Vehicle Theft Prevention System Using Image Processing

Dr.S.Mary Joans[1], Harini.K.R[2], Malathi.N[3], Ramya.B[4], Sherline Keerthana.K[5]
[1, 2, 3, 4, 5] Dept Of Electronics And Communication Engineering
[1, 2, 3, 4, 5] Velammal Engineering College, Chennai- 600 066

Abstract- *In this project, smart vehicle security is implemented using raspberry pi 3 processor and face recognition method. A smart vehicle security system is connected to your vehicle's Wi-Fi network so that you can monitor and control your device using your smart phone. The system described in this project automatically captures the image of the person who tries to open the car and compares the image, with the image which is already stored in the database, to check whether he is an authorised person or not. If he is not an authorised person, an alarm will be activated along with that the person's image will be sent to the concerned person. An extra safety measure has been added to the project which checks for the vehicle nearing in close proximity.*

I. INTRODUCTION

The use of vehicle becomes important everywhere in the world and also preventing it from theft is required. Vehicle manufacturers are attaining the security features of their products by introducing advanced automated technologies to avoid the thefts particularly in case of cars. Biometric and non-biometric methods usually provide such security features. Sometimes these systems fail due to hacked password and encryption of decrypted data, but it is almost impossible to make replica of distinctive characteristics. Biometric systems are modern and use techniques like fingerprint recognition, iris recognition and face recognition. Of these face recognition and detection systems are more sophisticated, easy to deploy and people can be identified without their knowledge. In vehicle security system, the objective 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. This can be done by first enabling the IR sensor which is used to sense certain characteristics of its surroundings by either emitting or detecting infrared radiation, and then the webcam is used to capture the image and to check whether the person is authorised person or not.

II. IMAGE PROCESSING

Image processing is one form of signal processing. In image processing the input is an image, and the output may be either an image or, a set of characteristics related to the image. Most image-processing techniques treat the image as a two-dimensional signal and apply standard signal processing techniques to it. Image processing is an emerging trend in detection and authentication system. Image processing has extensive applications in many areas, including medical industry, biometrics, remote sensing, defence, computer vision and robotics. Image processing techniques like face detection and face recognition methods provide a non-contact identification mechanism for finding the identity of the person. Such systems when employed inside the vehicles can provide extra security by monitoring the presence of intruders inside your vehicle.

III. CONVENTIONAL SECURITY SYSTEMS

Smartcards, Encrypted keys, Passwords and biometric systems.

Disadvantage of these conventional access control security

- They depend only on data given to system.
- Provides no information about person who is accessing.

IV. ADVANTAGES OF FACE RECOGNITION

I. Safety:

In order to ensure safety, an IR sensor is attached to car's main door to prevent the vehicle from theft, and an ultrasonic sensor which is used to prevent accident.

II. Theft prevention:

The face images of all the members who can use the vehicle are stored in database. So, now it is easier to identify the person who wants to use the vehicle is an authorized person or not. If any unknown person is detected, it is

designed such that his image is sent to the android application and a buzzer will be activated so that theft can be prevented. Hence user can rely on this system from security point of view.

III. Evidence:

Evidence becomes very useful parameter in any theft case. The proposed system is capable of capturing image as soon as IR sensor senses the person. This image is uploaded on web page with that respective time of any intruder's detection. Through this user has a strong proof in his/her hand for further investigation.

V. METHODOLOGY

1. In this project smart vehicle security system is implemented using Raspberry pi processor and face recognition method.
2. Whenever any person tries to open the car's main door, an IR sensor which is attached to the car's main door will sense the presence of person and automatically webcam is activated.
3. The webcam will capture the image of a person, and compares it with the images which is stored in the database.
4. If both the images are matched, then it is assured as authorised person and the car's door can be opened.
5. After above procedure, an ultrasonic sensor is fixed to the car's back door in order to prevent from accident.
6. An ultrasonic sensor is attached to the car's back door. If any other vehicle comes closer to our vehicle, the ultrasonic sensor will sense and a notification will be enabled in the dashboard along with that, a buzzer will be activated.

VI. VEHICLE THEFT PREVENTION USING IMAGE PROCESSING

The system comprises of both software module and hardware module. Hardware module includes Raspberry Pi 3, Web Cam, DC motor, IR sensor, ultrasonic sensor, USB and power supply. Software module includes image processing. Image processing involves face detection and face recognition.

1. USB CAMERA:

Webcams come with software that needs to be installed on the computer to help users record video on or stream it from the Web. Webcams are capable of taking pictures as high-definition videos.

2. IR SENSOR :

An IR led is also known as IR transmitter or receiver, which is a special purpose LED that transmits infrared rays in the range of 760nm wavelength. Such LED's are made of gallium arsenide and aluminium gallium arsenide. These are commonly called as sensors. The appearance is same as normal LED. Since the human eye cannot see the infrared radiations, it is impossible for human to identify whether an IR LED is working or not unlike a normal LED.

IR LEDs allow for cheap, efficient production of infrared light, which is electromagnetic radiation in the 700 nm to 1mm range. IR LEDs are useful in a number of types of electronics, including many types of remote controls for televisions and other electronics. Used with infrared cameras, IR LEDs can act like a spot light while remaining invisible to the naked eye.

Because IR LEDs can be used in conjunction with a number of different types of sensors, they are becoming common in machine-to-machine (M2M) environments and Internet of Things (IoT) applications.

3. ULTRASONIC SENSOR:

An ultrasonic sensor is a device that can measure the distance to an object by using sound waves. It measures distance by sending out a sound wave at a specific frequency and listening for that sound wave to bounce back. By recording the elapsed time between the sound wave being generated and the sound wave bouncing back, it is possible to calculate the distance between the sonar sensor and the object.

distance = (speed of sound * time taken)/2

4. FACE DETECTION

Face detection is the first step towards face recognition. Face detection helps to extract face region alone from the whole image. There are different algorithms present to detect face. Face can be detected using skin colour. Main disadvantage of this approach is that region with colour similar to skin will be wrongly determined as face. Neural networks can also be used for face detection. Here for face detection we use colour segmentation and morphological process based algorithm.

Face detection in general terms is defined as to isolate human faces from their background and exactly locate their position in an image. A webcam is used to take photo of the driver. At first fifteen photos of the driver with different pose will be taken. These photos are treated with algorithm to extract face portion alone.

5. Haar cascade algorithm:

This algorithm was proposed by Viola and Jones in 2001. This is a machine learning based approach where a cascade function is trained from a lot of positive and negative images. It is then used to detect objects in other images based on the threshold value calculated.

A Haar-like feature considers neighbouring rectangular regions at a specific location in a detection window, sums up the pixel intensities in each region and calculates the difference between these sums. This difference is then used to categorize subsections of an image. An example of this would be the detection of human faces. Commonly, the areas around the eyes are darker than the areas on the cheeks. One example of a Haar -like feature for face detection is therefore a set of two neighbouring rectangular areas above the eye and cheek regions.

Advantage: Calculation speed is high.

6. Algorithm for face recognition

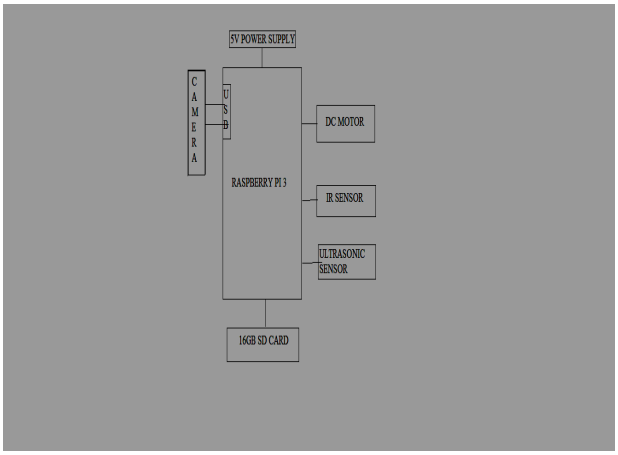
Face recognition is the second phase. It involves comparing the input face with faces in the database. Photos in the database is called training images and the photo taken during authentication phase is called as test image.

Fisherface Algorithm:

The fisherface method of face recognition as described by Belhumeur et al uses both principal component analysis and linear discriminant analysis to produce a subspace projection matrix, similar to that used in the eigenface method. However, the fisherface method is able to take advantage of ëwithin-classí information, minimising variation within each class, yet still maximising class separation. Like the eigenface construction process, the first step is take each (NxM) image array and reshape into a ((N*M) x1) vector.

Fisherface Concept - Differing from the Eigenface concept, the fisherface method tries to maximize the ratio of the between-class scatter versus the within-class scatter. The result of this shapes the projections so that the distances between the classes are at a maximum, while the distances between samples of the same class are at a minimum. A possible disadvantage is if the between-class scatter is large, then the within-class scatter might also still be of a relatively large value.

VII. BLOCK DIAGRAM



VIII. FUTURE SCOPE

Facial recognition technique seems more challenging as compared to other biometrics, thus more efficient algorithm can be developed. The defects in face recognition technique like the inability to detect face when beard, aging, glasses and caps can be rectified and eliminated or reduced. If the cost of retina or iris recognition reduces, it can be used instead of face recognition.

IX. CONCLUSION

This project is still under development. The model shows the qualitative analysis of algorithms used based on the metrics of existing algorithms. According to the statistics HCA based face recognition is very accurate, requires less computation time and less storage space as trainee images are stored in the form of their projections on a reduced basis. After the completion of the project we will collect the quantitative aspects of the model and compare it with the qualitative results for further proof.

X. EXPERIMENTAL RESULT FOR FACE DETECTION

The above picture shows the experimental result of face detection and face recognition. This shows how the image of a person will be divided in terms of pixels and thus it classifies, detects the image of a person and verifies whether the person is authorised or not.

REFERENCES

[1] G. Cheng, J. Han, L. Guo, Z. Liu, S. Bu, and J. Ren, "Effective and efficient midlevel visual elements-oriented land-use classification using VHR remote sensing images," IEEE Trans. Geosci. Remote Sens., vol. 53, no. 8, pp. 4238–4249, Aug. 2015.

[2] Y. Chai, N. Ta, and J. Ma, "The socio-spatial dimension of behavior analysis: Frontiers and progress in Chinese behavioral geography," J. Geograph. Sci., vol. 26, no. 8, pp. 1243–1260, 2016.

[3] S. Jiang, X. Qian, T. Mei, and Y. Fu, "Personalized travel sequence recommendation on multi-source big social media," IEEE Trans. Big Data, vol. 2, no. 1, pp. 43–56, Mar. 2016.

[4] G. Zhao, X. Qian, and X. Xie, "User-service rating prediction by exploring social users' rating behaviors," IEEE Trans. Multimedia, vol. 18, no. 3, pp. 496–506, Mar. 2016.

[5] G. Zhao, X. Qian, X. Lei, and T. Mei, "Service quality evaluation by exploring social users' contextual information," IEEE Trans. Knowl. Data Eng., vol. 28, no. 12, pp. 3382–3394, Dec. 2016.

[6] Chandra Shekar Ramaiah, Zahid Hussain, Asif Hussain and Yahya Al Balushi, "Smart Vehicle Security System For Defending Against Collabrative Attacks By Malware " , 2016 3rd MEC International Conference on Big Data and Smart City published by IEEE .