VEHICLE ANTI-THEFT SYSTEM USING PCA ALGORITHM

Savitha R ¹, Priyaadharshini A S ², Rajalakshmi P ³, Selkia J ⁴, Shreeakalya M ⁵
Assistant Professor, Department of C.S.E, Jansons Institute of Technology, Coimbatore, India ¹
UG Students, Department of C.S.E, Jansons Institute of Technology, Coimbatore, India ²–⁵

ABSTRACT

In this modern age there is rapid increase in number of vehicles and so is the number of car theft attempts, locally and internationally. 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. In this proposed vehicle security system face detection system (FDS) is used to detect the face of the driver and compare it with the predefined face. Real-time vehicle security system supported computer vision provides an answer to the present problem. Thus the protection of vehicles from theft becomes important due to insecure environment. Real time vehicle security system based on computer vision provides a solution to this problem. The proposed vehicle security system performs image processing based on real-time user authentication using face detection and recognition techniques. As the person enters the parked car to the driver's seat of the vehicle activates the hidden camera fixed in an appropriate position inside the vehicle. As soon as the image is acquired from the activated camera, the face of the person is detected. The extracted face is recognized using the PCA. Face recognition is the technique in which the identity of a human being can be identified using ones individual face. Such kind of systems can be used in photos, videos, or in real time machines. The objective of this article is to provide a simpler and easy method in machine technology.

INTRODUCTION

As the person enters the parked car overcoming the existing security features, the infrared sensor attached to the driver’s seat of the vehicle activates the hidden camera fixed in appropriate position inside the vehicle. As soon as the image is acquired from the activated camera, face of the person is detected using Viola Jones algorithm. The extracted face is recognized using the enhanced Linear Discriminant Analysis (LDA) algorithm and additionally, license to be verified which discriminates much of the features rather than looking for exact pattern based on Euclidean distance and also reliable to be used with large Examples of data Performing authorization involves setting the threshold value and comparing with that of Euclidean distance above which the person is not authenticated.
The face of the person which is classified as unknown is sent to the mobile of the owner as a MMS through the operating GSM modem.

**KEYWORDS**

Vehicle security, face detection, face recognition, license verification, Warning message, authorization

**OBJECTIVE**

- 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 license verification system use enhanced algorithm for authentication.

**PROBLEM DEFINITION**

Vehicle theft is a problem that has plague our societies due to security issues. Currently, there is a rapid increase in vehicle theft as criminals are discovering new ways to foil antitheft measures provided by the vehicle manufacturers. The automobile antitheft features such as alarm, steering wheel, kill switch, hood-lock and baby monitor security have a lot of drawbacks and are regarded as being ineffective and unable to prevent vehicle theft.

However, due to the alarming rate of vehicle theft, people already have started using more effective anti-theft control systems like immobilizers in their vehicles [1]. But, immobilizer systems are expensive, time consuming to replace if lost and can be hacked easily, letting a thief steal the car.

To resolve these problems, there is a need to have intelligent systems that are capable of providing constant surveillance with the vehicles after they have been stolen and rapid response to attacks by maintaining constant communication with the vehicle owners. To overcome these kinds of problem, we propose the Vehicle Anti-Theft System Based On Face Recognition And License Verification Using PCA Algorithm

**EXISTING WORK**

In the existing system, people who are unauthorized also drive the vehicle. Global Navigation Satellite System is used to locate the vehicle and also to stop the vehicle if stolen. The most known car security system is car alarm which has a lot of drawbacks.

In expensive cars, there is an important feature of automatic parking of the car when the driver feels drowsy, which increasingly reduces the road accidents. Not only these, at present we have a connected car which gets connected with all sorts of facilities such as internet access and wireless LAN. Apart from all these we don’t have any system which would forbid the unauthorised persons from driving the vehicle.

**DISADVANTAGES:**

- When an unauthorised person drives a vehicle, it might result in drastic road accident.
- Persons who are underage also drive the vehicle which is not so good for the society.
- People face lot of difficulties because of forgetting about the renewal of license.
PROPOSED WORK

In order to create this system first we will have to make the datasets. When the image quality becomes favourable different procedures will take place in the face recognition system the tasks are performed using the python queries. The input will be taken from the dataset which will be received in the. There will be precision formatting in the system wherein face embedding for each face will occur. Secondly a file will contain all the required method the face of the person from the given image of the dataset. The given file will be executed by the python command .We can resize or turn the image for approximity with the goal for getting the desired output. The present classifier along with OpenCV libraries will enhance the outcome or results in the face recognition system.

ARCHITECTURAL DESIGN

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.

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.

**SYSTEM DESIGN**

This research paper manipulates two face detection methods: Haar feature and Local Binary Pattern feature.

**HAAR-LIKE FEATURES**

A cascade classifier based on Haar features is an effective object detection method. It is a machine learning-based approach where a cascade function is trained using many positive images (images of faces) and negative images (images without faces), afterward, it is used to identify faces in other images. Then an extraction for features is needed from it. This method based on machine learning, where numerous positive images and negative images are used to train the cascade function. This function is used later to identify faces from different images. Then an extraction for Haar-like features is needed from it as shown in Figure 1.

The local histograms are used to obtain the spatially enhanced feature vector. These histograms are named Local Binary Patterns Histograms (LBPH). This method offers an accuracy of about 70% which is not the best result, as these algorithms have some weak points like a front face that used in Haar cascade classifier where no side detection for turning face. The LBPH algorithm is used to reduce the effect of the light variation that affects Eigenface and fisher faces but still not perfect. So, for these reasons in addition to low accuracy, we decide to work with neural networks for better results.

**MODULE 1 - Face Recognition Using Convolutional Neural Network**

The first step is to make the image black and white to find all the faces, taking into account all the pixels surrounding each pixel and finding out how dark the current pixels compared to the pixels that surround them. Then, drawing an arrow towards the direction where the image becomes darker. In case this process is repeated for each pixel in the image, the image will turn into arrows. These arrows are called gradients and display the flow from light to dark through the entire image.

After clipping the face from the image, a face direction problem occurs. A preprocessing step is added to solve this issue, where every image is rotated so that the eyes and lips are consistently in the center of the image (Affine Transformation) which makes the comparison of faces easier. The basic idea is to hold out 68 specific points (called landmarks) on each face. After that, the machine learning algorithm is trained to be able to detect 68 landmarks for every face as illustrated in Figure 2.
After completing the face recognition process for the proposed system, the important data will be uploaded to the cloud using the File Transfer Protocol (FTP) protocol.

**MODULE 2 - Train Database of User**

As per the database shown in Fig 3, 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.

![Figure 2: Face Landmarks](image)

**USER RECOGNIZED**

![Authorized Person](image)

Fig.3. Face recognized according to the database

In Fig 3, 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

**MODULE 3 - Car Recognized**

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”
RESULTS
We would want our model to detect the moving object in a video as illustrated in the image above. The moving car is detected and a bounding box is created surrounding the car. There are multiple techniques to solve this problem. You can train a deep learning model for object detection or you can pick a pre-trained model and fine-tune it on your data. However, these are supervised learning approaches and they require labeled data to train the object detection model.

CONCLUSION AND FUTURE WORK
The above input and output analysis of the proposed system proves that the vehicle can be ensured that it is been driven only by the authorized persons. The system also provides facility for the learner’s licenses to drive by keeping a licensed person near them. It also gives time to get the system repaired if any malfunction exists. Though implementation of the proposed system may take time, it would be of great use for the safety of drivers and irregularities can be kept at check without any loopholes. The developed prototype serves as an impetus to drive future research, geared towards developing a more robust and embedded real-time biometric authentication-based ignition systems in vehicles. The present module can be interfaced with simulation GSM module which would be of great use in future. The combined module can be used to monitor from remote location about the vehicle. The data can be used to monitor about the person who is driving the vehicle, by this way, theft can be minimized since it would help to find the person driving along with location details.

REFERENCES
[8] RoyChowdhury, A., Lin, T. Y., Maji, S., & Learned-Miller, E.,"Face identification with
