Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Real Time Vehicle Security System Using Face Recognition and Finger Print

B. Ajay Bhargav[1], D. Hari Krishna[2], U. Syed Abudhagir[2],
M. Tech Student[1], Associate Professor [2],
B. V. Raju Institute Of Technology, Narsapur-502313

Article Info
Page Number: 1731 – 1744
Publication Issue:
Vol. 71 No. 3s2 (2022)

Abstract: - As the vehicles are precious things they need to be protected precisely, no matter how secure the parking area is there is always a possibility of vehicle theft. Unlicensed drivers are the main cause of fatal accidents on the roads. By taking these points into consideration, a vehicle safety and security system is designed. This proposed system consists of raspberry pi board, USB camera, fingerprint module, alcohol sensor, relay with a motor. When a person enters in to the vehicle, the system will check the driver license by facial recognition system which contain eigenface algorithm. The camera captures the image of the driver and compares it with the existing database. If it matches, the system will move further for fingerprint verification. The fingerprint module is the key for the vehicle ignition. If the fingerprint matches with the existing enrolled dataset, then ignition of the car is turned ON. If the person face is not matched fails in facial recognition the system will use Simple mail Transfer protocol SMTP server and sends an email alert to the vehicle owner and the buzzer will ring. If the person fails in fingerprint verification or in alcohol detection, then the vehicle ignition will not be turned ON, buzzer will ring. The experimental results shows that at a threshold value of $3.2*10^3$ and $3.5*10^3$ the accuracy of the proposed vehicle security system is 98.3% this is achieved in different illumination conditions

Keywords: Eigen Face recognition, Haar cascade classification technique, simple mail transfer protocol (SMTP), fingerprint module.

Article History
Article Received: 22 April 2022
Revised: 10 May 2022
Accepted: 15 June 2022
Publication: 19 July 2022

I. INTRODUCTION

In recent years, the vehicle sector has increased in popularity all around the world. Car crime, on the other hand, has increased dramatically. Physical keys, identification cards, and passwords/patterns are presently used to operate most autos. The growth of Internet of things (IoT) and other embedded mechanisms, on the other hand, is continually strengthening vehicle security measures. The driver's ownership and police workstation laws are the basis for these enhancements. They are obsessed not only with the theft of automotive items, but also with the loss of automobiles and the car owner's personal security concerns. There had been a wide range of fingerprint recognition identification and verification methods available. Fingerprints, facial features, and the iris were all used for security purposes in the past. Facial recognition is a typical biometric technology for vehicle security and burglar alarms that is based on the human face attributes and may function in a variety of situations.

As a result, majority of image processing algorithms are designed with a greater discriminating rate in mind. Furthermore, the face recognition method necessitates certain sophisticated computations; this study develops a dependable vehicle safety and security device. This technology turns images captured with the car's digital camera into picture

representations, allowing it to instantly detect and recognise faces. Face recognition accuracy is improved by combining the Ada Boost technique with the Feature Matching classifier. The suggested system then uses Principal component analysis (PCA) techniques to recognize the faces of drivers. The goal of this research is to use a combination of IoT technologies and sensors shielding to implement the proposed face detection and classification approach for vehicle surveillance equipment. To achieve the notion, the system employs a Raspberry Pi device B+ simulation platform and a smartphone. A alcohol sensor, fingerprint scanner, control electronics, and USB camera may all be connected to the Raspberry Pi 3 Model B+ development board.

A Raspberry Pi Type B+ can also be configured to send messages to a specific address, along with download and transmit files to a Synchronous server for real-time video analysis. When this technology identifies an illegal person's face, it analyses it and communicates the image across IoT networks to the vehicle's owner and/or a divisional police.

Existing security techniques

Various anti-theft solutions have been developed during the previous few decades. An Engine Management Unit is connected to the Insight Circuit Board with sensors within the vehicle electronic control unit (ECU) in the vehicle communication bus. The bus communicates with other automobiles, roadside transit, and mobile phones through wireless interfaces. Due to the data latency plus network delays, the system is unable to grasp dependable secure automotive communications. Other solutions include an engine immobilizer that is developed exclusively for in-vehicle use. If the component is illegally moved to another vehicle, the appliances' functionalities will be disabled.

This solution has the disadvantage of requiring the usage of a secure processing unit as well as card reader chips to store the Groups Identification Number. To track the car's position and current location, the sophisticated system uses the Global Navigation Satellite System (GNSS) or a Global Positioning System (GPS). The position in pattern supplied by the GPS device may be viewed using Google Earth. The major drawback of utilizing GPS would be that the signal might be reduced, and if the sky is severely obscured, the receiver equipment will be unable to provide location. Rainfall, mist, and snowfall are some of the other factors that affect it. Radio frequency identity (RFID) is employed in the Innovative Computerized Anti-Theft System [ICAT]. RFID cards are used to give secure access. Keyless RFID devices are easy to steal, which is a drawback. Furthermore, the key may malfunction if it comes in touch with a metallic item.

II. LITERATURE REVIEW

The IoT technology performs complex processes that aid in the prevention of automobile theft. Lot of research had been done on automobile security devices in order to give the finest techniques not only for vehicle content theft, but also for vehicle loss and the personal protection needs for the car's head.

Depending upon their efforts, they checked and created automobile systems that rely on "Biometric Authentication" kinds such as eyes, finger, facial recognition systems, and so on. Several recent suggestions for relevant cooperation are discussed in this section.

The authors in paper [1] proposed a car ignition system which recognizes the authorized person using finger print sensor and RFID sensor. This system is integrated into the vehicle. They used finger print authentication as a key to start the car ignition. In case, if the fingerprint sensor fail's to work, then the RFID tag is used to start the ignition of the car. By this alternative, RFID authentication system will improve the car security system.

The authors in [2] presented GSM based vehicle security system, a random OTP generation method is used to secure the system. The GSM module is used for communication between the vehicle and authorized person. They used STM32 controller that generates random OTPs and send to the registered Mobile Number. If the user enters the correct OTP then the car ignition is turned ON. This Random OTP generation method will improve the car's security system.

The authors of paper [3] proposed a vehicle security system which is used to monitor and theft control mechanism. This system is designed using Arduino which is interfaced with accelerometer which is used to detect the accident information and the location information is acquired from GPS module. This information was sent through SMS to the owner by using GSM module. The owner can also send a predefined SMS to stop the ignition of the car.

In [4], the authors proposed a smart ignition system for automobiles. This system has a biometric and safety system. The Finger print module is used for verifying the authorized person and an alcohol sensor is used to detect the drunken person in the vehicle. If unauthorized person enter into vehicle or a drunken person tries to drive the vehicle then the information is sent to the owner along with vehicle location information.

The work of authors [5] proposed a vehicle security system based on face reorganization and automatic license plate recognition method the system will protect the vehicle. For face reorganization the local binary pattern histogram (LPBH) is used. By a surveillance camera a dataset is created when a vehicle enters the parking area while leaving the parking area the face and the license plate of the vehicle is recognized. So the system identifies whether the correct person is taking out the vehicle from parking area or not. The accuracy of face reorganization technique is 96% in the developed system.

The authors in [6] vehicle ignition system based face reorganization is developed. This system will control the vehicle ignition based on the presence of the driver inside the car. This system contains a camera installed in the car which recognizes the face of the vehicle owner if unauthorized person tries to access the vehicle the ignition is turned OFF this system uses fisher face algorithm to recognize the faces. The accuracy of face reorganization technique is 83.04% in the developed system.

The work in paper [7] a vehicle theft detection system is developed which uses the face recognition system. In this system a principal component analysis (PCA) method is used to recognize the faces of unauthorized person and refuse the access of vehicle and send's the location information and image of the unauthorized person of the via a Multimedia Messaging Service (MMS).

So in the existing systems they used Radio frequency identification (RFID) technology for driver license authentication the problem identified here is driver has to carry the license and has to authorize manually. In the proposed system a face reorganization method is used for

driver license authentication and a storage device is present in this system which stores the images of the drives of the vehicle.

III. EXISTING SYSTEM

In this vehicle security system an RFID and fingerprint sensor based car safety system is designed, a microcontroller ATmega328p is used to process the data. This system can recognize the authorized and unauthorized person, based on RFID and fingerprint sensor. In this existing system an RFID reader and RFID tag is used for identifying the authorized person.

If the wrong tag is detected, the system will deny access and the siren will ring. The Other tags can also be added and deleted using a master tag. The stored tags information will not be lost even if the system is turned off. Because it stores the information in the EEPROM. The wipe key is used to delete the stored tags information which is present in EEPROM. The maximal write cycle of an EEPROM is 100,000. When you initially begin the task, it will ask to provide a master tag, which will be whatever tag you scan at the beginning of the system. The primary tag will act as a programmer, enabling you to add and delete tags as needed.

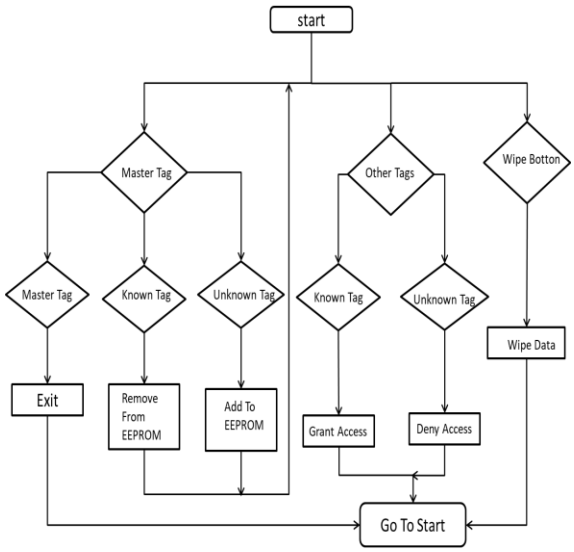


Fig 1 RFID based vehicle security system

An additional tag is needed other than the master tag. Once the master tag is created, by scanning the master tag this will put the machine into programming mode. In this mode, by scanning the tags it's information is added into the EEPROM so that whenever tag is keep near to the RFID reader the information inside the tag is scanned and the ATmega328 microcontroller will compare the read information with the existing information which is present in the EEPROM of RFID reader if the read information matches then the vehicle ignition will turn ON. The data is shown on the display, and the buzzer will ring if the data is not valid.

To reset the system, click the restart button just on Arduino and afterwards long press the wash button for 10 seconds. This will remove all data from the EEPROM, including the owner tag.

IV. PROPOSED SYSTEM

In this proposed vehicle security system. A face recognition algorithm is used to verify the license of the person for this purpose a camera is used, finger print sensor is used as a key of the vehicle, a SMTP server is used to send email alert, an alcohol sensor which identifies whether the person in the vehicle is drunk or not, a buzzer is used to alert the owner regarding unauthorized person as well as for alcohol detection and a DC Motor is used for indication of vehicle ignition ON/OFF. The raspberry-pi 3 model B CPU is used to process the data which is read from the different peripherals attached to it, and it performs necessary actions based on the read information. The proposed system block diagram is mentioned in the figure-2.

In this system initially a trained dataset of images are created using camera and stored in the SD card, and the finger print of the owners of the vehicle are scanned and stored in the memory. This complete system is installed in the vehicle. So now when an authorized person comes in front of the camera it captures the image and starts comparing with the existing dataset if it matches with the existing dataset. The system algorithm further move towards biometric verification, using finger print sensor the person finger print is scanned and compared with the existing enrolled data. If it is matched, then the system algorithm while perform the alcohol check using alcohol detector. If the alcohol is not detected then the vehicle ignition is turned ON.

If the person face is not matched with existing dataset then an image of the person is captured and sent to the owner by an E-mail, so that the owner can identify the person in the vehicle and a buzzer will ring as well as vehicle ignition is turned OFF.

If the person passed with the face reorganization authentication method and finger print authentication method and fail's at the alcohol detection then the vehicle ignition is turned OFF.

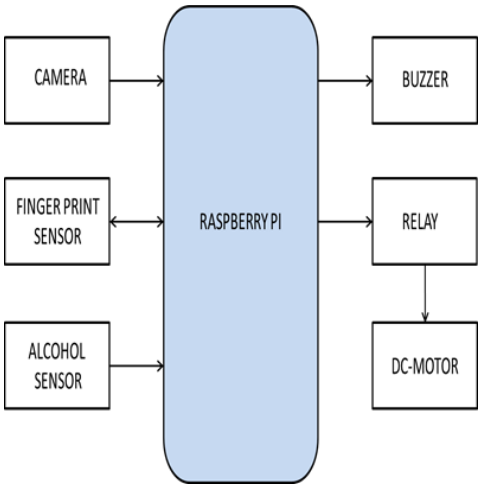


Fig 2: Block Diagram of Vehicle Security System

4.1 Hardware Design

The physical design of the proposed vehicle security system embedded with a Raspberry Pi model B+ microcontroller, finger print module, alcohol sensor, USB 3G Broadband flash Pi USB video camera, Micro SD Card, a relay which control's the DC-Motor and power source for the system are required.

Raspberry Pi version 3 Model B+: This version has some advantages over others. This version has a high number of Universal serial bus ports as well as GPIO pins. Furthermore, runs on the "Raspbian" operating system, which has excellent hardware integration and a graphical user interface with programming tools. It has a processing speed of 1.2GHz, so the system will work efficiently while processing the data. An internet connection is required for this project in order to send email alert with the help of simple mail transfer protocol (SMTP) to the owner as Raspberry pi has Wi-Fi based-network protocols by this the internet connection is established to the controller.

USB Camera: This is the camera that was designed exclusively to Raspberry Pi version 3 Model B+. Device was connected to the Raspberry Pi version 3 Model B+ through connectors, the camera consists a high-performance image processing chip. So that it can capture the images and process the image data as fast as possible. The camera captures 5MP images with a resolution of 640X480 pixels.

Module for Finger Printing: The R305 is a fingerprint sensor module that is used in biometrics for fingerprint detection and verification for security system. This device is interfaced with a UART protocol with a baud rate of 9600 with raspberry pi CPU. The fingertip have different ridges this ridges are identified by finger print sensor and mapped inside the memory as a dataset when the person keeps his/her fingertip on the fingerprint scanner it takes a digital photo and tries to compare it with the existing dataset if it matches it identifies the person has authorized person.

MQ3 Alcohol Sensor: MQ3 sensor is one of the most widely utilized in the MQ sensor series. It is a Metal Oxide Semiconductor (MOS) sensor. Because sensing is based on the change in resistance of the sensing material when exposed to alcohol, metal oxide sensors are also known as Chemiresistors. Alcohol concentrations can be detected by using it in a simple voltage divider network. The Pi's 5V dc supply pin was used to power it directly. Its output was attached to the programmable GPIO pin as an input.

DC-Motor Relay with: The relay is a electronic switch that open and close the circuit. It is a single channel relay that operates with a voltage range of 5Volts responsible for controlling the DC-motor. This DC-Motor is used to indicate the ignition of the vehicle.

Buzzer: The buzzer consists of a piezoelectric ceramic element and metal plate when current is applied to the buzzer it causes the ceramic disc to contract or expand this causes the surrounded dic to vibrate so the sound is produced. This device is responsible to make a sound alert when an alcohol is detected or else unauthorized person is identified.

4.2 Software Design

A) Initialization of the System: The system is initialized at the beginning, in this stage the raspberry pi CPU board will initialize the peripherals like buzzer, relay, alcohol sensor, fingerprint sensor and USB camera which are interfaced with the system. Simply it means that the raspberry pi CPU will organize the system resources. This is done by importing python libraries files and packages which are preconfigured to assist in the proper operation of the interface modules.

B) Creating a Trained Dataset:

For creating a dataset of images of the authorized person.

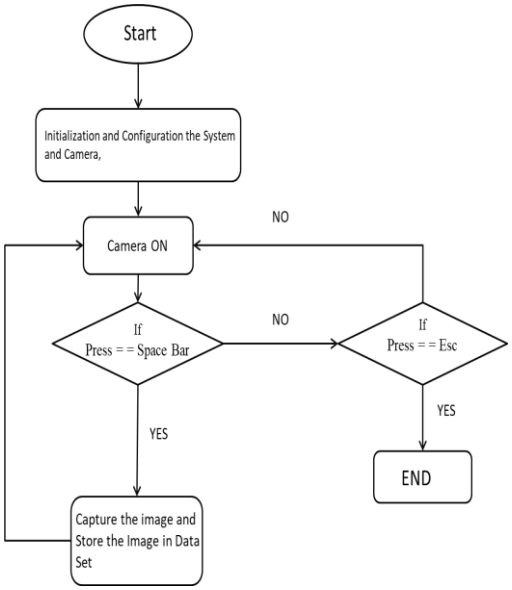


Fig 3: Creating Dataset of Images

Step1: The system gets initialized, and configures the camera with the USB port of the raspberry pi CPU.
Step2: Now the camera is turned ON based on the key pressed the further process is done.
Step3: If the key press is "space bar" then the image is captured and stored in the memory. This process is continued till required dataset is created. If the key press is "Esc" then the program will terminate and camera is turned OFF.

C) Face Detection and Recognition:

Face Detection: To recognize a face in a image first the face need to be detected in the image. The Haar cascade is an object detection algorithm used to identify faces in an image. This Haar cascade is machine learing based approach, where a lot of positive and negative images are used to train the classifier. The positive images are the one which the classifiers need to identify. The negative images are the one which do not contain required object in the image.

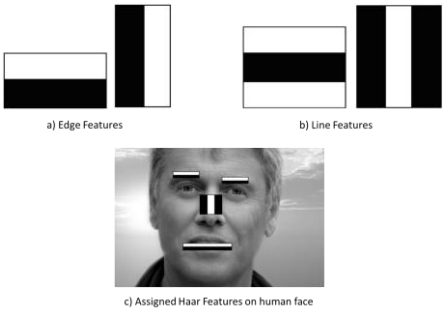
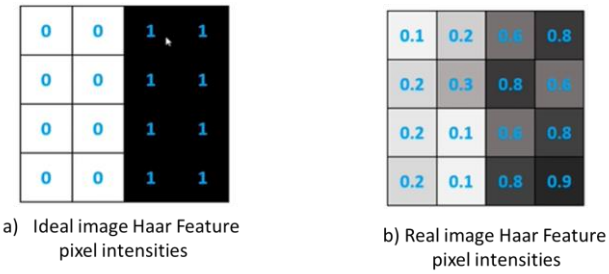


Fig 4: Haar Features Extraction

In haar feature extraction method the haar features are assigned to every single important feature of the human face, so by using edge and line features which are composed with black pixels and white pixels. Now in a gray scale image every single pixel has its own intensity level ranging from 0-1 here 0 means white and 1 means black so it is able to assign a value for each pixel based on its intensity. now haar features can be assigned to the most relavent

features on the human face. The algorithm can detect the facial features like eyes, nose, lips etc.



a) Ideal image Haar Feature pixel intensities

b) Real image Haar Feature pixel intensities

Fig 5: Haar Features Extraction using Pixel intensity

In the ideal image haar feature the white pixels are represented as 0's and black with 1's. In the real image haar feature the pixel intensity vary from 0 to 1. The viola-jones algorithm will compare how close the real scenario is to the ideal case.

$$\Delta \text{ = Dark - white} = 1/n \sum_{dark}^{n} \mathrm{I}(x) - \sum_{white}^{n} \mathrm{I}(x)$$

In this algorithm the white pixel intensities are summed up i.e. 0.75 and also the black pixel intensities are summed up i.e. 0.18 , and by findings the difference between the back and white pixel values as a result **Δ** for Real image Haar-Feature is 0.75 – 0.18 =0.56 and the result **Δ** for ideal image Haar-Feature is 1. If the value is closer to 1 the more likely we found a Haar-feature is matched. Note that the values 0 and 1 will not obtained as they are threshold values.

Face Recognition: The training set of images are converted into a set of Eigen faces E. so after that the weights are calculated for each image of the training set and stored in W. now calculate the weights of the new input image X and store it in $W_{x.}$ calculate the average Euclidean distance D between W and $W_{x.}$ now compare the D with the threshold value Θ. If the D> Θ it is a unknown image D< Θ then it is a known face.

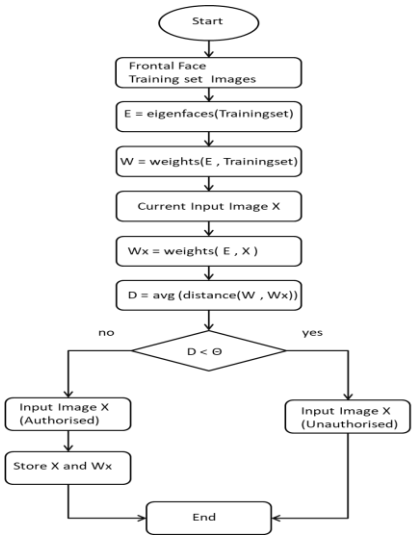


Fig 6: Face Reorganization Algorithm

For recognizing the faces of the authorized person of the vehicle an Eigen face algorithm is used the following steps are performed in the algorithm.

Step 1: Take a dataset of images I_1, I_2, I_3……I_m here number of images m=4 with an image size (N x N).

Step 2: convert the normal image I into vector image Γ_I i.e. Γ_1 , Γ_2 , Γ_3,..... Γ_m .

Step 3: Calculate the average of the total images present in the dataset i.e. mean face vector **ψ.**

$$\psi = \frac{1}{M}\sum_{i=1}^{m} \Gamma' i$$

Step 4: Find the difference between the vector image Γ_i and the mean image ψ so here $\Phi_i = \Gamma_i - \psi$, the difference matrix A = [Φ_1 , Φ_2, Φ_3,..... Φ_m]

Step 5: Calculate the covariance matrix C = $\frac{1}{m}$ A A^T with a matrix size (N^2 x N^2). Since the the dimensions of C matrix is big, compute the matrix L = A^T A with a smaller matrix size (M x M). C and L can be related as $\mathbf{u_i} = \mathbf{A}\, \mathbf{v_i}$. where $\mathbf{u_i}$ is the eigenvector of C and $\mathbf{v_i}$ is the eigenvector of L.

Step 6: Calculate the weight of the dataset images by $\Omega_k = u_k^T \Phi_i$ here Ω_k represents the weight of the trained dataset images.

Step 7: Now take a test image Γ_t using $\Phi_t = \Gamma_t - \psi$.

Step 8: Calculate the weight of the test image $\Omega = u_k^T \Phi_t$.

Step 9: Find the distance between the test image **Ω** and dataset image Ω_k which is known as Euclidean distance

$\varepsilon_k^2 = ||\Omega - \Omega k||^2$

Step 10: If the distance $\varepsilon_{k(min)} \geq \Theta$ then the image is unknown face, $\varepsilon_{k(min)} \leq \Theta$ then the image is known face.

D) Fingerprint Detection: The fingerprint module consists of an optical fingerprint sensor with a high speed DSP processor. This fingerprint module is interfaced with the UART protocol with a baud rate of 9600. In this system a bright light is emitted on the fingerprint and capture's the image which is sampled into a binary from 0's and 1's and stored in the memory.

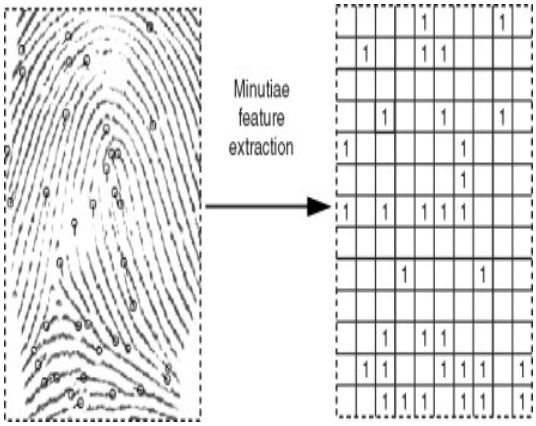


Fig 7: Finger print extraction

The fingerprint contains some ridges and valleys which are unique for very person so that it's easy for identification of the person. As a result, the fingerprint recognizer's job is to discover the fingerprint that is the most similar to the training set images.

E) Creating and sending an email:

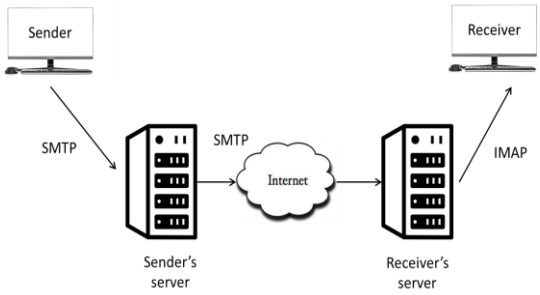


Fig 8: Sending Email Alert

The simple mail transfer protocol (SMTP) is a set of communication guidelines that allows the software to transmit an electronic mail (Email) over a internet. The SMTP is a application layer protocol which requires a connection oriented protocol that is transmission control protocol (TCP) for transmitting the data to the server. This TCP protocol will also provide an acknowledgment is sent back to the sender whether the email is sent properly or not.

The SMTP is a text based protocol that can only handle the messages containing 7-bit ASCII text, so to send the images of the unauthorized person a multipurpose internet email extension (MIME) is required. The MIME enable's the users to send and receive images, video, audio files in the messages.

The sent message is visible on the receiver end i.e. the user mobile/PC who is the owner of the vehicle, here the receiver uses an internet message access protocol (IMAP) to receive the emails.

4.3 Vehicle Security System:

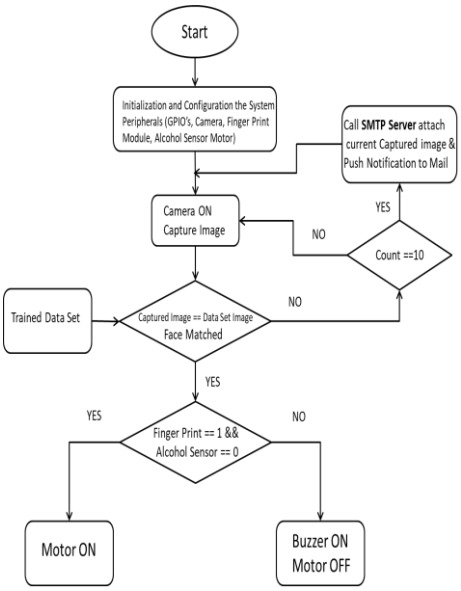


Fig 9: Software design of Vehicle Security System

Step1: The system will initialize and configure the peripherals which are interfaced with the system. The peripherals like buzzer, fingerprint module, alcohol sensor, motor with relay and USB camera are initialized initially after starting the system.

Step2: Now the camera is turned ON and capture's the image, the current image is compared with the existing dataset, if the current image is matched with existing dataset then the system move's to fingerprint verification.

Step3: If the current image is not matched with existing dataset more than ten times's then capture the current image and send an email with a image attachment to the vehicle owner through SMTP server.

Step4: If the person passed the facial recognition system. Then the system will check for the biometric verification, the person need to put the fingerprint on the fingerprint sensor if the current fingerprint is matched with existing dataset then system will perform alcohol detection.

Step5: Now the system check's the status of alcohol sensor if the status is low then the vehicle ignition is turned ON, if the status of alcohol sensor alcohol is high then the vehicle ignition is turned OFF and the system will start ringing the buzzer.

V. RESULTS AND ANALYSIS

The proposed vehicle security system is trained with the person who has a driving license.by collecting 100 photos for each authorized driver that is taught as Eigen faces. Then each approved driver was put through a series of tests. the tests are also done on unapproved person All tests were carried out on Raspberry Pi model 3 Series B+ microcontroller. If the system identifies the authorized person the DC motor will turn ON. Else the motor will turn OFF and with SMTP an email alert is sent and buzzer will ring.

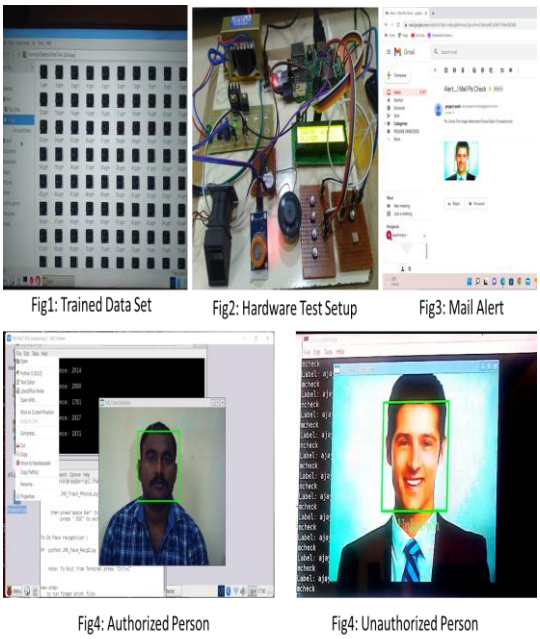


Fig 10 Project Test Results

The accuracy of the proposed system is identified as shown in below

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FN}$$

$$\text{Precision} = \frac{TP}{TP+FP}$$

Where, True negatives (TN): shows the number of normal events is successfully labeled as normal. False positives (FP): refer to the number of normal events being predicted as abnormal. False negatives (FN): Represent the number of abnormal events is incorrectly predicted as normal. True positives (TP): refer to the number of abnormal events is correctly predicted as abnormal.

Threshold	Correct Recognition (CR)	False Recognition (FR)	NOT Recognition (FR)
$2*10^3$	31	30	39
$2.25*10^3$	45	30	25
$2.50*10^3$	50	30	20
$2.75*10^3$	75	15	10
$3*10^3$	90	5	5
$3.25*10^3$	99	0	1
$3.50*10^3$	99	0	1
$3.75*10^3$	95	2	3
$4*10^3$	68	7	25
$4.25*10^3$	86	4	10
$4.50*10^3$	87	5	9
$4.75*10^3$	81	6	13

Table 1: Accuracy of the Vehicle Security system

This proposed vehicle security system accuracy is 98% in brighter illumination and the precision is 0.973 of the system in the proposed vehicle security system.

Technique	Our Dataset	
	Accuracy	Precision
PCA	88.9%	0.965
LBPH	96.2%	0.942
Fisher Face	83.4%	0.913
Proposed	98.3%	0.973

Table 2: Accuracy & Precision of system

VI. CONCLUSION

The proposed vehicle security system uses A face recognition algorithm i.e. Eigen face algorithm with Haar cascade classifier which is used for detecting the face in an image. By these two methods the face of the authorized person is verified. So for this purpose a camera is used, finger print sensor is used as a key of the vehicle, a SMTP server is used to send email alert, an alcohol sensor which identifies whether the person in the vehicle is drunk or not, a buzzer is used to alert the owner regarding unauthorized person as well as for alcohol detection and a DC Motor is used for indication of vehicle ignition ON/OFF. Initially a trained dataset of images are stored in the memory of the SD card when an authorized person comes in front of the camera the image is compared with the existing dataset if the it match's

then the system will move for fingerprint verification if this verification is passed the vehicle ignition is turned ON i.e. the motor is turned ON. If the Face recognition fails more than 10 times a email alert is sent to the owner with an image attachment and buzzer will ring. If both the verifications are passed and if alcohol is detected then buzzer will ring.

This vehicle security system shows that the accuracy is 98% on our dataset under different illumination conditions, when the value of threshold is kept as $3.2*10^3$ and $3.5*10^3$, and the Precision is 0.973 therefore as a result there is an increase in terms of accuracy in vehicle security system.

References

1. Nutan Sawant., Suvarna Sutar., Gayatri Ghumare., and Devendra Itole., "Fingerprint Based Car Ignition System Using Arduino And RFID," International Journal of Advance Scientific Research and Engineering Trends, vol.6, no.5, (ISSN 2021), 2456-0774.
2. Bharagavi Bh., Padmaja B.V.K., Mounika R.L., Manikanta K.V.K.S.S., Chandini N., and Sravani P., "Anti Theft System For Vechicle Security," International Research Journal of Engineering and Technology vol.7, no.6 (ISSN 2020), e-ISSN: 2395-0056, p-ISSN: 2395-0072.
3. Chandra Sekhar Reddy N., Srinivasa Rao M., Raja Rajeswari Thota., and Harini Reddy Y., "Vehicle Security System," International Journal of Innovative Technology and Exploring Engineering vol.9, no.3 (ISSN 2020), 2278-3075.
4. Nouby M. Ghazaly, M. M. A. . (2022). A Review on Engine Fault Diagnosis through Vibration Analysis . International Journal on Recent Technologies in Mechanical and Electrical Engineering, 9(2), 01–06. https://doi.org/10.17762/ijrmee.v9i2.364
5. Shailesh Dhomne., Pratik Bulkunde., Sourabh Lohakare., Ajit Ukey., Snehal Gajbiye., Shubham Deolekar., and Nilesh Shambarkar., "Smart Ignition System in Automobile Industries," International Journal of Innovation Research in Technology (IJIRT), vol.5, no.10 (ISSN 2019), 2349-6002.
6. Himanshu Chaudhary., Gaurav Singh., and Ms. Pratibha Singh., "Automated Vehicle Security System Using ALPR and Face Detection," Journal of Engineering Sciences (JES publication 2020), vol.11, issue no.7, ISSN NO: 0377-9254 DOI: 10.13140/RG.2.2.26163.45603.
7. R F Rahmat., M P Loi., S Faza., D Arisandi., and R Budiarto., "Facial Recognition for Car Security System Using Fisherface," The 3rd International Conference on Computing and Applied Informatics (IOP Publishing 2018), DOI:10.1088/1742-6596/1235/1/012119.
8. Bulla, P. . “Traffic Sign Detection and Recognition Based on Convolutional Neural Network”. International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 4, Apr. 2022, pp. 43-53, doi:10.17762/ijritcc.v10i4.5533.
9. Mr. Raj Rai., Prof. Dinesh Katole., Miss Nayan Rai.,"Survey paper on Vehicle Theft Detection Through Face Recognition System," International Journal of Emerging Trends & Technology in Computer Science(IJETTCS) vol.3, no.1, (ISSN 2278-6856), 2014.
10. Garg, D. K. . (2022). Understanding the Purpose of Object Detection, Models to Detect Objects, Application Use and Benefits. International Journal on Future Revolution in

Computer Science &Amp; Communication Engineering, 8(2), 01–04. https://doi.org/10.17762/ijfrcsce.v8i2.2066

11. Liu Z., Zhang A., and Li S., "Vehicle pro tracking system internet - Of - Things," IEEE International Conference on Automotive Systems and Safety ("ICVES"), Dongguan, 2013, pp. 48-52, doi: 10.1109/ICVES.2013.6619601.
12. Arun Sasi and Lakshmi R. N., "Vehicle Anti-Theft System That is based On An Embedded Platform," IJRET: International Journal of Research in Engineering & Science, vol. 2, no. 9, 2013,
13. P. M. Paithane and D. Kakarwal, “Automatic Pancreas Segmentation using A Novel Modified Semantic Deep Learning Bottom-Up Approach”, Int J Intell Syst Appl Eng, vol. 10, no. 1, pp. 98–104, Mar. 2022.
14. Tahesin A., Prajakta Ch., Vidhi P., Megha G., and Debajyoti M., "An Attempt to Develop an IoT-based Vehicle Security System," 2018 IEEE International Symposium in Smart Communications Systems (iSES) (Formerly iNiS), 0-7695-6618-9/18/31.00, 2018 IEEE, DOI 10.1109/iSES.2018.00050.
15. Jian X. and Haidong F., "A Low-cost Easily deployable Framework for Embedded Car Security Security System," IEEE International Conference on Communication, Sensing, and Control, Okayama, Japan, March 26-29, 2009.
16. Shruthi K., Ramaprasad P., Ray R., Naik M. A., and Pansari S., "Design of anti-theft car monitoring system with a smartphone application," 2015 "International Conference on Information Processing," Pune, pp. 755-760. doi:10.1109/INFOP.2015.7489483.
17. T. D. Narayan and S. Ravishankar, "Face Detection and Recognition Using the Viola-Jones Algorithm and the Fusion of LDA and ANN," IOSR Journal of Computer Science and engineering (IOSR-JCE), 18(6), PP 01-06, 2016.
18. K. S. Kumar, P. Shitala, B. S. Vijay, R. C. Tripathi, "REAL TIME FACE RECOGNITION USING ADABOOST IMPROVED FAST PCA ALGORITHM," International Journal on Artificial Intelligence and Applications (IJAIA), 2(3), July 2011.
19. Shaik M. A. et al., "An Inexpensive Secure Authentication System That relies on a Novel Facial Structure," IJETT, 4(9), 2013.
20. Mohammad D., Amin A., and Olivier D., "Face Identification Using Viola and Jones Method and Neural Networks," International Conference on Information and Communications Research (ICTRC2015), pp. 40-43, 978-1-4799-8966-9/15/31.00, IEEE 2015, 978-1-4799-8966-9/15/31.00, IEEE 2015.
21. Garg, K. . (2022). Beltrami’s Conjecture. International Journal on Recent Trends in Life Science and Mathematics, 9(2), 33–40. https://doi.org/10.17762/ijlsm.v9i2.133
22. Ahmed A. E., "Internet - of - things Eflcient Tamper Detect Mechanism for Healthcare Application," International Journal of Network Security, vol. 20, no. 3, pp. 489-495, May 2018 (DOI: 10.6633/IJNS.201805.20(3).11).
23. Siddarth R., P. Dattatreya, and N. Sadique, "Face recognition using PCA and LDA: Analysis and comparison," IEEE International Convention on Advances in Emerging Technology in Communication and Computing, pp. 6-16, 2013.