Int. J. Chem. Sci.: 14(S3), 2016, 869-872
ISSN 0972-768X
www.sadgurupublications.com

METHOD OF FINGERPRINT IDENTIFICATION AND DEDUCTION OF FOR AUTOMATED TELLER MACHINE USING GSM

B. SIVACHANDRA MAHALINGAM[*], M. D. SAFDER ALI KHAN, SANTOSH KUMAR YADAV and DEEPAK KUMAR RAVI

Department of ECE, Aarupadai Veedu Institute of Technology, CHENNAI (T.N.) INDIA

ABSTRACT

In this paper, fingerprint identification has received more and more attention and has been widely used because of its distinctiveness, stability and acceptability. Efforts for fingerprint identification are mainly focused on: an identifying the system of one or more steps of automatic fingerprint verification. Using multiple sources of a fingerprint to get a higher accuracy for security purpose. Though fingerprint identification is widely used now, in areas such as ATM, the access control of nuclear power stations, etc. For high security applications, particularly low false accept rate and as low as possible false reject rate are desired at the same time, which is called double low problem. In this paper, a method of fingerprint identification concept is conveyed for an ATM machine to be functioned or accessed by authorized person. Only 6.6% fingerprints are falsely rejected on the average under zero false accept rate with our method.

Key words: Automated teller machine, Universal asynchronous Rx/Tx, Density of pixel per inch, Global system for mobile.

INTRODUCTION

Fingerprinting technologies are related to the biometric sciences and make use of characteristic features of the fingerprint to verify the identity of persons. Finger-scan technology is the deployed biometric technology, used in a wide range of substantial access and reasonable access. Every one of the fingerprints has unique characteristics and patterns. The ordinary fingerprint pattern is made up of lines and spaces and the lines are called ridges even as the spaces between the ridges are called valleys. It is through the pattern of these ridges and valleys that a single fingerprint is matched for verification and authorization. These unique fingerprint character are termed “minutiae” and comparisons are made based on these character. Fingerprint verification methods include minutiae-based and image-

[*]Author for correspondence; E-mail: sivabala_82@yahoo.com

based methods. Using the ATM when provide customer with the convenient banknote trading is very common. But, the financial crime interfere with the ATM terminal, steal user's credit cards and password by illegal means. Incase by mistake one user card is lost and the code word stolen, then the criminal draws all the cash in the shortest time. How to carry on the valid identity to the customer becomes the focus in current financial circle. Therefore, it is so important that the biometric thumb impression is to provide the main identification proof of any unknown person. So for ATM security using the hybridizing method with biometric fingerprint verification.

Proposed system

In this paper, we are going to implement method of fingerprint identification and deduction of flash entry for high security applications. GSM are the security applications we are using in this paper. We are using this security system in ATM. On one occasion, the finger print identified it will request for the password. If the password entered is wrong the buzzer alarms. If it is right the amount can be withdrawal. A message will be sent to the registered mobile number. But when an unauthorized person will try to access the account of authorized user, the fingerprint will not be matched and the buzzer will start to give warning to try again for first two attempt and after if it is still an unauthorized attempt to infiltrate the security then buzzer will start to alarm that you cannot access the account and it will lock the account temporarily. Meanwhile the real user will receive the message of all unauthorized attempts made by the culprit. So, he can take an immediate action about it. In this system we can apply more than two fingerprints, so that the if in any incident case the user loses his/her fingerprint so he/she will be able to access his/her account by using another finger.

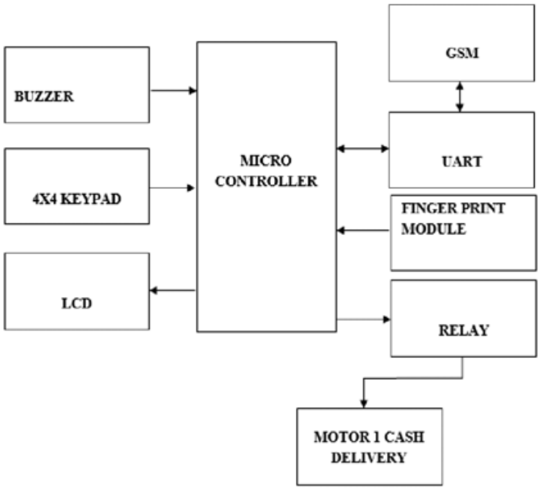

Fig. 1: Hybrid fusion method of fingerprint identification

RESULTS AND DISCUSSION

The paper presented is the design of an ATM access system using finger print technology. The system consists of finger print module, DC motor, LCD display and interfaced to the PIC microcontroller. When a user registers the fingerprint to the finger print module, this is taken as input to the microcontroller. The micro controller is automatic in such a way that the input from the user is checked and verified with user database and displays the relevant information on the LCD display. When an authorized person is recognized using finger print module the door is accessed by DC motor.

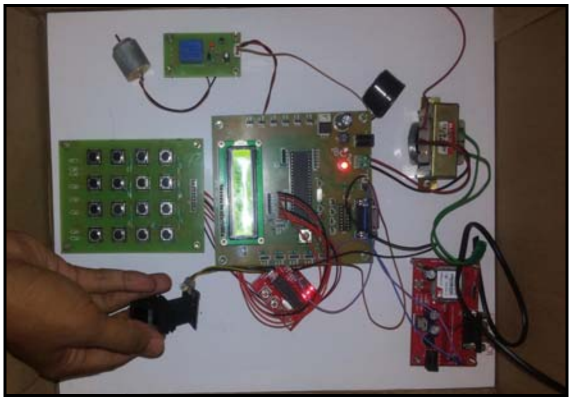

Fig. 2: The hardware of fingerprint based ATM

Fingerprint readers are being used by banks for ATM authorization and are becoming more common at grocery stores where they are utilized to automatically recognize a registered customer and bill their credit card or debit account. Finger-scanning technology is being used in a novel way at some places where cafeteria purchases are supported by a federal subsidized meal program. The system is used and extended by using a GSM module. This module sends alert post to the respective establishment when unauthorized person’s finger print is found. Like that, the security level is uppermost and the people and their money will be secured.

REFERENCES

1. D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar, Handbook of Fingerprint Recognition, Springer, London (2009).
2. S. Nanavati, M. Thieme and R. Nanavati, Biometrics: Identity Verification in a Networked World, John Wiley & Sons (2002).

3. J. Ashbourn, Biometrics: Advanced Identity Verification, Springer-Verlag, London (2002).

4. E. Spinella, Biometric Scanning Technologies: Finger, Facial and Retinal Scanning, SANS Institute, San Francisco, CA (2003).

5. John B. Peatman, Design with PIC Microcontrollers, Pearson Education, India (1998).

6. Microchip Technology Inc., PIC16F87XA data sheet, DS39582C (2013).

7. A. K. Jain and A. Ross, Multibiometric Systems, Communications of the ACM, **47(1)**, 34-40 (2004).

8. Moses Okechukwu Onyesolu and Ignatius Majesty Ezeani, ATM Security Using Fingerprint Biometric Identifer: An Investigative Study, (IJACSA) Int. J. Adv. Comput. Sci. Applicat., **3(4)**, 68-72 (2012).

9. A. K. Jain, J. Feng and K. Nandakumar, Fingerprint Matching, IEEE Computer Society, 36-44, 0018-9162/10 (2010).

10. V. Epsinosa-Duro, Minutiae Detection Algorithm for Fingerprint Recognition, IEEE AESS Systems Magazine, 7-10 (2002).

11. E. Saatci and V. Tavsanogh, Fingerprint Image Enhancement Using CNN Gabor-Cpe Filter[C], Proceedings of the 7th IEEE International Workshop on Cellular Neural Networks and their Applications, 377-382 (2002).

12. J. Gu, J. Zhou and D. Zhang, A Combination Model for Orientation Field of Fingerprints, Pattern Recognition, **37**, 543-553 (2004).

13. J. Cheng and J. Tian, Fingerprint Enhancement with Dyadic Scale-Space, Pattern Recognition Lett., **25(11)**, 1273-1284 (2004).

14. Chen H, Tian J. A Fingerprint Matching Algorithm with Registration Pattern Inspection, J. Software, **16(6)**, 1046-105 (2005).

15. G. F. Smits and E. M. Jordaan, Improved SVM Regression using Mixtures of Kernels[A], Proceedings of the 2002 International Joint Conference on Neural Networks[C], Hawaii: IEEE, 2785-2792 (2002).

Accepted : 11.10.2016