IMPLEMENTATION OF SECURITY ENHANCED AUTHENTICATION SYSTEM IN ATM

K.Abhinaya[1], K.R.Nivetha[2], A.R.Aravind[3]

[1]*B.E, ECE, Prince Shri Venkateshwara Padmavathy Engineering College, TN, India*
[2]*B.E, ECE, Prince Shri Venkateshwara Padmavathy Engineering College, TN, India*
[3]*B.E, M.Tech, ECE, Prince Shri Venkateshwara Padmavathy Engineering College, TN, India*

ABSTRACT

In today's technically advanced world, autonomous systems are gaining rapid popularity. As the social computerization and automation has been increased and the ATM and credit card has been installed and spread out to simplify the financial activity, the banking activity has been simplified. ATM's security is the field of study that aims at solutions that provide multiple points of protection against physical and electronic theft from ATMs and protecting their installations. However the crime related with financial organization has been increased in proportion to the spread of automation and devices. Those crimes for the financial organization have been increased gradually from year to year. In this system the sensor at the entry door of the ATM, will restrict the entry to a single person. The RFID card reader is used as an identity for a particular user. If there is more than one entry into the ATM room, it will be blocked. Then the system detects facial feature and decides whether the person is wearing a mask. After authenticating the users, the card details are accessed for the authentication procedure for electronic transaction .In case of any malpractice or robbery occurs inside the ATM the information is sent to the nearby police station and corresponding bank through the GSM. Hear LCD display board is used to show the output warnings and messages continuously. This will prevent the robbery and the person involved in robbery can be easily caught.

Keyword: - *Facial Feature, GSM, LCD Display, RFID card reader.*

1. INTRODUCTION

This paper is used to mainly describe the enhanced security system in ATM. Security in ATM networks is necessary because ATM is widespread and many areas such as financial or medical applications, network administration, etc. require very sensitive handling of the data. Misuse of the ATM network, manipulation of transmitted data and spoofing would be a great threat to one's financial activities. An automated teller machine is an electronic banking outlet, which allows customers to complete basic transactions without the aid of a branch representative or teller. Using an ATM, customers can access their bank deposit or credit accounts in order to make a variety of transactions such as cash withdrawals, check balances, or credit mobile phones. Billions of people are making use of ATMs daily in day-today life.

In the previous system, ATM related crimes such as robberies, breaking into ATMs, ATM password hacking, etc. were going on and there must be the invention of technology to minimize the effects of it. Card cloning was also a major problem in which the criminals create a duplicate copy of credit/debit card containing relevant details of card holder. PIN numbers can be hacked and scanned easily by using ATM scanning devices and by video cameras. Also, man source was needed as a security and it also does not provide any entry level protection.

In the proposed system, it focuses on developing the secure ATM system**.** Here, advanced level protection is made both inside the ATM and also at the entrance level. This mechanism is proposed to reduce anonymity and increase authenticity, confidentiality as well as user's trust towards ATM electronic transaction security. In this process, entry level sensor is used to monitor the count of the person. It uses the local binary pattern algorithm to determine the facial feature of the person and also RFID is used for unique identity purpose.

Our implementation of this project is analyzed by the following steps. At the entrance level, sensors are used to monitor the count. In our project, it is such that only single person is allowed to enter into the ATM.With the help of MATLAB Technology, signal processing of the person's features are determined. If the person wears a helmet or mask, voice board warning is given to insist users to remove them. Also RFID card is shown and the PIN is entered. Then, it asks for the user to enter the cash amount and cash delivery is done. For incorrect pin or any malpractice gets occurred within ATM, GSM Technology is used for alert purpose, LCD Display is used to show the output warnings.

This paper significantly improves the security than the previous work. Specifically in the case (i) provide more security (ii) minimizes the ATM theft in greater extent (iii) to prevent any unauthorized access (iv)restrict entry to a single person.(v) Voice Board is used to insist users to remove helmet before entry(vi) GSM Technology is used for alert purpose.

The paper is organized as follows. Section II reviews the concept and work that needs to be understood before moving in-depth of the project. Section III introduces our approach, together with the considered application scenarios. It describes how the entire internal process works. The results of our experimental evaluation are presented in Sec. IV, and conclusions are drawn in Sec. V.

2. RELATED WORK

In this section we review the various concepts and approaches that are dealt in this system to get the clear perspective. As far as we know, no previous work is used to determine some of the advances entry level protection that is used here.

2.1 IMAGE PROCESSING ALGORITHM

Local Binary Pattern Algorithm is used for image processing because it is proven to be highly discriminative and quite robust and it does not get affected by lightening condition, image rotation and aging of persons. Here, some of the steps are followed in recognizing the face. A threshold value is computed based on the value of the centre pixel and binary code is determined. The face is captured and then the face is divided into various blocks based on the requirements.LBP applied image is determined. Feature extraction is done and histogram is calculated .It is used to compute the processing of histogram and if the essential features are matched, then the face image is represented .It consists of three steps:

- **Face representation:** The input face is considered and in this step it is mainly used to determine whether the considered image determines the facial features or not.
- **Feature extraction:** Here, the most useful and unique features of the face image are extracted and the analysis is done.
- **Classification:** Here, the extracted features are compared with the database and the output of this is the identity of the face image with the highest matching score, thus considering the small differences compared to the input image.

Here, the facial image is divided into local regions and texture descriptors are extracted from each region independently. The descriptors are then concatenated to form a global description of the face. Also, uniform pattern is considered because it contains the amount of pixels namely 99% of the original image.

2.2 RFID TECHNOLOGY

RFID enables identification from a distance, and unlike earlier bar-code technology, it does so without requiring a line of sight. Furthermore, RFID systems can discern many different tags located in the same general area without human assistance. The RFID devices are classified into two classes: active and passive. Active type requires a battery and coil and it is long ranged. Passive RFID do not require battery and it contains the coil and the range is limited. It uses frequency in the range of 13.56 MHz to 916 MHz. The antenna emits radio signals to activate the tag

and to read and write data to it. The reader emits radio waves in ranges of anywhere from one inch to 100 feet or more, depending upon its power output and the radio frequency used. When an RFID tag passes through the electromagnetic zone, it detects the reader's activation signal. The reader decodes the data encoded in the tag's integrated circuit in the form of silicon chip and the data is passed to the host computer for processing.

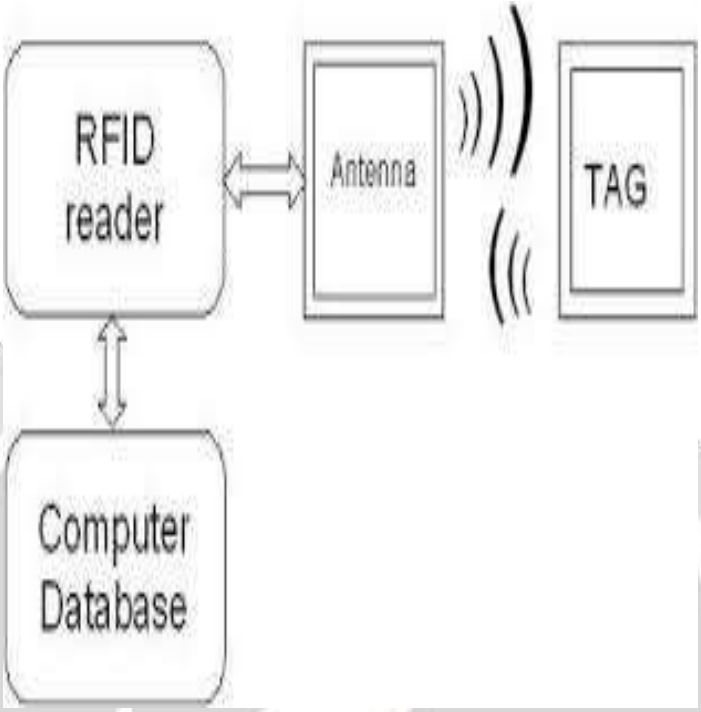

Fig -1: RFID Working

3. PROPOSED SYSTEM

3.1 Infrared Sensor

The IR Sensor is mainly used to monitor the count of the person. Here, reflectance type infrared sensor is used which consist of the IR transmitter and receiver module. This sensor emits its own short wavelength infrared beam. The rays emitted by IR transmitter strike the object body and only after the reflection of rays from the surface to the IR receiver, the count is calculated. It detects the infrared that is reflected back to it from any human or non-human object within its automatically programmable detection zone.

3.2 Keypad

A keypad is a set of buttons arranged in a block or 'pad' which usually bear digits, symbols and usually a complete set of alphabetical letters. The keypad switches are connected in a matrix of rows and columns. Here, we are using 4*4 Keypad. The rows of the matrix are connected to four output port lines. The columns of the matrix are connected to four input port lines. The rows of the matrix are connected to four input lines. When no key is pressed, the column lines are high. When a key is pressed, it connects a row to a column. If we can determine the row and column of a key, then we can determine which key it is and so we can assign to it an ASCII code.

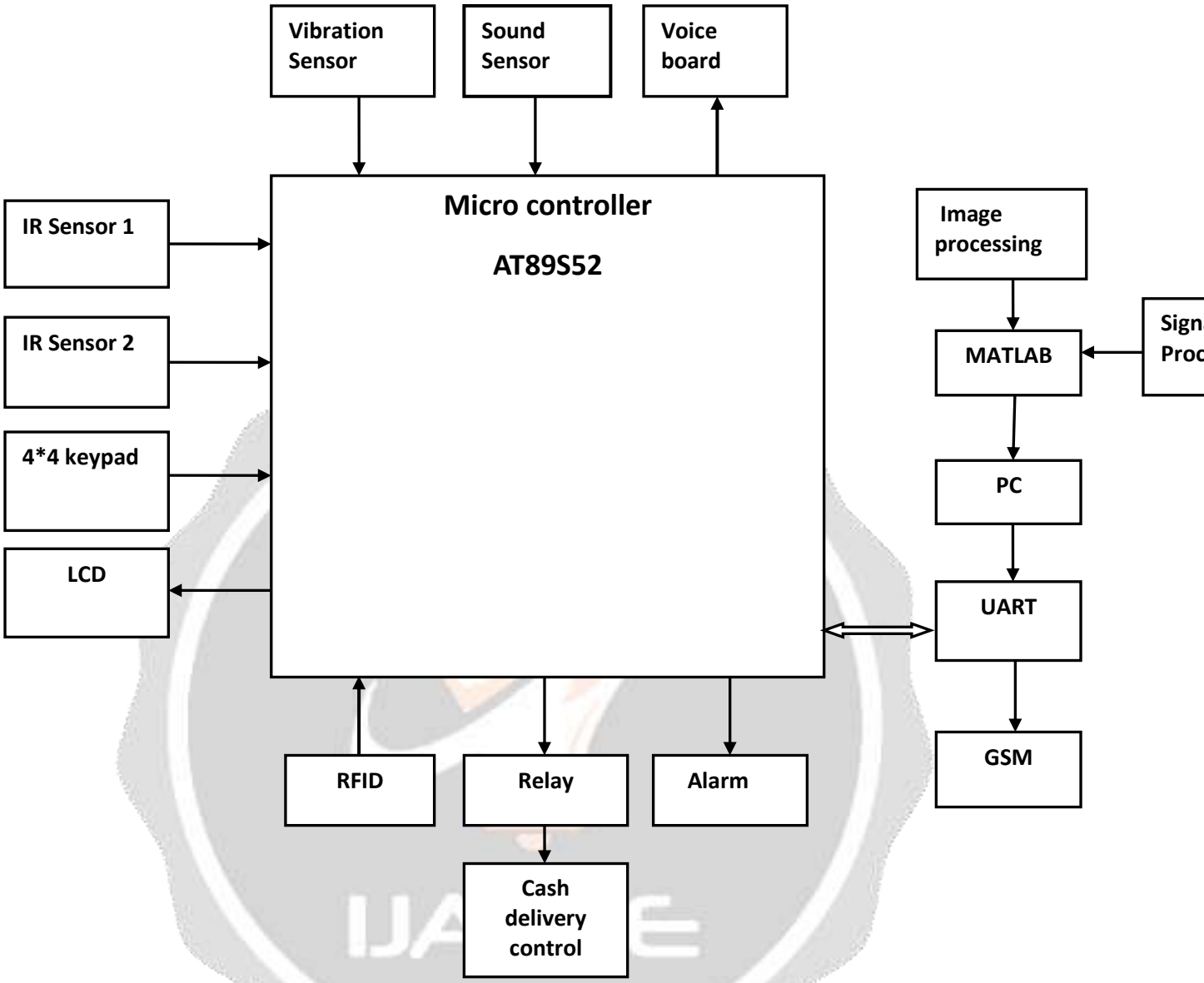

Fig -2: Block Diagram

3.3Voice Board

In our project, we use voice board to insist users to remove their helmet at the entry level. If the user denies removing the helmet or mask, he cannot access ATM and alarm is raised. The basic function is that the prerecorded voice will be stored in the database and after the face is processed, it takes not more than 60 seconds to display the output via a microphone. The module which we are going to use here is APR9600.

3.4 LCD Display

Here, 16*2 LCD display is used. It is such that it can display 16 characters per line and there are 2 such lines. The LCD has 2 registers: Command and Data. Command is a special set of data which is used to give the internal command to LCD like clear screen, setting up the cursor etc. The data is the ASCII value of the character to be displayed on the LCD.

3.5 UART

An UART, universal asynchronous receiver / transmitter is responsible for performing the main task in serial communications with computers. The device changes incoming parallel information to serial data which can be sent on a communication line. The UART performs all the tasks, timing, parity checking, etc. needed for the communication**.** It is mainly used for interfacing with the AT89S52 microcontroller.

3.6 GSM Technology

Here, it is used to inform the nearby police station, bank personnel in case of any emergency. Here the module is SIM900A is used. This is mainly activated in the cases where there occurs the incorrect PIN entered by the user or if either the vibration sensor or sound sensor is activated or if the door gets automatically locked. It is mainly used for alert purpose.

3.7 Sound Sensor

Whenever systems detect the shock or the sound that is above the normal threshold, this is activated. The module of sound sensor used here is the normal microphone and the threshold is hence determined. This is mainly used if there occurs any threat to the person who comes to withdraw money or if he is getting beaten.

3.8 Vibration Sensor

Vibration sensor will sense the vibration happen in ATM and it will be placed where money is been kept and if someone attempts to break it or if someone tries to steal the money, this is activated. Here, we are using piezoelectric module sensor and the threshold is fixed as 65 V db. Signals from this sensor are sent to the microcontroller, then only it will send the signal to android device to send the sms alert to the nearby police station and bank authorities.

3.9 Cash Delivery Control

It is mainly used in the case where the user is authenticated and if the PIN entered is correct then after the successful transaction, the motor is run and cash delivery is made.

3.10 Relay

It is nothing but an electronic switch. The voltage required to operate is +12V.It is used for automatic door open and lock at the entry level. If the user enters the incorrect pin for more than three times, the door gets automatically locked and the information is sent to control room.

4. EXPERIMENTAL EVALUATION

The evaluation is made from both the software and the hardware in our project. Face recognition at the entry is carried out using MATLAB and the output is indicated in the dialog box in the figure as ‘Authenticated’ or ‘Not Authenticated’ which will be issued as a warning by the voice board in real time. Considering the hardware, the count is determined and then the person shows the RFID card and the processing is done and it asks the user to enter the PIN. If it is correct the amount is entered and there occurs the successful transaction.

5. CONCLUSION

In this paper, a simple approach for recognition of the facial features is determined with the help of local binary pattern algorithm and also some parameters are analyzed using hardware part of the system. The system also contains additional verifying methods which are entering owner's password associated with RFID sent by the controller and can block the account’s transaction in case of wrong password and also GSM is used to send SMS alert to the concerned person or to nearby bank. Thus the proposed system is considered to be an efficient method of providing the necessary security which is essential for today’s scenario in ATM.

6. REFERENCES

[1].Ajaykumar M. and Bharath Kumar N. (2013) 'Anti-Theft Machine Using Vibration Detection Sensor' in International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE),Volume 3 Issue 12, pp. 416-418.
[2].Anitha Julian and Raj M. (2015) 'Design and Implementation of Antitheft ATM Machine using Embedded Systems' in International Conference on Circuit and Power Computing Technologies (ICCPCT), pp. 01-05.
[3]. Aru, Ihekweaba Gozie and Okereke Eze (2013) 'Facial Verification Technology for Use in ATM Transaction' in American Journal Of Engineering Research (AJER), Volume 3, Issue 5, pp. 188-193.
[4]. Dhirendra Pandey and Shweta Sankhwar (2016) 'A Safeguard against ATM Fraud' in Institute of Electrical and Electronic Engineers (IEEE),Sixth International Conference on Advanced Computing, pp. 701-705.