Biometrics Controlled Vehicle Security System with GPS and GSM Technology

Shruthi B M[*1], Priyanka K R[*3], Kavana M D[*3], Pruthvi P R[*4]
**Asst.Professor, Dept of CSE* GSSS
Institute of Engineering and Technology for Women,
Mysuru, India

Abstract: In this current world where technology is growing up day by day and scientific researchers are presenting new era of discoveries, the need for security is also increasing in all areas. At present, the vehicle usage is basic necessity for everyone. Simultaneously, protecting the vehicle against theft is also very important. Traditional vehicle security system depends on many sensors and cost is also high. When the vehicle is stolen, no more response or alternative could be available to help the owner of the vehicle to find it back. The main goal of this paper is to protect the vehicle from any unauthorized access, using fast, easy-to-use, clear, reliable and economical fingerprint recognition technique. This vehicle security system intimates the status of the vehicle to the authoritative person (owner) using Global Systemfor Mobile (GSM) communication technology. If the person is certified, vehicle access is allowed. Else SMS will be sent to the owner and the engine will be immobilized. The prototype model for the security system is built on the embedded platform using PIC Microcontroller which controls all the processes and cost is also very stumpy. On higher end theft attempts like cutting battery power supply, protection to the vehicle is provided by Engine Control Unit (ECU) embedded on microcontroller. By using GPS technology, vehicle can be identified very easily. Thus, the system provides security at both levels, i.e. when battery supply is provided or not.

Keywords: Microcontroller Unit (MCU); Attention (AT) Command; Global System for Mobile (GSM); Engine Control Unit; Global Positioning System (GPS); Anti-theft mechanisms.

1. INTRODUCTION

In this new era, automobile thefts are increasing at a startling rate around the globe. Most of the vehicles are entrenched with many anti-theft systems. One can come across beepers, fire alarm, latest age doors and windows, security camera and personal safety products. But, all these commercially available products are very high-priced. Hence, this paper provides a taciturn attempt to design and develop a trouble-free, low cost vehicle theft control scheme using a microcontroller. It also includes a GSM and GPS technology for the communication purposes.

Some of the reasons due to which vehicle protection is limited are given below:
a. Due to longer distance (range), siren cannot be heard.
b. Most of the cars have similar sounds.
c. Physically, alarms can be disabled on theft attempts.
d. Alarm sound can be mitigated in crowded areas.

In this paper existing scenarios and proposed structural design are explored, describing the various modules in detail and the corresponding working methodology. The entire security system concept is implemented as a system prototype model. Recent statistics on vehicle theft across various countries are shown in TABLE I:

Table 1. Vehicle Theft Reports

Countries	Vehicle thefts	Year
Italy	1,99,950	2014
France	1,85,811	2013
United States	8,23,100	2015
Brazil	1,96,500	2013
Egypt	1,25,900	2014
United Kingdom	1,86,650	2013

2. EXISTING SECURITY TECHNIQUES

Various anti-theft systems have been developed over the few decades. An Engine Control Unit (ECU) is connected to the Info-Security Circuit Board and sensors inside the vehicle bus. The bus communicates with other vehicles, road-side transportation and mobile phones with wireless interfaces. The shortcoming of this system is that the data timeliness and network delays to apprehend reliable secure car communications [2].

Other systems include a component specifically in-vehicle engine immobilizer. The component will not enable the functions of the appliances if it finds itself is illegally moved to another car [3]. The negative aspect of this system is that it requires a secure processor and smart card chips to store in the Group Identification Number.

The highly developed system uses the Global Positioning System (GPS) to track the position of the vehicle and its existing location. GPS uses global navigation satellite system. The position in sequence provided by GPS system can be visualized using Google earth. The main complication of using GPS is that the signal can become degraded and receiver system will not provide location if view of the sky is severely limited. It is also inclined by other factors like rainfall, fog and snowfall [4].

Radio frequency Identification (RFID) is used in Intelligent Computerized anti-theft system [ICAT].RFID cards are used to provide secured access. The restriction here is that keyless RFID cards can be easily stolen. In addition, key may malfunction on contact with metallic object [5].

Some systems use Auto cop mechanism which is a video surveillance solution that can be fitted into the vehicle. The camera will continuously monitor the actions inside the corresponding vehicle [6]. The main drawback is the camera will not detect accurately when there are changes in the lighting conditions in and around the system.

3. SYNOPSIS OF THE SYSTEM

The vehicle security system has the following modules. Fingerprint recognition technique, embedded main board with various components and human machine communication module.

3.1 FINGERPRINT RECOGNITION SYSTEM:

Biometrics is the method of identifying human by their own unique characteristics. There are various biometric patterns which include face, iris, fingerprint, DNA, retina, palm print, ear, voice, signature, hand shape, typing rhythm and gait. But no single biometric has yet been proven to be perfectly reliable or secure. For illustration, palm prints are usually frayed; Voice, signature, hand shapes and iris images are easily forged; Due to various lightening conditions and face-lifts, face recognition will result in poor accuracy. In addition, iris and face recognition are susceptible to spoofing attacks [7].

The Fingerprint biometrics is the gifted biometric pattern for personal detection in terms of security and reliability. It is difficult to forge or steal. It is accepted worldwide. Live fingerprint readers based on optical, thermal and ultrasonic approach are used. The two commonly used fingerprint matching techniques are minutiae-based matching and pattern matching. In pattern matching technique only the similarity between two images are compared. Minutiae matching relies on minutiae points i.e. location and direction of each point [12]. The fingerprint recognition system contains mainly an image capturing module, feature extraction module and pattern matching module. The representation of these modules is represented in Figure 1

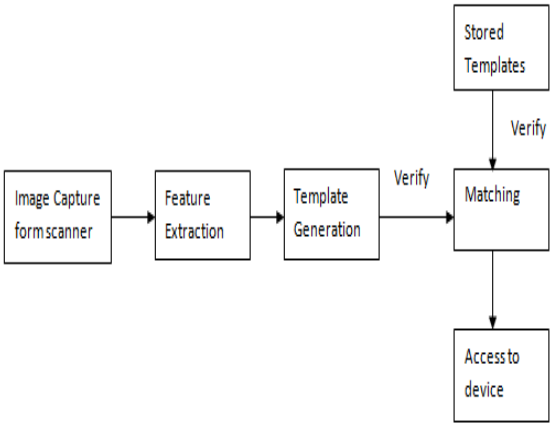

Fig 1. Working of Biometric System

The fingerprint recognition system used is based on ultrasonic sensors which avoids fake authentication. The optical sensors just capture the images on the surface of the scanner and hence it can be fooled easily [15]. Whereas, Ultrasonic sensors captures the minutiae from epidermal layer of the skin and it is efficient for liveness detection [13]. The system expected to have very low FRR (False Rejection Rate) of 0.1% and FAR (False Acceptance Rate) of 0.01% respectively.

3.2 WORKING OF THE EMBEDDED SYSTEM:

The security system mechanism contains two approaches: first, if the battery supply is ON and system is active. When an unauthorized person tries to turn on the vehicle, then alert message will be sent to the authenticated user in system and vehicle will be moved to OFF condition. In second mode, when the battery supply is cut during theft attempts, authorized person can will be authenticated and given access using GPS and ECU which is embedded within the microcontroller.

The main component (BRAIN) of this system is PIC (Peripheral Interface Controller) microcontroller. It is responsible for all monitoring and generating the inputs and outputs respectively. The output of the system will be displayed on LCD of SMS arrival status and configuration etc. Proper LCD display is obtained through programming and LCD interface design. Totally three trials will be given to the user and if the scan matches access will be given to the owner. Else if intruder is accessing the system and three trials are failed then alert message will be sent to the owner's vehicle. On receiving the SMS from owner using GSM technology, the alarming system will be activated. In case of network error on the owner position, the second alert message may be sent to nearby police station.

The serial communication is provided by RS232 cable. It interfaces the programming to the prototype model. The interfacing between microcontroller and GSM is through UART (Universal Asynchronous Receiver Transmitter) communication which is serial communication protocol [8]. The Overall System is represented using the flowchart in the Figure 2.

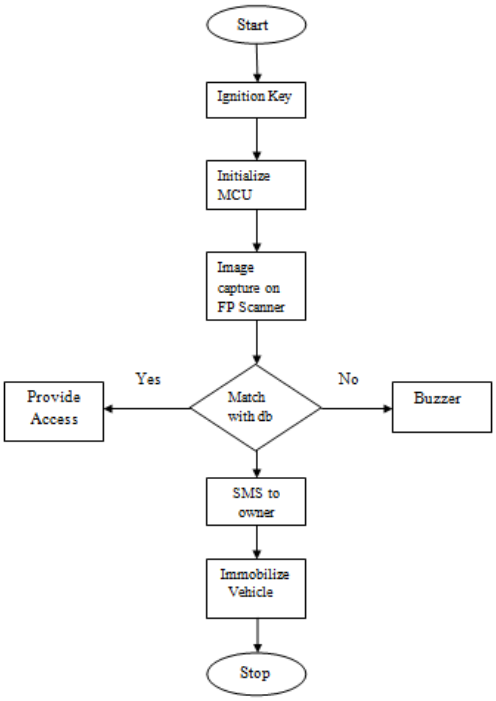

Fig 2. Overall representation of the system

The embedded unit consists of engine control unit (ECU). The ECU determines the ignition timing, monitors the engine and other parameters which gathers the signal information coming from sensor devices. All the peripherals are attached to the ECU which acts as a brain of the system**.**

3.3HUMAN-MACHINE COMMUNICATION MODULE:

Human machine communication represents the Global System for Mobile (GSM) that acts as an intermediate between owner and system. GSM is the worldwide accepted standard for digital cellular communication. GSM modems are most frequently used to provide mobile internet connectivity and many are used for sending and receiving Short Message Service (SMS). A wireless link is provided between the owner's cell phone and MCU (Microcontroller Unit) by GSM (Global System for mobile) module. It is similar to dial-up modem. The main dissimilarity between them is that in dial-up modem transmission and reception of data is through fixed telephone line whereas wireless modem uses radio waves. PIC uses AT (Attention) commands to control modems [9]. GSM modem maintain set of standard AT commands. The functions of AT commands are given below

a. Reading, writing and deleting SMS messages.
b. Sending SMS messages.
c. Monitoring the signal strength.
d. Monitoring the charging status and charge level of the battery.
e. Reading, writing and searching phone book entries

4. SYSTEM DESIGN

An anti-theft vehicular system has the following components. The hardware and software design is explained in this session:

4.1. HARDWARE DESIGN:

The detailed hardware composition is shown in Figure 3:

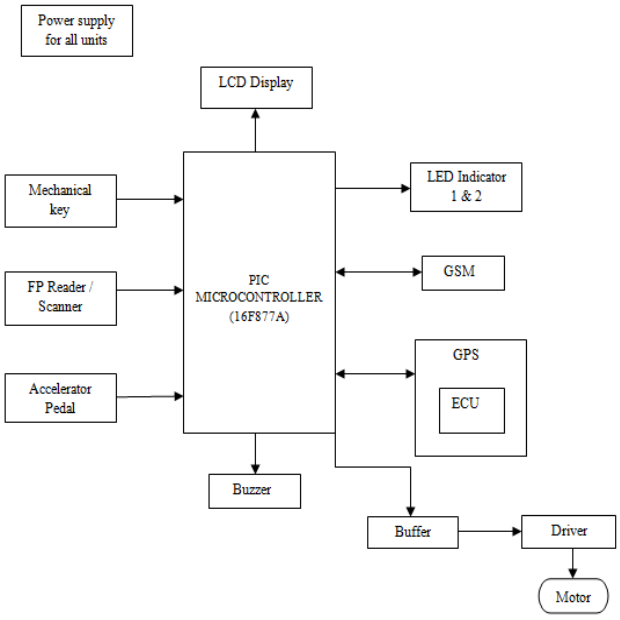

Figure 3: Block diagram representation for security system.

Liquid Crystal Display (LCD): LCD represents display of numeric and alphanumeric characters in dot matrix and segmental displays. LCD requires 3 control lines and 8 I/O lines for the data bus.

Pin	Symbol	Description
1	Vss	Ground terminal of Module
2	Vdd	Supply terminal of Module
3	Vo	Power supply to liquid Crystal Drive
4	RS	Register Select
5	RW	Read/Write
6	EN	Enable
7-14	DB0-DB7	Bidirectional Data Bus
15	LAMP (L+)	LED or EL lamp power supply
16	LAMP (L-)	Enable

Table 2. LCD Pin Description

RELAY:

The relay is an electromagnetic switch. When relay is activated, it closes the loop of ignition and starts the engine. When relay is de-activated, it opens the loop of ignition and stops the engine. Stepper motor is connected with relay replicating the automobile engine to verify the operation of the system.

FINGERPRINT SCANNER:

Fingerprint biometrics is one of the efficient, secure, cost effective, ease to use technologies for user authentication. Because of the intellectual property protection and commercial profits, it is used in the field of automobiles for providing security and theft protection [11]. The representation of fingerprint scanner is given in Table 3

Features	**Depiction**
Power	DC : 3.6v -6.0v

Interface	UART
Working current	100mA- 150mA
Matching mode	1:1 and 1: N
Image acquiring time	<0.5s
Template size	512 bytes
False Acceptance Rate	(FAR) <0.001%
False Rejection Rate	(FRR) <0.1%
Searching time	<0.4s:

Table 3. Fingerprint Scanner Features

BUZZER:
A buzzer or beeper is a signaling device, usually electronic, typically used in automobiles, household appliances such as a microwave oven, or game shows. It most commonly consists of a number of switches or sensors connected to a control unit that determines if and which button was pushed or a preset 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 [13].

4.2. SOFTWARE DESIGN:

MPLAB IDE: MPLAB Integrated Development Environment (IDE) is a free, integrated toolset for the development of embedded applications on microchip's PIC and other microcontrollers [10]. It is used in construction of C compilers, macro assemblers, real-time kernels, debuggers, simulators, integrated environments and evaluation boards for PIC, ARM and other microcontroller families. The coding is done using Embedded C and tested in MPLAB integrated environment.

.

PROTEUS SIMULATOR:
Proteus is a Virtual System Modelling (VSM) that combines circuit simulation, animated components
and microprocessor models to co-simulate the complete microcontroller based designs. It is the perfect tool to test the microcontroller designs before constructing a physical prototype real time. It allows the users to interact with the design using on-screen indicators and/or LED and LCD displays along with the switches and buttons. The hex file generated in mplab is fed as input to Proteus. Proteus execute those files and provide a real time execution of the entire system virtually.

EMBEDDED C:
Embedded C is the set of C language extensions for the embedded systems. It is used for microcontroller based applications. Embedded C uses the resources (RAM, ROM, I/Os) of the embedded processor. The code for the security system is done using Embedded C. It is interfaced to the prototype model using RS232 serial communication.

5. CIRCUIT DIAGRAM

The security system consists of interfaces like fingerprint scanner, LCD, GSM Modem, Motor Driver, Buzzer etc. The power supply is provided to all the units. The entire circuit is constructed using PCB design layout tool. The circuit diagram is represented in Fig 4.

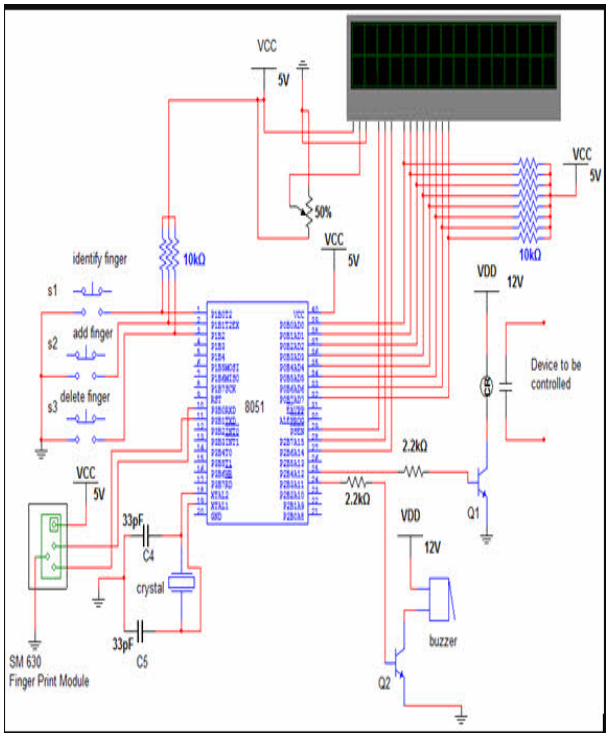

Fig 4. Circuit diagram for the system

6. CONVENTION OF GPS IN SECURITY SYSTEM:

Global Positioning System can be used to provide security throughout the off state condition of the vehicle. Even there is a possibility to drive away vehicle in switch off condition. There are cases where one vehicle can be totted in another higher vehicle. Thus, GPS prevents vehicle lifting and theft detection. The working of the system is described in Fig 5. Initially, on parking the vehicle current location will be stored. The Engine Control Unit (ECU) continuously monitors the engine function.
While engine is in off condition but if GPS location changes significantly, alert SMS will be sent to the authorized person. Hence it provides security even when there is no battery supply to the engine unit. The Engine Control Unit is powered by internal battery.

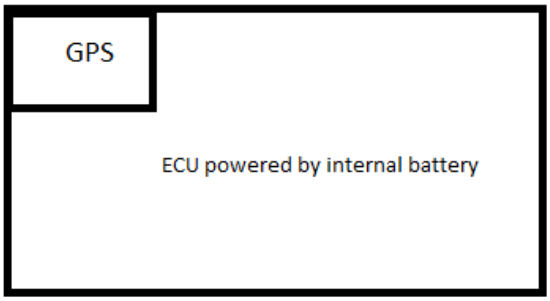

Fig 5. GPS in Vehicle Security

CONCLUSION

Security is fundamental criteria in all kind of applications. This project is aimed at improving the level of security for vehicles. As the fingerprint is a promising biometric pattern for identifying a person in terms of both security and ease of use. This is a unique method of conniving and assembling a low-cost, packed in theft control system for an automobile which is highly reliable. The work presented demonstrates the initial phase of an embedded car that will be visible in near future. Customized vehicles will not only provide a more interesting drive but also safer one.

REFERENCE:

[1] [1].Motor theft statistics as given http://en.wikipedia.org/wiki/Motor_vehicle_theft#
[2] [2]Sukeerti Singh and Ayushi Mhalan, Vehicle Theft Alert System using GSM, Int. Journal of Engineering Science and Technology
[3] (IJEST), May 2013
[4] [3.]M.Sunitha, V.Vinay Kumar and G. Raghu, Embedded Car Security System, Int. Journal of Engineering Development and
[5] Research (IJEDR), 2012
[6] [4.]Z. M. Win and M. M. Sein, Fingerprint recognition system for low quality images, presented at the SICE Annual Conference, Waseda University, Tokyo, Japan, Sep. 13-18, 2011.
[7] [5.]Upendran Rajendran and Albert Joe Francis, Anti Theft Control System Design Using Embedded System, Proc. IEEE, vol. 85, page no. 239- 242, 2011
[8] [6.]Vikram Kulkarni and G. Narsimhulu, A Low cost Extended Embedded Smart Car Security System on Face Detection and
[9] Continuous Video Monitoring System, Int. Journal of Engineering Science and Advanced Technology (IJESAT), May 2012
[10] [7.]Kaisheng Zhang, Study on the Embedded Fingerprint Image Recognition System, Int. Conference of Information Science and Management Engineering, 2010
[11] [8.]Megha Kulshrestha and V.K. Banga, Finger Print Recognition: Survey of Minutiae and Gabor Filtering Approach, Int. Journal of Computer Applications(1995-8887), Volume 50-No.4, July 2012.
[12] [9].Jayanta Kumar Pany and R.N. Das Choudhury, Embedded Automobile Engine Locking System Using GSM Technology, Int. Journal of Instrumentation, Control and Automation (IJICA) ISSN : 2231-1890 Volume -1, Issue -2, 2011
[13] [10]. http://en.wikipedia.org/wiki/MPLAB
[14] [11]. Sruthy Sebastian, Literature survey on Automated Person Identification Techniques, Int. Journal of Computer Science and Mobile Computing(pg.232-237), Vol.2,Issue.5,May 2013.
[15] [12]. E.Walia and S.Kumar, Analysis of various biometric techniques, Int. Journal of Computer and Information Technologies, Vol.2,no.3,2011
[16] [13]. Mudit Singhal and Sudeep Singh, An Embedded Interface for GSM Based Car Security System, Int. Conference on Computational Intelligence, Communication Systems and Networks, IEEE Computer society, 2012.
[17] [14]. Jiao She and KAisheng Zhang, Study on the Embedded Fingerprint Image Recognition System, Int. Conference of Information Science and Management Engineering, IEEE Computer Society,2010.
[18] [15]. T.Ignatenko and F. M. J Williams, Biometric Systems: Privacy and Secrecy aspects, IEEE Transactions on Information Forensics and security, IEEE, vol.4,no.4, December 2009.