IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

Personal Authentication System for Illegal Usage of Arms

Chhaya C Athavale[1], Sivaraj K R[2], Pratik Jain[3], Bhagyashri Jogdand[4], Ankit Sharma[5]

Assistant Professor, Department of Electronics and Telecommunication, Sinhgad Academy of Engg, Pune, India[1]

Student, Department of Electronics and Telecommunication, Sinhgad Academy of Engg, Pune, India [2, 3, 4, 5]

Abstract: Authentication system has become necessary to overcome the security threats faced by many armed personnel these days. Nowadays, there is increase in unethical usage of weapons by stealing it from armed personnel. A result of this is the use of these weapons for various crimes. It is not uncommon to see these weapons of law enforcement being used to break the law instead. The problem is that the pistols do not recognize their rightful owner and thus anybody who has the gun can use it freely. The need of the hour is of a system that checks the identity of the person who holds the gun before he can fire it. Hence there is only one alternative i.e. authentication system which includes RFID security and biometric technology. The system uses RFID technology and biometrics to identify the rightful owner of the gun. The RFID reader is installed on the weapon to detect the tags placed on the authorized person (installed on wrist watch, belt, etc.) then the system captures the fingerprint image and scans the database for a match. If both the object and captured image belong to a registered user, access is granted and the trigger can be pulled for a definite time period; otherwise the system remains locked and the user will not be able to pull the trigger. Thus this paper describes the design of authentication system for unethical usage of arms.

Keywords: RFID, Fingerprints, Arduino, Solenoid lock.

I. INTRODUCTION

As we know, misuse of personal weapon is common. A system can be designed using RFID and biometric technology to overcome such problem. Only authorized person will be allowed to use the weapon by installing this system on weapon. In such a way, unethical use of arms by unauthorized person will be stopped.

The system hardware consists of RFID tags, RFID readers, arduino, fingerprint module and solenoid lock. The RFID reader placed on the gun detects the certain special objects called RFID tags on the body of the user and then fingerprint module captures the fingerprint image and scans the database for match. Thus the authenticity is verified. Thus the system allows access only to the authorized person. This system authentication and identification process is carried out at two sub-levels namely the detections of RFID tags on the body and the scanning of fingerprints.

All these processes communicate with each other through database information. G. Ostojic [1] has developed an automatic vehicle parking control system based on RFID technology in the city of Novi Sad, Republic of Serbia. The hardware of the system consists of RFID tag and reader operating at a frequency of 13.56MHz for authentication purpose, inductive loop for metal detection purpose, a capacity sensor for counting vehicles, Siemens MC 39i GPRS modem for communication between entrance and exit gates and FEC FC440 programmable logic controller (PLC) which is the heart of the system. When the car stops on the inductive loop at the entrance, RFID tag is read by the reader. The data on the tag includes the unique identification number (UID), expiry date and check bit for checking the parking status. This data is manipulated by PLC and access is granted to the vehicle for parking if tagged information contains correct UID, expiry date and parking status. After the vehicle has entered the parking lot, its parking status will be changed by the RFID reader/writer to prevent the entry of another vehicle on the same card. The same procedure is repeated while exiting the parking lot.

This paper discusses the design of an authentication system using RFID technology and biometrics technology. The system is comprised of three modules namely detection of unique objects from user, scanning of fingerprints and triggering the solenoid lock. These modules communicate to the each other through arduino. After the information from these modules is processed by the arduino, the control commands are issued to the modules for granting or denying access to the user.

II. OVERVIEW OF RFID TECHNOLOGY

RFID system consists of three components namely tag, reader and arduino containing the database [2]. Below shown is the figure 1of a RFID system. The tag data is read by the reader and transmitted to the arduino for authentication. The information is processed and after verification, access is granted. Further RFID tags are

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

classified into active and passive tag, which are determined by their source of energy. In case of active tag battery is needed for powering the circuit and transmission of tag information. But, these tags are very expensive and are rarely used. On the other hand, source of energy for passive tag is the reader itself. Hence passive tags are cost-effective so they are widely used. In this design, passive RFID tags are used. A passive RFID tag transmits electronically stored information to the reader when it comes in the proximity of electromagnetic field generated by the reader. This phenomenon is based on Faraday's law of electromagnetic induction.

The current flowing through the coil of reader produces a magnetic field which links to the tag coil hence producing a current in the tag coil. The tag coil then varies this current by changing the load on its antenna. This variation is actually the modulated signal which is received by the reader coil through mutual induction between the coils.

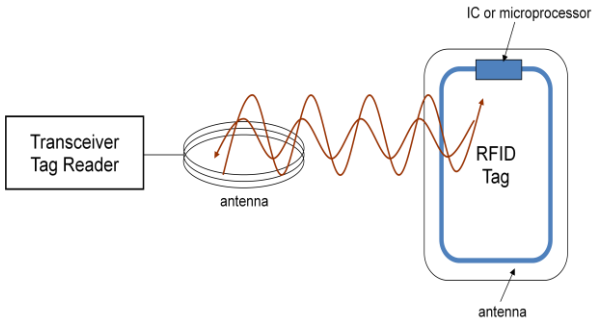

Fig.1 Working principle of RFID System

III. OVERVIEW OF BIOMETRICS

Accurate personal identification is becoming more and more important. There are different types of Biometrics available they are: Physiological, Face, Fingerprint, Hand geometry, Retina, Iris recognition, Behavioural, Signature, Voice Biometrics. Fingerprint recognition [3] is the most widely used technique for personal identification. This design is developed to provide security to authorized persons. Biometrics authentication requires comparing enlisted biometric samples with the newly apprehend biometric sample i.e. captured during a login. This is a three-step process includes Capture, Process and Enroll that is followed by an identification process which is explained in fig.2.During Capture process, raw biometric data is captured by the fingerprint sensor After performing the first step we now go to next step here we capture all the important points of the pattern like pattern area, core point, delta, ridges count, ridges pattern. Next step does the process of enrollment. So now during the authentication process, the unique biometric pattern is stored in the memory of Arduino which will be useful in future for analysing the biometric pattern.
As the biometrics play an important role in the authentication process some of the global features stated below which should satisfy the Global Standards [4]:-

- Pattern Area
- Core Point
- Delta.
- Line types
- Ridge Count
- Ridge Pattern.

As we have seen that the fingerprint biometrics consists of different types of stages like fingerprint scanning, fingerprint matching, fingerprint, identification now we move on some depth of biometrics. The biometrics image capturing are of different types they are Optical Capturing, Thermal capturing, Capacitance Capturing, Ultra Sound Capturing [5].

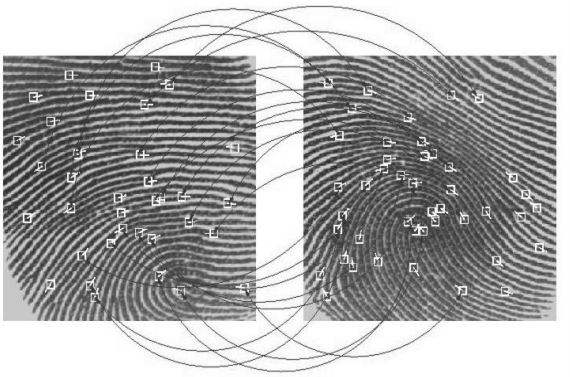

Fig.2 Comparison of Miniature Points

The Biometrics verification and identification takes place by the process of Minutia Matching Process which is nothing but comparing all the points of the pattern like ridges point, ridges pattern etc.

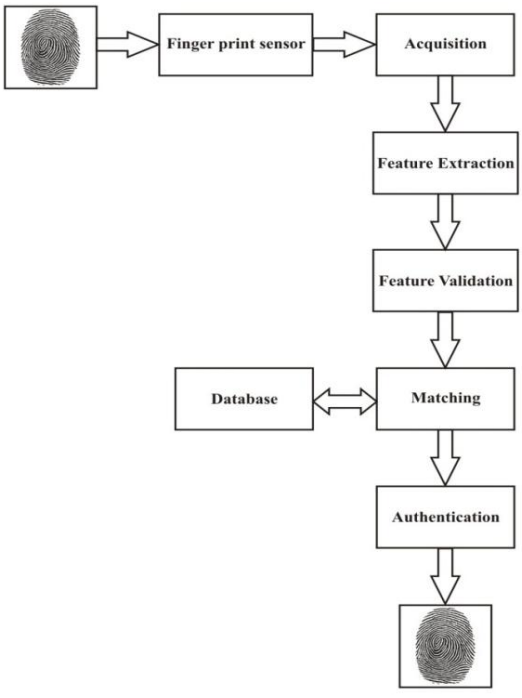

Fig.3 Biometric System

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

IV. SYSTEM COMPONIENTS

A. RFID Module (MFRC522)[6]
The MFRC522 is a highly integrated reader/writer IC for contactless communication at 13.56 MHz. Some of the RFID module features are: Handling capacity of FIFO buffer is 64 bytes for sending and receiving purpose, Interrupt modes are flexible, power-down done with the help of software, Timer is programmable, It needs 2.5 V to 3.3 V for power supply, programmable I/O pins.

B. Arduino
Arduino is an open-source platform used for building electronics projects. Arduino consists of both a physical programmable circuit board and a piece of software, or IDE (Integrated Development Environment) that runs on computer, used to write and upload computer code to the physical board. It consists of Microcontroller ATmega328 and has features like operating voltage 5V, input voltage 7-9 V, digital I/O Pins 14 (of which 6 provide PWM output), analog Input Pins 8 (of which 4 are broken out onto pins), DC Current per I/O Pin 40 mA, flash memory 32 KB (2 KB used by bootloader), SRAM 2 KB, EEPROM 1KB, Clock Speed 16 MHz.

C. Biometric Sensor
The user can store the finger print data in the module and can configure it in 1:1 or 1: N mode for identifying the person. The FP module can directly interface with 3v3 or 5v Microcontroller. A level converter (like MAX232) is required for interfacing with PC serial port. It has features like Character file size: 256 bytes Template size: 512 byte Storage capacity: 250, Resolution 500 DPI, Voltage: 3.6-6.0 VDC Working current: Typical 90 mA, Peak 150mA.

D. Solenoid Lock
A solenoid lock is a type of electronic-mechanical locking mechanism. Solenoids are basically electromagnets: they are made of a big coil of copper wire with an armature in the middle.

When the coil is energized, the armature is pulled into the center of the coil. This makes the solenoid able to pull from one end. It draws 650mA at 12V, 500 mA at 9V when activated [7].

V. SYSTEM OPERATION

This design is a 3 Tier Authentication System. It mainly starts with the RFID Authentication Tier 1 using the first tag i.e. some unique object placed on the person's body to authenticate.
Similarly RFID Authentication Tier 2 using the Tag 2. If both the levels are authenticated then only it will be passed on to the next level where it will check the Biometric Authentication. In Biometric authentication it will consist of Stored Biometric Print where it will be used for matching thereby helping the controller for decision. Once all the Authentication Tier is confirmed the controller will drive the solenoid which is placed behind the trigger. A solenoid is simply a specially designed electromagnet. The solenoid consists of a coil and a movable iron core called the armature. When current flows through a wire, a magnetic field is set up around the wire. More the number of turns stronger will be the magnetic field, flowing around the coil and through its center. When the coil of the solenoid is energized with current, the core moves to increase the flux linkage by closing the air gap between the cores.

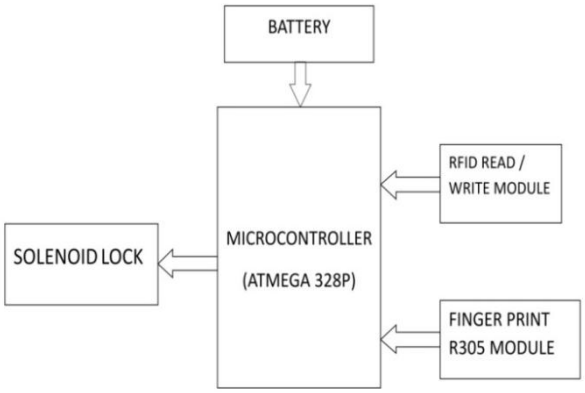

Fig.4 System Block Diagram

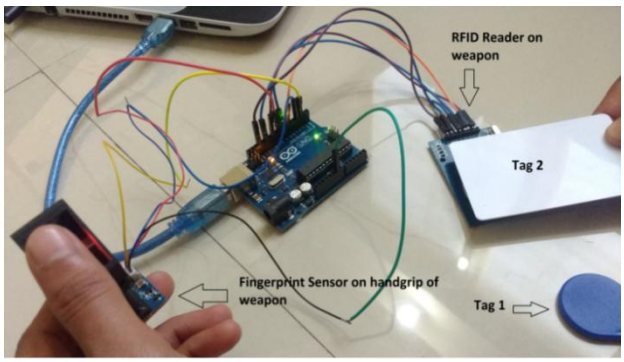

Fig.5 Prototype to be installed on weapon

The movable core is usually spring-loaded to allow the core to retract when the current is switched off. The duration after which the current will be switched off will be set by the controller with the help of timer. The force generated is approximately proportional to the square of the current and inversely proportional to the square of the length of the air gap.Thus trigger gets unlocked for finite time period after which it gets locked automatically. So the person has to do the authentication process once again, by this way anyone stealing the weapon after authentication can use the weapon for only a finite time period.

VI. SIMULATION RESULTS

Proteus software is a very important platform for simulating an electronic design before the hardware stage. So to interface hardware components with Proteus design like RFID Module and Finger Print Module. So to

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

interface the modules we use virtual serial port emulation (VSPE) software. VSPE is helpful for the designers to create applications that use serial ports. It can create various virtual devices which may be used for transmitting data or receiving.

a. Arduino interfaced with COMPIM connector, this is used to connect virtual serial port to proteus simulator.

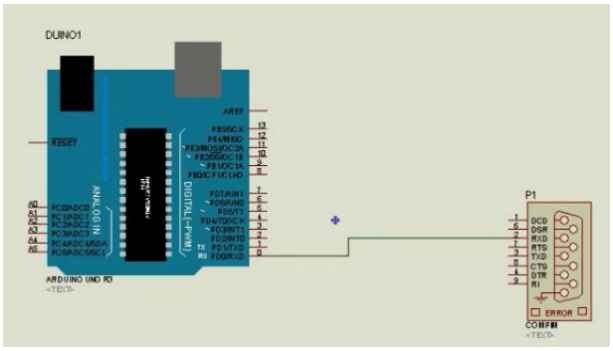

Fig.6 COMPIM Connector interfaced with Arduino connector

b. Input and Output are viewed at Virtual terminal.

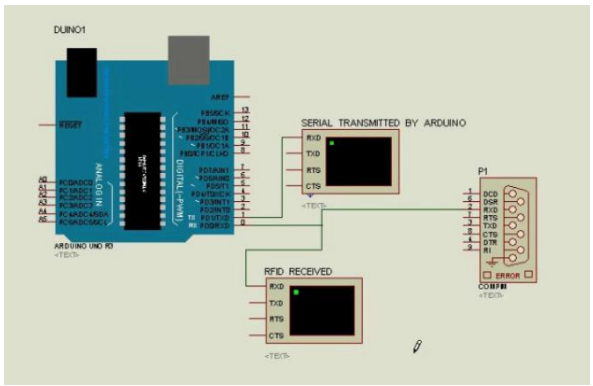

Fig.7 Virtual Terminal added to the circuit for observation purpose

c. Card information received successfully when the card is swiped near the reader.

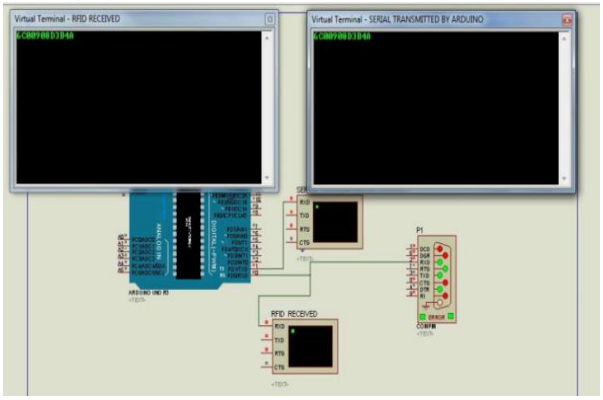

Fig.8 RFID card swiped near the reader.

VII. CONCLUSION

In this paper, the design of a personal authentication system for illegal usage of arms is presented. The system uses radio frequency identification with biometrics technology to differentiate between legitimate and illegitimate users. The system accomplishes the security and access control task by processing information from sub-controllers. These controllers include RFID reader and tags, biometric sensors and Arduino. The response time can be improved by using dedicated processors instead of the single processor.

REFERENCES

[1] G. Ostojic, S. Stankovski, and M. Lazarevic, “Implementation of RFID technology in parking lot access control system,” in Proc. Annual RFID Eurasia Conference, 2007.
[2] U. Farooq, Mahmood ul Hasan, M. Amar, A. Hanif, and Muhammad Usman Asad, “RFID Based Security and Access Control System”.
[3] Woodward, J. D., Orlans, N. M., & Higgins, P. T. (2003). Biometrics. McGraw-Hill.
[4] D. Addy, P. Bala “Physical Access Control Based On Biometrics and GSM” International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 5, May 2016.
[5] M. Reinhardt “Guide to Fingerprint Identification and Classification”, July, 2016.
[6] S. Lahiri, RFID sourcebook, Westford, Massachusetts, 2006.
[7] Histand, Alciatore, "Introduction to Mechatronics and Measurement Systems," McGraw-Hill, 1999.