Smart and Secure ATM Surveillance System for Banking Networks

Dr.K.G.Revathi [1], Anisha J[2], Archana R[3], Benisha B[4]
[1] *Professor, Department of ECE, DMI College of Engineering, Tamilnadu 600123*
[2,3,4]*UG Students, Department of ECE, DMI College of Engineering, Tamilnadu 600123*

Abstract **- Authentication based on biometric provides various advantages in ATM (Automated Teller Machine) systems. The weakness of existing authentication scheme in ATM is the usage of PIN (Personal Identification Number) numbers as password. Because PIN numbers are easily traceable and misused. Our proposed system is developed to provide better security to the ATM. Here, the PIN numbers are replaced with biometric security. The main objective of the work is to eliminate the use of ATM cards completely and to ensure better security. We provide user friendly access, instead of many ATM cards we compact it with enhanced security by providing fingerprint authentication. By comparing different technologies that are used for ATM security, it observes that fingerprint technology performs better and safer than other technologies. The entire security module is combined with detection of unknown activity and vibration sensor cum alarm, which alerts the nearest police station as well as the bank security wing. This overall system proves to be an autonomous, continuous and secured surveillance system.**

Index Terms **- ATM, Accessing, Authentication, Embedded System, Biometrics, Verification, Fingerprint, Security.**

INTRODUCTION

Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. Biometric-based solutions are able to provide for confidential financial transactions and personal data privacy. The various features used are face, fingerprints, hand geometry, handwriting, iris, retina, vein and voice [1]. Fingerprinting or finger-scanning technologies are the oldest of the biometric sciences and utilize distinctive features of the fingerprint to identify or verify the identity of individuals. Finger-scan technology is the most commonly deployed biometric technology, used in a broad range of physical access and logical access applications. All fingerprints have unique characteristics and patterns. A normal fingerprint pattern is made up of lines and spaces. These lines are called ridges while the spaces between the ridges are called valleys. It is through the pattern of these ridges and valleys that a unique fingerprint is matched for verification and authorization. These unique fingerprint traits are termed “minutiae” and comparisons are made based on these traits [2]. On average, a typical live scan produces 40 “minutiae”. The Federal Bureau of Investigation (FBI) has reported that no more than 8 common minutiae can be shared by two individuals.

There are five stages involved in finger-scan verification and identification. Fingerprint (FP) image acquisition, image processing, and location of distinctive characteristics, template creation and template matching [3]. A scanner takes a mathematical snapshot of a user's unique biological traits. This snapshot is saved in a fingerprint database as a minutiae file. The first challenge facing a finger-scanning system is to acquire high-quality image of a fingerprint. The standard for forensic-quality fingerprinting is images of 500 dots per inch (DPI). Image acquisition can be a major challenge for finger-scan developers since the quality of print differs from person to person and from finger to finger. Some populations are more likely than others to have faint or difficult-to-acquire fingerprints, whether due to wear or tear or physiological traits. Taking an image in the cold weather also can have an effect. Oils in the finger help produce a better print. In cold weather, these oils naturally dry up. Pressing harder on the platen (the surface on which the finger is placed, also known as a scanner) can help in this case.

Image processing is the process of converting the finger image into a usable format. This results in a series of thick black ridges (the raised part of the

fingerprint) contrasted to white valleys. At this stage, image features are detected and enhanced for verification against the stored minutia file. Image enhancement is used to reduce any distortion of the fingerprint caused by dirt, cuts, scars, sweat and dry skin [3]. The next stage in the fingerprint process is to locate distinctive characteristics. There is a good deal of information on the average fingerprint and this information tends to remain stable throughout one‟s life. Fingerprint ridges and valleys form distinctive patterns, such as swirls, loops, and arches. Most fingerprints have a core, a central point around which swirls, loops, or arches are curved. These ridges and valleys are characterized by irregularities known as minutiae, the distinctive feature upon which finger-scanning technologies are based. Many types of minutiae exit, a common one being ridge endings and bifurcation, which is the point at which one ridge divides into two. A typical finger-scan may produce between 15 and 20 minutiae. A template is then created. This is accomplished by mapping minutiae and filtering out distortions and false minutiae. For example, anomalies caused by scars, sweat, or dirt can appear as minutiae. False minutiae must be filtered out before a template is created and is supported differently with vendor specific proprietary algorithms. The tricky part is comparing an enrollment template to a verification template. Positions of a minutia point may change by a few pixels, some minutiae will differ from the enrollment template, and false minutiae may be seen as real. Many finger-scan systems use a smaller portion of the scanned image for matching purposes. One benefit of reducing the comparison area is that there is less chance of false minutiae information, which would confuse the matching process and create errors.

RELATED WORK

Most finger-scan technologies are based on minutiae. Samir Nanavati [3] states that 80 percent of finger-scan technologies are based on minutiae matching but that pattern matching is a leading alternative. This technology bases its feature extraction and template generation on a series of ridges, as opposed to discrete points. The use of multiple ridges reduces dependence on minutiae points, which tend to be affected by wear and tear [4]. The downside of pattern matching is that it is more sensitive to the placement of the finger during verification and the created template is several times larger in byte size.

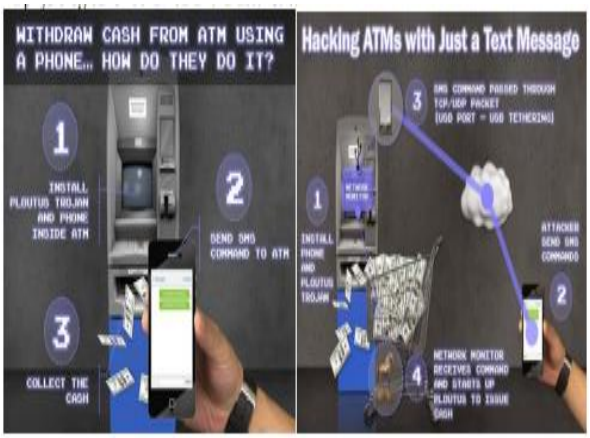
Finger-scan technology is proven and capable of high levels of accuracy. There is a long history of fingerprint identification, classification and analysis. This along with the distinctive features of fingerprints has set the finger-scan apart from other biometric technologies. There are physiological characteristics more distinctive than the fingerprint (the iris and retina, for example) but automated identification technology capable of leveraging these characteristics have been developed only over the past few years. The technology has grown smaller, more capable and with many solutions available. Devices slightly thicker than a coin and an inch square in size are able to capture and process images. Additionally, some may see the large number of finger-scan solutions available today as a disadvantage; many see it as an advantage by ensuring marketplace competition which has resulted in a number of robust solutions for desktop, laptop, physical access, and point-of-sale environments. Biometric data are separate and distinct from personal information. Biometric templates cannot be reverse-engineered to recreate personal information and they cannot be stolen and used to access personal information [5].

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.

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.



METHODOLOGY

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. To implement the proposed security for ATM terminals with the use of fingerprint recognition, we use the different hardware and software platforms. An embedded system is a combination of software and hardware to perform a dedicated task. Some of the main devices used in embedded products are microprocessors and microcontrollers. In this paper a fingerprint-based ATM cashbox accessing system using atmega 328 microcontroller is implemented. Microcontroller forms the controlling module, and it is the heart of the device. Initially we store the fingerprint of bank manager and that will be verified with the fingerprint that we are giving when the time of authentication. If both the fingerprints are matched then ATM cashbox will open, otherwise buzzer will give alarm. The task related instructions are loaded into the atmega 328 microcontroller which is programmed using Embedded C language. The system consists of Microcontroller Unit, Fingerprint module, LED indicators and a buzzer alarm system and microcontroller that collect data from the fingerprint module. As it is based on the fingerprint authentication there is no chance of disclosing of password or pin to the third parties.

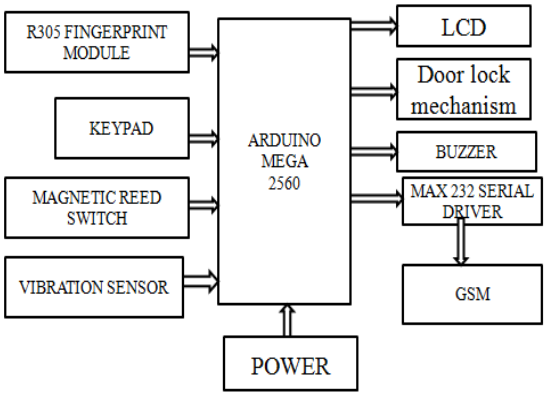


Fig 1: Block Diagram

Hardware Requirements

- Arduino Uno R3
- R305 Fingerprint Sensor
- Reed Switch
- Sim 800c Gsm Modem
- Vibration Sensor
- Keypad
- Door Lock Mechanism
- Buzzer
- Power Supply Unit
- 16*2 Lcd

Software Requirement

- ARDUINO IDE
- Embedded C

HARDWARE IMPLEMENTATION

Arduino UNO

The Arduino UNO is an open-source microcontroller board based on the Microchip ATmega328P microcontroller and developed by arduino. The board is equipped with sets of digital and analog input/output (I/O) pins that may be interfaced to various expansion boards (shields) and other circuits. The board has 14 Digital pins, 6 Analog pins, and programmable with the Arduino IDE (Integrated Development Environment) via a type B USB cable. It can be powered by a USB cable or by an external 9-volt battery, though it accepts voltages between 7 and 20 volts. It is also similar to the Arduino Nano and Leonardo. The hardware reference design is distributed under Common Creative Attribution Share-Alike 2.5 license and is available on the arduino website. Layout and production files for some versions of the hardware are also available. "UNO" means one in Italian and was chosen to mark the release of Arduino Software (IDE) 1.0. The UNO board and version 1.0 of arduino Software (IDE) were the reference versions of arduino, now evolved to newer releases. The UNO board is the first in a series of USB arduino boards, and the reference model for the arduino platform. The ATmega328P on the arduino UNO comes preprogrammed with a boot loader that allows uploading new code to it without the use of an external hardware programmer. It communicates using the original STK500 protocol. The UNO also differs from all preceding boards in that it does not use the FTDI USB-to serial driver chip. Instead, it uses the Atmega16U (Atmega8U2 up to version R2) programmed as a USB-to-serial converter.

Fig -2: Arduino Board

Fingerprint Module

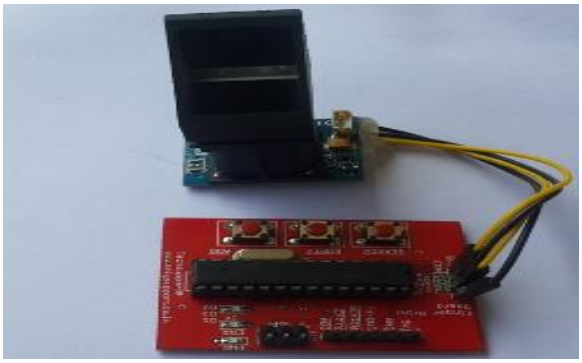


Figure 3: Fingerprint Sensor

Secure with biometrics - this all-in-one optical fingerprint sensor will make adding fingerprint detection and verification super simple. These modules are typically used in safes - there's a high-powered DSP chip that does the image rendering, calculation, feature finding and searching. Connect to any microcontroller or system with TTL serial, and

send packets of data to take photos, detect prints, hash and search. You can also enroll new fingers directly up to 162 fingerprints can be stored in the onboard FLASH memory. There is a red LED in the lens that lights up during a photo, so you know it's working as shown in fig.3.

LCD

Liquid Crystal Display (LCD) is used to display the output to the user in the form of GUI (Graphic User Interface) and a mono chromatic display. LCD used in this project is JHD162A series. There are 16 pins in all. They are numbered from left to right 1 to 16 (if you are reading from the backside). Generating custom charcters on LCD is not very hard. It requires the knowledge about custom generated random-access memory (CG-RAM) of LCD and the LCD chip controller. Most LCDs contain Hitachi HD4478 controller. CG-RAM is the main component in making custom characters. It stores the custom characters once declared in the code. CG-RAM size is 64 byte providing the option of creating eight characters at a time. Each character is eight byte in size.

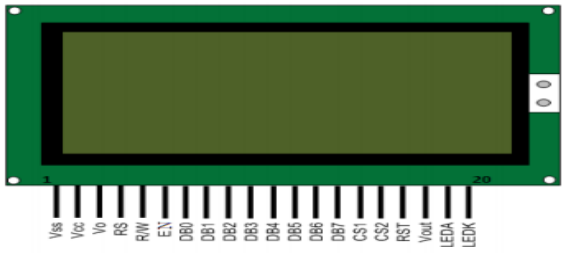


Fig -4: LCD

Keypad module

A toggle may be a category of electrical switches that area unit manually motivated by a mechanical lever, handle, or rocking mechanism. The phrase "toggle switch" is applied to a switch with a brief handle and a positive snap-action, whether or not it really contains a toggle mechanism or not. once the actuator-the toggle itself-is affected, the coil within the switch moves the transferable contact into position either energizing the circuit or de-energizing it.

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 Arduino.

RESULTS AND DISCUSSION

The figure shows the basic arrangement of fingerprint-based security system for ATM which includes fingerprint module, microcontroller, motor driver, motor, LCD display. The display shows the messages for fingerprint access and whether the fingerprint is matched. Accordingly a pulse will be given and motor rotates as, ATM security is accessed by fingerprint system.

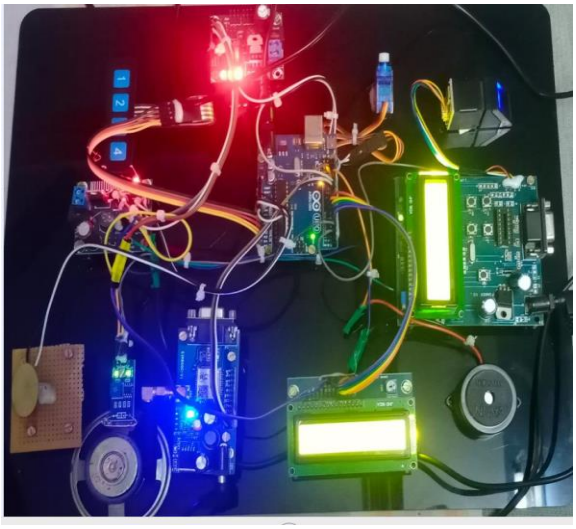


Fig 5. Experimental Setup

While tampering or lifting the ATM machine it leads to buzzer alarm and simultaneously the door will lock as shown in fig. 6 and fig. 7 respectively.

Fig. 6. Before door lock

Fig.7 After door lock

In case of any theft, an immediate alert message is sent to the nearby police station and respective bank authority as shown in fig. 8

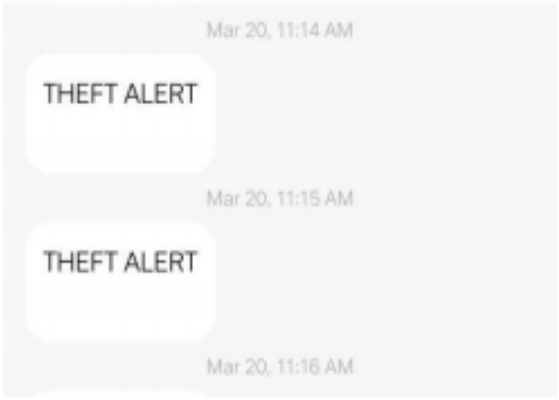


Fig. 8 Theft alert message

CONCLUSION

The implementation of ATM security by using fingerprint also contains the Original verifying methods, which were inputting customer fingerprint, which is send by the controller and verified properly. The security Features were enhanced largely for the stability and reliability of owner recognition. The whole system was built on the fingerprint technology, which makes the system safer, reliable and easy to use. This will be most promising technology at electronic money transaction. The future scope of this research can include face recognition using thermal camera. Thus, it provides double authentication for the user which enhances the security of the system. For senior citizen and disabled people, the fingerprint and face recognition of the guardian can be included to reduce their difficulties.

REFERENCES

[1] "An IOT Based ATM Surveillance System" by V. Jacintha, J Nagarajan, K Thanga Yogesh, S Tamilarasu, S Yuvaraj, IEEE International Conference on Computational Intelligence and Computing Research, 2017.

[2] "Real time Security Framework for Detecting abnormal events at ATM Installation" by Vikas Tripathi, Ankush Mital, Vishnukanth, Journal of Real-Time Image Processing, 2016.

[3] "Smart ATM Surveillance System" by S. Shriram, Swastik B. Shetty, Vishnu Prasad P. Hegde, K C R Nisha, V Dharmambal, International Conference on Circuit, Power and Computing Technologies (ICCPCT), 2016

[4] "Smart ATM Security System using FPR, GSM and GPS", by Bharati M Nelligani, N Reddy, N Awasti, International Conference on Inventive Computation Technologies (ICICT), 2016.

[5] "Biometric Based Smart ATM Using RFID" by S Gokul, S Kukan, K Meenakshi, S S Vishnu Priyan, J Rolant Gini, M E Harikumar, Third International Conference on Smart Systems and Incentive Technology (ICSSIT), 2020.

[6] "An Intelligent Vision System for Monitoring Security and Surveillance of ATM" by Sambarta Ray, Souvik Das, Anindya Sen, Annual IEEE India Conference (INDICON), 2015