ATM Terminal Security using Fingerprint Recognition

Lavanya M[1] Meghana A[2] Ramya H S[3] Ramya Keerthi M R[4]
[1,2,3,4]Department of Electronics & Communication Engineering
[1,2,3,4]Dr. Ambedkar Institute of Technology, Bengaluru, India

Abstract— There are many Biometric techniques of which, fingerprint recognition is one of the most reliable and secure means of personal identification technologies. Fingerprint verification using Biometrics has been used since long time. The fingerprint trait is chosen, because of its availability, reliability and high accuracy. The fingerprint based biometric system can be implemented easily for securing the ATM machine. Using biometrics it identifies the fingerprint and gives accurate result whether it is valid or not. This system can be employed at Real time application with enhanced security, high accuracy, reliability and uniqueness of fingerprints. It is convenient due to its low power requirement and portability. In this way we can try to control the crime circle of ATM and secure it.

Key words: Fingerprint Recognition, Biometrics, User Application, Reliability, Real Time Application

I. INTRODUCTION

Rapid development of banking technology has changed the way of banking activities. ATM is a computerized machine designed to dispense cash to bank customers without need of human interaction. Nowadays the number of ATM users has increased. ATM cards are used for banking transactions like balance enquiry, mini statement, withdrawal, etc. The ATM machine has card reader and keys as input devices and display screen, cash dispenser, receipt printer, speaker as output devices. The pin is the 4 digit number given to all ATM card holders. ATM card holder's pin is different from each other. The number is verified by the bank and allows the customers to access their account. The password is the only identity so anyone can access the account when they have the card and correct password. Once the card is stolen by the culprit and if he comes to know the password he can withdraw money which may cause huge financial losses to the users. In the recent days, there have been many such ATM fraud cases. Physical characteristics include fingerprint, hand or palm geometry, retina, iris and face while popular behavioral characteristics are signature and voice. Some of the characteristics of biometric system are:

1) Universality - each person around the world obligatorily must have the physiological or behavioral characteristic.
2) Uniqueness - this characteristic varies from person
3) Permanence - this characteristic must be enough invariant during a certain period of time
4) Collectability - this characteristic can be measured quantitatively, and can be stored.

II. BLOCK DIAGRAM

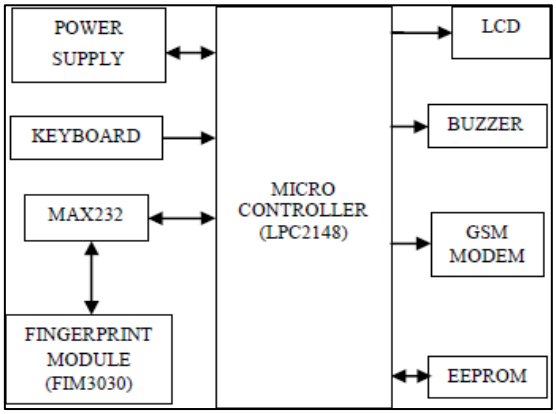


Fig. 1: Proposed hardware design

To overcome these problems associated with the present ATM System, in our project we are using biometric features. Biometric technology is a secure means of authentication because it is unique, cannot be shared, copied or lost.

III. WORKING

To obtain high security in ATM terminal and to minimize the theft threat, we have proposed this project which includes integration of biometrics with the existing system. One more feature that we've added is the use of OTP to reduce the risk of criminal activities.

There are two modes of operations:

1) Enrollment mode: In this mode customer's fingerprint along with their mobile number are stored in the database.
2) Banking mode: In this mode fingerprint authentication is done. This software system is designed as follows: first of all the Linux kernel and the File systems are loaded into the ARM 7 controller.
3) In next step, the system is initialized to check specific task, such as checking ATM terminal, GSM module and so on, and then each module is reset for ready to run commands. Before accessing ATM system, the mobile number and fingerprint of the customer are needed to be authenticated.
4) On placing the finger on the biometric device, Feature extraction process occurs. Comparison of fingerprint with the stored database. Decision is made whether the user is authorized for further transaction. If the person is authorized then an OTP is sent to his registered mobile number. If the entered OTP matches with the sent OTP then the transaction is successful else the buzzer is ON

IV. HARDWARE REQUIREMENTS

A. LPC2148

The microcontroller LPC2148 belongs to ARM7 family which is the core controller in the system. It has ARM7TDMI core which is a member of the Advanced

RISC Machines (ARM), a family of general purpose 32-bit microprocessors. It offers high performance for very low power consumption and price. The ARM architecture is based on RISC (Reduced Instruction Set Computer) principles, and the instruction set and related decode mechanism are much simpler than those of micro-programmed Complex Instruction Set Computers (CISC).This simplicity results in a high order output and remarkable real-time interrupt response from a small and cost-effective chip.

B. Fingerprint Module (FIM3030)

The important module of the system is fingerprint scanner. We used FIM3030 by NITGEN. It has ADSP-BF531 as central processing unit with 8 MB of SDRAM and 1 MB of flash ROM. It uses overall supply voltage of 3.3 V. The communication with the fingerprint module is made through RS-232 via UART0 of LPC2148.A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern.The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching.

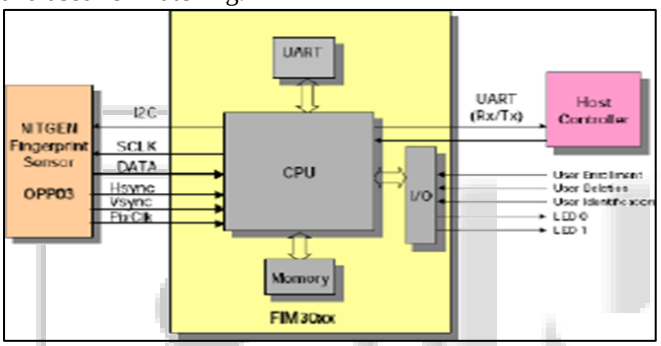


Fig. 2: Fingerprint module (FIM3030)

C. GSM Modem

Global System for Mobile Communications (GSM: originally from Group Special Mobile) is the most popular standard for mobile phones in the world. GSM uses a variation of Time Division Multiple Access(TDMA) and GSM is the most widely used of the three digital wireless telephone technologies (TDMA, GSM, and CDMA). GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900 MHz or 1,800 MHz frequency band. GSM is a cellular network, which means that mobile phones connect to it by searching for cells in the immediate vicinity.

D. LCD

One of the most common output devices used is LCD. A liquid-crystal display (LCD) is a flat panel display or the electronically modulated optical device that uses the light-modulating properties of liquid crystals. Liquid crystals do not emit light directly, instead using a backlight or reflector to produce images in color or monochrome. It requires 3 control lines and 8 I/O lines . The 3 control lines are EN, RS and RW. The EN line is called Enable. This control line is used to tell LCD that user is sending data. Enable line should be made high to send data and then set the other two Control line and put data on the data bus. When other lines are ready, EN should be made low.

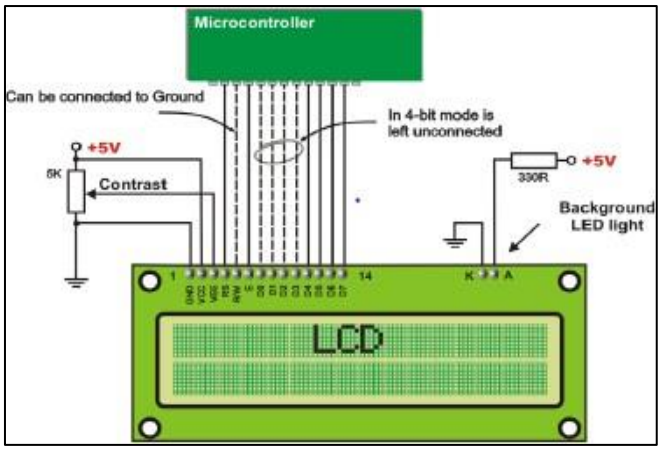
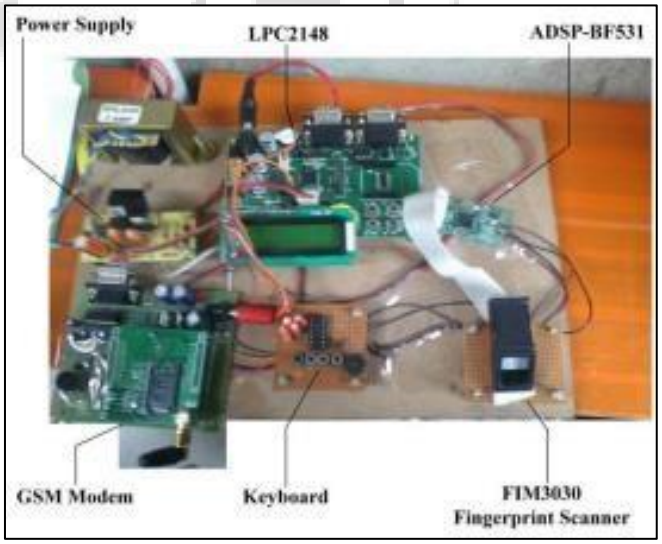


Fig. 3: Interfacing of 20x4 LCD

V. SOFTWARE SPECIFICATIONS

The LPC2148 is programmed with KeilµVision4. It is a window-based software platform that combines a robust and modern editor with a project manager and make facility tool for development. It integrates all the tools to develop embedded applications including a C/C++ compiler, macro assembler, linker/locator, and a HEX file generator. µVision helps expedite the development process of embedded applications by providing the IDE (Integrated Development Environment). KEIL is used to create source files; automatically compile, link and covert using options set with an easy to use user interface and finally simulate or perform debugging on the hardware with access to C variables and memory.

VI. RESULTS



From the proposed hardware setup using LPC2148 ARM7 microcontroller and FIM3030 fingerprint module secured transaction can be achieved after fingerprint authentication. Hence it has been demonstrated successfully.

VII. ADVANTAGES

Biometric traits cannot be lost or forgotten (while passwords can). Biometric traits are difficult to copy, share and distribute (passwords can be announced in websites). They require the person being authenticated to be present at the time and point of authentication.

1) Reliability: Fingerprint scanning systems provide a reliable way to track customers and you don't need to worry about storing extra data, since the system only requires a fingerprint.
2) Security: Fingerprint-based systems provide additional security, since criminals cannot easily fake a fingerprint, fingerprints cannot get misplaced.
3) Cost-effective: Fingerprint-based systems can save money on hardware and material costs. Fingerprint scanning systems tend to consist of a simple fingerprint reader and software that identifies the individual.
4) Maintenance: It is very easy for maintenance.

VIII. CONCLUSION

After testing the system developed, we came to know that ATM can be efficiently used with fingerprint recognition. Since, password protection is not used in our system, the fingerprint recognition done after it yielded fast response and is found to be of ease for use. Fingerprint images cannot be recreated from templates; hence no one can misuse the system. LPC2148 and FIM3030 provide low power consumption platform. Speed of execution can be enhanced with the use of more sophisticated microcontroller. The same hardware platform can be used with IRIS scanner to put forward another potential biometric security to the ATMs.

ACKNOWLEDGMENT

This research was permitted and encouraged by our Institution, Dr.Ambedkar Institute of Technology. We thank all the people responsible for the same.

We further thank our HOD, Dr.Jayaramaiah G V, who provided insight that greatly assisted the research.

We would also like to show our gratitude to our respective families for their constant show of affection and care during the research period

REFERENCES

[1] Vaibhav R. Pandit , Kirti A. Joshi and Narendra G. Bawane, "ATM Terminal Security Using Fingerprint Recognitional" , (IJAIS)-ISSN: 2249-0868, Foundation of Computer Science FCS,M New York, USA and 2nd National Conference on Innovative Paradigms in Engineering & Technology (NCIPET 2013).
[2] Mithun Dutta , Kangkhita Keam Psyche and Shamima Yasmin," ATM Transaction Security Using Fingerprint Recognition" American Journal of Engineering Research 2017
[3] Yun Yang, Jia Mi, "ATM Terminal Design is based on Fingerprint Recognition", IEEE 2010, pp. 92-95, 978-1-4244-6349-7/10
[4] P.K.Amurthy and M.S. Reddy, "Implementation of ATM Security by Using Fingerprint recognition and GSM", International Journal of Electronics Communication and Computer Engineering vol.3, no. 1, pp. 83-86, 2012.

