IRO Journal on Sustainable Wireless Systems (ISSN: 2582-3167)
www.irojournals.com/irosws/

A Hardware Vehicle Security and Accident Notification System using the Haar Cascade Algorithm

S. Syed Rafiammal[1], C. Parnasree[2], A. Ambika[3], M. Manaas[4]

Department of Electronics and Communication Engineering, B S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, India

E-mail: [1]rafiammal@Crescent.education, [2]prernasree@crescent.education, [3]ambika@crescent.education, [4]manasmujibrahman@gmail.com

Abstract

Low-cost vehicle security and accident notification system is essential in this modern society as vehicle theft and accidents that occur are increasing daily. In this proposed system, hardware for vehicle security is implemented, with authentication, and accident notification. Authentication is achieved by face detection and recognition using an open CV. The defaulter information is forwarded to the authenticated mobile number of the person by whom the vehicle is owned, using the GSM module and a notification email. The face authentication module was developed using the discrete wavelet transform-based Haar cascade algorithm. In addition to the face authentication, accident notifications will be sent to family members of the vehicle owner. Micro electrical mechanical system sensor was utilized to detect accident incidents using the accelerometer concept.

Keywords: Haar Cascade Algorithm, Vehicle Management System, Accident Notification, Face Detection.

1. Introduction

Vehicle security and authentication play a crucial role in Vehicle Management. It helps keep the vehicle safe in any condition to secure it from theft. Many proposals have been demonstrated for vehicle security management system. [1] Z. Brijet, et al., (2019) proposed a

DOI: https://doi.org/10.36548/jsws.2023.4.001
Received: 21.09.2023, received in revised form: 11.10.2023, accepted: 25.10.2023, published: 04.11.2023

method of vehicle security, and it led to the development of an antitheft system in a car using the AT mega 328. The fingerprint is detected using an inside-the-vehicle fingerprint sensor. The reading of the fingerprint sensor in the AT mega 328 is compared to the pre-assigned data. The engine ignition system starts after identifying the person as the automobile owner or an authorized fingerprint user who can take control of the vehicle. The engine will never start if it is an invader. Improvement: While other security systems can be hacked, fingerprints are employed as the key, which is unique to each individual and provides greater security. [2] Syed Umaid Ahmed et al., (2020) proposed research that includes innovative features to enhance the safety of the person by developing a safety gadget. The development of an intelligent helmet provides the highest level of assurance for a rider's or worker's safety. Smart emergency includes smart pre-safety collision avoidance techniques. Several parts of the prototype are controlled and programmed using Raspberry Pi microcomputers. [3] According to Amrutha et al. (2020), tilt sensors, RFID, GPS-GSM modules, fingerprints, and a PIC16F876A microcontroller were used in the construction of an anti-theft vehicle security system. The automobile is started using a a password, fingerprint, or RFID. [4] In order to prevent collisions, Prabal Deep Das et al. (2020) suggested employing a combination of bluetooth modules, sensors, and a video camera. Additionally, an accident control unit has been suggested in order to give information to both the driver and the police. (5) Padmapriya S. and others (2018), used the Ada-boost algorithm that recognizes the authorized face. After deciding if the given image contains a face or not, Ada-Boost learning is used to select a small number of weak classifiers and merge them into a strong classifier. Then, by comparing the principle components of the current face to those of the known individuals in a facial database that has been pre-built, a specific face can be identified using the principal component analysis (PCA) algorithm. [6] A review using analytical modelling for offloading-mobile edge-computing decisions based on deep reinforcement learning (DRL) and machine learning techniques for the Internet of Vehicles (IoV) has been carried out by Elmustafa et al. in 2021. [7] To detect theft and accidents in vehicles, Das et al. proposed a system using a smart camera, Blue tooth LabVIEW, and vision software tools.

The objectives of the proposed work are,

- Implementing anti-theft alarming system using face detection algorithm and machine learning.

- Accident notification using GSM and MEMS sensors.

2. Methodology

The workflow of the proposed system is given in Figure 1. It consists of two modules. The security authentication module consists of a Camera and Haar cascade-based model that is trained to authenticate face images of the Vehicle owner. The accident notification module consists of a MEMS sensor and a rule-based classifier. The user output module is interfaced with the proposed system using the GSM module. The entire module is embedded in a Raspberry Pi board.

2.1. Security Authentication Module or Face Detection Module

(i) Hardware Components

Pi camera with specifications of 3280×2464 pixels' resolution and dedicated camera serial interface (CSI) interface is used for capturing the image of the user. The camera is interfaced with Raspberry Pi board. The Global System for Mobile Communication (GSM) and buzzer are interfaced with Pi board for user interface.

(ii) Raspberry Pi Board

In this proposed model, Raspberry pi 3+ is employed. Raspberry Pi boards are equipped with ARM-based processors. raspberry boards are mini-computers or SoC which consists of ARM microcontroller and input output interface provisions These boards typically come with varying amounts of RAM, which affect their multitasking capabilities and overall performance. Raspberry Pi boards feature a variety of input and output ports, including USB ports for connecting peripherals like keyboards, mice, and external drives, HDMI ports for connecting to displays, GPIO (General Purpose Input/ Output) pins for hardware interfacing, and more. These pins are used to connect and control various sensors, displays, and other hardware components.

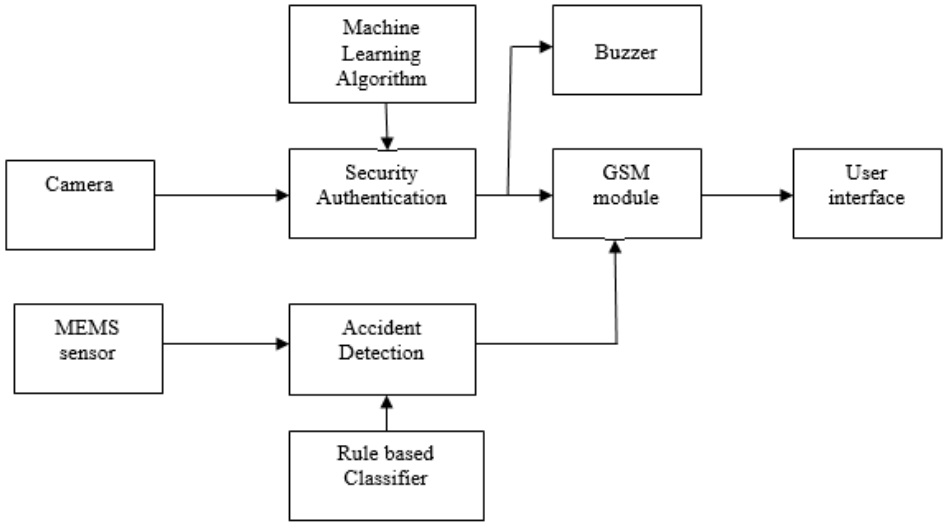

Figure 1. Block Diagram of the Proposed System.

(iii) GSM Module

SmartElex GSM module is employed in thisresearch for sending SMS to the vehicle owner about the unauthenticated access of the vehicle. It is embedded with a cellular antenna and a SIM card holder. It is connected to the Raspberry board via the serial interface.

(iv) Software Algorithm

Haar Cascades algorithm is an object detection method used to identify objects in images or video. They are based on the Haar-like features, which are rectangular filters that can be used to describe the patterns in an image. These Haar features are used as input to a machine learning algorithm, typically a variant of the AdaBoost algorithm, to train a classifier to distinguish between positive and negative examples of the object you want to detect. The training data set is created by the collection of authenticated person's face images. Various poses of the face are also collected for the dataset. The Haar algorithm is trained with these data set. The discrete wavelet -Haar Cascade-based detection algorithm is used for detecting the authorized faces of vehicle management systems [8-12].

The algorithm of Haar cascade method is given below:

- Haar-like Features: This algorithm uses Haar-like features as the basis for detecting objects. These features are rectangular patterns that represent different aspects of an

object, such as edges, lines, or textures. A rectangular Haar-like feature provides special notification about the image. The Haar-like feature computes at a high speed based on the pixel count inside the rectangle and edge feature rather than each pixel value in the image. Haar-like feature value was calculated using integral image to provide object detection value.

Given an image I(x, y), the integral image (II) at any point (x, y) is calculated as:

$II(x, y) = \sum\sum I(i, j)$, where $i <= x$ and $j <= y$

This equation represents a cumulative sum of pixel values in the original image.

A Haar-like feature can be defined as:

$Haar(x, y, w, h) = II(x, y) + II(x + w, y + h) - II(x + w, y) - II(x, y + h)$

- Machine Training: During training, the algorithm learns to identify the Haar-like features that are most relevant for distinguishing between positive and negative samples. Positive images consist of object of interest and negative images does not have any objects.

- Integral Images: Integral images allow for quick computation of rectangular sums of pixel values in an image, making feature calculation faster. To efficiently calculate Haar-like features over an image, the algorithm uses integral images.

- Cascade Classifier: The Haar cascade classifier consists of multiple stages, each of which is a collection of weak classifiers.

  A weak classifier is defined as:

H(x) = { 1, if (sum of pixel values within the Haar-like feature) * (weight) < (threshold) else -1 }

- Adaptive Boosting (AdaBoost): AdaBoost is used to select the most informative Haar-like features and assign weights to them. Features that perform well are given higher weights, while those that perform poorly are given lower weights. This allows the algorithm to focus on the most discriminative features.

- Cascade Structure: The cascade structure consists of multiple stages, each with its own set of weak classifiers. The stages are arranged in a way that progressively reduces the false-positive rate. If an image region passes all the stages, it is considered a positive detection; otherwise, it is rejected.

- Sliding Window: To apply the Haar cascade to an image, a sliding window of varying sizes is moved over the image. At each position and scale of the window, the Haar-like features are calculated and evaluated using the cascade of weak classifiers.

- Thresholding: The output of each weak classifier is combined, and if the combined response exceeds a certain threshold, the region is considered a potential object. Otherwise, it is rejected.

- Non-maximum Suppression: To eliminate duplicate detections, a non-maximum suppression step is often applied. This step removes overlapping rectangles and keeps only the most confident detection.

- Object Detection: The final output of the Haar Cascade algorithm is a list of detected faces in the input image.

(v) Accident Notification Module

This module consists of MEMS sensor and GSM module for notifying the accident incidents to user. The block diagram of this module is given in Figure 2.

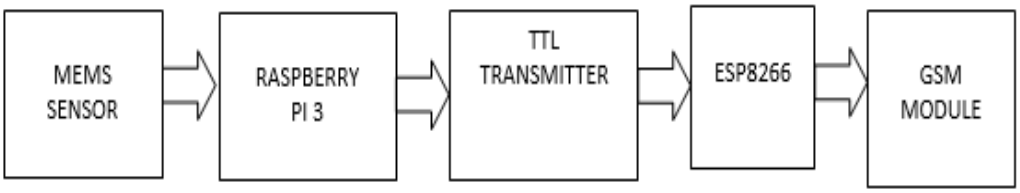

Figure 2. Flow Chart of Accident Notification Module

(vi) MEMS Sensor

MPU6050 inertial measurement unit is used to measure the vibration and acceleration. This module is a combination of an Accelerometer and a Gyroscope. This module measures

the acceleration, vibration, and orientation of the vehicle. Whenever an accident occurs these parameters will change. A rule-based algorithm is implemented in the Pi board to activate the GSM module based on the changes in the vehicle vibration and acceleration and position.

(vii) USB to TTL Transmitter

This module is used to transmit the signals from Raspberry Pi to GSM module for SMS and email notification

(viii) ESP8266

The main purpose of an ESP8266 Wi-Fi module, which is a SOC microprocessor, is to construct Internet of Things (IoT) end-point applications. It is an independent wireless transceiver. It is utilised to make the internet connection possible for many embedded system applications.

3. Results and Implementation

The proposed system is implemented using Raspberry Pi hardware. The face detection and accident notification algorithms are implemented using python programming and Open CV. The notifications are sent to the authorized users through SMS and email notifications. The MEMS sensor is used to detect the accident incidents in the vehicle. The Figure. 3 shows the prototype developed.

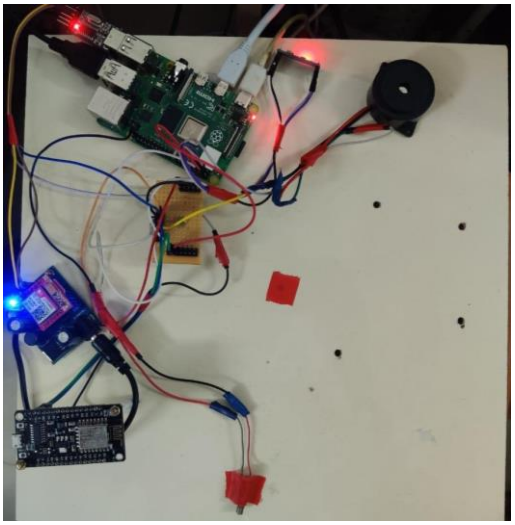

Figure 3. Prototype of Proposed Model

The machine learning algorithm was trained using 100 user datasets. The trained model is implemented in hardware. The Pi camera is attached with a LCD screen that is used for testing the authentication of vehicle. Using Open CV algorithm, the face detection of authorized user was achieved. The Haar cascade algorithm detects the authorized person's face using edge detection method. The screen shot of sample face authorization is given in Figure 4(a) and 4(b).

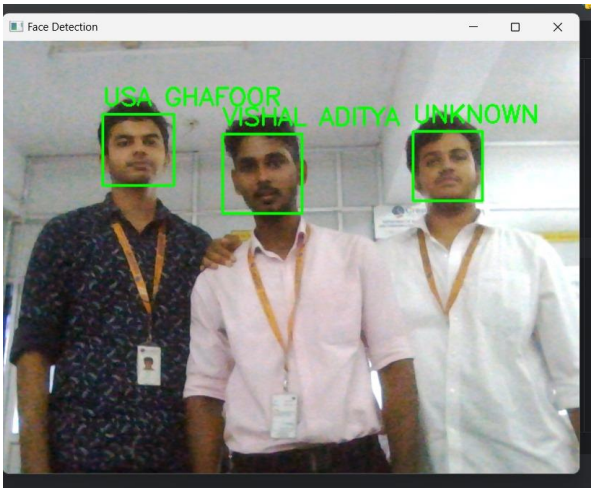

Figure 4 (a). The Detection of Authorized Faces and Unauthorized Face Detection

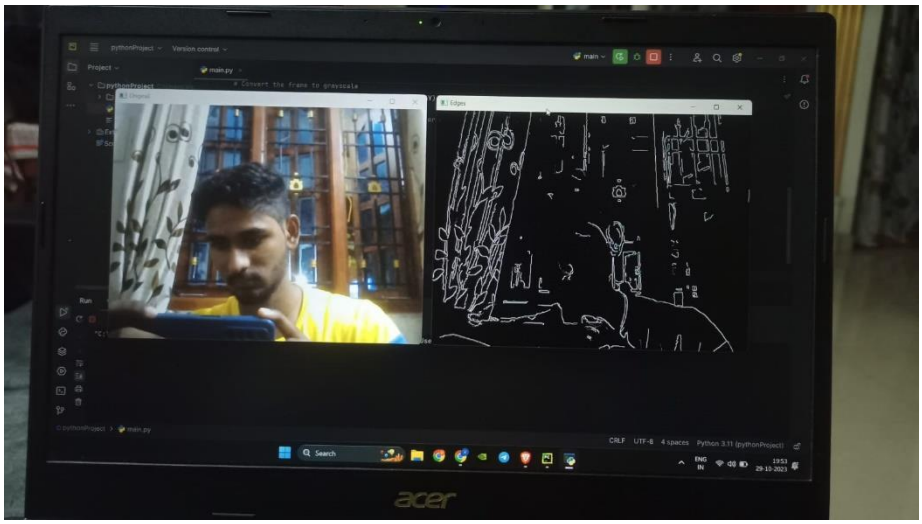

Figure 4 (b). Edge detection using Haar Cascade Algorithm.

The email notification of unauthorized access is sent to the user. In this proposed system the authorized user email is shoyabxxx19@gmail.com from the email account" raghuxxxx057@gmail.com". The screen shot of the email notification is given in Figure 5.

The SMS notification of accident notification will be sent to one of the authenticated users"85xxxxxx09" from the current user. Figure 6 shows the screenshot of the SMS accident notification.

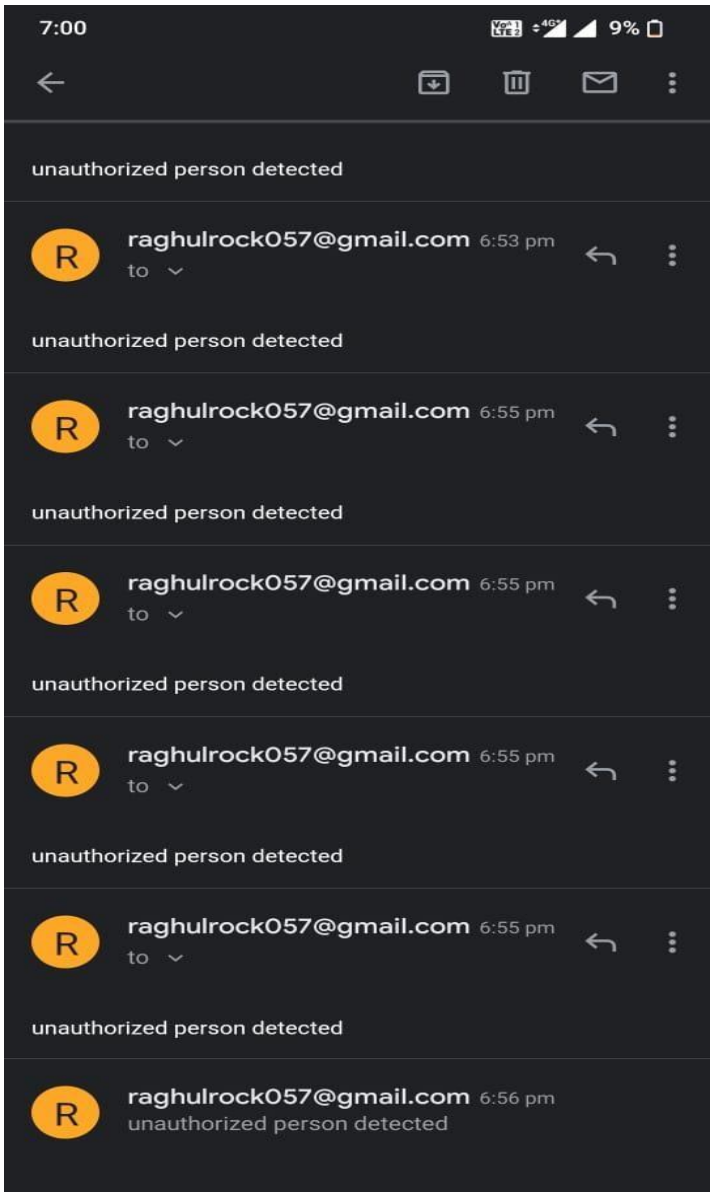

Figure 5. Email Notification on Unauthorized Access

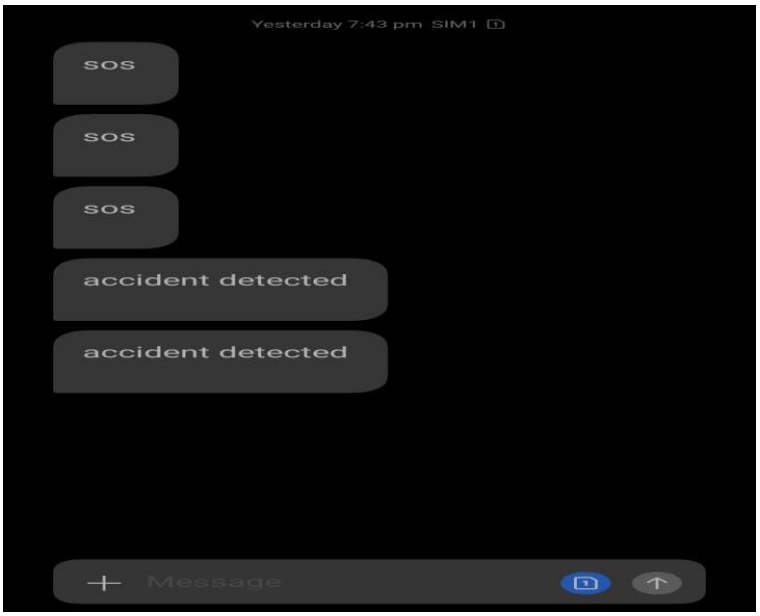

Figure 6. SMS Notification on Accident Occurrence

Performance Metrics

The Model accuracy is determined using the formula shown below:

= No. of accurate authorized faces detected / Total No. of predictions.

The accident event was identified by the angle alteration and the vibrations sensed by the MEMS sensor.

Accuracy = No.of correct events/ Total No. of predictions

4. Conclusion

Anti-theft notification system and accident notification system are major aspects of vehicle security system. In this proposed work, machine learning based security system was designed using OpenCV. The face detection-based authentication was proposed using Haar cascade algorithm and the MEMS sensor-based accident identification system was implemented in Raspberry-Pi hardware.

In this research work, facial recognition system was utilized for user authorization and unauthorized vehicle access are notified by alarm and email also accident notification will be sent via SMS.

In this work, the accuracy of 80% was achieved for user authentication and 70 % accuracy was achieved for accident notification. In future this work can be implemented in real time applications.

References

[1] Z. Brijet, N. Santhosh Kumar “Vehicle Anti-Theft System using fingerprint recognition”.OpenAcademic Journal of Advanced Science and TechnologyDOI: 10.33094/5.2017.11.36.4,2019

[2] Ahmed, S.U., Uddin, R. and Affan, M., 2020, September. Intelligent gadget for accident prevention: smart helmet. In *2020 International Conference on Computing and Information Technology (ICCIT-1441)* (pp. 1-4). IEEE.

[3] Chandran, A., & Shiny Malar, F.R. (2020). "A Smart Anti-Theft System for Vehicle Security." International Journal of Advanced Research Trends in Engineering and Technology, 7(10).

[4] P. Deep Das and S. Sengupta, "Implementing a next generation system to provide protection to vehicles from thefts and accidents," *2017 International Conference on Innovations in Green Energy and Healthcare Technologies (IGEHT)*, Coimbatore, India, 2017, pp. 1-6, doi: 10.1109/IGEHT.2017.8094045.

[5] Padmapriya, S., & KalaJames, E. A. (2018). Real time smart car lock security system using face detection and recognition. 2012 International Conference on Computer Communication and Informatics. doi:10.1109/iccci.2012.6158802

[6] Elmustafa Sayed Ali, Mohammad Kamrul Hasan, Rosilah Hassan, Rashid A. Saeed, Mona Bakri Hassan, Shayla Islam, Nazmus Shaker Nafi, Savitri Bevinakoppa, "Machine Learning Technologies for Secure Vehicular Communication in Internet of Vehicles: Recent Advances and Applications", Security and Communication Networks, vol. 2021, Article ID 8868355, 23 pages, 2021. https://doi.org/10.1155/2021/8868355

[7] Das, P. D., & Sengupta, S. (2016). Proposing the systems to provide protection of vehicles against theft and accident. 2016 IEEE International Conference on Recent

Trends in Electronics, Information & Communication Technology (RTEICT). doi:10.1109/rteict.2016.7808119

[8] L. Cuimei, Q. Zhiliang, J. Nan and W. Jianhua, "Human face detection algorithm via Haar cascade classifier combined with three additional classifiers," *2017 13th IEEE International Conference on Electronic Measurement & Instruments (ICEMI)*, Yangzhou, China, 2017, pp. 483-487, doi: 10.1109/ICEMI.2017.8265863.

[9] Abdurrahman, Muhammad Hanif, Haryadi Amran Darwito, and Akuwan Saleh. "Face Recognition System for Prevention of Car Theft with Haar Cascade and Local Binary Pattern Histogram using Raspberry Pi." EMITTER International Journal of Engineering Technology 8, no. 2 (2020): 407-425.

[10] Pankajavalli, P. B., V. Vignesh, and G. S. Karthick. "Implementation of haar cascade classifier for vehicle security system based on face authentication using wireless networks." In International Conference on Computer Networks and Communication Technologies: ICCNCT 2018, pp. 639-648. Springer Singapore, 2019.

[11] Truong, Quoc Bao, Tan-Loc Tran, Thanh Tan-Kiet Nguyen, and Huu Cuong Nguyen. "The Face and number plate recognition for car anti-theft." CTU Journal of Innovation and Sustainable Development 15 (2023): 110-118.

[12] GV, Hindu Kumari, H. C. Nithyashree, Ranjana A. Bali, R. Tejeswini, and R. C. Sreevidya. "Theft Prevention System for Vehicles Using Biometric Traits."