ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 9, March 2018

Android Mobile Phone Finger Print Sensor Recognition Based Car Lock System by Using Wifi Technology

Mrs.N.Hemalatha[1]
Assistant Professor Dept of ECE
Idhaya Engineering College for women
hemasubha26@gmail.com

Ms.P.Princy Pushpa[2]
Assistant Professor dept of ECE
Idhaya Engineering College for women
Princeprincy4792@gmail.com

Abstract: **The use of vehicle is a must for everyone. In the same way, safeguarding the vehicle against theft is also very essential. Impediment of vehicle theft can be done remotely by an authorized person. Wireless with Embedded computing technology is an emergent field used in all the areas. This automotive security system is designed using embedded system. In addition to this system various technologies are used namely Wi-Fi and android mobile Fingerprint Recognition. The survey mainly emphasizes on major approaches for automatic person identification, namely fingerprint recognition and various existing vehicle security system. The security system can be implemented using Microcontroller. Making use of advanced technologies like biometric systems protected digital locks is the demand of the time. Using biometric systems for security lays more emphasis not on what all you know about the security of the place but who you are with respect to the place. In juxtaposition with the normal lock and key system, the advantages of Biometric security systems are umpteen, but the biometric security system alone cannot provide us with a pragmatic security system. In this project, elaborate the idea of using a Biometric Protected System for the security of a place, viz. car.**

Keyword- authentication scheme, smart card, biometric, elliptical curve cryptosystem

I INTRODUCTION

Wireless, is the transfer of information or power between two or more points that are not connected by an electrical conductor. The most common wireless technologies use radio waves. It encompasses various types of fixed, mobile, and portable applications, including two-way radios, cellular telephones, personal digital assistants (PDAs), and wireless networking [1].

A. Embedded System

Embedded System is a small computer system that is generally hidden inside equipment [machine, electrical appliances, or electronic gadget] to increase the intelligence of the equipment for better or more efficient functionality. This kind of system always involves both the software and the hardware co-development. Embedded Systems are often easier understood in terms of Smart devices, intelligent or automated equipment. Hence Embedded System can be defined as follows:

- It is embedding or inserting human intelligence by means of software into a Microcontroller chip and designing hardware for the purpose.
- It is a combination of software and hardware with automatic working without user interface.
- It performs specific functions in host systems like satellites, remote controllers, televisions, robotics, ATMs, pagers, laser printers, missile launch systems, etc.

B. Applications Of Embedded System

It includes aerospace/defines systems, telecommunication equipment and switches, mobile computing, broadcast, auto motives, industrial process control and monitoring, medical electronics, consumer electronics, etc.

Main hardware components of an embedded system are microprocessor or micro controller, and supporting ICs. The combination of micro-controller and ICs are application specific. Commonly used microprocessors are, Motorola 680XX series, IBM PowerPC series processors, MIPS processors, Intel 386 and compatible CPUs, ARM processors, Sun SPARC series, etc.

Embedded systems need memory for storing programs and data, and usually programs are stored in ROM or EPROM. Often these systems have a serial port network interface, I/O interface for interacting with sensors and actuators in the case of process controlling systems [2] [3].

II BASIC CONCEPTS OF AUTOMATIC SECURITY SYSTEM

The block diagram of electronic lock using android mobile fingerprint [1] recognition system is a process of verifying the fingerprint image to open the electronic locking car is shown in fig 1.

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 9, March 2018

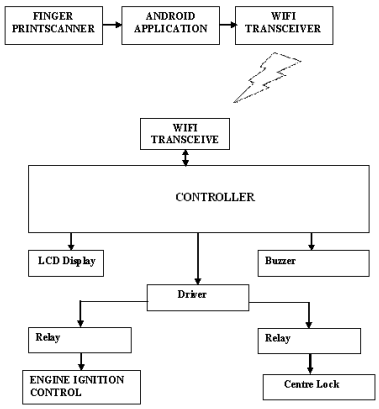

Fig. 1 Block diagram

A. *Buzzer*

A buzzer given in fig 2 is a device, typically used in automobiles, household things such as a washing machine, or refrigerator used for signal indication. It consists of a number of sensors and switches which connected to a control unit that determines if and which button was pushed or a present time has lapsed, and usually illuminates a light on the appropriate button or control panel, and sounds a warning in the form of a continuous or intermittent buzzing or beeping sound. Initially this device was based on an electromechanical system which was identical to an electric bell without the metal gong (which makes the ringing noise) [4] [5] [6].

Another implementation with some AC-connected devices was to implement a circuit to make the AC current into a noise loud enough to drive a loudspeaker and hook this circuit up to a cheap 8-ohm speaker. Nowadays, it is more popular to use a ceramic-based piezoelectric sounder like a Son alert which makes a high-pitched tone. Usually these were hooked up to "driver" circuits which varied the pitch of the sound or pulse the sound on and off.

Fig. 2 buzzer

B. *Circuit description*

The circuit is designed to control the buzzer. The buzzer ON and OFF is controlled by the pair of switching transistors (BC 547). The states of transistors are given in table I. The buzzer is connected in the Q2 transistor collector terminal. When high pulse signal is given to base of the Q1 transistors, the transistor is conducting and close the collector and emitter terminal so zero signals is given to base of the Q2 transistor. Hence Q2 transistor and buzzer is turned OFF state. When low pulse is given to base of transistor Q1 transistor, the transistor is turned OFF. Now 12v is given to base of Q2 transistor so the transistor is conducting and buzzer is energized and produces the sound signal [7].

TABLE I TRANSISTOR STATES

Voltage from MC or PC	Transistor Q1	Transistor Q2	Transistor Q3
1	ON	OFF	OFF
0	OFF	ON	ON

C. *RELAY*

A relay is a switch that opens and closes under control of another electrical circuit. In the original form, the switch is operated by an electromagnet to open or close one or many sets of contacts. It was invented by Joseph Henry in 1835. Because a relay can control an output circuit of higher power than the input circuit, it can be considered, in a broad sense, to be a form of electrical amplifier [10] [11].

1) *Operation*

When a current flow through the coil, the resulting magnetic field attracts an armature that is mechanically linked to a moving contact. The movement either makes or breaks a connection with a fixed contact. When the current to the coil is switched off, the armature is returned by a force approximately half as on as the magnetic force to its relaxed position. Usually this is a spring, but gravity is also used commonly individual motor starters. Most relays are manufactured to operate quickly. In a low voltage application, this is to reduce noise. In a high voltage or high current application, this is to reduce arcing.

If the coil is energized with DC, a diode is frequently installed across the coil, to dissipate the energy from the collapsing magnetic field at deactivation, which would otherwise generate a spike of voltage and might cause damage to circuit components. If the coil is designed to be energized with AC, a small copper ring can be crimped to the end of the solenoid. This "shading ring" creates a small out-of-phase current, which increases the minimum pull on the armature during the AC cycle.

2) *Pole & Throw*

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 9, March 2018

SPST - Single Pole Single Throw.These have two terminals which can be switched on/off. In total, four terminals when the coil is also included. These have one row of three terminals. One terminal (common) switches between the other two poles. It is the same as a single change-over switch. In total, five terminals when the coil is also included.

DPST - Double Pole Single Throw.

These have two pairs of terminals. Equivalent to two SPST switches or relays actuated by a single coil. In total, six terminals when the coil is also included. This configuration may also be referred to as DPNO.

DPDT -Double Pole Double Throw.

These have two rows of change-over terminals. Equivalent to two SPDT switches or relays actuated by a single coil. In total, eight terminals when the coil is also included.

QPDT - Quadruple Pole Double Throw.

Often referred to as Quad Pole Double Throw, or 4PDT. These have four rows of change-over terminals. Equivalent to four SPDT switches or relays actuated by a single coil or two DPDT relays. In total, fourteen terminals when the coil is also included.

Normally Open (NO), Normally Closed

The contacts can be either Normally Open (NO), Normally Closed (NC), or change-over (CO) contacts. Normally-open contacts connect the circuit when the relay is activated; the circuit is disconnected when the relay is inactive. It is also called Form A contact or "make" contact. Form A contact is ideal for applications that require to switch a high-current power source from a remote device. Normally-closed contacts disconnect the circuit when the relay is activated; the circuit is connected when the relay is inactive. It is also called Form B contact or "break" contact. Form B contact is ideal for applications that require the circuit to remain closed until the relay is activated. Change-over contacts control two circuits: one normally-open contact and one normally-closed contact with a common terminal. It is also called Form C contact or "transfer" contact.

3) Relay application considerations

Selection of an appropriate relay for a particular application requires evaluation of many different factors: Number and type of contacts - normally open, normally closed, changeover (double-throw) In the case of changeover, there are two types. This style of relay can be manufactured two different ways. "Make before Break" and "Break before Make". The old style telephone switch required Make-before-break so that the connection didn't get dropped while dialing the number. The railroad still uses them to control railroad crossings.

Rating of contacts - small relays switch a few amperes, large contactors are rated for up to 3000 amperes, alternating or direct current Voltage rating of contacts - typical control relays rated 300 VAC or 600 VAC, automotive types to 50 VDC, special high-voltage relays to about 15,000 V Coil voltage - machine-tool relays usually 24 VAC or 120 VAC, relays for switchgear may have 125 V or 250 VDC coils, "sensitive" relays operate on a few mill amperes Package/enclosure - open, touch-safe, double-voltage for isolation between circuits, explosion proof, outdoor, oil-splash resistant Mounting - sockets, plug board, rail mount, panel mount, through-panel mount, enclosure for mounting on walls or equipment Switching time - where high speed is required "Dry" contacts - when switching very low level signals, special contact materials may be needed such as gold-plated contacts Contact protection - suppress arcing in very inductive circuits Coil protection - suppress the surge voltage produced when switching the coil current Isolation between coil circuit and contacts Aerospace or radiation-resistant testing, special quality assurance Accessories such as timers, auxiliary contacts, pilot lamps, test buttons Regulatory approvals Stray magnetic linkage between coils of adjacent relays on a printed circuit board.

III SOFTWARE SPECIFICATIONS

CCS developed the first C Compiler for Microchip microcontrollers to provide software solutions to developers of embedded applications using PIC® MCU and PIC24/dsPIC® DSC devices. CCS compilers are easy to use and quick to learn. For the less experienced programmer, a detailed textbook explaining the C language and how it may be applied to PIC® microcontrollers.

Our compiler products include pro-level optimization, the largest library of built-in functions, powerful PIC® MCU specific pre-processor commands, and ready-to-run programs to quickly jump-start any project. Our massive customer base provides us access to understanding our customer's requirements while developing advanced features with frequent releases and rare bugs.

A. Key Compiler Features

- Easily migrate between all Microchip PIC® MCUs devices
- Minimize development time with: peripheral drivers and standard C constructs
- C++ style input/output streams with full data formatting to any device or for strings
- Convenient functions like #bit and #byte allow C variables to be placed at absolute addresses

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 9, March 2018

- The integral one-bit type (Short Int) permits the compiler to generate very efficient Bit-oriented code
- Easily define, set-up and manage interrupts.

B. String Optimization

- **7-bit ASCII String Compression** - Decrease system usage through improved string compression
- **Switch Statements** - Easily perform string comparisons which result in tighter and more maintainable source code and a smaller ROM footprint
- **Variable Length Constant Strings**
- printf - Reduce usage of multiple string output through use of this function

IV SIMULATION RESULTS

Flexible constant data structure handling allows the compiler to handle lookup tables that are virtually unlimited in size. This is of particular interest to developers using large lookup tables for trigonometric functions or storing FPGA configuration memory images in on-chip MCU memory. Constants (including strings and arrays) are saved in program memory. DSP performance can be enhanced by manually assigning variables to data spaces for faster access with pre-processor directives.

A. Transmiiter Access

The transmitter access shows the waiting to receive signal from android mobile as given in fig 3.

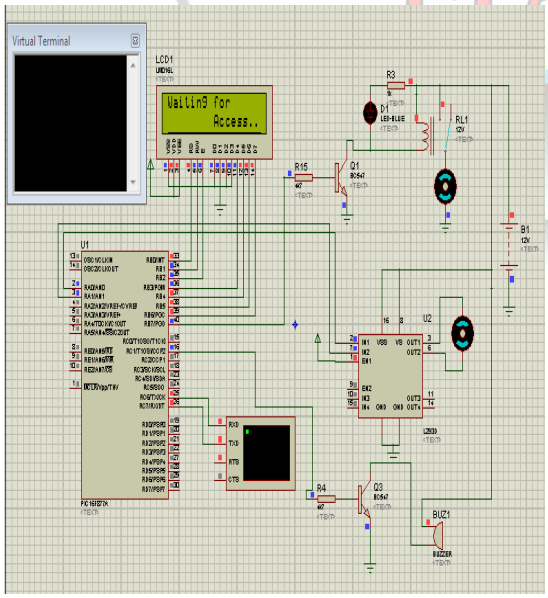

Fig. 3 Transmitter access

B. Door Unlock Only

Commend received to unlock Door only. Fig 4 shows the simulation Command "A" sends to Unlock the vehicle door only.

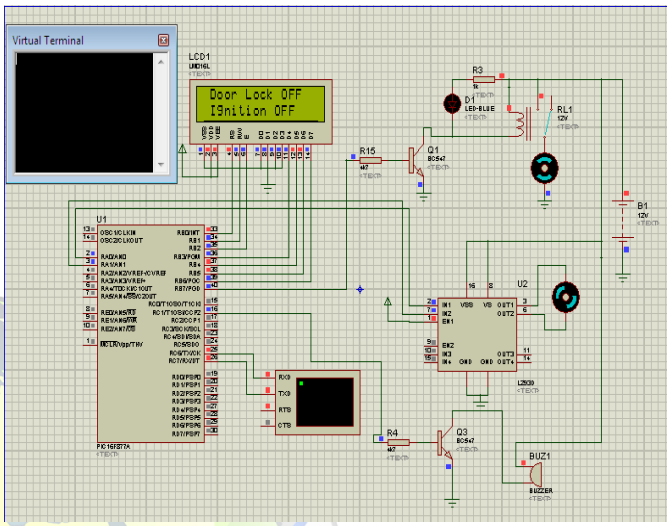

Fig 4 Door unlock

C. Door Lock Only

Commend received to Lock Door only. Fig 5 shows the simulation Command "a" sends to lock the vehicle door only.

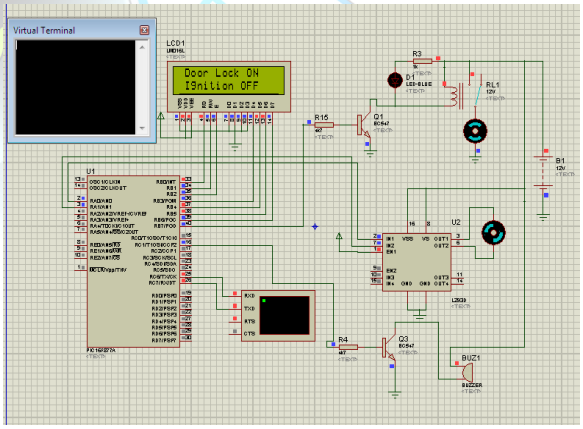

Fig 5 Door lock

D. Ignition On Only

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 9, March 2018

Commend received ignition power supply ON only. Fig 6 shows the simulation Command "B" sends to turn on the vehicle ignition power supply.

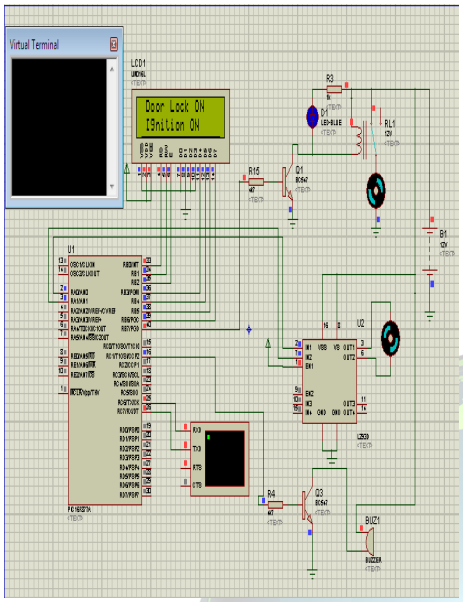

Fig. 6 Ignition on

E. *Ignition Off Only*

Commend received ignition power supply OFF only. Fig 7 shows the simulation Command "b" sends to turn OFF the vehicle ignition power supply.

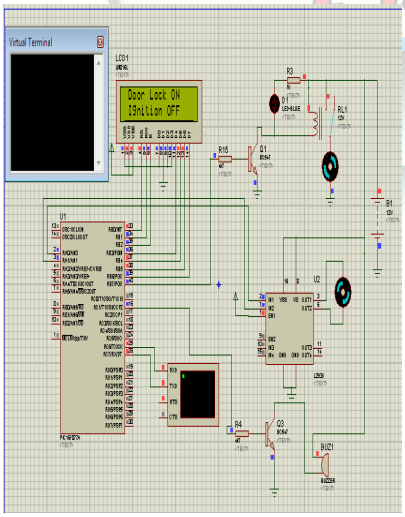

Fig 7 Ignition off

F. *Both Ignition And Door Unlock*

Commend received ignition power supply ON and unlock the Door. Fig 8 shows the simulation Command "D" sends to turn ON the vehicle ignition power supply and unlock the Door.

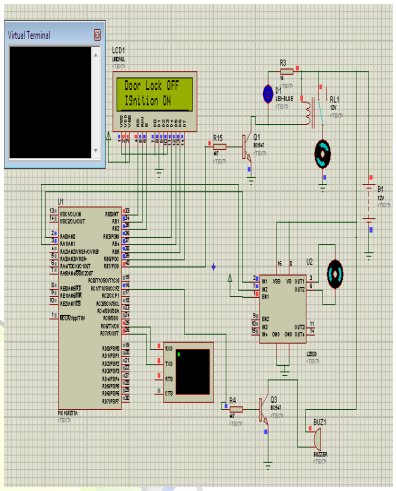

Fig. 8 Both ignition & door unlock

G. *Both Ignition And Door Lock*

Commend received ignition power supply OFF and lock the Door. Fig 9 shows the simulation Command "d" sends to turn OFF the vehicle ignition power supply and lock the Door.

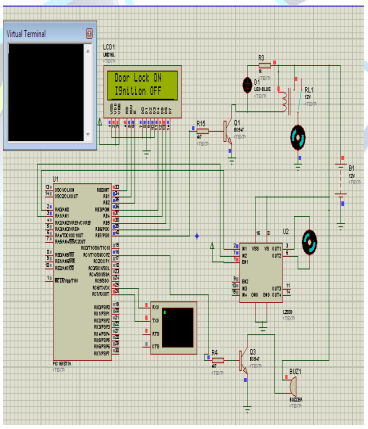

Fig 9 Both ignition & door lock

V CONCLUSION

Any user can unlock or ignite the vehicle; his/her fingerprint image matched against the fingerprints and face stored in this database while users with no match in the database are denied access to the system. Biometric method requires the physical presence of the person to be identified.

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 9, March 2018

Thus, biometric recognition systems offer greater security and convenience than traditional methods of personal recognition.

REFERENCES

[1] Anton S. (2002) "Sorting it out: Machine learning and finger-prints", Paper presented at the seminar on Telematik finger-print, Siemens Corporate Technology, Munich, Germany.

[2] Burnett A, Byrne F, Dowling T and Duffy A(2007) "A biometric identity based signature scheme," Int.J.Netw.security,vol.5,no.3pp.317-326.

[3] C.-T. Li and M.-S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," *J. Netw. Comput. Appl.*, vol. 33,no. 1, pp. 1–5, Jan. 2010.

[4] Das A.K(2011) " Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards," IET Inf.Seurity,vol.5,no.3,pp.145-151.

[5] He, Security flaws in a biometrics-based multi-server authentication with key agreement scheme, Tech. Rep. 2011/365, ePrint Archive. [Online].Available: http://eprint.iacr.org/2011/365.pdf

[6] Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. New York, NY, USA: Springer-Verlag, 2009.

[7] Yoon and K. Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem,"*J. Supercomput.*, vol. 63, no. 1, pp. 235–255, Jan. 2013.

[8] Li and M. K. Khan, "A biometric identity-based signcryption scheme, *"Future Gener. Comput. Syst.*, vol. 28, no. 1, pp. 306–310, Jan. 2012.

[9] Graevenitz G.A. (2003) "Introduction to fingerprint technology", A&S International, Vol. 53, pp. 84 – 86.

[10] PravadaP.Wankhade and Prof. S.O. Dahad (2011) "Real Time Vehicle Locking and Tracking System using GSM and GPS Technology-An Anti-theft System" Vol.2, No.3.

[11] N. D. Sarier, "Generic constructions of biometric identity based encryption systems," in *Proc. Security Privacy Mobile Devices WirelessCommun.*, 2010, pp. 90–105.

[12] Sarier N.D (2011)"A new biometric based encryption scheme secure against Dos attack," security communication Netw. vol.4, no.1, pp.2-32.

[13] Wang M and Tang D(2012) "A bovel biometric signcryption scheme that is identify-based and group-oriented," Appl. Math.Inf.Sci., vol.6, n0.3s, pp.849-854.

[14] X. Li, J. Niu, and M. K. Khan, "Robust Biometrics Based Three-Factor Remote User Authentication Scheme with Key Agreement," in *Proc.IEEE Int. Symp. Biometr. Security Technol.*, 2013, pp. 105–110.

[15] X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. Deng, "A generic framework for three-factor authentication: preserving security and privacy in distributed systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 8,pp. 1390–1397, Aug. 2011.

[16] Yang Y, Hu Y and Zhang L(2013) "An efficient biometric based signature scheme," KSII Trans. Internet Inf. Syst., vol.7,no.8,pp.2010-2026.