ATM Systems Authentication Based On Fingerprint Using ARM Cortex-M3

Mr. John Mashurano[1], M.E Signal and Information Processing.

Mr. Wang liqiang[2], Associate Professor, Optics Lab.

School of Electronics Engineering, Tianjin University of technology and education.
Tianjin China 300222

Abstract

The main purpose of this project is to design a system that will improve the authentication of customers using ATM machines, in most country existing ATM machines system use magnetic card reader, customer is identified by inserting ATM card with magnet stripe or plastic smart card with a chip that contain a unique information such as card number and some security parameters ,Authentication is provided by the bank customer (user) entering personal identification pin (Password), customer can access bank account in order to make cash withdraw or other services provided by the bank.
Cases of card fraud is another problem once user's bank card is lost and the password is stolen, or simply steal a customer's card along with its PIN (Password) the criminal will draw all cash in the shortest time, which will bring enormous financial losses to customer, this type of fraud has spread globally. So to rectify this problem we are implementing this system, the chip of STM32F103RBT6 is used as ARM 32bit cortex –M3 CPU core, and algorithm of fingerprint image in order to improve authentication of customer using ATM machine and confidence in the banking sector.

1. Introduction

Existing system of ATM client authentication example NCR personas series 77 &86 ATMs there is magnetic card reader, client using the ATM (Automatic Teller Machine) require Bank card and password which provide customers with the convenient banknote withdraw and other services, a newer high-tech method of operating sometimes called card skimming or card cloning involves the installation of a magnetic card reader over the real ATM's card slot and the use of a wireless surveillance camera or a modified digital camera or a false PIN keypad to observe the user's PIN. Card data is then cloned into a duplicate card and the criminal attempts a standard cash withdrawal. The availability of low-cost commodity such as wireless cameras, keypads, card readers, and card writers has made it a relatively simple form of fraud, PIN theft which is mostly as a result of congestion at ATM points. Nowadays accurate personal identification is becoming more and more important. Usual means smart cards, passwords, have shown their limits. Biometrics (i.e. analysis of personal biological characteristics) can bring a satisfying answer to those problems. Currently fingerprint recognition is the most widely used technique for personal identification. Fingerprints are made up of locally parallel ridges with singular points (minutiae), and they constitute a unique permanent universal pattern.

In this project the fingerprint sensor sense the thumb impression of the corresponding person and that image will be compared with registered image, if the both images are unique, then the finger print device activates particular task like access to the system, identification of the customer. The project operation contains 2 modes, the first one is Administration mode and the second is User mode. The Administration mode is used to register the new user and gives the mode of authorization. The Administration mode has the ability to create and delete the users. The user mode is mode used for the authentication of the bank customer. In user mode of authorization, creation and deletion of a user cannot be performed.

The Administrator mode operations are done directly through interfacing the Optical fingerprint identification module (FPM10A) using a standard serial port to communicate, with the ARM development board. The bank customer details along with biometric information database are stored in the flash memory of the Fingerprint module. The ARM ST32F103 is programmed to operate under user mode. In user mode Fingerprint image is scanned by the fingerprint device. When a finger is kept at the finger print reader, it will give the information accordingly to CPU core by sending appropriate commands to the reader and which is displayed on the LCD,

If the scanned image matches with the registered image then ARM sends the authorization to customer to enter password in order to access ATM. In case the scanned image do not match with registered image, or if the information provided by the user is incorrect or mismatch in finger prints is detected then access is denied and device will send out message to indicate unauthorised person is accessing ATM machine. It will be easy for security officer or bank staffs to identify specific ATM and place so easy identify the criminal.

2. The characteristics of the system

The embedded ATM client authentication system is based on fingerprint recognition which is designed after analyzed existing ATM system the chip ST32F103RBT6 is Used as the core of this embedded system which is associated with technology of fingerprint recognition.

The primary function are shown as follows,

- Fingerprint recognition; the finger print information was used as standards of identification it must certify the feature of the human fingerprint before using ATM.
- Remote authentication; System can compare current client fingerprint information with remote fingerprint data server.
- GSM ;Once an exception happen such as fake identity, the system will send message to inform security department or bank staff as soon possible.
- Two discriminate analysis method; beside the fingerprint recognition the mode of password recognition can be also used for the system.

3. Hardware and Software Design

The design of entire system consisted of two part which are hardware and software, the hardware are designated by the rule of embedded system and the steps of software consisted of several parts.

3.1 Hardware design

The chip STM32F103RBT6 is used as the core of entire hardware ,the module of LCD ,Keyboard, GSM Module, fingerprint recognition scanner are connected with main chip STM32F103RBT6 , the EEPROM are also embedded in the system ,There are some modules consisted of the system as follows;

- LCD Module ; ILI9331 is a 262,144-color one-chip SoC driver for a-TFT liquid crystal display with resolution of 240RGBx320
- Keyboard Module; It can be used for inputting passwords.
- Fingerprint recognition module ; Optical fingerprint identification module (FPM10A)
- MINI STM32 development board.
- Power supply.
- TC35 GSM engine

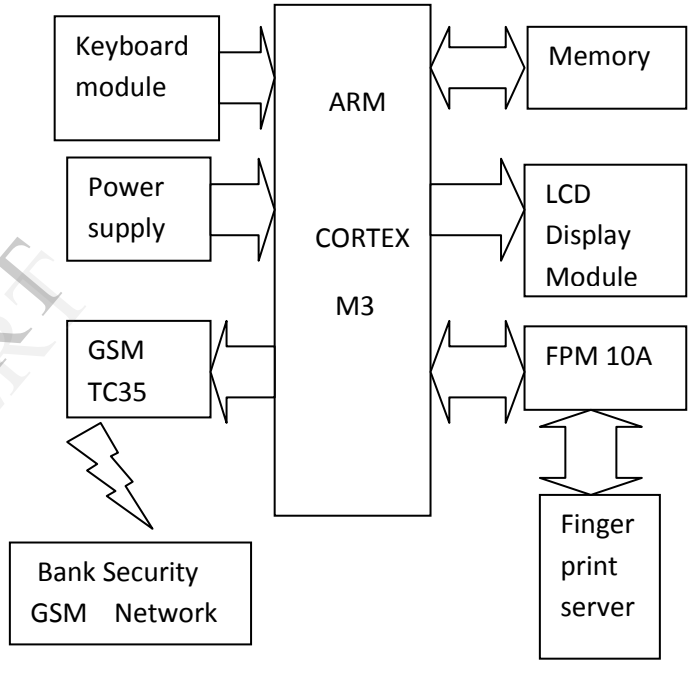

Fig.1: Block Diagram of Hardware Design.

3.2 Software design

The design of software is very important for this embedded system, like typical computer programmers, embedded system designers use compilers, assemblers and debuggers to develop embedded system software. The design was component of several parts included the design of main program flow chart, the initializing ones, and the algorithm of fingerprint recognition flow chart.

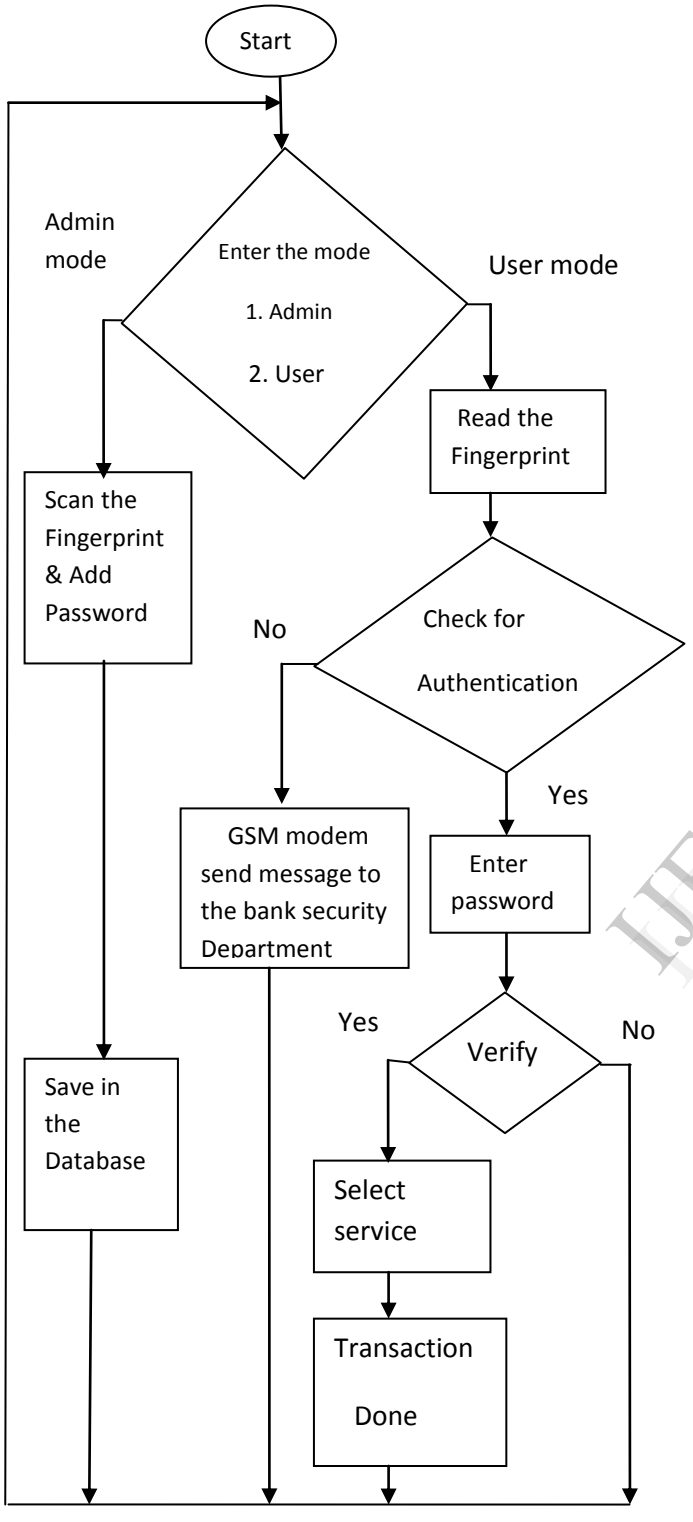

Fig.2: The overall flow chart of Software.

The system require the Administrator set the mode ,Admin mode this represent bank side used for administration purpose to control, setting and data entry ,the system in user mode customer accessing ATM machine require customer fingerprint if all the recognition is right ,the system would allow customer to enter password (PIN) for accessing ATM machine ,if authentication failure then it send the message notification to the bank security department indicating location of ATM ,and Time. The overall software flow chart is shown on the fig 2.

4. Fingerprint recognition

A fingerprint recognition system is done using three steps known as Image acquisition, Minutiae extraction and Minutiae matching. The block diagram of basic fingerprint recognition system is shown in fig 3.below

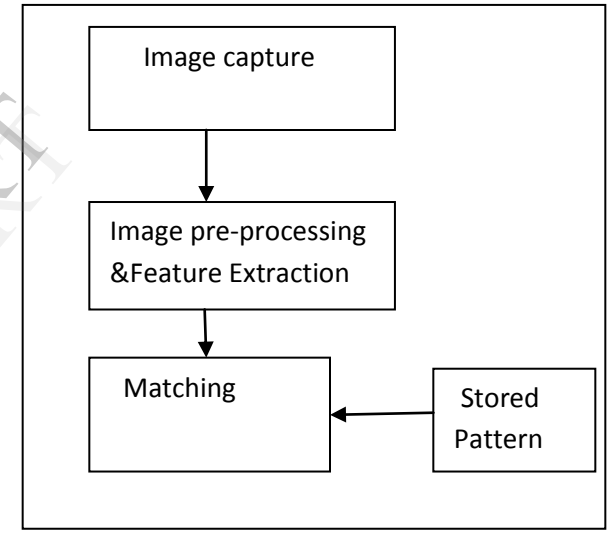

Fig.3: Block diagram of basic fingerprint recognition

4.1 Detail of fingerprint recognition process.

The first step was the acquisition of fingerprint image by above device mentioned in the algorithm, and the results could be sent to the following process. Secondly, pre-processing the images acquired. After obtain the fingerprint image, it must be pre-processing. Generally, pre-processing of one's is filtering, histogram computing, image enhancement and image binarization. Lastly, the characteristic value was extracted, and the results of the above measures would

be compared with the Information of owner's fingerprint in the database so as to verify whether the character is matched, and then the system returned the results matched or not.

Fingerprints are one of those bizarre twists of nature. Human beings happen to have built-in, easily accessible identity cards. You have a unique design, which represents you alone, literally at your fingertips, fingerprints are a unique marker for a person, even an identical twin. Fingerprints are one of many forms of biometrics, used to identify individuals and verify their identity. This part touches on two major classes of algorithms and four sensor designs (optical, ultrasonic, passive capacitance, and active capacitance) The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns It is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies.

The three basic patterns of fingerprint ridges are the arch, loop, and whorl:

i. arch: The ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger.

ii. Loop: The ridges enter from one side of a finger, form a curve, and then exit on that same side.

iii. Whorl: Ridges form circularly around a central point on the finger

Fig.4a. The Patterns of fingerprint

Fig.4b. The pattern of fingerprint

5.0 GSM

Global System for Mobile Communication (GSM) is a set of standards specifying the infrastructure for a digital cellular service . The standard is used in approx. 85 countries in the world , TC35 GSM engines operate in the GSM 900 MHz and GSM 1800 MHz frequency bands. Designed to easily provide radio connection for voice and data transmission both modules integrate seamlessly with a wide range of GSM application platforms and are ideally suited to design and set up innovative cellular solutions with minimum effort. The complete RF part is incorporated and the GSM protocol runs autonomously on a GSM baseband processor. The GSM engine uses a single 40-pin ZIF connector that connects to the cellular device application. The ZIF connector establishes the application interface for control data, audio signals and power supply lines. The cellular device application forms the Man-Machine Interface (MMI). Access to the GSM engine is enabled by a serial interface .

The mobile communications has become one of the driving forces of the digital revolution. Every day, millions of people are making phone calls by pressing a few buttons. Little is known about how one person's voice reaches the other person's phone that is thousands of miles away. Even less is known about the security measures and protection behind the system. The complexity of the cell phone is increasing as people begin sending text messages and digital pictures to their friends and family. The cell phone is slowly turning

into a handheld computer. All the features and advancements in cell phone technology require a backbone to support it. The system has to provide security and the capability for growth to accommodate future enhancements. General System for Mobile Communications, GSM, is one of the many solutions out there. GSM has been dubbed the "Wireless Revolution" and it doesn't take much to realize why GSM provides a secure and confidential method of communication.

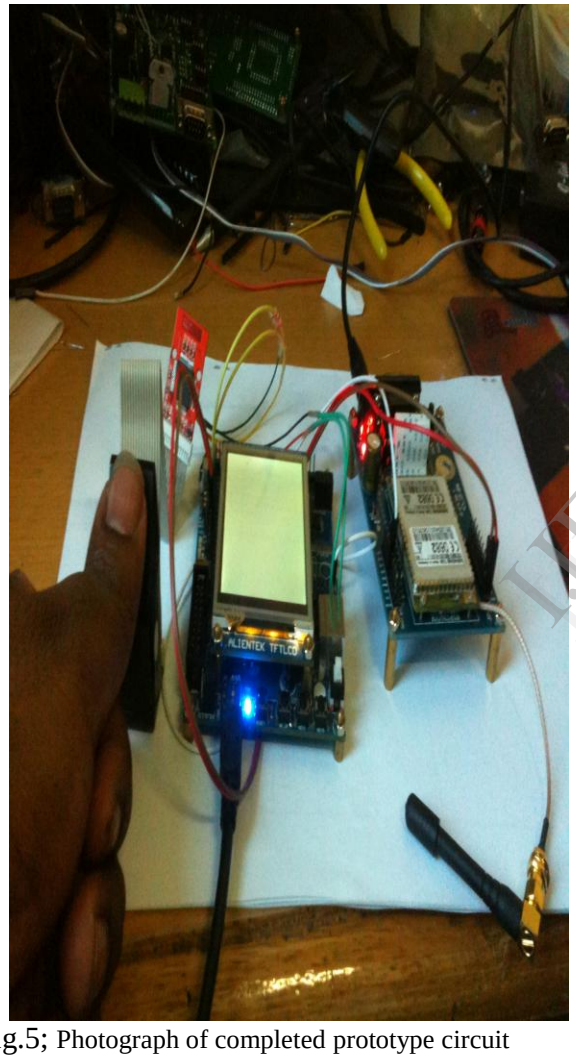

Fig.5; Photograph of completed prototype circuit

6.0 Results and Conclusions.

The project has been successfully implemented. The prototype of ATM systems authentication based on fingerprint identification has been implemented. The idea presented here is to build a system that will be stable and safe to use. In the results, it can be deduced that the use of biometric security systems offers a much better authentication of ATM systems and took advantages of the stability and reliability of fingerprint characteristics, and a new biological technology based on the image enhancement algorithm. Additional, the system also contains the original verifying methods which are inputting owner's password.

These days, still majority of ATM machine in many countries there are using magnetic card reader, so there is a need to change a method of authentication in future in order to eliminate the drawbacks identified in this project. The whole system was built on the technology of embedded system which makes the system more safe, reliable and easy to use.

,

7.0 Future scope.

In this project we are using fingerprint module as mode of authentication. This project is depending on the biometrics i.e. fingerprint. In future it will be very easy to implement because each person has his own fingerprints with the permanent uniqueness. The system will provide many advantages such as,

We do not forget our fingers, Users respect them, fraudsters are afraid of them, Protects privacy. Fingerprints do not change over time, Fingerprints stop unauthorized access, all fingers are unique, which allows each person to have ten easy uses of identifiers, Base of all world-wide identification

In future systems using biometric will be preferred as method to provide security and authentication this will eliminate forgery and fraud in many organizations.

8.0 References.

[1] ATM terminal dual verification process using finger print recognition Scanner and GSM by Golla Jayaraju **"**journal of innovation in electronics and communication vol.1 [1] Oct 2011 – march 2012"

[2] ATM terminal design is based on fingerprint recognition for security purpose by Jeohaddad & idhabihigue "*(IIETRC) INTERNATIONAL INSTITUTE OF ENGINEERING AND TECHNOLOGY RESEARCH CENTER VOL NO. 1, ISSUE NO. 2, 030 – 036.*

[3] Implementation of ATM Security by Using Fingerprint recognition and GSM by Pennam Krishnamurthy & M. Maddhusudhan Redddy "International Journal of Electronics Communication and Computer Engineering Volume 3, Issue (1) NCRTCST, ISSN 2249 –071X"

[4] Fingerprint **Based ATM Security by using ARM7** by D. Vinod kumar, & Prof.M R K Murthy "*IOSR Journal of Electronics and Communication Engineering (IOSRJECE) ISSN : 2278-2834 Volume 2, Issue 5 (Sep-Oct 2012), PP 26-28 www.iosrjournals.org"*

[5] Fingerprint Verification System – A Fusion Approach M.Mani Roja & Dr.Sudhir Sawarkar *International Journal of Computer Applications (0975 – 8887) Volume *– No.*, _____ 2011*

[6] STM32F10xxx reference manual. The reference and Flash programming manuals are both available from the STMicroelectronics website www.st.com.

[7]How Fingerprint Scanners Work ' http://computer.howstuffworks.com/fingerprint-scanner.htm

[8]http://en.wikipedia.org/wiki/Automated_teller_machine "Automated teller Machine "

[9] Fingerprint Verification using Gabor Co-occurrence Features by S.Arivazhagan, T.G.ArulFlora "International Conference on Computational Intelligence and Multimedia Applications 2007"

[10] Siemens cellular engines TC35 Module manual **version 04.00**