach is to serve the purpose both the identification and authentication that card and PIN do [1] [2].

a. What is Identification Authentication?

Identification is the process by which the identity of a user is established, authentication is the process by which a service confirms the claim of a user to use a specific identity by the use of credentials. Biometrics is very reliable for authentication. The difference is between a system that looks at a hand geometry and says "this is Doctor Hunk" (identification) versus a man‟swho says "I, Doctor Hunk, present my hand to prove who I am? And the system confirms this hand matches Doctor Hunk‟s template (authentication). Biometric authentication is feasible today [10][16].

b. What is biometric authentication?

Biometrics is biological authentications, based on some physical characteristics of the human body. The list of biometric authentication technologies is still growing. There are two categories of biometric identifiers include physiological and behavioural characteristics. Physiological characteristics are related to the shape of the body, and include but are not limited to: fingerprint, face recognition, DNA, palm print, hand geometry, iris recognition (which has largely replaced retina). Behavioural characteristics are related to the behaviour of a person, including but not limited to: typing rhythm, gait, digital signature and voice. More traditional means of access control include token-based identification systems, such as driver‟s license or passport, and knowledge-based identification systems, such as password or Personal Identification Number (PIN) [13].

V. ADVANTAGES

- Installation and maintenance cost is less.
- Economically viable.
- Can save money even after losing ATM card and PIN.

Disadvantages

- System failure can occur in the absence of power to the unit.

Applications

- Home automation
- Industrial security system
- Banking system

VI. FUTURE SCOPE

With the ongoing changes taking place in today's technology the entire unit can be made into a simple and compact device with the existing VLSI techniques. The same module can be incorporated with the other biometric standards for faster processing. In addition to finger print and face recognition, DNA based biometric would be the highest safety.

VII. CONCLUSION

We have been able to develop a fingerprint mechanism and face recognition mechanism as a biometric measure to enhance the security features of the ATM for effective banking transaction. The prototype of the developed application has been found promising on the account of its sensitivity to the recognition of the customers ‟finger print & face recognition as contained in the database. This system when fully deployed will definitely reduce the rate of fraudulent activities on the ATM machines such that only the registered owner of a card access to the bank account. An embedded fingerprint biometric authentication scheme for ATM banking systems is proposed in this paper along with face recognition authentication for more security; also included in this paper. Finally, conclusions are drawn out after observing the face recognition & Fingerprint Biometric Authentication scheme results.

REFERENCE

[1] Tian Wang, Snoussi, H., "Histograms of Optical Flow Orientation for Visual Abnormal Events Detection", in IEEE Ninth International Conference on Advanced Video and Signal-Based Surveillance (AVSS), 2012, pp. 13-18.

[2] Moses Okechukwu Onyesolu, Ignatius Majesty Ezeani, "ATM Security Using Fingerprint Biometric Identifer: An Investigative Study", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No.4, 2012, pp. 68-72

[3] Der Chin Chen, "Portable Biometric System of High Sensitivity Absorption Detection", Biometric Systems, Design and Applications, 2011, ISBN: 978-953-307-542- 6

[4] Lili Cui, Kehuang Li, Jiapin Chen, Zhenbo Li, "Abnormal event detection in traffic video surveillance based on local features", in Image and Signal Processing (CISP), 2011, pp. 362-366.

[5] Sugandi, B., Hyoungseop Kim, Joo Kooi Tan, Ishikawa, "Tracking low resolution objects by metric preservation", in Computer Vision and Pattern Recognition (CVPR), 2011, pp. 1329-1336.

[6] Nan Jiang, Heng Su, Wenyu Liu, Ying Wu, "Tracking low resolution objects by metric preservation", in Computer Vision and Pattern Recognition (CVPR), 2011, pp. 1329 – 1336.

[7] Anil K. Jain, Jianjiang Feng, Karthik Nandakumar, "Fingerprint Matching", IEEE Computer Society 2010, pp. 36-44, 0018-9162/10 [4] Virginia Epsinosa-Duro, "Minutiae Detection Algorithm for Fingerprint Recognition", IEEE AESS Systems Magazine, March 2002, pp. 7-10.

[8] K.Srinivasan, K.Pokumaran, G.Sainarayan, "Improved Background Subtraction Techniques for Security in Video Application", in Anti-counterfeiting, Security, and Identification in Communication, 2009, pp. 114-117.

[9] Donovan H. Parks and Sidney S. Fels, "Evaluation of background subtraction Algorithm with Post-processing", in IEEE Fifth International Conference on Advanced Video and Signal Based Surveillance, 2008, pp. 192 – 199.

[10] Alper Yilmaz, Omar javed and Mubarak Shah, "Object Tracking: A Survy", ACM computing survey, 2008,volume 38, article 13.

[11] Adam A., Haifa, Rivlin, E., Shimshoni, I., Reinitz, D. ,"Robust Real-Time Unusual Event Detection using Multiple Fixed- Location Monitors", in IEEE Transactions on Pattern Analysis and Machine Intelligence, 2008, pp. 555-560.

[12] Y. Chen, Y. Rui, and T. Huang. "Multicue hmm-ukf for realtime contour tracking", IEEE Transactions on Pattern Analysis and Machine Intelligence, 2006, pp. 1525 –1529.

[13] D. Cremers, "Dynamical statistical shape priors for level setbased tracking" in IEEE Transactions on Pattern Analysis and Machine Intelligence, 2006, pp. 1262 –1273.

[14] Burkey Birant Orten, "Moving Object Identification and Event Recognition in Video Surveillance Systems", MS Thesis in Electrical and Electronics department in METU, 2005.

[15] Anil K. Jain and Arun Ross, "Multibiometric Systems", Communications Of The ACM, January 2004/Vol. 47, No. 1, pp. 34-40.

