RESEARCH ARTICLE OPEN ACCESS

The Evolvement of ATM Using Fingerprint

V. Ajantha Devi [1], A. Priyanka [2]
Assistant Professor [1], Research Scholar [2]
Department of Computer Science
Sri Adi Chunchanagiri Women's College, Cumbum,
Tamil Nadu - India

ABSTRACT
The main aim of this system is to develop a system, which is used for ATM security applications. In these systems, Bankers will collect the client finger prints and mobile number while opening the accounts then client only access ATM machine. The working of these ATM machine is when client place finger on the finger print module when it access automatically generates every time different 4-digitcode as a message to the mobile of the allowed client through GSM modem related to the microcontroller. The code usual by the client should be entered by imperative the keys on the screen. After incoming it checks whether it is a valid one or not and allows the client further access.
Keywords :— ATM, biometric, fingerprint, PIN, security.

I. INTRODUCTION
An Automated Teller Machine (ATM) is a mechanized telecommunications device that enables the clients of any financial institution to perform financial transactions like deposit, transfer, balance enquiries, small report, removal and fast money etc. without the need for a cashier, human clerk or bank teller. There are two types of ATMs: first, it is a easy ATM used only for cash withdrawal and to receive a report on account's sense of balance and the second is a composite unit, which is used for deposits and money transfer. The first type of ATM in popularly and frequently used. To enhance security and authentication of the client's account, the concept of using the fingerprint of the client as password instead of PIN is future, since biometric fingerprint is unique for each and every human being and it has more authentication than the PIN[1].

A. *Uses*
People use the ATM for transactions such as cash withdrawal, money transfer and payment of power and telephone bills. ATM is the most suitable to access the accounts and funding transactions.

B. *Fingerprint*
There are many biometric characteristics like fingerprint, hand geometry, iris, retina, ear, voice and face. Each of this character has its own advantages and disadvantages, and hence the selection among the biometrics depends on the requirements and authentication of the application. Among these, fingerprints are chosen. Fingerprints are patterns formed on the epidermis of the finger, composed of ridges and valleys[2]. This interleaved model of ridge and valleys make an important and evident point of the fingerprint.

II. PROPOSED METHODOLOGY
An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

A. Implementation Process
A growing security issue in ATM machine especially the use of card-PIN method has been of great concern to my researchers because the attacker can easily compromise the machine by using different methods. In view of this, this paper try to see how these problems of card-PIN can be reduced if not completely eradicated; this paper comprises of the following implementation process: The process of enrolment involve the account holder opening an account and register with the bank of their choice this will enable the bank to have all the enrolee's information and all necessary details that unease the enrollment 's and take the biometric data capture of the Person that own the report and store in the database, which will be used later for the process of verification and further inform of in sequence.[3]The process of removal and confirmation make used of minutiae-base techniques. This is to obtain an efficient and thoughtful result in order to reduce or eradicate the problems which is associated with the use of Card-PIN and high rate in security people faced in using ATM machine.

B. Enrollment Process:
Before an Account holder being identified or confirmed by a biometric device, the enrolment's process must be complete. The plan of this enrolment process is to create a summary profile of the user (Card Holders')[4]. The process consists of the following:

i. Bio Data
ii. Fingerprint Image Capture
iii. Rotation And Displacement Of Image
iv. Template Database Storage
v. Conversion And Encryption

vi. The Enrollee Storage

i. Bio data:

This comprise the next: first name and last name which get alphabetic font, type: Current, or Saving this also take alphabetic characters, picture of the enrollment 's which be able to take binary font, people of the enrollment take alphabetic and string lettering, date of birth take string characters and the date account was issue take string characters too.

ii. Fingerprint Image Capture:

The Account Owner fingerprint will be captured with fingerprint scanner for a minimum of two or three biometric readings, by placing a finger in a fingerprint person who reads. Not all the sample will be store; the knowledge analyze and actions various data points unique to each individual. The number of measured data points varies in accordance to the type of device .Minutiae Feature Extraction from Image: this is where the minutiae extraction is done and of course processes like binarization, thinning and bifurcation would be done have a perfect minutiae feature extraction from the image.

iii. Rotation and Displacement of Image:

This is where the image is normalized to get an authentic and effective image to be stored in the database, which aids the process of matching.

iv. Template Database Storage:

This part stores all the templates and information that are been generated from the process of minutiae extraction and rotation and displacement of image.

v. Conversion and Encryption:

The Account Owner measurements and data points are converted to a mathematical algorithm and encrypted. These algorithms cannot be upturned to obtain the original image. The algorithm may then be stored as a user's pattern in the database servers and on the ATM card.

vi. The Enrollment Storage:

This has all the details of all the community that have been enrollment and its stores them with the bank account number. When there is need to view enrollment's details or make amends this can easily be done with the use of bank account number to copy individual's details and it makes the development of confirmation easier and faster as it saves time.

III.FINGERPRINTS FOR IDENTIFICATION

A. Electronic recording

There has been a newspaper report of a man selling stolen watches sending images of them on a mobile phone, and those images included parts of his hands in enough detail for police to be able to identify fingerprint patterns. Classifying fingerprints before computerization replaced manual filing systems in large fingerprint operations, manual fingerprint classification systems were used to categorize fingerprints based on general ridge formations (such as the presence or absence of circular patterns on various fingers), thus permitting filing and retrieval of paper records in large collections based on friction ridge patterns alone.

The most popular ten-print classification systems include the ROSCHER system, the JUANVUCETICH system, and the Henry Classification System. Of these systems, the ROSCHER system was developed in Germany and implemented in Germany and Japan, the VUCETICH system (developed by a Croatian-born Buenos Aires Police Officer) was developed in Argentina and implemented throughout South America, and the Henry system was developed in India and implemented in most English-speaking countries. In the Henry system of classification, there are three basic fingerprint patterns: Loop, Whorl and Arch, which constitute 60–65%, 30–35%and 5% of all fingerprints respectively. There are also more complex classification systems that break down patterns even further, into plain arches or tented arches, and into loops that may be radial or ulnas, depending on the side of the hand the tail points towards. Whorls may not have subgroup classifications it including only plain whorls[5].

IV. FINGERPRINT RECOGNITION

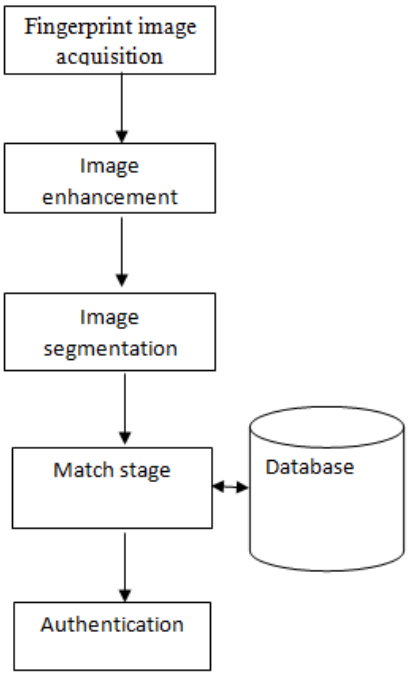

Fig 1: Fingerprint Recognition

A. Image Acquisition

The acquisition of a fingerprint images was very skilful by using off-line sensing or live-scan. Off-line sensing is defined as ink-technique. An individual place his fingerprint

black ink then his finger is pressed in a paper card .after that the paper is scanned in a scanner to produce the digital image. This type of scanning is common in crime scene to get a hidden fingerprint. However, live-scan scanners become currently more frequent, because of its simpleness in usage. There is no need for ink. The digital image is directly received by pressing against the surface of the scanner[6].

B. Image Enhancement

Fingerprint Image enhancement is used to make the image clearer for easy further operations. Since the fingerprint images received from scanner or any other media are not certain with perfect quality, those enhancement methods, for increasing the contrast between ridges and valleys and for connecting the false broken points of ridges due to not enough amount of ink, are very useful for keep a higher accuracy to fingerprint recognition.

Fig 2: Image Enhancement

C. Image Segmentation

Image Segmentation of the fingerprint image is to decide which part from the image is related to the foreground and which part is related to the background. Due to the nature of fingerprint image and the presence of noise, the decision for separation these two regions is critical. The fingerprint image can be affected by many conditions that perform the segmentation to be a challenging job. The first problem is the presence of dust and grease in the scanner's sensor. The second one is the presence of some traces from previous image learning. The last one is the contrast of fingerprint that can be influenced by the dryness or the wetness of the finger. For dry finger, fingerprint contrast is low and for wet finger, the contrast is high.

D. Match Stage

The final match ratio for two fingerprints is the number of total matched pairs divided by the number of minutia of the template fingerprint. The score is 100*ratio and ranges from 0 to 100. If the score is larger than a pre-specified point where something begins or changes (usually 80%), the two fingerprints are from the same finger.

E. Database

A database of fingerprint images and methods of using such a database are disclosed. The database may have at least two fingerprint images that are impression images produced by a single finger. Each impression image shows a different part of the friction ridge surface of the finger. Methods using the database may be focused on figuring whether a match exists between a fingerprint sample and the database images.

F. Authentication

Authentication is also often used in the ATM field for secure transaction. By using a biometric for authentication process. Authenticating a user means to let the system know the user's identity without any concern about the mode.

V. ATM PROCESS

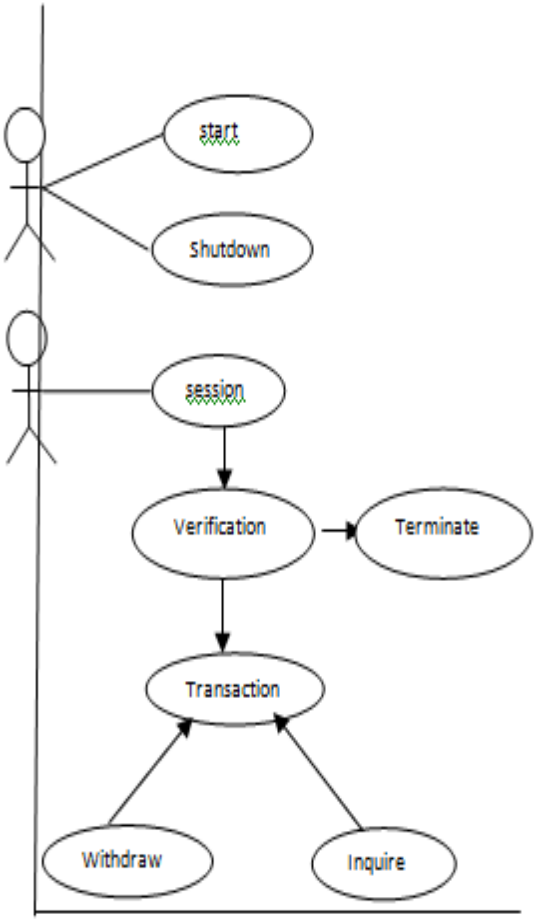

Fig 3: ATM process

VI. 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 off 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[7].

A fingerprint sensor is an electronic device used to record by a computer a digital image of the fingerprint pattern. The record by a computer 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 confirmation. FIM3030 has functions of fingerprint enrollment, identification, partial and whole deletion and reset in a single board, there by offering convenient development surroundings conditions.

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 confirm (1:1) or identify (1: N) can be stored on non unstable memory, or be sent by RS-232 port .

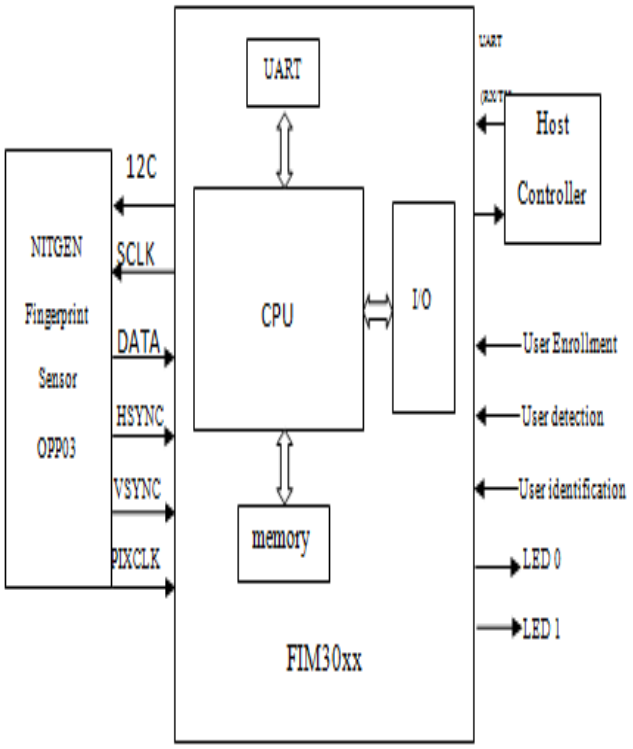

Fig 4: Fingerprint Module FIM3030 showing OPP03 sensor and serial interface.

Here this FIM 3030 supports the sequential communication protocol which is RS-232 while LPC2148 works on TTL logic. Interfacing of FIM3030 to LPC2148 for bidirectional communication is made possible through IC called MAX-232 used as a level converter for reading and writing data.

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 use and price. The ARM architecture is based on RISC (Reduced Instruction Set Computer) values, and the instruction set and related decode mechanism are much simpler than those of micro-programmed Complex Instruction Set Computers (CISC).

This ease results in a high instruction throughput and impressive concurrent interrupt response from a small and gainful chip. All parts of the processing and memory systems can operate continuously since, pipelining is employed. Normally, while one instruction is being executed, its successor is being decoded, and a third instruction is being fetched from memory. The ARM memory crossing point has been designed to allow the performance possible 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 help the abuse of the fast local access modes offered by industry standard active RAMs[8].

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 following difference of templates, the system will initialize the GSM module to send message to the enrolled user and at the same time 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 change times as low as 2.44 µs per channel.

e) Single 10-bit D/A converter provide changeable analog output.

f) Multiple sequential 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[8].

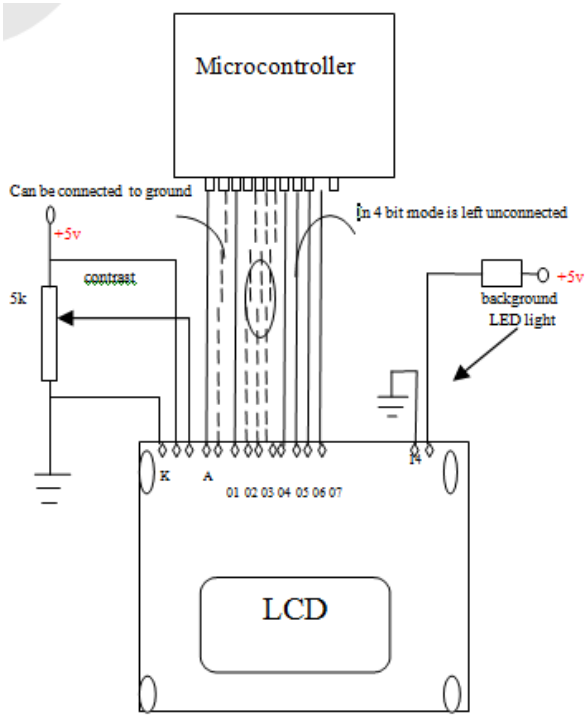

Fig 5: Interfacing of 16 x 2 LCD with microcontroller LPC2148.

B. GSM Modem

While accessing the system, we don't replace the password confirmation. If password is correct, the system will capture and match fingerprint of the client. As shown in Fig 5, if fingerprint does not match with the account registry for three times, buzzer will be made ON and a message will be delivered to client's cell phone and bank authority. So, GSM MODEM to communicate with the mobile phone to which we are going to send the message is also interfaced with LPC2148[9].

C. 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.

D. 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 fix 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 changeable power V to LPC2148.

VII. CONCLUSION

ATM provides economic services to an increasing segment of the population in many countries. Fingerprint scanning, continues to gain acceptance as a reliable identification and verification processes. This paper identifies a model for the change of existing ATM systems to cheaply incorporate fingerprint scanning PLUS blood group; and, outlines the advantages of using such system. It should be noted that the clients' perception cannot be generalized as it was highly affected by the tradition or culture of the users involves.

REFERENCES

[1] Mahesh A. Patil ,Mr. Sachin P.Wanere Mr.Rupesh, P.Maighane, Mr.Aashay, R.Tiwari"ATM Transaction Using Biometric Fingerprint Technology" International Journal Of Electronics, Communication & Soft Computing Science And Engineeringissn: 2277-9477, Volume 2, Issue 6.

[2]Awotunde, Joseph B. University School, University Of Ilorin, Ilorin, Kwara State, Nigeria"Fingerprint Authentication System: Toward Enhancing ATM Security "International Journal Of Applied Information Systems (IJAIS) – ISSN : 2249-0868 Foundation Of Computer Science FCS, New York, USA Volume 7– No.7,August 2014.

[3]Awotunde, Joseph B. University School, University Of Ilorin, Ilorin, Kwara State, Nigeria"Finger Minutiae Format For Data Interchange" ANSI INCITS 378.Information Technology -,2004.

[4]Khan, M., Zhang, J.:"Implementing Templates Security In Remote Bio-Metric Authentication System"International Conference On Computationalintelligence And Security (2006) 1396-1400.

[5]Anil K. Jain, Jianjiangfeng, Karthiknandakumar, "Fingerprint Matching", IEEE Computer Society 2010, Pp. 36-44, 0018-9162/10

[6]Ing.Martin Drahansky,"Biometric Security Systems Fingerprint Recognition Technology",IEEE 2003, No.FR0835/2003/G1.

[7]Doc.Ing.Frantisekzboril,Csc. Dr. Rer. Nat. Ludeksmolik"Biometric Security Systems Fingerprint Recognition Technology", June 16,2003,March 30,2005.

[8]Avinash Kumar Ojha, ATM Security using Fingerprint Recognition International Journal of Advanced Research in
Computer Science and Software Engineering, Volume 5, Issue 6, June 2015.

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

[10] Yuliang He, Jie Tian, Xiping Luo, Tanghui Zhang. Image enhancement and minutiae matching in fingerprint verification. Pattern Recognition Letters 24 (2003)1349-1360

[11] 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.

[12] 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.