Volume 5, Issue 6, June 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

ATM Security using Fingerprint Recognition

Avinash Kumar Ojha
MCA Department, Mumbai University,
Maharashtra, India

Abstract: Identification and verification of a person today is a common and crucial thing; which include lock system, safe box and vehicle control or even at accessing bank accounts via Automated teller machine, etc which is requisite for securing personal information. The traditional methods like ID card verification or signature does not issue perfection and reliability. Rapid development of banking technology has changed the way banking activities are dealt with. One banking technology that has impacted positively and negatively to banking activities and transactions is the advent of automated tellermachine (ATM). The systems employed at these places must be fast enough and robust too. Use of the ATM (Automatic Teller Machine) that provides clients with the suitable note commerce is facing a brand new challenge to hold on the valid identity to the customer. Since, in standard identification ways with ATM, criminal cases are increasing creating financial losses to customers. For resolution the bugs of early ones, the author styles a new ATM terminal client recognition systems. The chip of S3C2440 is used for the core of microchip in ARM9, moreover, Associate in Having improved enhancement algorithm of fingerprint image increase the security that client use the ATM machine.. This system can be employed at any application with enhanced security because of the uniqueness of fingerprints. It is convenient due to its low power requirement and portability.

General Terms: Fingerprint Recognition, ATM Security
Keywords: LPC2148, FIM3030, S3C2440, GSM Fingerprint Recognition, Image Enhancement, Gabor Filtering

I. INTRODUCTION

Biometrics is a technology that helps to make your data extremely secure, unique all the users by way of their personal physical characteristics. Biometric information can be used to perfectly identify people by using their fingerprint, face,speech, iris, handwriting, or hand geometry and so on. Using biometric identifiers offers several advantages over traditional and current methods. Tokens such as magnetic stripe cards, smart cards and physical keys, can be stolen, lost, replicated, or left behind; passwords can be shared, forgotten, hacked or accidentally observed by a third party . There are two key functions offered by a biometric system. One technique is identification and the other is verification. In this paper, we are concentrating on identifying and verifying a user by fingerprint recognition. A modern ATM is typically made up of the devices like CPU to control the user interface and devices related to transaction, Magnetic or Chip card reader to identify the customer, PIN Pad, Secure crypto-processor generally within a secure cover, Display to be used by the customer for performing the transaction, Functionkey buttons, Record Printer to provide the customer with a record of their transaction, to store the parts of the machinery requiring restricted access -Vault , Housing for aesthetics, Sensors and Indicators.

Fingerprint technology is the most widely accepted and mature biometric method and is the easiest to deploy and for a higher level of security at your fingertips. It is simple to install and also it takes little time and effort to acquire one's fingerprint with a fingerprint identification device. Thus, fingerprint recognition is considered among the least intrusive of all biometric verification techniques. Ancient times officials used thumbprints to seal documents thousands of years ago, and law agencies have been using fingerprint identification since the late 1800s.We here carry the same technology on digital platform. Although fingerprint images are initially captured, the images are not stored anywhere in the system. Instead, the fingerprints are converted to templates from which the original fingerprints cannot be recreated; hence no misuse of system is possible.

II. LITERATURE REVIEW

To implement this concept, we have studied different investigated works and found following data. For fingerprint recognition, a system needs to capture fingerprint and then follow certain algorithm for fingerprint matching. The research paper discusses a minutiae detection algorithm and showed key parameters of fingerprint image for identification. For solving the bugs of traditional identification methods, the author of designs a new ATM terminal customer recognition system with chip of S3C2440 is used for the core of microprocessor in ARM9 and an upgraded enhancement algorithm of fingerprint image intensify the security of bank account as well as ATM machine. For image enhancement, the Gabor filter algorithms and direction filter algorithms are used. In research paper, authors showed that Gabor filters (GFs) play an important role in the extraction of Gabor features and the enhancement of various types of images. If images of fingerprint are shoddy images, they result in missing features, leading tothe degrading performance of the fingerprint system. Hence, it is very important for a fingerprint recognition system to evaluate the quality and validity of the captured fingerprint images.

Existing approaches for this estimation are either to use of local features of the image or to use of global features of the image. Outmoded fingerprint recognition approaches have demerits of easy losing rich information and poor presentations due to the complex type of inputs, such as image turning, poor quality image conscription, incomplete input image, and so on. In paper, fuzzy features match (FFM) based novel method on a local triangle feature is set to match the deformed fingerprints. Fingerprint here is represented by the fuzzy feature set: the local triangle feature set. In paper, a test chip has been fabricated using a 0.5 µm standard CMOS process.

The total execution time for attaining and processing a fingerprint image is less than 360 ms at 10 MHz and the power feeding is below 70 mW at 3.3 V supply voltage. We found development of a sensor with CMOS technology in. Also, a chip architecture that integrates a fingerprint sensor and an identifier in a single chip is proposed in. The sensing element senses capacitances formed by a finger surface to capture a fingerprint image. To have good speed of operation for fingerprint matching, in depending on the spectral minutiae features two feature reduction algorithms are given: the Column Principal Component Analysis and the Line Discrete Fourier Transform feature reductions. It can efficiently compress the template size with a reduction rate of 94%. Spectral minutiae fingerprint recognition system shows a matching speed with 125000 comparisons per second on a PC with Intel Pentium D processor 2.80 GHz, 1 GB of RAM.

III. RESARCH BACKGROUND

Crime at ATMs has become a countrywide issue that faces not only customers, but also bank hands and this financial crime case rise frequently in recent years. A lot of criminals tamper with the ATM terminal and steal customers' card details by unlawful means. Once user' bank card is lost and the password is pinched, the user' account is exposed to attack. Traditional ATM systems validate generally b using a card (credit, debit, or smart) and a password or PIN which no doubt has some defects. The prevailing practises of user authentication, which involves the use of either passwords and user IDs (identifiers), or identification cards and PINs (personal identification numbers), suffer from several boundaries. Biometrics can be defined as measurable physiological and behavioural characteristic that can be captured and subsequently compared with another instance at the time of verification. It is automated methods of recognizing a person based on a physiological or behavioural characteristic.

WITHDRAW CASH FROM ATM USING A PHONE... HOW DO THEY DO IT?
1
INSTALL PLOUTUS TROJAN AND PHONE INSIDE ATM
2
SEND SMS COMMAND TO ATM
3
COLLECT THE CASH

Hacking ATMs with Just a Text Message
3
SMS COMMAND PASSED THROUGH TCP/UDP PACKET (USB PORT – USB TETHERING)
NETWORK MONITOR
1
INSTALL PHONE AND PLOUTUS TROJAN
ATTACKER SEND SMS COMMANDS
2
4
NETWORK MONITOR RECEIVES COMMAND AND STARTS UP PLOUTUS TO ISSUE CASH

IV. HARDWARE DESIGN

To implement the proposed security for ATM terminals with the use of fingerprint recognition, we use the different hardware and software platforms. Fig 1 shows the major system modules and their interconnections.

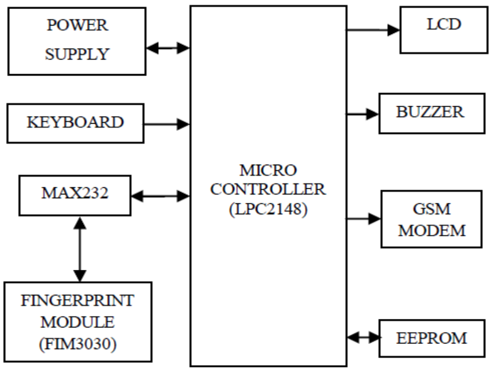

Fig 1: Overview of the system.

4.1MICRO CONTROLLER: Microcontroller (LPC2148)

The system uses LPC2148 from ARM7 family. It 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 orderoutput and remarkable real-time interrupt response from a small and cost-effective chip. All parts of the processing and memory systems can operate continuously since, pipelining is employed. Typically, while one instruction is being performed, its successor is being decoded, and a third instruction is being got from memory. The ARM memory interface designed to allow the performance potential to be realized without suffering high costs in the memory system. Speed-critical control signals are pipelined to allow system regulates functions to be implemented in standard low-power logic, and these regulates signals facilitate the exploitation of the fast local access modes offered by industry standard dynamic RAMs. The LPC2148 is interfaced to different modules via GPIO (General Purpose I/O) pins. It receives the fingerprint template produced by the fingerprint module. It will match the same with the reference template stored at installation of the system. If the acknowledged template gets matched with the reference one, the person is allowed to access the further system. In case of successive mismatch of templates, the system will initialize the GSM module to send message to the enrolled user and simultaneously will raise the alarm through buzzer.

We have used LPC2148 from NXP semiconductors (founded by Philips). It shows features as follows-

a) 16/32-bit ARM7TDMI-S microcontroller in a tiny LQFP64 package.
b) 240 kB of on-chip static RAM and 512 kB of on-chip flash program memory.
c) In-System/In-Application Programming (ISP/IAP) via on-chip boot-loader software.
d) Two 10-bit A/D converters provide a total of 14 analog inputs, with conversion times as low as 2.44 μs per channel.
e) Single 10-bit D/A converter provide variable analog output.
f) Multiple serial interfaces including two UARTs (16C550), two Fast I2C-bus (400 kbit/s), SPI and SSP with buffering and variable data length capabilities.
g) Vectored interrupt controller with configurable priorities and vector addresses.
h) Up to 45 of 5 V tolerant fast general purpose I/O pins in a tiny LQFP64 package .

4.2 Fingerprint Module

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 offlash 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. FIM3030 is an evolutionary standalone fingerprint recognition module consisted of optic sensor OPP03 and processing board. As CPU and highly upgraded algorithm are embedded into a module, it provides high recognition ratio even to small size, wet, dry, calloused fingerprint. High speed 1: N identification and 1: N verification. FIM3030 has functions of fingerprint enrolment, identification, partial and entire deletion and reset in a single board, thereby offering convenient development environment.

Off-line functionality stores logs on the equipment memory (up to 100 fingerprints) and it's identified using search engine from the internal algorithm. Evolutionary standalone fingerprint recognition module FIM3030 is ideal for on-line applications, because allows ASCII commands to manage the device from the host. On-line functionality, fingerprints to verify (1:1) or identify (1: N) can be stored on non volatile memory, or be sent by RS-232 port [30].

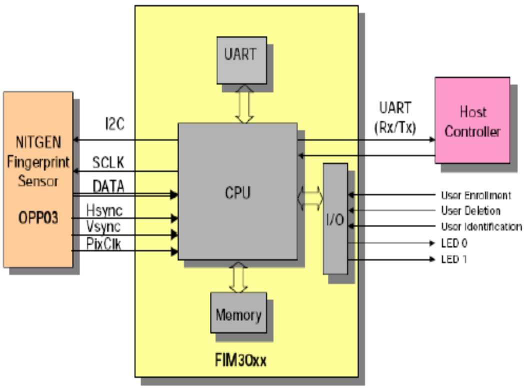

Fig 2: Fingerprint Module FIM3030 showing OPP03 sensor and serial interface.

4.3 GSM Modem

While accessing the system, we don't replace the password verification. If password is correct, the system will capture and match fingerprint of the customer. As shown in Fig 4, if fingerprint does not match with the account registry for three times, buzzer will be made ON and a message will be delivered to customer's cell phone and bank authority. Thus, GSM MODEM to communicate with the mobile phone to which we are going to send the message is also interfaced with LPC2148.

4.4 User Interface

The user interface makes the communication between user and the system model easier. It includes a display unit and a function keyboard. For displaying the status of the process running in system and instructional steps for the user, we interfaced 16 x 2 LCD matrixes with LPC2148 through GPIO pins of port 1.

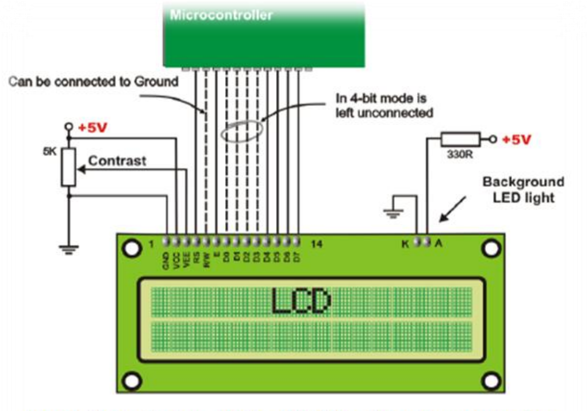

Fig 3: Interfacing of 16 x 2 LCD with microcontroller LPC2148

4.5 Power Supply

This section is meant for supplying power to all the sections mentioned above. It basically is consisted of a transformer to step down the 230V ac to 18V ac followed by diodes. The diodes are used to rectify the ac to dc. After rectification process, the obtained rippled dc is filtered using a capacitor Filter. A positive voltage of 12V and 5V are made available through LM7812 and LM7805. Further, LM317 is used to provide variable power e.g. 3.3V to LPC2148.

V. SOFTWARE DESIGN

The embedded platform discussed above is programmed in C language with KeilµVision4 to follow the program logic shown in Fig 4 as follows.

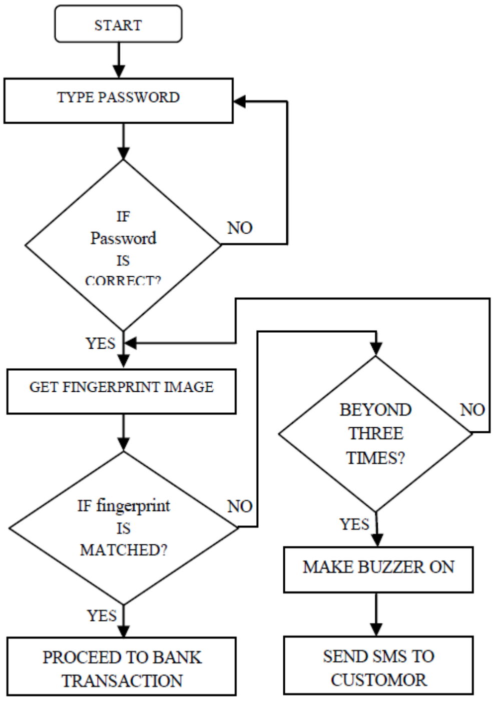

Fig 4: Realization of flow of tasks for the proposed system.

5.1 LPC2148 with Keil µVision4

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. Unless we have to use the tolls on the command line, the choice is clear. This IDE i.e. KEIL Greatly simplifies the process of creating and testing an embedded application. The user of KEIL centres on projects. A project is a list of all the source files required to build a single application, all the tool options which specify exactly how to build the application, and if required how the application should be simulated. A project is exactly the binary code required for the application. Because of the high degree of flexibility required from the tools, there are many options that can be set to configure the tools to operate in a specific and desired manner. It would be very tedious to have to set these options up every time the application is being built; therefore they are stored in a project file. Loading the project file into KEIL informs KEIL which source files are required, where they are, and how to configure the tools in the correct way. KEIL can then execute each tool with the correct options. Source files are added to the project and the tool options are set as required. The project can then be saved to preserve the settings. The project is reloaded and the simulator or debugger started, all the desired windows are opened.

5.2 Simulator & Debugger

The simulator/ debugger in KEIL can perform a very detailed simulation of a micro controller along with external signals. It is possible to view the precise execution time of a single assembly instruction, or a single line of C code, all the way up to the entire application, simply by entering the crystal frequency. A window can be opened for each peripheral on the device, showing the state of the peripheral. This enables quick trouble shooting of mis-configured peripherals. Breakpoints may be set on either assembly instructions or lines of C code, and execution may be stepped through one instruction or C line at a time. The contents of all the memory areas may be viewed along with ability to find specific variables. In addition the registers may be viewed allowing a detailed view of what the microcontroller is doing at any point in time.

5.3 Embedded C Language

The KeilµVision4 platform put forward the options for assembly language and high level language programming. C language being the most convenient language to access different port pins of LPC2148, we programmed the algorithm to control the FIM3030 fingerprint module through host controller LPC2148 in C language. The program follows the control actions as shown in the flowchart. The program segments to access UART, LCD, RTC, ADC, DAC, are included by linking through UART0.h, LCD.h, RTC.h, ADC.h, DAC.h header files respectively.

5.4 Flash Programming Utility

For downloading the application program into Flash ROM, this utility tool is necessary. The program code generated in C language after processing produces object code in hex form. It is referred as .hex file. To dump this hex code in the flash ROM of the controller the facility is provided with Keil version 4. For programming with older versions, the same task is completed with the help of software called Flash Magic.

VI. CONCLUSION

This type of ATM prototype can be efficiently used with fingerprint recognition. Since, password protection is not bypassed 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 security options were increased for the most part for the stability and dependableness of owner recognition. The whole system was built on the technology of embedded system that makes the system additional safe, reliable and straightforward to use. The same hardware platform can be used with IRIS scanner to put forward another potential biometric security to the ATMs.

REFERENCES

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

[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] 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

[5] ESaatci, 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 2002: 377-382.

[6] Gu J, Zhou J, Zhang D.A combination model for orientation field of fingerprints. Pattern Recognition, 2004, 37: 543-553.

[7] Cheng J, Tian J. Fingerprint enhancement with dyadic scale-space. Pattern Recognition Letters, 2004, 25(11): 1273-1284.

[8] Chen H, Tian J. A fingerprint matching algorithm with registration pattern inspection. Journal of Software, 2005,16(6): 1046-105.

[9] Smits G FJordaan E M.Improved SVMRegression using Mixtures of Kernels[A]. Proceedings of the 2002 International Joint Conferenceon Neural Networks[C]. Hawaii: IEEE. 2002. 2785-2.

[10] FU Zhenghua, LI Yongjun, Tian Mi(2007). "The embedded monitoring system based ARM". JOURNAL OF 7INSTRUMENT TECHNOLOGY, Vol. 07, No. Ipp. 01-2.

[11] Jun Zhou, Guangda Sua, Chun hongJiang. A face and fingerprint identity authentication system based on multi-route detection. Neurocomputing 70 (2007)922-931.

[12] Yuliang He, Jie Tian, Xiping Luo, Tanghui Zhang. Image enhancement and minutiae matching in fingerprint verification. Pattern Recognition Letters 24 (2003)1349-1360. [10] Wei Wang, Jianwei Li, Feifei Huang, Hailiang Feng. Design and implementation of Log-Gabor filter in fingerprint image enhancement. Pattern Recognition Letters 29 (2008)301-308.

[13] Lin Hong, Wan Yifei, Anil Jain. Fingerprint image enhancement: algorithm and performance evaluation[J]. IEEE Transactions on Pattern Analysis and Machine intelligence. 1998, 20(8): 777-789.