JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 06, ISSUE 03, 2019

Development of a Car Theft Deterrent System Using Permutation of Fingerprints Technique

Beril Susan Philipi[1], Kancheti Spandana[2]

Assistant Professor[1,2]

Department of ECE

MREC

Abstract- In this paper we present a novel car theft deterrent control system that tries to prevent the theft of a vehicle. The aim of this project is to develop a functional prototype to work as a car theft deterrent system. Fingerprints (viz., a Biometric Characteristic) are used to verify the user's identity in order to allow the user to start the vehicle. The aim is to apply the concept of using permutation of fingerprints like a password for the verification process. The system makes use of a biometric fingerprint verification module to verify the user's identity and a GSM module to send text messages. The system is designed in such a way that it accepts fingerprints for verification in form of a permutation i.e. a predefined chronological order to enter the finger prints (for e.g.: thumb followed by index finger and ring finger). Thus BIOmetric PERMmutation of fingerprint is being called Bio-Perm. Only if the finger prints are entered in the defined order the car can't be started. The proposed system is designed to work as follows – The system has three levels. The 1st Level i.e., the fingerprint recognition level by giving three different finger scans to verify his identity, which is a prerequisite criterion to be fulfilled to be able to start the car. Next the user can start the car engine by turning the ignition on. The engine immobilizer will prevent the engine from running when a duplicate key is used to start the engine. This forms the 2nd Level of Security. Failing to clear any one of the above two levels is considered as an act of theft and an alert is issued to the cops from the GSM module in the car and a buzzer sound's. The location of the car can be tracked with the help of the GSM module.

Index Terms- About four key words or phrases in alphabetical order, separated by commas. Keywords are used to retrieve documents in an information system such as an online journal or a search engine. (Mention 4-5 keywords)

I. INTRODUCTION

The aim of this paper is to develop a functional prototype to work as a car theft deterrent system. Fingerprints (viz., a Biometric Characteristic) are used to verify the user's identity in order to allow the user to start the vehicle. The aim is to use the concept of permutation of fingerprints, which functions like a password (BioPerm), for the verification process to gain access to the vehicle. The objectives of this project are as follows:

a) To provide access only to authorized users of the car.
b) To be able to give intimation messages to the remaining users when a particular user is using the car.
c) To keep the response time of the system as less as possible.
d) To raise the difficulty of theft to an infeasible level.
e) To greatly reduce the chances of theft even by Biometric Impersonation.
f) To give alert messages when someone who is not authorized is trying to breach the security and start the vehicle.

The following are the assumptions based upon which we carried out this paper:

a) No two persons can have identical fingerprints. [Refer to Appendix A for more insight]
b) The proposed system can reach its full potential when it is integrated with an Engine Immobilizer which acts as the second level of security.
c) The immobiliser along with the proposed system unit should be connected securely to the vehicle's electronic engine control unit, using the car's internal data network.
d) Encryption keys used to transmit data between the key fob, receiver and engine match the security offered by openly published versions such as the **Advanced Encryption Standard (AES)** adopted by the US government to encrypt classified information.

The objectives of this paper are as follows:

g) To provide access only to authorized users of the car.
h) To be able to give intimation messages to the remaining users when a particular user is using the car.
i) To keep the response time of the system as less as possible.
j) To raise the difficulty of theft to an infeasible level.
k) To greatly reduce the chances of theft even by Biometric Impersonation.
l) To give alert messages when someone who is not authorized is trying to breach the security and start the vehicle.

ISSN- 2394-5125 VOL 06, ISSUE 03, 2019

II. EXISTING WORK OR LITERATURE SURVEY

A theft deterrent system is any device or method used to prevent or deter the unauthorized appropriation of items considered valuable. Theft is one of the most common and oldest criminal behaviours. From the invention of the first lock and key to the introduction of RFID tags and biometric identification, theft deterrent systems have evolved to match the introduction of new inventions to society and the resulting theft of them by others.

Humans have always felt very possessive of their belongings. Everyone worth his salt thinks of protecting his hard earned possessions. Cars are expensive. Other than a house, perhaps, few purchases we make will compare to a new car. And just like any other expensive asset, a car brings with it a secondary cost -- the risk of theft. The first documented case of car theft was in 1896, only a decade after gas-powered cars were first introduced. From that early era to today, cars have been a natural target for thieves: They are valuable, reasonably easy to resell and they have a built-in getaway system. Some studies claim that a car gets broken into every 20 seconds in the United States alone.

From the day that cars have been a popular medium of transport, they've also been popular with thieves. In earlier days, cars had very less or zero theft prevention systems fitted in and this made them easy takeaways for car stealers. But cars are now far more advanced and carry a decent amount of expensive equipments which not only make them a status symbol but also eye candy for criminals. Car thefts have become extremely common and this has been rising year on year. According to Interpol, almost 50 Lakh vehicles are stolen across the world every year and the sale of these stolen vehicles is valued at US $39 billion!

The American FBI's Uniform Crime Report shows that a motor vehicle is stolen every 28.8 sec in the United States. These figures dictate that the U.S. tops the list of number of car thefts and other developed countries follow it in the list.

With increase in car anti-theft technologies, the sophistication of car lifters too has increased. In several cases, thieves even work in groups and even belong to organised crime networks. According to statistics, the actual theft happens within a time frame of 30 seconds to 3 minutes. The stolen vehicles are disposed of just as soon as they are picked up. The most common ways to dispose vehicles are breaking it up and selling the parts, revamping the car completely thereby making it unrecognizable, and driving it out of the city to be sold in a distant and remote area.

In light of this startling statistic, it's not surprising that millions of Americans have invested in expensive alarm systems. Today, it seems like every other car is equipped with sophisticated electronic sensors, blaring sirens and remote-activation systems. These cars are high-security fortresses on wheels! In some laid-back parts of the world, locking the doors may be enough to ward off the threat. Everywhere else, it's a good idea to arm yourself and your car with some security.

III. PROPOSED WORK

The following are the sequence of steps we followed to complete this paper:

1. Design the Block Diagram for the proposed system based on its specifications.
2. Design the Electrical Circuit or the Schematic as per the block diagram.
3. Design the PCB Layout as per the Schematic.
4. Make a PCB.
5. Develop the Source Code.
6. Virtually simulate the working of the system in a software.
7. Testing of Hardware.

Block diagrams are a visual language for describing actions in a complex system. The first step towards achieving the aim of our project was to design a block diagram to divide the entire operation of the system into smaller tasks and assign each of these tasks to different individual blocks, thereby defining their inputs, outputs and functionalities. A block diagram is a specialized, high-level type of flowchart. Its highly structured form presents a quick overview of major process steps and key process participants, as well as the relationships and interfaces involved.

It is a diagram of a system, in which the principal parts or functions are represented by blocks connected by lines that show the relationships of the blocks. They are frequently used in the engineering world in hardware design, electronic design, software design, and process flow diagrams.

The block diagram is typically used for a higher level, less detailed description aimed more at understanding the overall concepts and less at understanding the details of implementation. Contrast this with the schematic diagram and layout diagram used in the electrical engineering world, where the schematic diagram shows the details of each electrical component and the layout diagram shows the details of physical construction.

ISSN- 2394-5125 VOL 06, ISSUE 03, 2019

The block diagram of the proposed system is as follows:

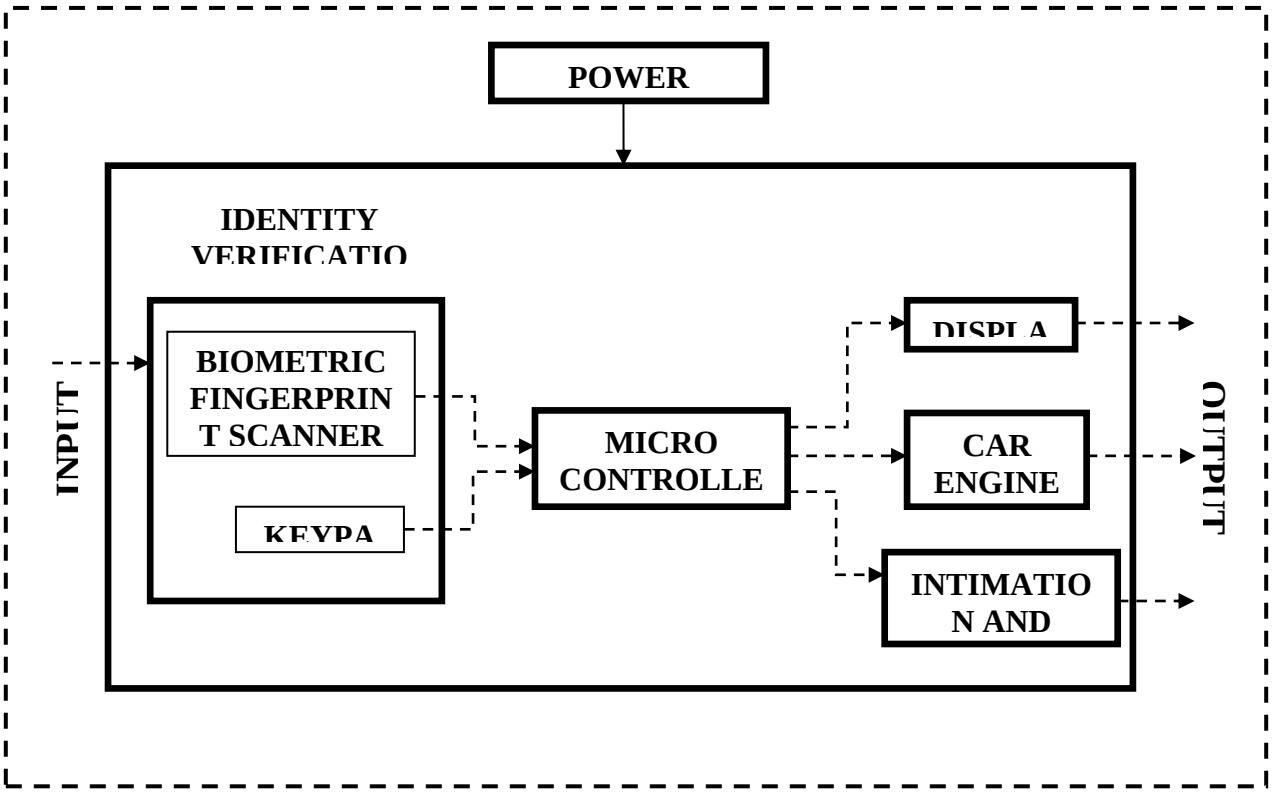

Fig 1 Block Diagram

IV. RESULTS

The final results of the proposed system are demonstrated by a functional prototype. The prototype working is explained in the steps below:

1. When the prototype is powered up, it waits for the user to enter his/her BioPerm.
2. If the BioPerm is correct, the user can proceed to start the vehicle.
3. When one user is accessing or using the vehicle an intimation message is sent to all the other users.
4. If the BioPerm entered is incorrect, the user cannot start the vehicle even though he/she has the original keys.
5. If the user happens to enter a BioPerm he can try once again by entering a 5 digit PIN to reinitiate the scanning process.
6. Even after the second try the user fails to give the correct BioPerm then the vehicle is locked down and an alert is sent to the cops and other authorized users as well.

System testing

System testing of software or hardware is testing conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements. System testing falls within the scope of black box testing, and as such, should require no knowledge of the inner design of the code or logic. [1] System testing is performed on the entire system in the context of a Functional Requirement Specification(s) (FRS) and/or a System Requirement Specification (SRS). System testing tests not only the design, but also the behaviour and even the believed expectations of the customer. It is also intended to test up to and beyond the bounds defined in the software/hardware requirements specification(s).

Tests Performed: The following are the different types of tests that we have performed on the system:

- Usability testing
- Security testing
- Response Testing

ISSN- 2394-5125 VOL 06, ISSUE 03, 2019

Usability Testing

Usability testing is a black-box testing technique. The aim is to observe people using the product to discover errors and areas of improvement. Usability testing generally involves measuring how well test subjects respond in four areas: efficiency, accuracy, recall, and emotional response. The results of the first test can be treated as a baseline or control measurement; all subsequent tests can then be compared to the baseline to indicate improvement.

- *Performance* -- How much time, and how many steps, are required for people to complete basic tasks? (For example, find something to buy, create a new account, and order the item.)
- *Accuracy* -- How many mistakes did people make? (And were they fatal or recoverable with the right information?)
- *Recall* -- How much does the person remember afterwards or after periods of non-use?
- *Stickiness* -- How much time he/she spends
- *Emotional response* -- How does the person feel about the tasks completed? Is the person confident, stressed? Would the user recommend this system to a friend?

***Results*:**

***Performance*:**

Time Consumed: 15 seconds

Recall:

90% of the users have been able to

Security Testing:

Security testing is a process to discover the the possible vulnerabilities and how secure is the system to such vulnerabilities. The different steps involved in this are:

- Vulnerability Scan
- Penetration Test

Vulnerability Scan:

Biometric Impersonation

Penetration Test:

Due to use of BioPerm the choice of permutation for each user is 5040.

Response Testing:

In this test we measure the time required for a user to complete the verification process and start the car. This gives us the response time of the system. Repeating this test on a various number of occasions we have obtained almost the consistent results.

Response Time = 15 seconds

But this is not the actual response time of the system as we have introduced time delays in the programming to have enough time in order to be able to read the text displayed on the LCD Screen. If we eliminate these delays the total response time would decrease.

Comparison:

Table 1

Immobilizers	Proposed System
Key cloning is possible.	Fingerprint cloning is very difficult. Cloning of multiple fingerprints perfectly is a difficult task.
Keys can be lost or stolen .	Fingerprint Module stores the prints in an encrypted form. Reverse engineering to obtain the images is not possible.
Only 1 layer of security.	This has multiple layers of security.
Tracking of vehicle is not possible in case of theft	Tracking is possible .
	Vehicle reports its own FIR in case of theft.

ISSN- 2394-5125 VOL 06, ISSUE 03, 2019

V. CONCLUSION

A car theft deterrent system with biometric identity verification to provide access only to authorized users has been developed. This system has reliability when compared to the systems existing currently in the market. Also the probability of fooling this system through Biometric Impersonation is low owing to the Permutation Technique implemented in the verification stage.

REFERENCES

1. http://www.askmen.com/cars/car_tips_150/161_car_tip.htm/
2. http://articles.economictimes.indiatimes.com/2007-07-14/news/28412490_1_anti-theft-devices-passenger-car-honda-siel-cars
3. http://en.wikipedia.org/wiki/Anti-theft_system.
4. http://www.avrfreaks.net/
5. http://www.topspeed.com/cars/car-accessories/gadgets/biometric-immobiliser-ar10867.html
6. http://www.money-zine.com/Financial-Planning/Leasing-or-Buying-a-Car/Car-Anti-Theft-Devices/
7. http://www.besafe.in/antitheft.html