ADVANCED BIOMETRIC VEHICLE SECURITY SYSTEM

Mr. KAUSHAL S. PATHARE

Abstract— In today's world the facilities are increasing but with the increase is a facility there is also increase in theft, robbery and many more vehicle related issues. Just to improve the security of our vehicle we are inventing a new way of car inter locking system and vehicle security controlling system. In our project we are using one of the most unique thing that we have in our body ie. the finger prints. Every human present in earth have different finger prints. This would help us to improve the security of the vehicle. In this the vehicle would know who all are the owners of the vehicle are and who are trying to open it forcefully. Not only this much we are also controlling the vehicle but we are also controlling the engine of the vehicle which will improve the security of the vehicle even more. The engine controlling is done by a newly made component name carObit.

Index Terms— *inter locking system, finger prints , microcontroller , biometricstechnology , GSM-GPS module*

———————— ◆ ————————

1 INTRODUCTION

Because of increasing number of theft cases of the Automobile there is a need to security level. The new and modern lock must be unique in itself i.e. it must be only unlocked by special and specific key. This type of feature is available in the biometrics enhance the security level of the vehicles. Traditional and commonly used key locks available in the vehicles are easily unlocked by the professional thieves. With the help of master key it becomes very easy to unlock the lock of the vehicles by the thieves. This creates the demand of such type of lock which is new and provides an additional locks i.e. the lock which can only be locked and unlocked by the human body features. Biometrics can include: face recognition, voice recognition, fingerprint recognition, eye (iris) recognition.

Leaving that conventional method behind came in the concept of igniting the vehicles using key. And now, Keys are being replaced by Push start buttons. This paper was started with the sole purpose of eliminating keys as conventional method of starting the vehicle. With the introduction of Biometrics in the 18th century, security advancement in technology has gone up to various levels. In the 18th century it was used to verify the employees working for the British

HISTORICAL DEVELOPMENT OF BIOMETRIC TECHNOLOGY

The earliest form of Biometrics appeared on the scene back in the 1800's. Alphonse Bertillon, a Perisian anthropologist and police desk clerk, developed a method for identifying criminals that became known as Bertillonage. Bertillonage was a form of anthropometry, a system by which measurements of the body are taken for classification and comparison purposes. Bertillons system of anthropometry required numerous and percise measurements of the bony parts of a humans anatomy for identification. It also involved recording shapes of the body in relation to movements and differential markings on the surface of the body such as scars, birth marks, tattoos, etc. Bertillon estimated that the odds of duplicate records were 286,435,456 to 1 if 14 traits were used. This was the primary system of criminal identification used during the 19th century.

The Henry Classification system, named after Edward Henry who developed and first implemented the system in 1897 in India, was the first method of classification for fingerprint identification based on physiological characteristics. The system assigns each individual finger a numerical value (starting with the right thumb and ending with the left pinky) and divides fingerprint records into groupings based on pattern types. The system makes it possibleto search large numbers of fingerprint records by classifying the prints according to whether they have an "arch," "whorl," or "loop" and the subsequently assigned numerical value.

In 1901 the Henry system was introduced in England. In 1902 the New York Civil service began testing the Henry method of fingerprinting with the the Army, Navy, and Marines all adopting the method by 1907. From this point on, the Henry System of fingerprinting became the system most commonly used in English speaking countries.

Fingerprinting can be traced as far back as the 14th century in China. Though the use was most likely as a signature and the unique identification abilities of the fingerprint not entirely known. Fingerprints were first looked at as a form of criminal identification by Dr. Henry Faulds who noticed fingerprints on ancient pottery while working in Tokyo. He first published his ideas about using fingerprints as a means of identifying criminals in the scientific journal, *Nature* in 1880.

William Herschel, while working in colonial India, also recognized the unique qualities that fingerprints had to offer as a means of identification in the late 1870's. He first began using fingerprints as a form of signature on contracts with locals. Sir Francis Galton, who had been privy to Faulds research through his uncle, Charles Darwin, would also be credited as making significant

2.2 LITERATUREE SURVEY

3) LITERATUREE SURVEY

Researchers are continuously working beyond their ability to develop best security system for the required application. This paper provides an overview on the different technologies developed for security system for various applications. The security is demanded mainly for home for preventing the house from thieves and unfortunate accidents, as well as it is effectively required for Bank locker system, Research Labs where profound information and research is preserved. Vehicle security system kept in market circumstances is a serious problem now a day [1]. Embedded solution have proved itself everywhere, when the problem arises a solution is ready with the help of embedded system. In this paper different technologies are discussed using embedded system for security. Initially, embedded home security system is discussed with the help of some sensors used for detection purpose in section 2. Palm Vein technology is discussed for research lab security system in section 3. Similarly, Mobile based car security system, GSM and RFID based bank locker system and finally border security system is explained

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: Microcontroller Microcontroller is the BRAIN of the security system. The microcontroller is fed with the program containing the

logic required to control motor of the vehicle. The microcontroller implied is PIC 16F877A (Peripheral Interface Controller). The PIC architecture is characterized by the following features: a. Separate code and data spaces (Harvard architecture) for devices other than PIC32, which has Von Neumann architecture. b. A small number of fixed length instructions c. Most instructions are single cycle execution (2 clock cycles), with one delay cycle on branches and skips d. One accumulator (W0), the use of which (as source operand) is implied (i.e. is not encoded in the opcode) e. All RAM locations function as registers as both source and/or destination of math and other functions. f. A hardware stack for storing return addresses g. A fairly small amount of addressable data space (typically 256 bytes), extended through banking h. Data space mapped CPU, port, and peripheral registers i. The program counter is also mapped into the data space and writable (this is used to implement indirect jumps).

Motor

prototype model uses DC motors. DC motors are part of the electric motors using DC power as energy source. These devices transform electrical energy into mechanical energy. The basic principle of DC motors is same as electric motors in general, the magnetic interaction between the rotor and the stator that will generate spin.The motor is connected through motor driver to the port of microcontroller.

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

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

SOFTWARE AND HARDWARE REQUIREMENTS

Hardware Requirements

- *Mr. KAUSHAL S. PATHARE is currently pursuing degree program in mechanical engineering in Savitribai Phule Pune University INDIA, PH-7775895762. E-mail: kaushalpathare00@gmail.com*

ARM 7 MICROCONTROLLER

POWER SUPPLY UNIT

METAL SENSOR

LCD DISPLAY UNIT

IR SENSOR

RELAY DRIVER

GPS

GSM

FINGERPRINT MODULE

BLOCK DIAGRAM

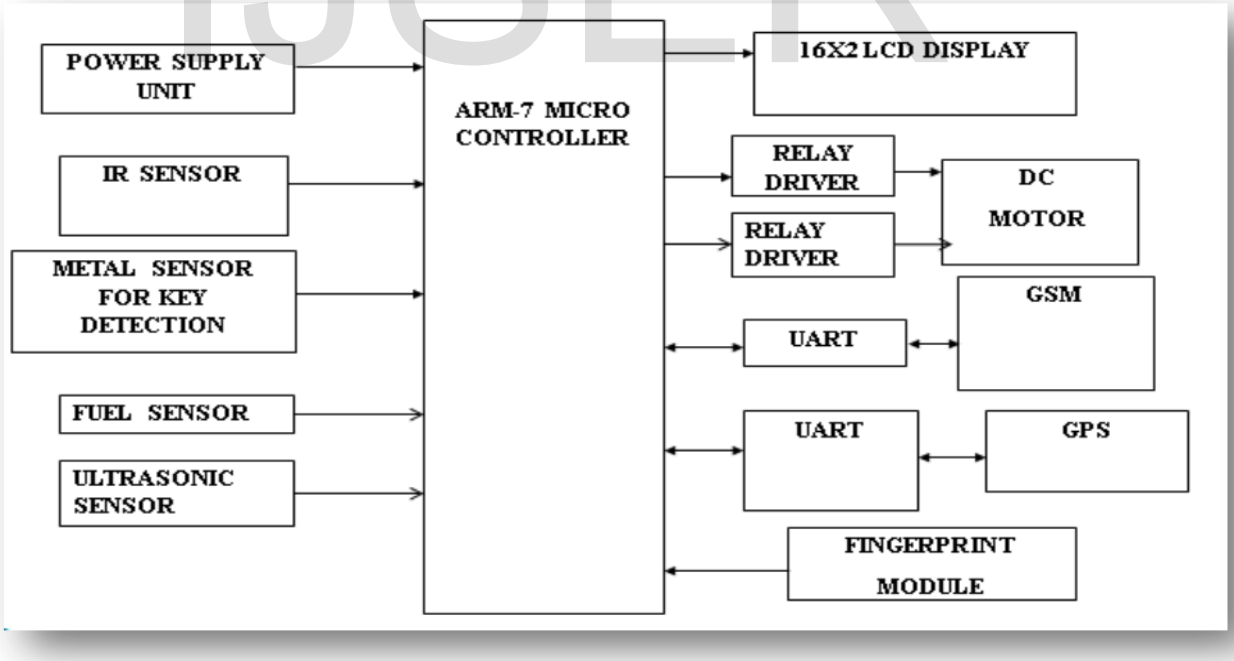


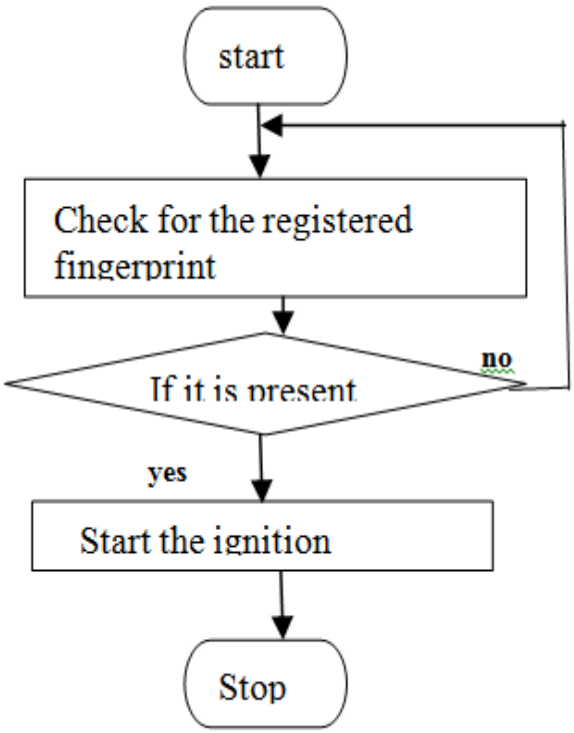
FIG1: HARDWARE REQUIREMENTS

TECHNOLOGY OVERVIEW

The researchers have several conclusions and observations during the development of the Fingerprint Engine Starter among which are the following existing Electric Engine Starter still has more rooms for improvement. The developed Fingerprint Engine Starter is a better alternative to the existing Electric Engine Starter. There is significant difference in the over-all acceptance of the respondents of the existing starter system and the developed starter system.

6)BIOMETRIC SECURITY SYSTEM WORKING

Case1: When user gives his fingerprint



Case2: When there is any motion near vehicle(IRSensor)

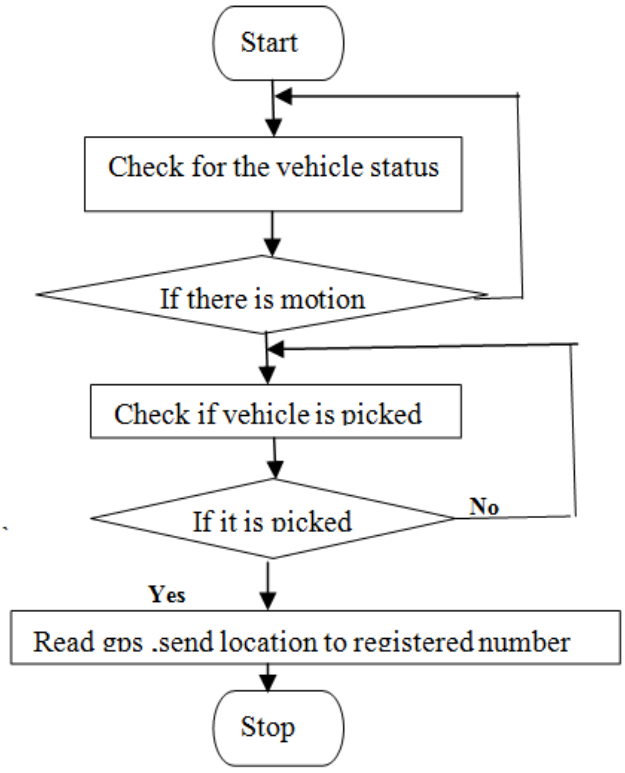


Fig2 Fig3

Case3: When metal key is inserted in vehicle (MetalSensor)

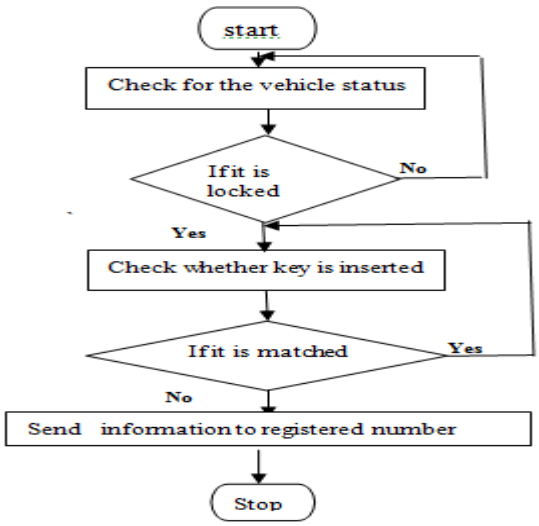


Fig4

Case4:When fuel is theft(Fuel Sensor)

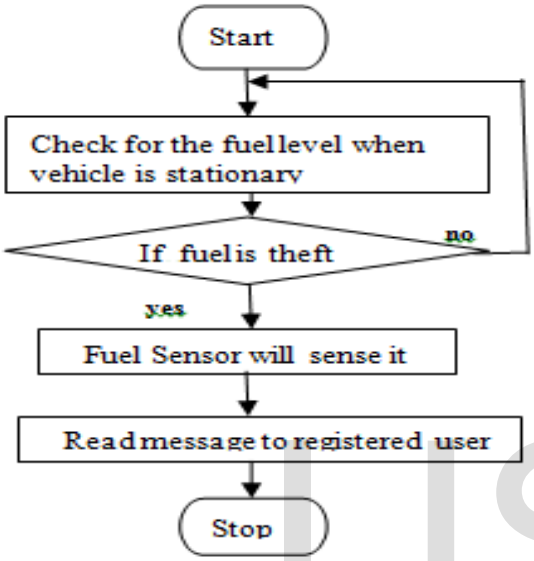


Fig5

START-UP THE ENGINE USING FINGERPRINT

Fingerprint Recognition was the image is first analyzed and then identified, extracted and stored the images in the file of database. For the identification process, first it compare the query image against with the image stored in the database and then it verified. From the above result, it has been cleared that the use of the biometric system offers the better and more reliable resultant. Moreover, it is restricting the starting of the vehicles by unauthorized user. Only the fingerprint image verified has this ability to access the engine of the vehicle.first biometric approach to verify the person by downloading the images of sample in the database.

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.

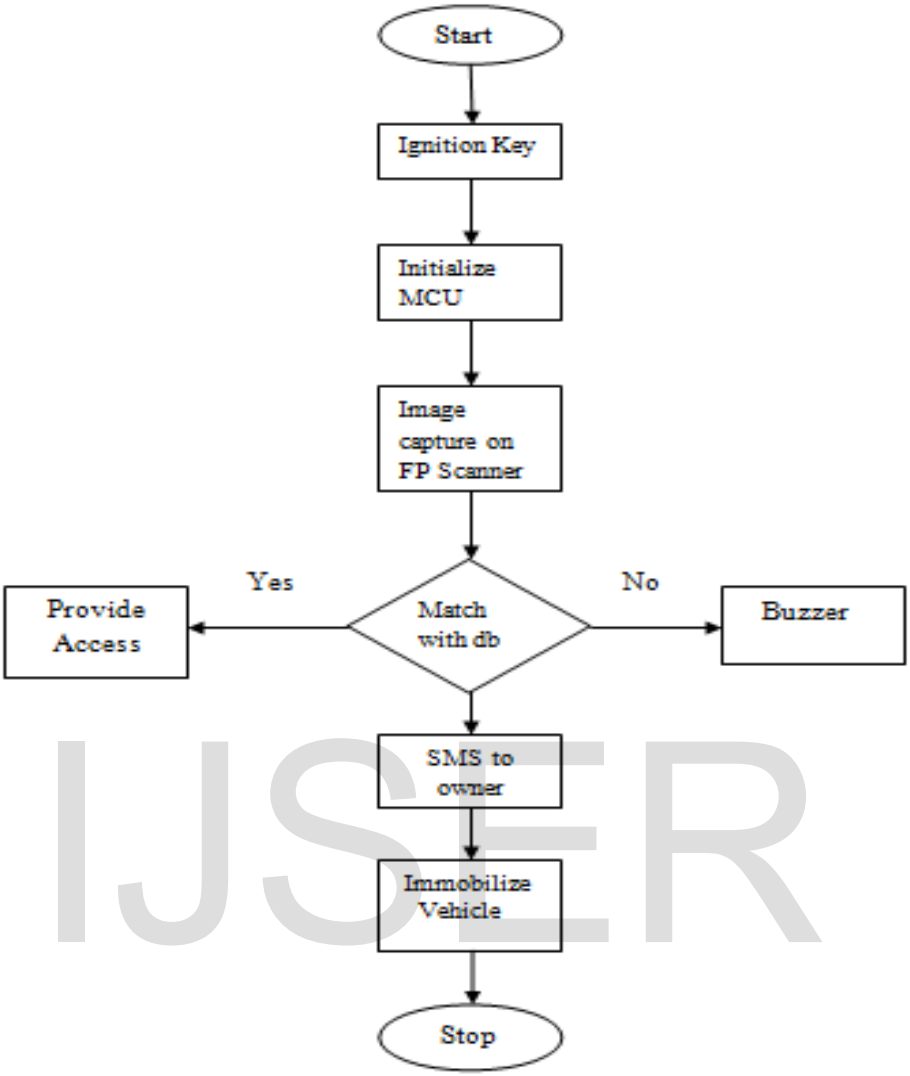


Fig6: Working of the embedded system

ADVANTAGES

1) The first advantage of using this new technology is the uniqueness and it is also the main characteristic which allows biometricstechnology to become more and more important in our lives. With uniqueness of biometrics technology, each individual'sidentification will be single most effective identification for that user. A chance of two users having the same identification in the
biometrics security technology system is nearly zero

2) Secondly, the highly secure way of identifying users makes this technology less prone for users to share access to highly sensitivedata. For example, users can share their fingerprints, iris and so forth allowing other users access to secure information. Each traitused during identification is a single property of that user. In other

words, it is extremely hard or impossible to make duplicate or share biometrics accessing data with other users. This makes it ever more secure allowing user information and data to be kept highly secure from unauthorized users

3) Lastly, this identification of users though biometrics cannot be lost, stolen or forgotten. This aspect of biometrics technology allows it to become more popular in its use. This method of identifying and giving access to user makes user identification a lot easier. Finally, most biometrics security systems are easy to install and it requires small amount of funding for equipment (except modern biometrics technology such as: DNA/retinal/iris recognition)

DISADVANTAGES

1) Even though, there are many advantages of biometrics security system, it still has many flaws in its system. Each biometrics application method has weaknesses which can cause problems for its users. For example, if the biometrics security system uses fingerprints to identify its users and an accident causes a user to lose his/her finger then it can be a problem during the verification process. For voice recognition methods, illnesses such as strep throat can make it hard for authorized users to get access to their information. Another factor that can influence voice recognition systems is the continuous aging of its users. Noise in an environment where voice recognition is used to identify its users can also make it hard for users to be identified.

2) For iris or retinal scanning applications, users may find it very intrusive. Users may also have the concern for the safety of their eyes during the iris or retinal scan. Furthermore, databases used to store user identification data will be very large which might form a potential threat. For scanning retinal/iris characteristics and storing large amount of database, biometrics system requires new and modern technology. Therefore, the cost for equipment is also expensive Finally, lots of people are still concerned about biometrics technology in different aspects such as: security, adaptability to rate of change in life, scalbility, accuracy, privacy and others.

3)Environment and usage can affect measurements

FUTURE SCOPE

The developed system ensures that only authorized drivers can drive the vehicle and misuse of vehicles by others can be prevented. The system also provides facility for monitoring seat belt status. It also gives time to get the system repaired if any malfunction exists. The system makes sure that vehicle's access is given to only authorize personal and thus accidents can also be averted. The developed prototype serves as an impetus to drive future research, geared towards developing a more robust and embedded real-time fingerprint based ignition systems in vehicles. The present module can be extended to including a GSM-GPS module for additional safety so that even if the vehicle is stolen by trespassing the security module we can relocate the vehicle using satellite coordination.

APPLICATIONS

1. Industrial application

2. Home or domestic application

3. Bank Lockers or security safes

4. Vehicle security systems

CONCLUSION

In conclusion, biometrics technology is a new technology for most of us because it has only been implemented in public for short period of time. There are many applications and solutions of biometrics technology used in security systems. It has many advantages which can improve our lives such as: improved security and effectiveness, reduced fraud and password administrator costs, ease of use and makes live more comfortable. Even though the biometrics security system still has many concerns such as information privacy, physical privacy and religious objections, users cannot deny the fact that this new technology will change our live for the better.

REFERANCE

[1] 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.

[2] http://en.wikipedia.org/wiki/Biometrics.

[3] 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.

[4] J. C. Yang, N. X. Xiong, A. V. Vasilakos and Zh. J. Fang, "A fingerprint recognition scheme based on assembling invariant moments for cloud computing communications", IEEE Systems Journal, vol. 5, no. 4, Dec. 2011.

[5] S. Malathi and C. Meena, "An efficient method for partial fingerprint recognition based on Local Binary Pattern", in Proc.Communication Control and Computing Technologies, pp. 569572, IEEE, 2010.