Vehicle Theft Detection Using Face Recognition

Prof. P.R. Shahane[1],Subhashi Gupta[2], Rajat Shrivastav[3], Vignesh.S[4], Sushant Singh[5]

[1]Professor, Dept.of Electronics and Telecommunication Engineering, Sinhgad Academy Of Engineering, Pune, Maharashtra, India
[2,3,4,5]Students,Dept.of Electronics and Telecommunication Engineering, Sinhgad Academy Of Engineering, Pune, Maharashtra, India

---***---

Abstract – *Now-a-days number of vehicles can be seen on roads. Most people in this modern age prefer to have at least one vehicle for themselves or their family. With the invention of strong stealing techniques, owners are in fear of having their vehicles being stolen from common parking lot or from outside their home.Face Recognition concept is one of the successful and important applications of image analysis. It's a holistic approach towards the technology and has potential applications in various areas such as Biometrics, Information society, Smart cards, Access control etc. This concept of facial recognition can be used for vehicle security as well. The use of vehicle is must for everyone. At the same time, protection from theft is also very important. Prevention of vehicle theft can be done remotely by an authorized person. This can be done by recognizing the face of the authorized person to unlock the engines. In case of any theft, the system will not let the engines start and it will send a request to the owner through a application in the pre installed system of the vehicle which will then depend on the owner to let the driver unlock the engines by sending back the system a pass code. The main advantage of the application is the wider range of transmission and reception over the internet which will help to notify the authorized person being anywhere in the world.*

Key Words: **Image processing, PCA algorithm, MQTT protocol, Android application, Theft detection.**

1.INTRODUCTION

To ensure security of a vehicle to a greater extent, the system in the vehicle has to be upgraded technologically. At present, people are buying vehicles that are technologically futuristic with more options for comfort and safety. For once, comfort of the vehicle can be put hold but when it comes to safety then it becomes a crucial factor for the buyer/owner of the vehicle. Safety of the vehicles is challenged when it is tried to be stolen in absence of the owner and that is why many companies and technicians are trying to implement new techniques to conquer the theft of vehicles getting stolen from parking spots of public areas .

1.1 Existing Scenario

With current techniques of lock and alarm in the vehicle does not ensure maximum security. That is why there are many cases of vehicle being stolen from places.

According to some stats, four vehicles were stolen from Delhi every hour in 2017, with the total number of such thefts rising to over 39,000 from 36,702 in 2016. Out of the 39,080 vehicles stolen last year, just over 10% (4053) were recovered by police stated in a report by Hindustan times.

With such less chance of recovery, it is very essential to develop a security system inside the vehicle itself so that it can be secured by the system to a good extent.

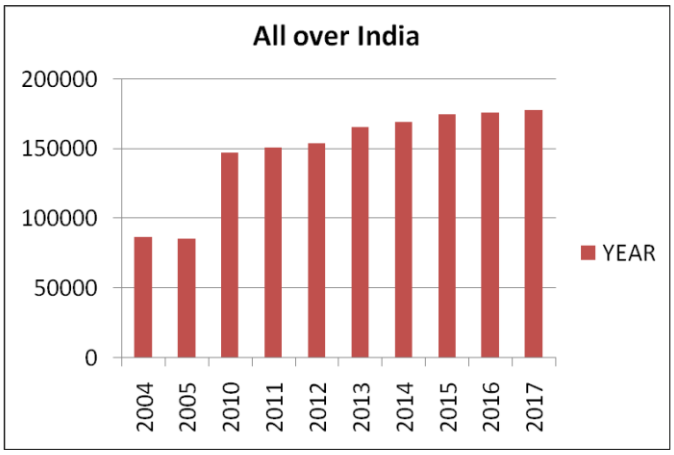


Fig.1. Statistics on Car stealing

1.2 Objectives

- To study Image processing techniques and apply an algorithm for facial recognition.
- To build an android application for the system.
- To develop a Graphical user interface (GUI) in MATLAB.
- To design a automatic system to control vehicle theft using image processing.

2. Literature Survey

The real time extendable emergency system with microcomputer comprises image processing control unit and microprocessor to prevent the parked vehicle from theft. Face detection and recognition system use enhanced algorithm for authentication. Hence ARM 7 microprocessor is used as the control unit in the system. The passive infrared sensor attached to the seat of the driver activates the hidden camera fixed inside the vehicle through the ARM 7 microprocessor control of the microcomputer once the intruder enters the car. The camera acquires the image of the person inside the car fixed in an appropriate position in front of the driver seat. Once the image of the person is acquired, the system now tries to detect the face[1].

The system described in this paper automatically takes photos of driver and compares his or her face with database to check whether he is an authenticated driver or not. He can have access to the vehicle only if he is an authenticated driver. If he is not an authenticated driver an alarm rings and electrical connections are not activated. The technology used here is face recognition and face detection in real time[2].

The proposed security system for smart cars used to prevent them from loss or theft using Advanced RISC Machine (ARM) processor. It performs the real time user authentication using face recognition, using the PCA algorithm. In this project an extendible emergency response is used where the Face Detection Subsystem (FDS) aims at detecting somebody's face who tries to access the car. By using PCA algorithm common Eigen values of the person is achieved and it compares the image by finding the nearest value in some mathematical form which is like a function. If the person matches vehicle starts or owner will get MMS and GPS values of the vehicle as an SMS[3].

3. Proposed System

In vehicle security system, major concern is to prevent the theft of vehicle and ensure safety of vehicle by avoiding the means of theft. One level of ensuring authentication of driving is through face recognition system that authenticates a user being an authorized person to have access to the ignition system. Face is detected and recognized using algorithm overcoming the pose and illumination constraints. The recognized image is compared with the authorized image of users in the database.

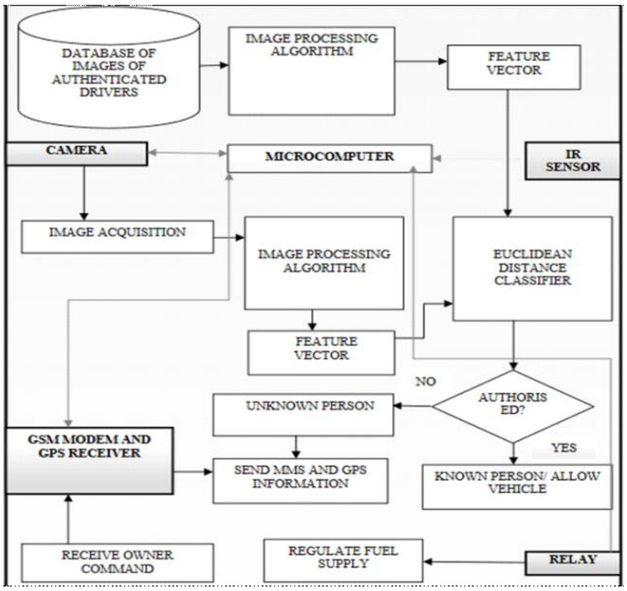

DATABASE OF IMAGES OF AUTHENTICATED DRIVERS
IMAGE PROCESSING ALGORITHM
FEATURE VECTOR
CAMERA
MICROCOMPUTER
IR SENSOR
IMAGE ACQUISITION
IMAGE PROCESSING ALGORITHM
EUCLIDEAN DISTANCE CLASSIFIER
FEATURE VECTOR
NO
AUTHORISED?
UNKNOWN PERSON
GSM MODEM AND GPS RECEIVER
YES
SEND MMS AND GPS INFORMATION
KNOWN PERSON/ ALLOW VEHICLE
RECEIVE OWNER COMMAND
REGULATE FUEL SUPPLY
RELAY

Fig.2. Flowchart of proposed system

3.1 MQTT protocol

An MQTT system consists of clients communicating with a server often called a "broker". A client may be either a publisher of information or a subscriber. Each client can connect to the broker. The MQTT connection is always established between the client and the broker, two clients are never connected directly with each other. The client establishes the connection with the broker with the CONNECT message. In response to this CONNECT message broker sends CONNACK (connect acknowledgement) message. The return code in CONNACK message determines if the connection was successful or not. Figure below shows the MQTT connection establishment between the client and the broker. After the client connects successfully with the broker, it can now publish or subscribe messages to the broker.

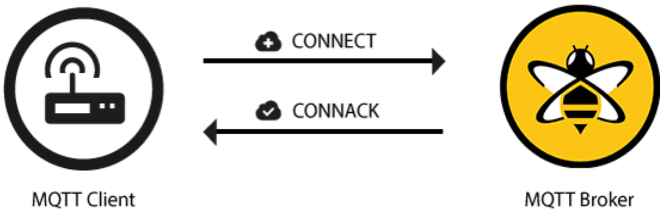


Fig. 3. MQTT client and MQTT broker

3.2 Principal Component Analysis (PCA) algorithm

Principal component analysis (PCA) has been called one of the most valuable results from applied linear algebra. PCA is used abundantly in all forms of analysis - from neuroscience to computer graphics - because it is a simple, non-parametric method of extracting relevant information from confusing data sets. With minimal additional effort PCA provides a roadmap for how to reduce a complex data set to a lower dimension to reveal the sometimes hidden, simplified structure that often underlie it. PCA is a statistical approach used for reducing the number of variables in face recognition. In PCA, every image in the training set is represented as a linear combination of weighted eigenvectors called Eigen faces. These eigenvectors are obtained from covariance matrix of a training image set. The weights are found out after selecting a set of most relevant Eigen faces. Recognition is performed by projecting a test image onto the subspace spanned by the Eigen faces and then classification is done by measuring minimum Euclidean distance. A number of experiments were done to evaluate the performance of the face recognition system.

Eigen Face using PCA algorithm for Face Recognition

One of the simplest and most effective PCA approaches used in face recognition systems is the so-called Eigen face approach. This approach transforms faces into a small set of essential characteristics, Eigen faces, which are the main components of the initial set of learning images (training set). Recognition is done by projecting a new image in the Eigen face subspace, after which the person is classified by comparing its position in Eigen face space with the position of known individuals. The advantage of this approach over other face recognition systems is in its simplicity, speed and insensitivity to small or gradual changes on the face. The problem is limited to files that can be used to recognize the face. Namely, the images must be vertical frontal views of human faces.

4. System Testing

4.1 Train Database of User

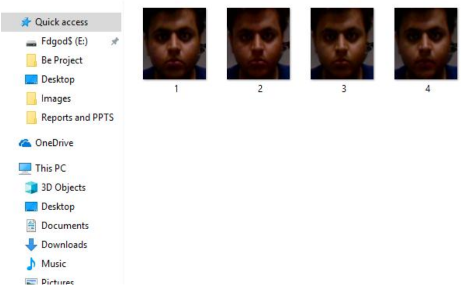


Fig.4. Database of the user having photos of his face

As per the database shown in Fig.4, a user has photos of his face that must be included in the train database set so that his face gets recognized once the system detects it. Here four photos have been uploaded but one can make a database of as many photos as per his/her requirements. The database is not limited to just one person. The user can share his photos with that of his family and friends also.

User would just have to add their face as photos in the same set. The system will automatically detect whose face is getting recognized.

4.2 User Recognized

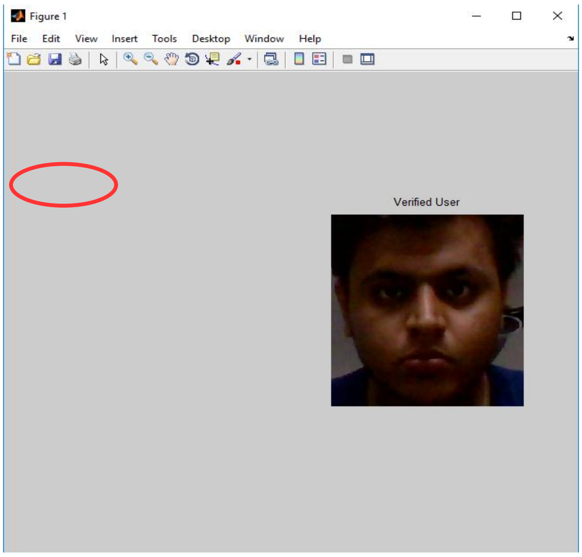
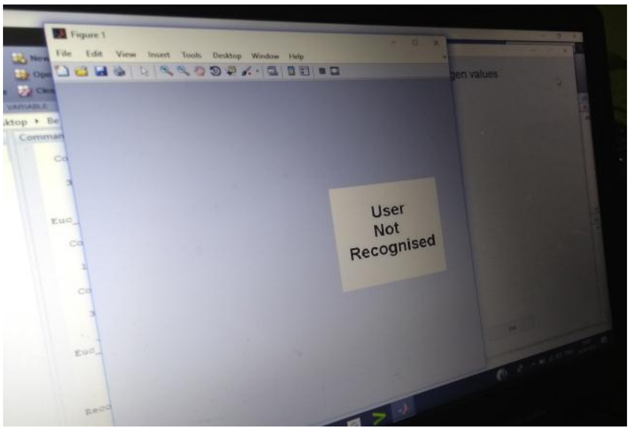


Fig.5. Face recognized according to the database

In Fig 5. the user's face can be seen recognized as per the database and once it is recognized the system shows "verified user" as shown in figure. After the face is successfully recognized then the engine of the vehicle will turn on. This would also happen with other users as well, the only requirement is that the photos of their face has to be included with the primary user in the set.

4.3 User Not Recognized



User
Not
Recognised

Fig.6. Face does not match with database

If the algorithm detects any theft then it doesn't verify the user and the system will not let the engine of the vehicle turn on.

Users having their faces in the database can access the system. If an unrecognized person would try to access the system then it will show “User Not Recognized” as shown in Figure.

5. CONCLUSION

In this project, it is expected that as soon as a face is sensed by the IR sensor the face recognition algorithm will start working and it will detect and recognize the person’s face saved in the database. If face does not get recognized, then the system will send a request to the owner through a Local application using MQTT protocol demanding a pass code to start the relay.

REFERENCES

[1] C. Nandakumar, G. Muralidaran and N. Tharani “Real Time Vehicle Security System through Face recognition” *Division of Mechatronics, Department of Production Technology, Madras Institute of Technology, Anna University, Chennai, INDIA.*

[2] A. Pazhampilly Sreedevi, B. Sarath S Nair “Image Processing Based Real Time Vehicle Theft Detection And Prevention System”

[3] D. Narendar Singh, K. Tejaswi “Real Time Vehicle Theft Identity and Control System Based on ARM 9” International journal of latest trend in engineering and technology(IJLTET)