International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Theft Prevention System for Vehicles Using Biometric Traits

Hindu Kumari G V[1], Nithyashree H C[2], Ranjana A Bali[3], Tejeswini R[4], Dr Sreevidya R C[5]
[1, 2, 3, 4]Student, Department of CSE, BNM Institute of Technology, Bangalore, Karnataka, India-560070
[5]Assistant Professor, Department of CSE, BNM Institute of Technology, Bangalore, Karnataka, India-560070
Email address: gvhindukumari @ gmail.com[1], nithyahc1998 @ gmail.com[2], ranjana.bali1998 @ gmail.com[3], tejeswinir0098 @ gmail.com[4]

Abstract**—** *Today with the exponential increase in population the usage of vehicles has also increased exponentially. Many new companies introduce new vehicles in the market with the latest and advanced features. Some features are related to luxury and comfort while the others are related to safety measures. The access control can be done using various techniques like smartcards, passwords and biometric systems. The proposed system uses biometrics like face and fingerprint to authenticate the users and various machine learning algorithms are used to recognize the biometrics. Facial recognition is the primary task for realizing surveillance system for human computer interaction using Haar based cascade classifier and Local Binary Pattern Histogram. Similarly finger print based authentication uses Minutiae matching. The system beeps a buzzer when it is accessed by an unauthorized person. Thus, the biometric based anti-theft security system helps the owners to protect their vehicle from intruders*.

Keywords**—** *Haar based Cascade Classifier, LBPH, Minutiae matching, Face recognition, Fingerprint Recognition*.

I. INTRODUCTION

Stealing the vehicle could be a major threat to vehicle owners. When a vehicle is stolen, it becomes hard to track it, which considerably decreases the possibilities of recovering it. Antitheft vehicle security has been developed to mitigate this problem. A key is the only way to start the vehicle or provide ignition to the engine. The biometric-based vehicle ignition system replaces the need of the key to start the vehicle. The objective is to achieve luxurious features and the safety concern, which is feasible by employing various automotive electronics.

The Internet of Things (IoT) is a system of interrelated computing devices and objects that are given with unique identifiers (UIDs) and also has the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. IoT is largely the combination of various fundamental forms of technology and has different layer of communication level.

Biometric authentication is a user identity verification process that involves biological input, or scanning and analysis of some part of the body. Biometrics deals with recognition of individuals based on their behavioural or biological characteristics. It is widely known as the most effective type of authentication because it is extremely difficult to transfer biological material or features from one user to another. The most common and evolving types of biometric authentication involve facial scanning and fingerprint-based authentication.

A facial recognition system is a technology capable of identifying a person's face from a digital image or a video frame from a video source. The recognition system work by comparing selected facial features from given image with faces within a database.

A fingerprint is an impression left by the friction ridges of an individual human finger. Fingerprint based authentication uses minutiae matching and information where highly significant features are used for Automation Recognition System. It uses feature extraction algorithms where the set of patterns are expressed as a Boolean matrix, allowing the information to be viewed as factorization of matrices and uses pattern intersection methods. The anti-theft security system enhances the probabilities of recovering the vehicle.

II. RELATED WORK

To Prevent vehicles from being stolen there are many methods introduced in the nineteenth century. According to the mode of operation of the vehicle they are divided as tracking method of vehicle and other is the biometric method, the biometric method is further subdivided on the basis of "Biometric Authentication" types such as finger, iris, face etc.

Tahesin Attar et al. [2] proposes a system based on wireless communication and a low-cost Bluetooth module where, GSM is used for sending messages. The user can control the engine/ignition and also employs a password for opening of door as well as wearing of a seat belt. IR module/sensor detects the intruder. Vidhyotma et al. [3] proposes to provide a fool-proof mechanism against vehicle theft. Smart phones are used to design the user interface that allows access of the vehicle to an intended person only.

Mahesh R et al. [1], Syed fasiuddin et al. [5], Mayank Kumar Rusia et al. [7], Aftab Ahmed et al. [8], Prayag Bhatia et al. [9], Vijay Kumar Sharma et al. [10] has proposed a system which uses Local Binary Histogram Patterns (LBPH) algorithm for face recognition. LBP is considered as a 3x3 matrix and converted into binary value which is then converted into decimal value until a new image is formed. Histogram is extracted from the new image and compared against the trained data. It uses Euclidean distance to measure the distance from trained set.

Mridhula Ramesh et al. [4] has established a procedure for the ignition of a two-wheeler using fingerprint-based verification process and Global System for mobile communication module (GSM). The use of GSM helps the

Hindu Kumari G V, Nithyashree H C, Ranjana A Bali, Tejeswini R, and Dr Sreevidya R C, "Theft Prevention System for Vehicles Using Biometric Traits," *International Research Journal of Advanced Engineering and Science*, Volume 5, Issue 3, pp. 67-71, 2020.

owner to easily track the location of the vehicle, thereby reducing the possibility of the vehicle being accessed the intruders.

Ratna Yustiawati et al. [11] proposed a method for securing room using face identification. Haar based classifier method was proposed to detect and recognize the face. This method detected the face with more accuracy as a greater number of features detected.

Hemalatha S et al. [12], Prof. Dr. Asaf VAROL et al. [13] has proposed a system which uses minutiae. Minutiae are defined to be the key points in any fingerprint-image and are possibly classified to be the ends of ridges and bifurcations. Minutiae matching process facilitates the comparison of original images with dataset images for the purpose of actual recognition using minutiae features extracted. The three major types of minutiae points that exist are, ridge endings or termination points, bifurcation points and spots. Binarization converts fingerprints into a binary form.

Deepak et al. [14] has proposed a biometric based authentication mechanism for the recognition of fingerprint using feature extraction and also generating a hash value by using a technique called Perceptual hashing. The user finger print template is registered in the database along with the hash value and the template is matched using Structural Similarity Score and the similarity score is recorded. An additional validation is provided by sending one-time password to the registered user.

Jana Kalikova et al. [15] has proposed a novel method for the identification of drivers in vehicles using machine learning technique called Artificial Neural Network. The temperature distribution information on the driver's face is provided using a technique called thermogram normalization. The normalized values are stored in an external unit and the driver is recognized if the similarity ratio is greater than 0.7.

Marc Roeschlin et al. [17], in the domain of security has references to the utilization of biometrics in the authentication of VANET message.

Praveen balaji D et al. [18], Anissa Lintang Ramadhani et al. [6] provides superiority of facial recognition over other biometric based authentication mechanism for ID photo verification and has also provided a comparative study of different facial recognition algorithms like Principal Component Analysis (PCA), Independent component Analysis, Eigen face method, Support Vector Machine and also Eigen Face with PCA method. The different facial features are classified and selected using AdaBoost algorithm and recognized using Eigen face approach. After the evaluation it was found that the success rate was the highest in case of Eigen face with PCA method.

The work presented in this paper is useful as it guarantees personal privacy of the vehicle. It is cost effective as the camera and the scanner are easily affordable.

III. METHODOLOGY

The proposed system uses Raspberry Pi 3 Model B+ for image processing and detection. Raspberry Pi takes user data, processes and computes the data using Python as the programming language. Various biometric authentication models are used to authenticate any individual. On success the motor runs and on failure the alarm beeps and owner get an alert.

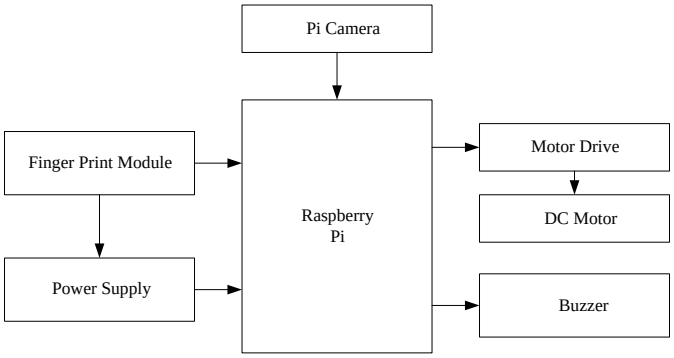

Fig. 1. Block diagram of proposed system

Different security mechanisms used include finger print and facial recognition. Haar feature based cascade developed by Viola Jones are used for facial detection and Local Binary Pattern Histogram algorithm is used for Facial Recognition. Finger print recognition is done using minutiae-based matching. After the user is authenticated using either of the methods, the vehicle is ignited.

A. Face Detection and Recognition

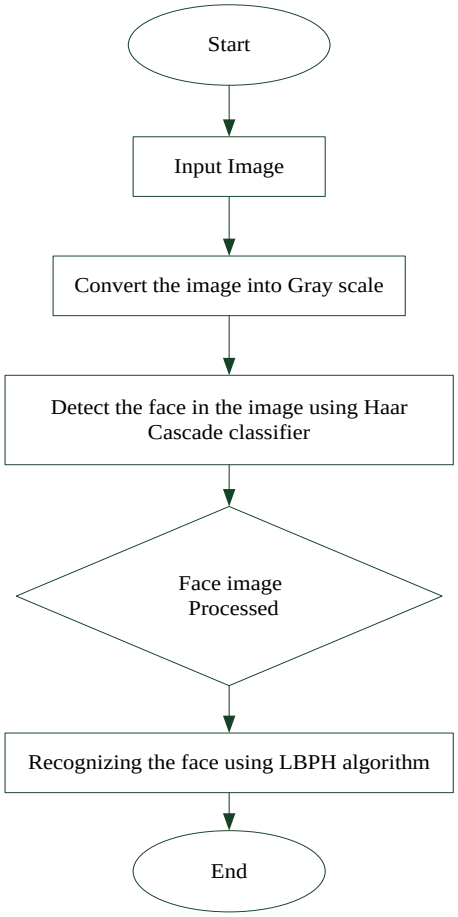

Fig. 2. Workflow of Face Recognition System.

Hindu Kumari G V, Nithyashree H C, Ranjana A Bali, Tejeswini R, and Dr Sreevidya R C, "Theft Prevention System for Vehicles Using Biometric Traits," *International Research Journal of Advanced Engineering and Science*, Volume 5, Issue 3, pp. 67-71, 2020.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Face detection from an image is a tedious task. But Haar feature-based cascade classifier algorithm, is an effective method to detect the face, where a cascade function is trained from lots of positive and negative images. Within the detection phase of the Viola-Jones object detection framework, a window of the target size is moved over the input image, and for each and every subsection of the image the Haar-like feature is calculated.

Face recognition using LBPH creates an intermediate image that describes the original image, by highlighting the facial characteristics. This algorithm uses an idea of sliding window, based on the parameter radius and neighbours. We can extract histograms by dividing the image into multiple grids by using Grid X and Grid Y parameters. This histogram is employed to represent image from the training dataset. To find if the image matches the input image, we need to compare two histograms and return the image with the closest histogram.

B. Fingerprint Recognition

Fingerprint identification is done by the most popular approach called Minutiae matching. It is usually based on lower-level features determined by singularities in ridge patterns of finger called minutiae. Minutiae matching essentially include finding the most effective and best alignment between the template and a subset of minutiae within the input fingerprint, through a geometrical transformation. The two approaches of minutiae extraction process are based on binarization and ridge thinning stage. The fingerprint recognition system is split into three steps that are fingerprint image pre-processing, feature extraction and matching.

Algorithm:
Step 1: find the dimensions of the image.
Step 2: find the label connected in 2-D binary image.
Step 3: scan the fingerprint image to detect the minutiae.
Step 4: if there is one neighbour for the pixel minutiae considered as ridge ending, and ridge bifurcation if there are at least 3 neighbours for the pixel.
Step 5: store the ridges in the mat lab files.
Step 6: end.

In the proposed system the user has to first authenticate himself through fingerprint, if successful then the vehicle ignites, else they have to authenticate through face recognition. If the person is an authorized user the vehicle ignites, or else the buzzer beeps and the alert notification will be sent to the owner's email.

IV. RESULTS

The Anti-theft system is represented using a prototype as shown in Fig. 3.

Biometric Authentication of the user is done. The system uses Haar based cascade classifier to detect the face and LBPH to recognize the face. Minutiae matching is used to recognize the fingerprint of the authorized person. The System is first trained with certain inputs of biometrics like fingerprints and face images in different angles.

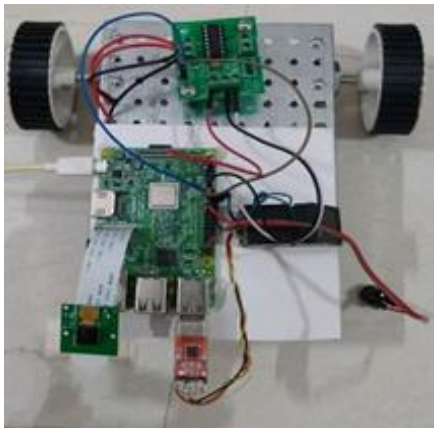

Fig. 3. System Prototype.

Fig. 4. Training the model with fingerprint.

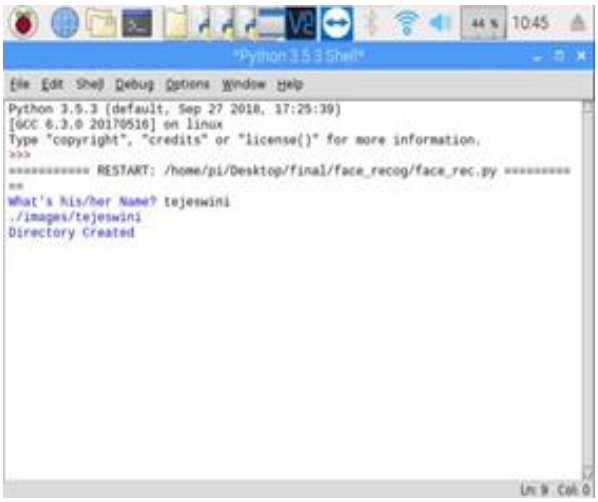

Fig. 5. Training the model with face images.

After the system is trained, we test the system by giving input through input devices like fingerprint scanner and PI camera respectively.

The user will authorize through fingerprint initially and in case if it fails the user will have chance to authenticate through face and even then, if the user fails then the buzzer beeps and the intruder gets caught.

Hindu Kumari G V, Nithyashree H C, Ranjana A Bali, Tejeswini R, and Dr Sreevidya R C, "Theft Prevention System for Vehicles Using Biometric Traits," *International Research Journal of Advanced Engineering and Science*, Volume 5, Issue 3, pp. 67-71, 2020.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

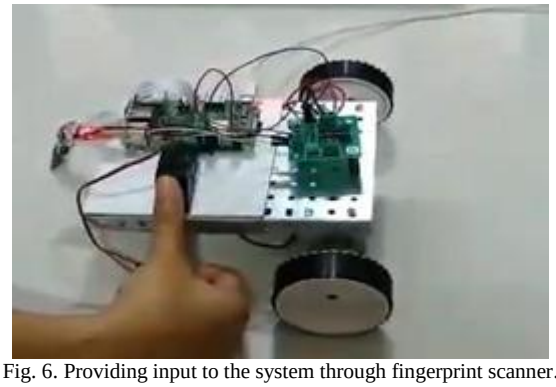

Fig. 6. Providing input to the system through fingerprint scanner.

The Fig. 8 represents the output of the successful and unsuccessful authentication of different users. After the successful authentication the message motor on is displayed and the wheels move for 5 seconds. If unsuccessful authentication is encountered then messages like 'motor off', 'buzzer on' and 'unauthorized person is detected' will be displayed.

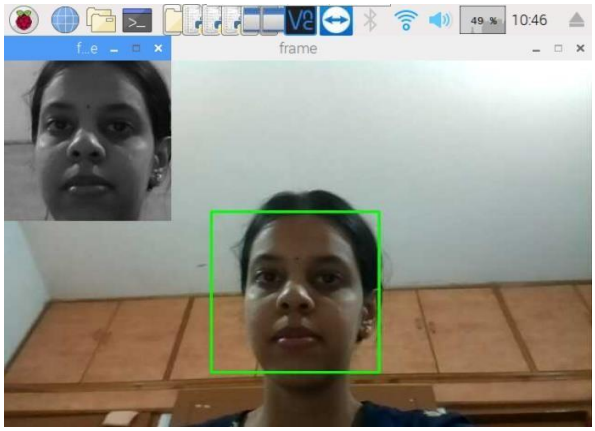

Fig. 7. Providing input to the system through PI camera.

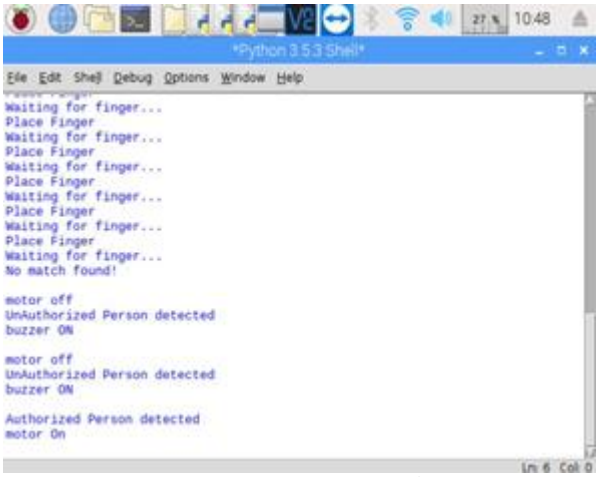

Fig. 8. Python shell indicating the results of authentication.

The figure 9 represents the output when an unauthorized person is detected the buzzer beeps and also a notification is sent through email to the owner with the intruder's image and the current location thereby helping the owner to easily track the vehicle.

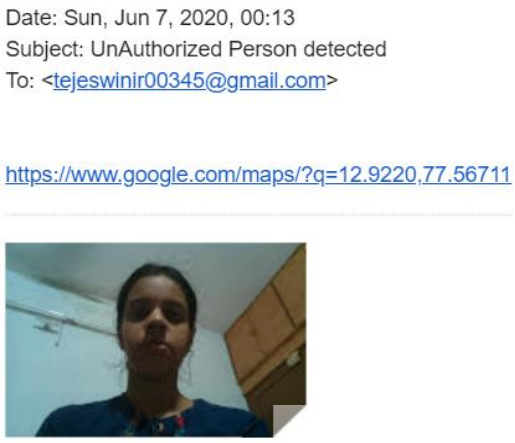

Fig. 9. Email notification sent to the owner.

V. Conclusion and Future Enhancements

The system designed allows only the authorized users to access the vehicle. The images of face and fingerprint are stored of an authorized person. The vehicle ignites if the captured image matches the stored image. If the images are not matched then the buzzer beeps. So, in this way owner of the vehicle can be rest assured about the safety of the vehicle. The proposed system can be enhanced by including a GSM and GPS tracker to track the vehicle. Also, an android application can be developed for registering the details of the owner that can be stored.

References

[1] Mahesh R. Pawar, Imdad Rizvi, "IoT Based Embedded System for Vehicle Security and Driver Surveillance", Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies, 2018, pp. 466-470.

[2] Tahesin Attar, Prajakta Chavan, Vidhi Patel, Megha Gupta, Debajyoti Mukhopadhyay, "An Attempt to Develop an IOT based Vehicle Security System" 2018 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS), pp. 195-198.

[3] Vidhyotma, Jaiteg Singh, Dapinder Virk, "Bluetooth Enabled Anti-Theft System Using Android Based Handheld Device", 2018 6th Edition of International Conference on Wireless Networks & Embedded Systems, pp. 122-125.

[4] Mridhula Ramesh, Akruthi S, Nandhini K, Meena S, Joseph Gladwin S, and Rajavel R "Implementation of Vehicle Security System using GPS, GSM and Biometric" 2019 Women Institute of Technology Conference on Electrical and Computer Engineering (WITCON ECE), pp. 71-75

[5] Syed fasiuddin , Syed Omer , Dr. Khan Sohelrana , Amena Tamkeen, Mohammed Abdul Rasheed "Real Time Application of Vehicle AntiTheft Detection and Protection with Shock Using Facial Recognition and IoT Notification" 2020 Proceedings of the Fourth International Conference on Computing Methodologies and Communication (ICCMC), pp. 1039-1044

[6] Anissa Lintang Ramadhani, Purnawarman Musa, Eri Prasetyo Wibowo, "Human Face Recognition Application Using PCA and Eigenface Approach", 2017 Second International Conference on Informatics and Computing (ICIC).

[7] Mayank Kumar Rusia, Dushyant Kumar Singh, Mohd. Aquib Ansari, "Human Face Identification using LBP and Haar- like Features for Real Time Attendance Monitoring",2019 Fifth International Conference on Image Information Processing (ICIIP).

[8] Aftab Ahmed, Jiandong Guo, Fayaz Ali, Farha Deeba, Awais Ahmed "LBPH Based Improved Face Recognition At Low Resolution", 2018 IEEE International Conference on Artificial Intelligence and Big Data.
[9] Prayag Bhatia, Shakti Rajput†,Shashank Pathak, Shivam Prasad, "IOT based facial recognition system for home security using LBPH algorithm", 2018 Proceedings of the International Conference on Inventive Computation Technologies (ICICT), pp. 191-193
[10] Vijay Kumar Sharma "Designing of Face Recognition System" , 2019 Proceedings of the International Conference on Intelligent Computing and Control Systems (ICICCS), pp.459-461.
[11] Ratna Yustiawati, Nyayu Latifah Husni, Evelina, Sabilal Rasyad, Iskandar Lutfi, Ade Silvia, Niksen Alfarizal, Adella Rialita "Analyzing Of Different Features Using Haar Cascade Classifier" 2018 International Conference on Electrical Engineering and Computer Science (ICECOS)
[12] Hemalatha S "A systematic review on Fingerprint based Biometric Authentication System" 20 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE).
[13] Prof. Dr. Asaf VAROL, Naveed AHMED "Minutiae Based Partial Fingerprint Registration and Matching Method" 2018 IEEE.
[14] Harish Kumar N, Deepak G "User Authentication for IOT Objects: A Two Factor Approach using Biometrics and Perceptual Hashing" 2018 IEEE.
[15] Jana KaliKova, Jan Krcal "Biometric identification of persons in a Vehicle", 2018 7th IEEE International Symposium on Next-Generation Electronics.
[16] Igor Tomicic, Petra Grd, Miroslav Baca "A review of soft biometrics for IoT", 2018 Opatija Croatia MIPRO.
[17] Marc Roeschlin, Christian Vaas, Kasper B. Rasmussen, and Ivan Martinovic "Bionyms: Driver-centric Message Authentication using Biometric Measurements", 2018 IEEE Vehicular Networking Conference (VNC).
[18] Praveenbalaji D, Srinivas R, Roopa S, Suresh M, Gayathri A "ID Photo Verification by Face Recognition", 2020 6th International Conference on Advanced Computing & Communication Systems (ICACCS).