ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 2, April 2017

A SELF BANKING MACHINE WITH FACE AND FINGER PRINT RECOGNITION

Mr.J.Manokaran M.E
Assistant Professor,
Department of Electronics Communication Engineering
Indra Ganesan College of Engineering
Trichy-12, Tamil Nadu, India

K.K.DHARINI, R.KEERTHIKA,
S.RATHNA BHARATHI.
Department of Electronics Communication Engineering
Indra Ganesan College of Engineering
Trichy-12, Tamil Nadu,India

***Abstract*— Aim of this proposed system to enhanced feature and improve the service of ATM cash withdrawal in less time with more level of security. There is no change required to the existing system but some addition required, which makes no impact on existing system. Face recognition and Finger print based security ATM system is proposed in this system. ATM card holder has to authorize with their face image in their corresponding bank. All ATM have the module of camera. Users can able to access the ATM only if their face is matched with their predefined trained image. ATM door will open only if the human face is detected otherwise it always in close condition. Along with these users can access the ATM system without using the ATM card. The finger print recognition uses the data about the persons finger print for comparision. It compares the given input with the stored data. If it matches the banking process can be carried out.**

***Index Terms*—ATM, ATM security ,Face recognition, Finger print recognition.**

I. INTRODUCTION

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 teller machine (atm). It is a computerized machine designed to dispense cash to bank customers without need of human interaction. Today the atm users are increasing in numbers. They use the atm cards for banking transactions like balance enquiry, mini statement, withdrawal, etc.

The ATM machine has card Reader and keys as input devices and display screen, cash dispenser, receipt printer, speaker as output devices. ATMs are connected to a host processor, which is a common gateway through which various ATM networks become available to users. Various banks, independent service providers owned this host processor. Account information of user is stored on the magnetic strip present at the back side of the ATM card. When we enter the card in the card reader, the card reader captures the account information and the information is used for the transaction purpose. And we have to insert the pin by keys. The pin is the 4 digit number given to all ATM card holders. ATM card holder's pin is different from each other. The number is verified by the bank and allows the customers to access their account. The password is the only identity so anyone can access the account when they have the card and correct password.

Once the card and is stolen by the culprit and if he/she comes to know the password by any means then the culprit can take more money from the account in the shortest period, it may bring huge financial losses to the users. In the recent days, there have been many such ATM fraud cases. Due to some of the flaws in our present ATM system such as use of static pin and ATM card, its users face many kinds of problem and there have been many issues associated with the present system. To overcome the problems associated with the present ATM System, in our project we are using biometric features. Biometrics technologies are a secure means of authentication because biometrics data are unique, cannot be shared, cannot be copied and cannot be lost. Physical characteristics include fingerprint, hand or palm geometry, retina, iris and face while popular behavioral characteristicsare signature and voice.

In the war of functionality versus security, the functionality wins more often. Security has always been viewed upon as an overhead or afterthought by software developers. But in the case of banking and money transactions, the security should hold highest priority. Increase in daily attacks on ATM and banking security the developers getting on right track and putting security their important aspect in developing projects. The multifactor authentication is an approach to authentication which requires the presentation of two or more authentication factors: a knowledge factor ("something only the user knows"), a possession factor ("something only the user has"), and an inherence factor ("something only the user is"). After presentation, each factor must be validated by the other party for authentication to occur.

In present days the ATM holds only one thing (i.e. PIN) to secure the money saved in the bank if we are not considering the physical attacks. In our system

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 2, April 2017

we are going beyond this level of security to enhance security of the ATM. This will send over customer's mobile number stored in records. In secure ATM, user will have to register mobile and its IMEI number in bank system. When user puts/swipes card into machine, user get request to insert PIN (which is current way of ATM banking.

II. SYSTEM MODELS

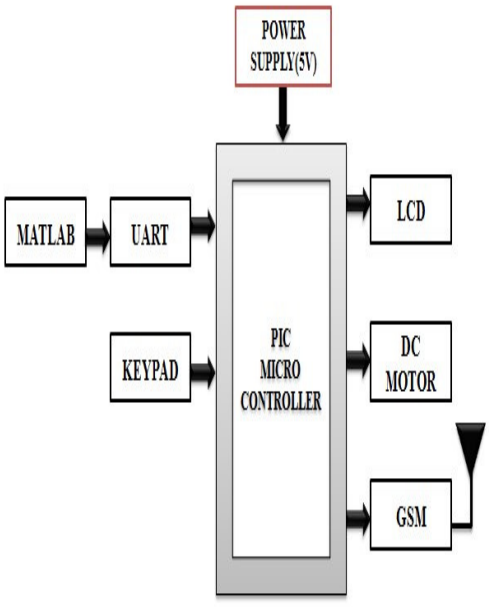
The cash in transit or stored in the ATM safe has been the asset traditionally targeted by ATM criminals, sometimes in rather violent ways. However, in the last years, attackers have turned their attention equally to soft assets present in the ATM, such as PINs and account data. Criminals use this stolen information to produce counterfeit cards to be used for fraudulent transactions increasingly around the world encompassing ATM withdrawals, purchases with PIN at the point of sale, and purchases without PIN tin card-not-present environments. PINs and account data are assets belonging to cardholders and issuers. They are inevitably in clear form at the ATM, when the card and PIN are entered. By attaching, for example, a pinhole camera and a skimmer to the ATM, a criminal can steal PINs and account data before they can be securely processed by the ATM.

These attacks require a relative low attack potential, in terms of both skills and material that is commercially available. The latest generations of skimmers and cameras are unnoticeable to untrained eyes and can be quickly installed and removed from the ATM without leaving any trace. In high traffic ATMs, dozens of PINs and associated account data sets can be stolen in a few hours. The first line of defense to these attacks has to be offered by the ATM itself. Counter measures at device level include detection of attached alien objects, disturbance of magnetic-stripe reading near the entry slot, etc. Alarms generated by the device should be acted upon promptly and complemented with inspections of the ATM, more frequently at higher-risk installations. Taking all these parameters under consideration a secured ATM transaction system is proposed using microcontroller which will effectively stop the misuse of ATM system & also to take the necessary
action against the culprit

The problem with current ATM banking is, every day there is something new that make bad impact on security related to ATM banking. This leads to necessity of new techniques or algorithms to deal with new possible attacks that can happen. This project will give a good way to solve problems like card fraud, skimming, card data stealing/trapping. This project will be presenting an algorithm, which will be capable of considering more than two factors to generate an OTP. While generating an OTP, the proposed algorithm will consider current time, location of ATM the IMEI number and mobile number of user. This project is also considering application based problem of ATM where the factors like, user forgot the mobile device at home, mobile battery is down, and user is not in the network coverage to make difficulties in OTP security service. For covering such difficulties another option is given in the ATM that is Biometric. By using biometric authentication legitimate user can do transaction even if he/she is not having his/her mobile device for receiving OTP. Security based ATM system is proposed in this system. When opening the account, users have to authenticated with their face. Each and every card holder has to store their face image.

The information is trained by MatLab. The trained image is stored in the database and also stored in their corresponding bank data base. While accessing the ATM, user have been check up their face by the camera. If it is matched with the predefined information then the OTP codes is generated from the ATM centre and send to the registered mobile number of the user through GSM. User can able to access their own account only if the received OTP code is given to ATM using keypad. This system also proposes, accessing of ATM without using the
ATM card

III Block Diagram



.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 2, April 2017

Fig.1 Block Diagram for Hardware Structure

All users face image has been trained in the Matlab. If the given face image will matched with the trained database information then that information is send from the PC to controller through RS232 cable.

After matched result user accessing the system with their account number. The input to the ATM system has been done by the keypad. All the information are shows on LCD.

If the finger print is matched with the account number then the message will generated to the registered user mobile number through GSM whose account is synchronized with mobile number in bank data base.

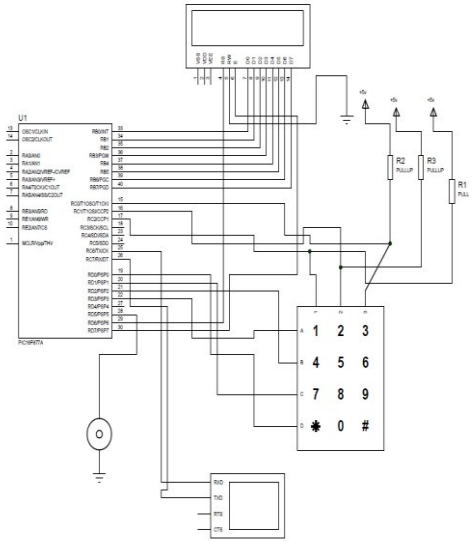


Fig.2 Circuit Diagram

IV SYSTEM SPECIFICATION

Peripheral Interface Controllers (PIC) is one of the advanced microcontrollers developed by microchip technologies. These microcontrollers are widely used in modern electronics applications. A PIC controller integrates all type of advanced interfacing ports and memory modules. These controllers are more advanced than normal microcontroller like INTEL 8051

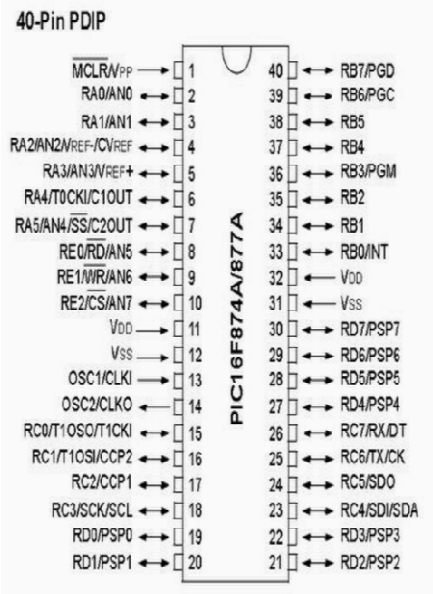


Fig.3 PIN Diagram

This example illustrates the use of the microcontroller's EUSART module. Connection to the PC is enabled through RS232 standard. The program works in the following way: Every byte received via the serial communication is displayed using LED diodes connected

to port B and is automatically returned to the transmitter thereafter

1. The desired baud rate should be set by using bits BRGH (TXSTA register) and BRG16 (BAUDCTL register) and registers SPBRGH and SPBRG.
2. The SYNC bit (TXSTA register) should be cleared and the SPEN bit should be set (RCSTA register) in order to enable serial port.

On 9-bit data transmission, the TX9 bit of the TXSTA register should be set. Power supply is a reference to a source of electrical power. A device or system that supplies electrical or other types of energy to an output load or group of loads is called a power supply unit or PSU. The term is most commonly applied to electrical energy supplies, less often to mechanical ones, and rarely to others. A liquid crystal display (LCD) is a flat panel display, electronic visual display, or video display that uses the light modulating properties of liquid crystals. Liquid crystals do not emit light directly. LCDs are available to display arbitrary images (as in a general-purpose computer display) or fixed images which can be displayed or hidden, such as preset words, digits, and 7segment displays as in a digital clock. They use the same basic technology, except that arbitrary images are

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 2, April 2017

made up of a large number of small pixels, while other displays have larger elements. An LCD is a small low cost display. GSM/GPRS Modem-RS232 is built with Dual Band GSM/GPRS engine- SIM900A, works on frequencies 900/ 1800 MHz. The Modem is coming with RS232 interface, which allows you connect PC as well as microcontroller with RS232 Chip(MAX232). The baud rate is configurable from 9600-115200 through AT command. The GSM/GPRS Modem is having internal TCP/IP stack to enable you to connect with internet via GPRS. It is suitable for SMS, Voice as well as DATA transfer application in M2M interface. A keypad is a set of buttons arranged in a block or "pad" which bear digits, symbols or alphabetical letters. Pads mostly containing numbers are called a numeric keypad. Numeric keypads are found on alphanumeric keyboards and on other devices which require mainly numeric input such as calculators, push-button telephones, vending machines, ATMs, Point of Sale devices, combination. Geared DC motors can be defined as an extension of DC motor which already had its Insight details demystified here. A geared DC Motor has a gear assembly attached to the motor. The speed of motor is counted in terms of rotations of the shaft per minute and is termed as RPM .The gear assembly helps in increasing the torque and reducing the speed. Using the correct combination of gears in a gear motor, its speed can be reduced to any desirable figure. This concept where gears reduce the speed of the vehicle but increase its torque is known as gear reduction.

V.SOFTWARE REQUIRED

A.MATLAB 2014

MATLAB (matrix laboratory) is a fourth-generation highlevel programming language and interactive environment for numerical computation, visualization and programming. MATLAB is developed by Math Works .It allows matrix manipulations; plotting of functions and data; implementation of algorithms; creation of user interfaces; interfacing with programs written in other languages, including C, C++, Java, and Fortran ;analyze data; develop algorithms; and create models and applications

. B. Simulation and Model-Based Design

Simulink is a block diagram environment for multi domain simulation and Model-Based Design. It supports system-level design, simulation, automatic code generation, and continuous test and verification of embedded systems. Simulink provides a graphical editor, customizable block libraries, and solvers for modeling and simulating dynamic systems. It is integrated with MATLAB®, enabling you to incorporate MATLAB algorithms into models and export simulation results to MATLAB for further analysis.

C. MPLAB IDE

A development system for embedded controllers is a system of programs running on a desktop PC to help write, edit, debug and program code – the intelligence of embedded systems applications – into a microcontroller. MPLAB IDE runs on a PC and contains all the components needed to design and deploy embedded systems applications. The typical tasks for developing an embedded controller application are:

- Create the high level design. From the features and performance desired, decide which PICmicro MCU or dsPIC DSC device is best suited to the application, then design the associated hardware circuitry
- Compile, assemble and link the software using the assembler and/or compiler and linker to convert your code into “ones and zeroes” – machine code for the PICmicro MCUs. This machine code will eventually become the firmware (the code programmed into the microcontroller).
- Test your code. Usually a complex program does not work the way imagined, and “bugs” need to be removed from the design to get proper results.
- “Burn” the code into a microcontroller and verify that it executes correctly in the finished application. Of course, each of these
- steps can be quite complex

D. PROTEUS

The microcontroller can understand a program written in assembly language, it must be compiled into a language of zeros and ones. Assembly language and Assembler do not have the same meaning. The first one refers to the set of rules used for writing program for the microcontroller, while the later refers to a program on a personal computer used to translate assembly language statements into the language of zeros and ones. A compiled program is also called Machine Code. . Looking around, we find ourselves to be surrounded by various types of embedded system. Be it a digital camera or a mobile phone or a washing machine, all of them has some kind of processor functioning inside it. Associated with each processor is the embedded software.

- It is small and reasonably simpler to learn, understand, program and debug.
- C Compilers are available for almost all embedded devices in use today, and there is a large pool of experienced C programmers.

VI.CONCLUSION

Using the two most stable physiological biometrics as a means of identification of an individual has made the system more reliable. Combining the software and hardware approach overcomes the drawbacks presented by the systems individually. Moreover building the

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 2, April 2017

whole system on the technology of the embedded system makes it non invasive, user friendly and secured. This paper gives a general idea of the proposed system with the implementation of both the hardware and software structures and the operation flow.

VII.FUTURE WORK

This proposed idea can be developed into many stages. Iris recognition can be used as replacement or in addition to the finger print recognition. This requires the attachment of the respective persons iris input with their bank account. Various such metrics can be used like skull identification, retina recognition, vein recognition etc.

REFERENCE

1. Balwir.S.P and Katol.K" Secured ATM transaction system using micro-controller", International Journal of Advanced Research in computer science and software engineering,Vol.4,Issue 4,April 2014.

2. Javier Galbally and Sebastien Marcel "Image Quality Assessment for Fake Biometric detection Application to Iris, Fingerprint and Face recognition",IEEE trans.on image processing ,vol. 23,No.2 February 2014.

3. Kriti Sharma and Hinanshu Mong, "Efficient Biometric Iris Recognition Using Hough Transform with Secret Key", International Journal of Advanced Research in Computer Science and Software Engineering. Vol.4,Issue 7, July 2014.

4. Mohsin Karovaliya and Saifali Karedia "Enhanced Security for ATM machine with OTP and facial recognition features",International Conferenceon Advance dComputing Technologies and Applications(ICATA-2015).

5. Shelkar Goud.D and Ishaq Md,P.J. "A Secured Approach for Authentication system using fingerprint and iris" ,Global journal of Advanced Engineering Technology,Vol,Issue3-2012.

