Anti-Theft System for Vehicles

Shruthi Chandrakumar[1], Anusuya K V[2], Harini C[3]
{18l149@psgtech.ac.in[1], kva.ece@psgtech.ac.in[2], 18l117@psgtech.ac.inaddress[3]}

Department of ECE, PSG College of Technology, Coimbatore, India[1,2,3]

Abstract. Over the years, the number of people who own a bike has considerably enlarged. Statistics show that there are around 21.8 million bike sales in India. The depressing fact is that motorbike theft has become so widespread, not just in India, but in different parts of the world. It turns out that, about 1.65 lakh bikes are stolen each year in India alone. Since a thief doesn't need to break into a motorcycle as it is done for a car, motorcycles are more vulnerable to theft than other vehicles. The present day's security offers little in terms of safety for the vehicles. However, some anti-theft devices can serve as both deterrents and theft prevention. The cost of an anti-theft security system is extremely expensive and hence an effective alternative is required. In this paper, an anti-theft system is developed to provide communication between the owner and the vehicle. This permits the user remote access to control the vehicle's fuel flow. The proposed system is smart enough to detect trusted owners.

Keywords: Antitheft, fuel flow, motorbike, remote access, security system

1 Introduction

For many people, a two-wheeler is one of the expensiveassets. These people are often among the most vulnerable, and the impact of the loss of their bike can be devastating. According to a survey, 50% of victims feel that investigation on this crime is poor, while those engaged in these thefts considerit as low risk in terms of being caught. So far, only 3% of stolen bikes are recovered. The existing technologies such as theftalarms, GPS tracking systems prevent vehicle theft up to acertain extent. But in some circumstances, the theft alarm turnson unnecessarily; hence people do not pay much attention to it. The proposed system monitors the parking mode of the motorbike. If it is, when a key is inserted, it checks the validityof the key. If the key is duplicated or it is any other metal, then the fuel flow to the ignition tank is shut down. Simultaneously, the image of the intruder is captured and processed. In case, if it is the owner himself, then there will be fuel flow from tank to ignition. Else, it raises an alarm to create awareness to thepassersby. Also, it sends a notification to the owner   via the IFTTT web service. Hence, it is proposed to develop   a responsive Anti-Theft System for vehicles. It detects anyintrusion in the vehicle and alerts the owner. It also receives theresponse of the owner like starting/stopping the vehicle and performing the necessary actions accordingly.

2 LITERATURE SURVEY

According to the National Crime Records Bureau (NCRB), in the year 2019, almost 674,414 vehicles were stolen in India.
A lot of research work has been done in this area and the following is the survey done. Anti-Theft Vehicle Security System (ATV2S) has been designed and implemented utilizing a sensor-network system that employs Global Positioning System (GPS) and Global System for mobile communication (GSM) technology to track the vehicle but it is not very effective [1]. In [2], the system designed is that the PIC16F877A microcontroller stores valid smart card unique RFID numbers. When the right smart card is scanned, the microcontroller sends a signal to the electromagnetic relay to close and will allow the user to start the vehicle. If an invalid smart card is scanned, the system allows the user to try three times and if failed, the microcontroller commands the GSM module to call the owner of the vehicle and the phone number is stored in the microcontroller.

In paper [3], an ARM 7 processor-based LPC2148 controller system is designed. The system consists of a smart card capable of storing the fingerprint of people used in the authentication of vehicles. These vehicles will consist of a cardreader to read the card data and a fingerprint module. To start the car, first, the card must be inserted in the card reader and the fingerprint is scanned. If the scanned fingerprint matches that in the license card, the system ignition turns ON, else the ignition will be in OFF position.

A paper [4] on real-time vehicle monitoring systems presented by P. Muruganandham et al., for the applications which require ceaseless area information of the car. For getting the autonomous positioning system that can transmit the regional data logically, active structures are generated. The device is a combination of a GPS/GSM module and an SMS feedback system. The main hardware in the car unit is the GPS/GSM module and a remote tracking server.

A paper on the vehicle hostile to burglary system [5] introduced by Ganesh G.S.P et al.., a combination of several steps of insurance with one supplementing the other, as altered to the regular against robbery system, where a specific system is just being utilized. This is one of the simplest vehicle protection systems which work only using GSM technology apart from GPS. The user can turn on and off the vehicle just by SMS and the details of the vehicle would be sent to the nearest base station. Though the simple structure, it consumes more time to operate the whole operation.

A constant automobile monitoring system introduced in paper [6] uses a Real-Time automobile monitoring system that obtains the automobile's area, the engine of the automobiles locked while unauthorized access attempt is found. The gathered data containing automobile location and access time is then sent to the user's phone. The system has no specific input method.

In paper [7], a novel radio recurrence distinguishing proof (RFID) based vehicle immobilizer system, which includes low hacking likelihood, while saving the wellbeing of the travelers is proposed. The immobilizer utilizes the dynamic RFID innovation where the tag is created with nearly huge character sets. The accepting unit is incorporated into three control circuits in the vehicle, to be specific, start circuit, control unit, and programmed adapt evolving system, empowering it to convey the vehicle speed down to zero. The counter robbery auto security system proposed here was tried under various climate conditions and conceivable flag mutilation circumstances to confirm its dependability.

In our proposed system, the Raspberry Pi 3B+ microcontroller is used. A few of the important features supported by our system are alerting the owner by notification about the theft attempt, allowing the user to control the system remotely, use of face recognition to authenticate the fuel flow.

3 PROPOSED METHODOLOGY

Initially, there is no fuel flow from the fuel tank to the ignition system. To start the vehicle, the key must be inserted in the key socket which in turn produces vibration. The vibration sensor detects the

vibration and sends a logic low signal to the microcontroller. The microcontroller then enables the transponder in the key, to check the originality of the key. The Transponder chip transmits the digital security code through the RF 433MHz transmitter. The radio frequency receiver receives the digital code and sends it to the microcontroller. The vehicle's fuel system cannot be activated when the code in the key and that already stored in the microcontroller mismatch. Hence, it prevents the engine from starting without using the vehicle's authorized key thus ensuring double security.

When the digital code matches, the solenoid valve is activated to open the fuel flow. Else an image is captured by the camera to perform face recognition. If the person is identified as the owner of the vehicle (in case the key is lost), then the solenoid valve is activated. For the detection of an unknown person, an alert message is sent to the owner's mobile phone through the IFTTT server. The owner can also send a response back to the microcontroller regarding his confirmation to start the vehicle. The owner makes use of Google assistant to send a response back to the microcontroller which in turn receives the command and processes accordingly.

One may also use the remote key to access the vehicle. So, the receiver is always active. Here a push button switch is used as the remote key. When the switch is pressed, the transmitter transmits the digital security code. If the code is correct, then fuel flow is allowed. Since all remote car keys transmit the security code at 433MHz, no action is taken, for the mismatch of the security code.

In case of any intrusion, the camera captures the image for face recognition. IFTTT server alerts the owner of an unauthorized person trying to steal the vehicle. A solenoid valve is used to open/close the fuel flow of the vehicle. Raspberry Pi is programmed to provide the necessary control signals to all modules used in this system.
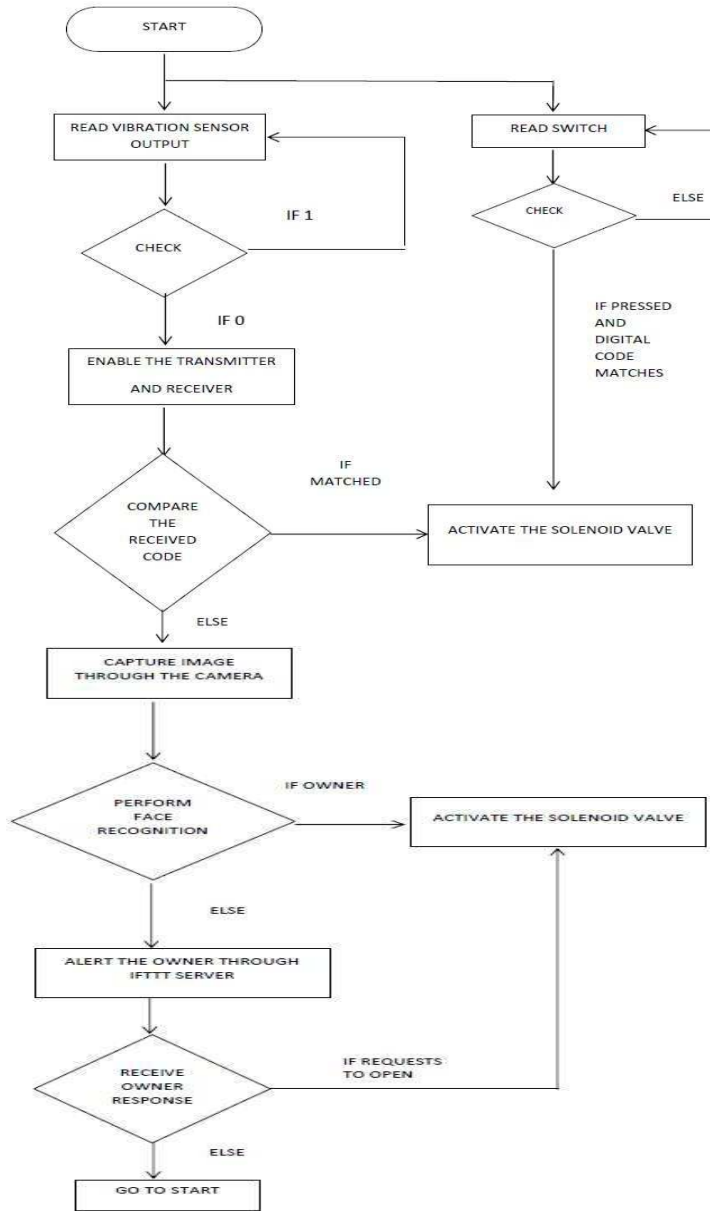
Fig. 1. Operation of the proposed system

4 HARDWARE DESIGN

Figure 1 illustrates the flowchart. During the insertion of the key, vibration is produced in the key socket and is captured by the vibration sensor. The transponder is a pair of RF transmitters and receivers used to transmit the digital code in the key.
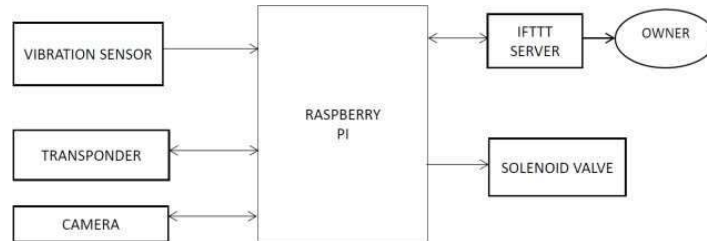

Fig. 2. System Block diagram

a.   IMPLEMENTATION

This section explains various modules used for the implementation.

b.   Raspberry Pi 3B+

RASPBERRY PI 3B+ development board in PI series is used as the overall controller of the system. CPU is a Quad-core 64-bit ARM Cortex A53 clocked at 1.2 GHz. It also hasa GPU of 400MHz Video Core IV multimedia and 1GB LPDDR2-900 SDRAM (i.e., 900MHz) memory. USB ports:
4. Video outputs: HDMI, composite video (PAL and NTSC) via 3.5 mm jack. Raspberry pi is programmed to provide the necessary control signals to all modules accordingly.

Fig. 3. Raspberry Pi 3B+

c.   Vibration sensor

A fake key cannot rotate freely in the key socket as freely as the genuine key. This results in acceleration change and can be detected by the vibration sensor. The output of the vibration sensor is connected to the linear actuator and the cameras capture the image of the intruder.
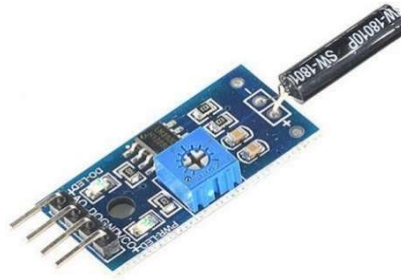
Fig. 4. Vibration sensor module - SW420

d. RF transmitter and receiver module (433MHz)

Conventional car remote key uses a transponder chip to transmit an alphanumeric security code to deactivate the engine immobilizer. The transponder has a transmitter and responder. The Engine Control Unit (ECU) of the car sends an electronic message to the key when the ignition is turned on or run. The car starts only when it receives the correct message back from the transponder. A similar method can also be applied to identify the originality of the physical key. Here, vibration sensor output triggers the transponder in the key. RF transmitter and receiver are used as a replica of a transponder chip.
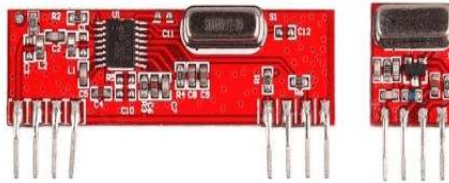

Fig. 5. Transmitter and receiver module 433 MHz

e. Solenoid valve

A solenoid valve is an electro-mechanical valve commonly employed to control the flow of liquid or gas. They are commonly used to shut off, release, dose, distribute or mix fluids. Solenoids generally offer fast and safe switching, long service life, high reliability, low control power, and compact design. This solenoid valve is connected to the circuit through the relay. The common and NO (normally open) from the relay are connected to it. When the relay gets the signal from the CPU, it forms a closed circuit with the solenoid valve, thus allowing the coil to energize which in turn lifts the plunger and opens the fuel flow.

Fig. 6. Solenoid valve

f.   Face recognition

The three important steps in building a face recognizer are Face Detection and Data Gathering, training the Recognizer, and performing face recognition. Python programming is used to program a face recognizer using modules such as OpenCV, pillow, and Haar cascade classifiers. When tampering is detected in the vibration sensor, it activates the camera. The camera captures the image of the intruder and sends it to a raspberry pi. It compares the image with a preexisting dataset that contains an image of the authorized persons. This enables the actuator to open the fuel flow path, thereby bike starts. This case is included to tackle problems like loss of key, else alert notification is sent to owner's mobile

g.   IFTTT Web Service

IFTTT derives its name from the programming conditional statement "if this, then that." It is a software platform that connects apps, devices, and services from different developers through chains of conditional statements to trigger one or more automation involving those apps, devices, and services. The conditional chains are called applets. This service is offered in freeware, subscription, and enterprise versions.

From the IFTTT web service, the Notification applet is used to send an alert to the owner's phone in case of any intrusion detected. Next, to receive a response from the owner, the Google Assistant in the mobile phone can be used. Here, it is set in such a way that if the owner says "allow the bike to start" through the Google Assistant, it will be received by the Adafruit IO applet which stores the value as 1 when the right response is received. This value indicates a high/low signal to be sent to the pi which in turn controls the opening of the fuel flow.

5 RESULTS

Fig. 7. Hardware setup

CASE 1: Normally in a key, the transponder transmits a certain frequency, and for a particular key, there will be a particular code. Here, we have used a 433MHz RF Transmitter Receiver module as a replica of the transponder chip circuit. The transmitter transmits a particular code that is received by the receiver and it is checked with the already programmed code. When this digital code is matched, then it implies that no intrusion is detected. Hence a high signal is sent to the GPIO 27 of the Raspberry Pi which in turn opens up the solenoid valve, thus allowing the fuel flow.
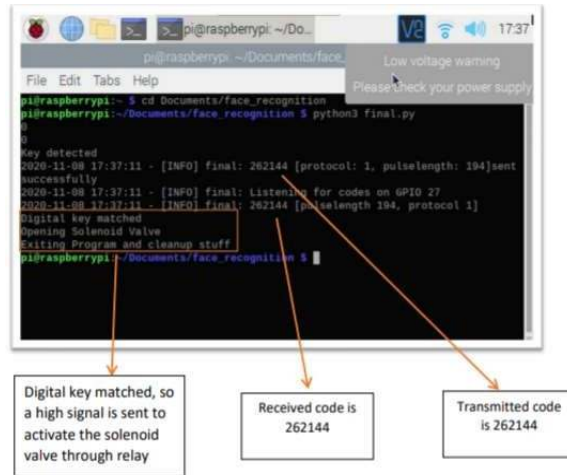

Fig. 8. Output of case 1

CASE 2: In this case, when a fake key is used, a different code will be transmitted. This code received will be checked with the already programmed code. Since the code does not match, this implies that an intrusion is detected. So, the system now performs the first level of verification i.e., face recognition. The camera captures the image of the intruder and it is compared with the existing dataset. When the right person is detected, the system identifies them as an authorized person, and hence a high signal is sent to the GPIO 27 of the Raspberry Pi which in turn opens up the solenoid valve, thus allowing the fuel flow.
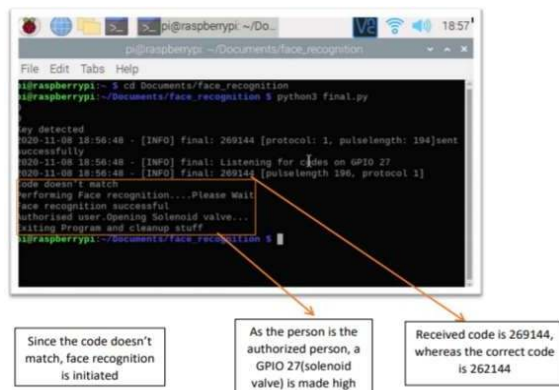

Fig. 9. Output of case 2

CASE 3: In this case, when a fake key is used, a different code will be transmitted. This code received will be checked with the already programmed code. Since the code does not match, this implies that an intrusion is detected. So, the system now performs the first level of verification i.e., face recognition. The camera captures the image of the intruder and compares it with the existing dataset. Here we consider the person to be unknown, so the system identifies them as an unauthorized person. It then proceeds to the second level of verification. At this level, an alert is sent to the owner's phonethrough the IFTTT web server with the message "intrusion detected". The owner can then decide whether to allow the bike to start or not. This response from the user is sent through the Google Assistant feature by saying "allow the bike to start" shown in Figure 12. This response is received by the Adafruit IO service through the IFTTT as in Figure 13 and hence a highsignal is sent to the GPIO 27 of the Raspberry Pi which in turn opens up the solenoid valve, thus allowing the fuel flow.

Regarding the anti-theft system, the owner is notified with an appropriate message in case of any tampering. This **provides security to the vehicle** and the owner can be at peace. Thus, an efficient model of a vehicle with inherent energy generation and anti-theft design is proposed.
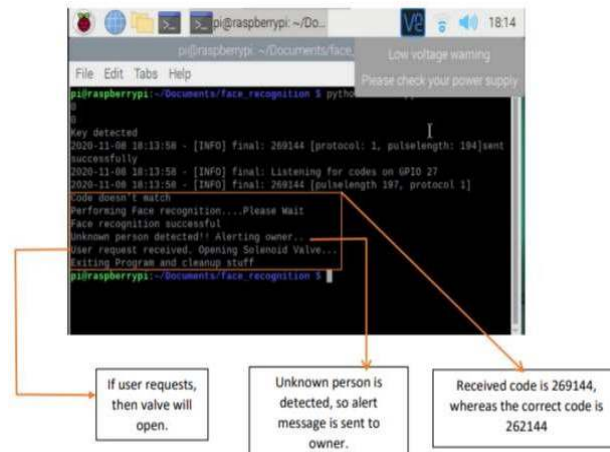

Fig. 10. Output of case 3

6 CONCLUSION

The purpose of developing this system is mainly to introduce an inaccessible and advanced security system that senses any intrusion, alerts the owner, accepts owner's commands, and also responds automatically to a security threat, comparedto existing systems in the industry which merely either track the vehicle or just send information to the user but not take anyaction to prevent the theft. It is also cost-effective. The systemis easy to use and

learn due to its simple message alert feature. Users require no special training to use this proposed system.

As a part of future works, the GPS module can be interfacedand the location can be sent to the user and the system can immediately disconnect the power supply to the engine ignition system if an intrusion is detected continuously more than three times. Also, emergency calling features wherein the police can be notified as well as easy vehicle accessing features for emergency conditions can also be included.

References

[1] K. A. Mamun and Z. Ashraf, "Anti-theft vehicle security system with preventive action," 2nd Asia-Pacific World Congress on Computer Science and Engineering, pp. 1–6, 2015.

[2] A. Z. Loko and A. I. Bugaje, "Usman Abdullahi," Microcontroller Based Smart Card Car Security System"," International Journal of Engineering Trends and Technology, vol. 29, no. 3, 2015.

[3] C. S. Prasad*, U. S. K. M.Tech, D. Y. av M.S., and P. (U.S.A, Eds., Advanced Authentication and Security system In Vehicles", IJESMR, 2016.

[4] P. Muruganandham and R. Mukesh, "Real-Time Web-Based Vehicle Tracking Using GPS"," World Academy of Science, Engineering and Technology, pp. 61–61, 2010.

[5] G. S. P. Ganesh, B. Balaji, and T. A. Varadhan, "Anti-theft tracking system for Automobiles," IEEE International Conference on AntiCoun- forfeiting, Security, and Identification (ASID), pp. 17–19, 2011.

[6] Y. A. M. A. Elahi, M. Malkani, and Fraz, "Design and Implementation of Real-Time Vehicle Tracking System," in 2nd International Conference on Computer, Control and Communication, 2009.

[7] S. Bana and D. D. Kaur, "Fingerprint Recognition using Image Segmentation," International Journal on Advanced Engineering Sciences and Technologies", no. 5, pp. 12–2