International Journal of Research in Engineering, Science and Management
Volume-2, Issue-5, May-2019
www.ijresm.com | ISSN (Online): 2581-5792

Combinational Security Lock System for ATM using Finger Print Identification

A. Nambikkai Nancy[1], S. Kavipriya[2]
[1]*Student, Department of Electronics and Communication Engineering, P. S. V College of Engineering and Technology, Krishnagiri, India*
[2]*Assistant Professor, Department of Electronics and Communication Engineering, P. S. V College of Engineering and Technology, Krishnagiri, India*

***Abstract*: In view of the mechanical locks used in the financial industry can no longer meet the needs of security and reliability of banking now. This new type of ATM safe lock system was composed of four parts which are respectively electronic combination lock host, pin identification using one-time password, finger print identification and host computer (PC) management center. The lower computer is composed of Cortex-M3 series MB9AFB44L processor module, fingerprint identification module and 2.4G wireless modem. Bank personnel who adds money is authorized by the integrated management system upper machine is sending a signal to notify the hand-held MCU to send packets in the authorized time after verification of hand-held fingerprint identification module, and the packets are also passed into combination lock host through 2.4G wireless module. When packets are received, combination lock host will compare and extract in advance, and ID number of hand-held device will be verified first. The contents of the packet will be extracted if the ID is meeting the permission scope, the unlock one-time password in the package content and the authorization record time are recorded at the moment, which is going to be matched with the password generated by combination lock host. The host will directly drive electromagnetic equipment to play the lock tongue. The whole process of verifying the unlock password must be done within the scope of authorization time, generally half a day or a day, which is determined by the bank management unit. In addition, with that vibration control is added in advance to protect the system from theft activity. That is to say, such a practice must be carried out within the control of management system. The lock is verified by actual operation in the bank that it can effectively improve the security of Bank ATM safe electronic password system, and it has a profound historical significance to promote the development of bank ATM safe electronic combination lock industry. Keywords: Cortex-M3 series MB9AFB44L processor module, fingerprint identification module and 2.4G wireless modem, vibration control. 1 Introduction Biometrics may be a technology that helps to create your information staggeringly secure, distinguishing all the users by way of their personal physical characteristics. Biometric data may be accustomed accurately determine individuals by exploitation their fingerprint, voice, face, iris, handwriting, or hand geometry and so on. Biometric identifiers supply many benefits over ancient and current strategies. Tokens like tape cards, smart cards and physical keys, can be stolen, lost, duplicated, or left behind; passwords can be shared, forgotten, hacked or unintentionally observed by a third party [1]. There are two key functions offered by a biometric system. One methodology is identification and also the different is verification.**

***Keywords*: Cortex-M3 series MB9AFB44L processor module, fingerprint identification module and 2.4G wireless modem, vibration control.**

1. Introduction

Biometrics could be a technology that helps to form your knowledge enormously secure, distinguishing all the users by means of their personal physical characteristics. Biometric info is accustomed accurately establish individuals by using their fingerprint, voice, face, iris, handwriting, or hand geometry and so on. Biometric identifiers offer several advantages over traditional and current methods. Tokens like magnetic tape cards, smart cards and physical keys, can be stolen, lost, duplicated, or left behind; passwords can be shared, forgotten, hacked or unintentionally observed by a third party.

1. There are two key functions offered by a biometric system. One methodology is identification and also the different is verification. In this paper, we are concentrating on distinguishing and confirming 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 Chip or card reader to identify the client, PIN Pad, Secure crypto processor typically at intervals a secure cowl, Display to be used by the customer for performing the transaction, Function key buttons, Record Printer to provide the client with a record of their dealing, to store the elements of the machinery requiring restricted access -Vault, Housing for aesthetics, Sensors and Indicators.
2. Fingerprint technology is that the most generally accepted and mature biometric methodology and is that the best to deploy and for a better level of security at your fingertips. It is easy to put in and additionally it takes very little time and energy to accumulate one's fingerprint with a fingerprint identification device. Thus, fingerprint recognition is taken into account

among the smallest amount intrusive of all biometric verification techniques. In ancient time officers used thumbprints to seal documents thousands of years ago, and law agencies have been using fingerprint identification since the late 1800s.

3. We here carries the same technology on digital platform. Although fingerprint pictures area unit at first captured, the images are not stored anywhere in the system. Instead, the fingerprints area unit regenerate to templates from that the first fingerprints cannot be recreated; thus no misuse of system is feasible.

A. Overview

The bank ATM safe lock has been a high-end product in financial machine. With the improvement of intelligent embedded technology, the lock system which offers cash box reliable protection is gaining the favor of the big Banks in term of its simple operation and high reliability, and now in the rapid development of China it has a large market demand. In view of the mechanical locks used by financial industry cannot meet the needs of banking security and reliability now, so a new product which can improve the safety of the locks meanwhile taking operating convenience for bank managers into account needs the new ATM safe lock system was designed to meet the requirements. This new type of ATM safe lock system was composed of four parts which are respectively electronic combination lock host, pin identification using one-time password, finger print identification and host computer (PC) management center. Its basic security principle is that using PC banking background management system products comprehensive control on the lock, through the dynamic password cooperated with the handheld intelligent key.

B. Literature survey

To implement this idea, we've studied totally different analysis works and located following data. For fingerprint recognition, a system has to capture fingerprint and so follow bound formula for fingerprint matching. The research paper [1] 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 [2] designs a new ATM terminal customer recognition system. The chip of S3C2440 is used for the core of microprocessor in ARM9 and an improved enhancement algorithm of fingerprint image increase the security of bank account and the ATM machine. For image improvement, the Dennis Gabor filter algorithms and direction filter algorithms are used.

In analysis paper [6], authors showed that {Dennis Gabor |physicist} filters (GFs) play a crucial role within the extraction of Gabor options and therefore the improvement of varied styles of pictures. For the aim of enhancing sinuous structures in wheezy pictures, sinuous GFs that regionally adapt their form to the direction of flow can even be used. If pictures of fingerprint area unit poor-quality pictures, they lead to missing options, leading to the degrading performance of the fingerprint system. Thus, it's important for a fingerprint recognition system to estimate the standard and validity of the captured fingerprint pictures. Existing approaches for this estimation are either to use of native options of the image or to use of worldwide options of the image.[7]In ancient fingerprint recognition approaches have demerits of simple losing wealthy data and poor performances because of the advanced kind of inputs, such as image rotation, poor quality image enrollment, incomplete input image, and so on.

In analysis paper [8], a new fingerprint recognition scheme based on a set of assembled invariant moment (geometric moment and Zernike moment) features to ensure the secure communications is proposed. In paper [9], fuzzy features match (FFM) based novel method on a local triangle feature is set to match the deformed fingerprints. Fingerprint here is depicted by the fuzzy feature set: the native triangle feature set.

In paper [10], a test chip has been unreal employing a zero.5 µm standard CMOS process. The total execution time for feat and process a fingerprint image is a smaller amount than three60 ms at ten Mc and therefore the power consumption is below seventy mw at 3.3 V supply voltage. We found development of a sensing element with CMOS technology in [11].

Also, a chip design that integrates a fingerprint sensing element and an identifier during a single chip is planned in [12]. The sensor senses capacitances fashioned by a finger surface to capture a fingerprint image. To have smart speed of operation for fingerprint matching, in [13] 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 will expeditiously compress the model size with a discount rate of 94%. Spectral trivialities fingerprint recognition system shows an identical speed with 125000 comparisons per second on a computer with Intel Pentium D processor 2.80 GHz, 1 GB of RAM.

C. Existing system

To implement this concept, we have studied different research works and found following information. Upon that the existing ATM security focused on making the terminals invulnerable to physical attack. The existing system of a mechanical lock system consist a cash box in it. The outer mechanical box is thick and designed for invulnerable. ATM cash loader is made up of a two level combinational lock in those two level numbering systems is used to open the lock tongue in the ATM. The authorized person who is going to fill the cash in ATM and four other armed people are taking the responsibility to open the cash box and filling the money. In this system the level of security is very less and also the authorized person may set the skimmer and he can help robbers. But in the case of proposed method the security level is increased. The existing system faces the following disadvantages like Ram-

raiding, Plofkraak and Digging a concealed tunnel under the ATM and cutting through the reinforced base to remove the money.

D. Proposed system

In view of the mechanical locks used by financial industry cannot meet the needs of banking security and reliability now, so a new product which can improve the safety of the locks meanwhile taking operating convenience for bank managers into account needs the new ATM safe lock system was designed to meet the requirements. This new type of ATM safe lock system was composed of four parts which are respectively electronic combination lock host, pin identification using one-time password, finger print identification and host computer (PC) management center. Its basic security principle is that using PC banking background management system products comprehensive control on the lock, through the dynamic password cooperated with the handheld intelligent key. The vibration control unit is the final level of security in that fingerprint is matched with the authorized person means the vibration unit will turn off until the cash refillment is fully completed. Otherwise the vibration unit will give an alert if anyone is trying to open the lock.

2. 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.

A. 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) [26].

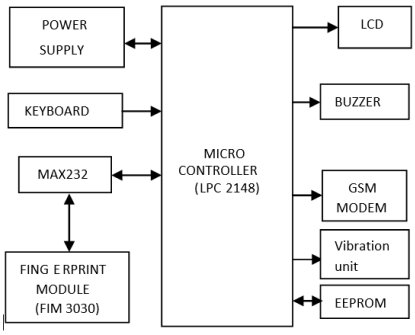

Fig. 1. Overview of the system.

This simplicity results in a high instruction throughput and impressive 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 executed, its successor is being decoded, and a third instruction is being fetched from memory [27]. The ARM memory interface has been designed to allow the performance potential to be realized without incurring high costs in the memory system. Speed-critical control signals are pipelined to allow system control functions to be implemented in standard low-power logic, and these control signals facilitate the exploitation of the fast local access modes offered by industry standard dynamic RAMs [28].

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 received 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,

1. 16/32-bit ARM7TDMI-S microcontroller in a tiny LQFP64 package.
2. 240 kB of on-chip static RAM and 512 kB of on chip flash program memory.
3. In-System/In-Application Programming (ISP/IAP) via on-chip boot-loader software.
4. Two 10-bit A/D converters provide a total of 14 analog inputs, with conversion times as low as 2.44 µs per channel.
5. Single 10-bit D/A converter provide variable analog output.
6. Multiple serial interfaces including two UARTs (16C550), two Fast I2C-bus (400 kbit/s), SPI and SSP with buffering and variable data length capabilities.
7. Vectored interrupt controller with configurable priorities and vector addresses.
8. Up to 45 of 5 V tolerant fast general purpose I/O pins in a tiny LQFP64 package [29].

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 detector is a 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 form a biometric model (a assortment of extracted features) that is hold on and used for matching. FIM3030 is an evolutionary standalone fingerprint recognition module consisted of optic

sensor OPP03 and processing board. As central processing unit and extremely upgraded algorithmic program area unit 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 enrollment, 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)

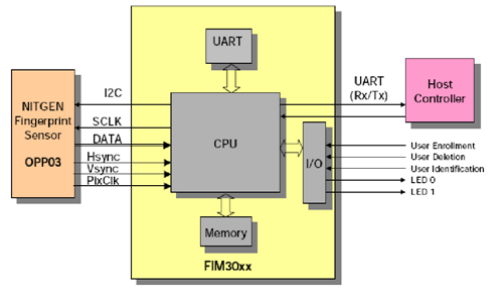

Fig. 2. Fingerprint Module FIM3030 showing OPP03 sensor and serial interface

can be stored on nonvolatile memory, or be sent by RS-232 port [30]. Here this FIM 3030 supports the serial communication protocol that is RS-232 whereas LPC2148 works on TTL logic. Interfacing of FIM3030 to LPC2148 for bidirectional communication is formed potential through IC known as MAX-232 used as grade convertor for reading and writing knowledge.

C. GSM Modem

While accessing the system, we don't replace the password verification. If arcanum is correct, the system can capture and match fingerprint of the client. 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 electronic equipment to speak with the portable to that we tend to are progressing to send the message is additionally interfaced with LPC2148.

D. User interface

The interface makes the communication between user and therefore the system model easier. It includes a display unit and a function keyboard. For displaying the standing of the method running in system and tutorial steps for the user, we tend to interfaced 16 x 2 digital display matrixes with LPC2148 through GPIO pins of port 1.

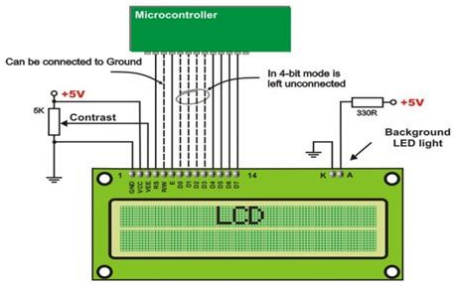

Fig. 3. Interfacing of 16 x 2 LCD with microcontroller LPC2148

E. Power supply

This section is meant for supplying power to all the sections mentioned above. It primarily is consisted of a electrical device to step down the 230V ac to 18V ac followed by diodes. The diodes are used to rectify the ac to dc. After rectification method, the obtained rippled dc is filtered using a capacitor Filter. A positive voltage of 12V and 5V are created out there through LM7812 and LM7805. Further, LM317 is employed to supply variable power e.g. 3.3V to LPC2148.

3. Software design

The LPC2148 is programmed with KeilµVision4. It is a window-based package platform that mixes a sturdy and fashionable editor with a project manager and create facility tool for development. It integrates all the tools to develop embedded applications together with a C/C++ compiler, macro assembler, linker/locator, and a HEX file generator. µVision helps expedite the event method of embedded applications by providing the IDE (Integrated Development Environment). KEIL is employed to form supply files; mechanically compile, link and covert victimization choices set with a straightforward to use interface and at last 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 method of making and testing an embedded application. The user of KEIL centers on projects. A project may be a list of all the supply files needed to make one application, all the tool choices that specify specifically a way to build the appliance, and if required how the application should be simulated. A project is precisely the computer code needed for the appliance. Because of the high degree of flexibility required from the tools, there are many options that can be set to where configure the tools to operate in a specific and desired manner.

It would be terribly tedious to own to line these choices up each time the appliance is being built; so they're keep in a project file. Loading the project file into KEIL informs KEIL which source files are required, they are, and how to configure the tools in the correct way. KEIL will then execute every tool with the right choices. Source files square measure adscititious to the project and therefore the tool choices square measure set as needed. The project will then be saved to preserve the settings. The project is reloaded and therefore the machine or

program started, all the desired windows are opened. [31].

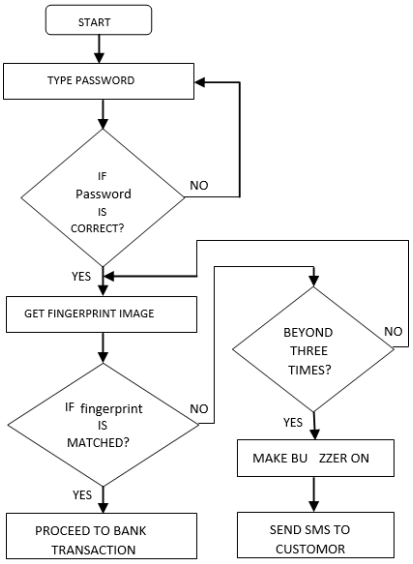

Fig. 4. Realization of flow of tasks for the proposed system.

A. *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 miss-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 [31].

B. *Embedded C language*

The KeilµVision4 platform advocate the choices for programing 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 management actions as shown within the flow diagram. 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.

C. *Flash programming utility*

For downloading the appliance program into Flash computer memory, this utility tool is necessary. The program code generated in C language when process produces computer code in hex kind. It is referred as .hex file. To dump this hex code within the flash computer memory of the controller the power is given Keil version four. For programming with older versions, the same task is completed with the help of software called Flash Magic.

4. Result

Fig 5 shows the hardware setup for planned system. It has been incontestable with success exploitation FIM3030 (Fingerprint scanner) and LPC2148 (ARM7 Microcontroller).

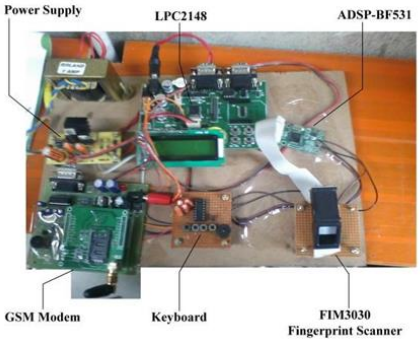

Fig. 5. Hardware setup developed for the proposed system.

5. Conclusion

After testing the system developed, we tend to came to understand that ATM model may be with efficiency used with fingerprint recognition. It will be done after it yielded fast response and is found to be of ease for use. Fingerprint pictures can't be recreated from templates; thus nobody will misuse the system. LPC2148 and FIM3030 provide low power consumption platform. Speed of execution may be increased with the utilization of additional sophisticated microcontroller. In future the same hardware platform can be used with cloud storage to store the data of authorized person like how Aadhar details are stored with 12-digit number, using this method we can store details of many people who is working in banking sector.

References

[1] Vaibhav R. Pandit, Kirti A. Joshi and Narendra G. Bawane, “ATM Terminal Security using Fingerprint Recognition,” in 2nd National Conference on Innovative Paradigms in Engineering & Technology, 2013.

[2] C. Fengjun, C. Xudong, W. Chen, Z. Yulong and Z. Xueer, "ATM safe electronic combination lock control system based on ARMV7 architecture," *2018 Chinese Control and Decision Conference (CCDC)*, Shenyang, 2018, pp. 360-364.

[3] R. Wang, “Behavior Characteristic of Using ATM Machine and Research on ATM Cash Management,” Southwestern University of Finance and Economics, 2011.

[4] Z. W. Tao, “A New Generation of Electronic Lock Management System, Realizing Security and Convenient Management of ATM Safe, Radio and Television Express CO., 50(4): 511–515, 2012.

[5] W. D. Ma, Exploring of about commercial Banks will be self-help equipment cleaning machine of printing and related business outsourcing management[J]. Times Finance, 2013,05:93-94.

[6] S. P. Mao, Study of using ATM dynamic electronic password lock, Financial Technology Era, 2012,03:65-69.

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

[8] 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.
[9] Anil K. Jain, Jianjiang Feng, Karthik Nandakumar, "Fingerprint Matching", IEEE Computer Society 2010, pp. 36-44.
[10] Virginia Epsinosa-Duro, "Minutiae Detection Algorithm for Fingerprint Recognition", IEEE AESS Systems Magazine, March 2002, pp. 7-10.
[11] Yun Yang, Jia Mi, "ATM Terminal Design is based on Fingerprint Recognition", IEEE 2010, pp. 92-95.
[12] Carsten Gosttschlich "Curved-Region-Based Ridge Frequency Estimation and Curved Gabor Filters for Fingerprint Image Enhancement", IEEE Transactions On Image Processing, Vol. 21, No. 4, April 2012, pp. 2220- 2227.
[13] Fernando Alonso-Fernandez, Julian Fierrez, Javier Ortega-Garcia, Joaquin Gonzalez-Rodriguez, Hartwig Fronthaler, Klaus Kollreider, Josef Bigun, "A Comparative Study of Fingerprint Image-Quality Estimation Methods", IEEE Transactions On Information Forensics and Security, Vol. 2, No. 4, December 2007, pp. 734-743.
[14] Jucheng Yang, Naixue Xiong, Athanasios V. Vasilakos, Zhijun Fang, Dongsun Park, Xianghua Xu, Sook Yoon, Shanjuan Xie, Yong Yang, "A Fingerprint Recognition Scheme Based on Assembling Invariant Moments for Cloud Computing Communications", IEEE Systems Journal, Vol. 5, No. 4, December 2011, pp 574-583.
[15] Xinjian Chen, Jie Tian, Xin Yang, Yangyang Zhang, "An Algorithm for Distorted Fingerprint Matching Based on Local Triangle Feature Set", IEEE Transactions On Information Forensics and Security, Vol. 1, No. 2, June 2006, pp. 169-177.
[16] Seong-Jin Kim, Kwang-Hyun Lee, Sang-Wook Han,Euisik Yoon, "A CMOS Fingerprint System-on-aChip With Adaptable Pixel Networks and ColumnParallel Processors for Image Enhancement and Recognition", IEEE Journal of Solid-State Circuits, Vol. 43, No. 11, November 2008, pp. 2558-2567.
[17] Marco Tartagni, Roberto Guerrieri, "A Fingerprint Sensor Based on the Feedback Capacitive Sensing Scheme", IEEE Journal of Solid-State Circuits, Vol. 33, No. 1, January 1998, pp. 133-142.
[18] Satoshi Shigematsu, Hiroki Morimura, Yasuyuki Tanabe, Takuya Adachi, and Katsuyuki Machida, "A Single-Chip Fingerprint Sensor and Identifier" IEEE Journal of SolidState Circuits, Vol. 34, No. 12, December 1999, pp. 1852-1859.
[19] Haiyun Xu, Raymond N. J. Veldhuis, Tom A. M. Kevenaar, and Ton A. H. M. Akkermans, "A Fast Minutiae-Based Fingerprint Recognition System" IEEE Systems Journal, Vol. 3, No. 4, December 2009, pp. 418-427.
[20] Dr. Kishore Reddy, A Ravi Shankar, R Laxmi Kanth, "Design of low Power Electronic Voting Machine using ARM Processor", International Journal of Emerging trends in Engineering and Development, Issue 2, Vol 6, September 2012.
[21] R. Rasu, P. Krishna Kumar, and M. Chandraman, "Security for ATM Terminal Using Various Recognition Systems", International Journal of Engineering and Innovative Technology, Volume 2, Issue 4, October 2012.
[22] Shan Juan Xie, Jucheng Yang, Dong Sun Park, Sook Yoon and Jinwook Shin, "Fingerprint Quality Analysis and Estimation Approach for Fingerprint Matching", State of the art in Biometrics, 2011, ISBN: 978-953-307-489-4.
[23] Amira Saleh, Ayman Bahaa and A. Wahdan, "Fingerprint Recognition, Advanced Biometric Technologies", 2011, ISBN: 978-953-307-487-0.
[24] Naser Zaeri, "Minutiae-based ―Fingerprint Extraction and Recognition", Biometrics, 2011, ISBN: 978-953-307-618-8.
[25] Der Chin Chen, "Portable Biometric System of High Sensitivity Absorption Detection", Biometric Systems, Design and Applications, 2011, ISBN: 978-953-307-542-6.
[26] Subhra Mazumdar, Venkata Dhulipala, San Diego, "Biometric Security Using Finger Print Recognition"
[27] S. M. Shamsheer Daula, K. E Sreenivasa Murthy "An Embedded ATM Security Design using ARM Processor with Fingerprint recognition and GSM", International Journal of Advanced and Innovative Research, Volume 1, Issue 2, July 2012.
[28] Steve Furber, ARM System-on-Chip Architecture, Second Edition, 2000, Addison Wesley, ISBN 0-201-67519-6.
[29] Andrew Sloss, Dominic Symes, Chris Wright, ARM System Developer's Guide, 2004, Morgan Kaufmann, ISBN: 1-55860-874-5.
[30] ARM7TDMI Data Sheet, Document Number: ARM DDI 0029E, Issued: August 1995, Advanced RISC Machines Ltd (ARM) UM10139, LPC214x Usermanual, NXP Semiconductors, Rev. 4 —23 April 2012.
[31] FIM30xx Datasheet, NITGEN Co., Ltd., 2006.
[32] MDK-ARM, KeilTM Tools By ARM, Keil0223-3 \ 01.11J.S.