International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

RASPBERRY PI-BASED VEHICLE STARTER SYSTEM USING FACE DETECTION AND RECOGNITION

Vyshnavi Thokala, S. Kalyan
Department of Electronics and Communication Engineering,
Jayamukhi Institute of Technological Sciences, Narsampet, Warangal, Telangana, India

ABSTRACT

Vehicle theft and unauthorized vehicle access remain important security concerns, particularly in systems that rely exclusively on conventional keys, passwords, remote controls, or RFID-based authentication. This paper presents a Raspberry Pi-based intelligent vehicle starter system that integrates computer vision, facial authentication, embedded processing, and relay-based ignition control. A Raspberry Pi 4 serves as the central processing and control platform, while a Pi Camera or USB camera captures the driver's facial image in real time. The proposed processing pipeline consists of image acquisition, preprocessing, face detection, facial feature extraction, face recognition, authorized-user verification, and ignition control. Registered facial information is maintained in a local database, allowing the authentication decision to be performed locally without complete dependence on cloud connectivity. When an authorized driver is successfully verified, a GPIO signal activates a relay interface to permit vehicle ignition. If authentication fails, the relay remains inactive and the ignition is kept locked. The architecture can additionally capture unauthorized access images and generate security notifications through email, SMS, or IoT services. A prototype implementation using Raspberry Pi, OpenCV, Haar Cascade face detection, and GPIO-controlled relay operation demonstrates the feasibility of integrating computer vision with physical vehicle access control. The proposed system provides a low-cost and contactless approach to intelligent vehicle security and establishes a platform for future integration of lightweight deep-learning recognition and anti-spoofing mechanisms.

Keywords: Raspberry Pi, face detection, face recognition, biometric authentication, vehicle security, OpenCV, embedded system, GPIO, ignition control, IoT.

I. INTRODUCTION

Vehicle theft and unauthorized vehicle access remain important security concerns, creating a need for authentication mechanisms that can provide reliable access control without depending entirely on conventional physical keys or passwords. Traditional vehicle-security approaches commonly employ mechanical keys, RFID tags, passwords, PINs, and electronic remote controls. Although these methods are widely adopted because of their simplicity and low implementation cost, they can be affected by loss, theft, duplication, sharing, or unauthorized disclosure. These limitations have motivated the investigation of biometric authentication techniques for vehicle-access applications. Biometric authentication identifies individuals using physiological or behavioral characteristics and can reduce the dependence on external authentication tokens. Among different biometric modalities, face recognition is particularly attractive for vehicle applications because it provides contactless authentication using a camera. The development of efficient face-detection and face-recognition algorithms has made camera-based biometric systems increasingly practical for embedded applications. The Viola–Jones framework established an efficient cascade-based approach for real-time face detection using Haar-like features, AdaBoost, and an attentional cascade structure [1]. Its computational efficiency makes it particularly relevant to resource-constrained systems. Subsequent advances in deep learning have significantly improved facial representation and recognition. FaceNet introduced a deep-learning framework that maps facial images into a compact embedding space in which distances between embeddings represent facial similarity [2]. The approach demonstrated the effectiveness of learned facial representations for verification and recognition and established an important foundation for embedding-based face-recognition systems. Other deep-learning approaches have further investigated robust facial representations under variations in pose, illumination, expression, and image quality. The Labeled Faces in the Wild dataset has also been widely used for evaluating face-recognition algorithms under unconstrained conditions [3].

The availability of low-cost embedded computing platforms has created opportunities to deploy computer-vision algorithms directly at the edge. Raspberry Pi provides processing, camera interfacing, storage, networking, and GPIO capabilities within a compact platform, making it suitable for security and automation applications. Raspberry Pi-based IoT security architectures have demonstrated the feasibility of performing monitoring and control functions using embedded computing and network connectivity [4]. The uploaded project specifically adopts Raspberry Pi 4 as the central processing and control platform together with a camera, facial-recognition software, authorized-user database, and GPIO-controlled relay.
For vehicle-security applications, however, simply detecting or recognizing a face is not sufficient. The authentication decision must be reliably connected to a physical access-control mechanism. A secure vehicle starter should therefore establish a direct relationship between driver identification and ignition authorization. The proposed system addresses this requirement by integrating camera-based face processing, local user authentication, Raspberry Pi-based decision making, and relay-controlled ignition access.

The proposed architecture captures the driver's facial image through a Pi Camera or USB camera and processes the acquired image on a Raspberry Pi 4. After face detection and feature extraction, the detected facial representation is compared with information corresponding to registered users. If the driver is authenticated, a GPIO signal activates the relay interface and permits vehicle ignition. If authentication fails, the relay remains inactive and the ignition remains locked. The system can additionally record unauthorized access attempts and optionally generate security notifications through email, SMS, or an IoT service. These functional elements are consistent with the architecture and objectives described in the uploaded project report.

The main contribution of this work is therefore the integration of facial authentication and physical vehicle access control within a low-cost embedded platform. Unlike a standalone face-recognition application, the proposed architecture uses the authentication result to directly control the vehicle-start authorization mechanism. The system is also designed to support local processing, thereby reducing dependence on continuous cloud connectivity. In addition, its modular structure allows lightweight or deep-learning-based recognition algorithms to be incorporated according to the computational requirements of the target vehicle platform.

II. RELATED WORK

Conventional vehicle authentication mechanisms primarily rely on mechanical keys, RFID tags, passwords, PINs, or electronic remote controls. Mechanical keys provide a simple and inexpensive solution but can be lost, stolen, or duplicated. Password- and PIN-based systems eliminate physical keys but introduce the possibility of disclosure, guessing, or unauthorized sharing. RFID-based systems provide convenient contactless operation but remain dependent on a physical tag that can potentially be lost or duplicated. The limitations of token- and knowledge-based authentication have encouraged the adoption of biometric techniques. Fingerprint, iris, voice, and face recognition have been investigated for access-control applications because biometric characteristics are associated more directly with the individual. For vehicle applications, face recognition provides an important advantage because authentication can be performed without requiring physical contact or an additional authentication token.

Face detection represents the first stage of a camera-based facial authentication system. Its purpose is to locate facial regions within an acquired image or video frame. Viola and Jones proposed one of the most influential real-time object-detection frameworks based on Haar-like features, integral images, AdaBoost-based feature selection, and a cascade of classifiers [1]. The cascade structure enables computationally inexpensive rejection of non-face regions while concentrating processing on candidate regions. The original work demonstrated the suitability of the approach for real-time object detection.

The computational efficiency of Haar Cascade makes it attractive for embedded platforms such as Raspberry Pi. Consequently, the proposed system considers Haar Cascade as a lightweight face-detection approach. However, its performance may degrade under substantial changes in illumination, pose, scale, facial expression, and occlusion. The project report similarly identifies Haar Cascade as a fast detection option and DNN-based detection as an alternative when improved robustness is required.

More recent face-detection research has increasingly adopted deep neural networks to improve robustness under challenging conditions. Such approaches can provide improved detection capability but generally introduce greater computational and memory requirements. Therefore, detector selection for an embedded vehicle-security system requires a balance between detection reliability and processing cost.

Following face detection, the system must determine the identity of the detected individual. Local Binary Pattern Histogram (LBPH) is a lightweight facial-recognition technique based on local texture characteristics. Its relatively low computational requirement makes it suitable for resource-constrained systems. The proposed project identifies LBPH as one possible recognition method for Raspberry Pi implementation. Multiple images of an authorized user can be captured during registration under different illumination conditions and facial orientations. The resulting facial information can then be stored in a local database for subsequent comparison. Although LBPH is computationally attractive, its performance can be affected by illumination, pose, facial expression, and image quality. Consequently, more advanced facial representations based on deep learning have become increasingly important for applications requiring improved robustness.

Deep-learning approaches have substantially changed the development of face-recognition systems by learning discriminative facial representations directly from image data. Instead of depending exclusively on handcrafted features, deep networks can transform a facial image into a compact feature representation that can subsequently be used for verification or identification. Schroff et al. proposed FaceNet, which learns a mapping from face images into a compact Euclidean embedding space [2]. Facial similarity can then be determined by comparing the corresponding embeddings. This embedding-based strategy is particularly suitable for an authentication system because registered users can be represented by stored facial embeddings and live facial images can be compared against those representations. The project report considers Dlib facial embeddings, FaceNet, and MobileFaceNet as possible recognition approaches. Dlib-based embeddings provide a practical intermediate solution between lightweight traditional recognition and computationally intensive deep-learning models, while MobileFaceNet is particularly relevant when computational efficiency is important.

Real-world facial authentication is affected by illumination, facial pose, expression, image quality, spectacles, occlusion, and camera position. The Labeled Faces in the Wild dataset was introduced to facilitate evaluation of face recognition under unconstrained conditions [3]. Such research highlights the importance of evaluating recognition systems beyond controlled laboratory environments.
These conditions are especially relevant to vehicle applications because a driver's face may be captured from different positions and under substantially different illumination conditions. Daytime and nighttime operation, shadows, spectacles, changes in facial orientation, and partial occlusion can affect recognition reliability. Therefore, the proposed registration procedure should capture multiple images of each authorized user under different conditions. The project report explicitly recommends multiple facial samples with variations in orientation and lighting.

The emergence of low-cost single-board computers has enabled computer-vision and IoT security applications to operate locally at the edge. Raspberry Pi provides a combination of processing capability, camera support, networking, storage, and GPIO interfaces, allowing image processing and hardware control to be implemented on the same platform. Previous Raspberry Pi-based security systems have demonstrated its suitability for monitoring, automation, and IoT-enabled access-control applications [4]. In the proposed vehicle-security system, Raspberry Pi 4 performs both computational and control

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

functions. It receives the camera stream, processes the facial information, performs the authentication decision, and generates the GPIO signal required for relay operation.

This integrated architecture avoids the need for a separate computer for image processing and a separate microcontroller for ignition control. The project report identifies Raspberry Pi 4 as the central unit responsible for image processing, recognition, database comparison, and GPIO control.

The application of biometric authentication to vehicle ignition has been investigated as a means of preventing unauthorized vehicle operation. Face-recognition-based ignition systems establish a direct relationship between user identity and vehicle-start permission. Such systems demonstrate that biometric verification can be incorporated into embedded vehicle-security architectures.

However, an important distinction exists between face detection and face recognition. Face detection only determines whether a face is present, whereas face recognition determines whether the detected face belongs to an authorized individual. For a secure vehicle starter, ignition authorization should be based on identity verification rather than face presence alone.

The literature demonstrates substantial progress in face detection, facial representation, deep-learning-based recognition, embedded computer vision, and biometric security. Nevertheless, several practical challenges remain when these technologies are integrated into a vehicle starter.

III. PROPOSED SYSTEM

The proposed vehicle-security system consists of five major functional layers namely Image acquisition layer, Image-processing and face-detection layer, Face-recognition and authentication layer, Vehicle-control layer, and Security monitoring layer.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

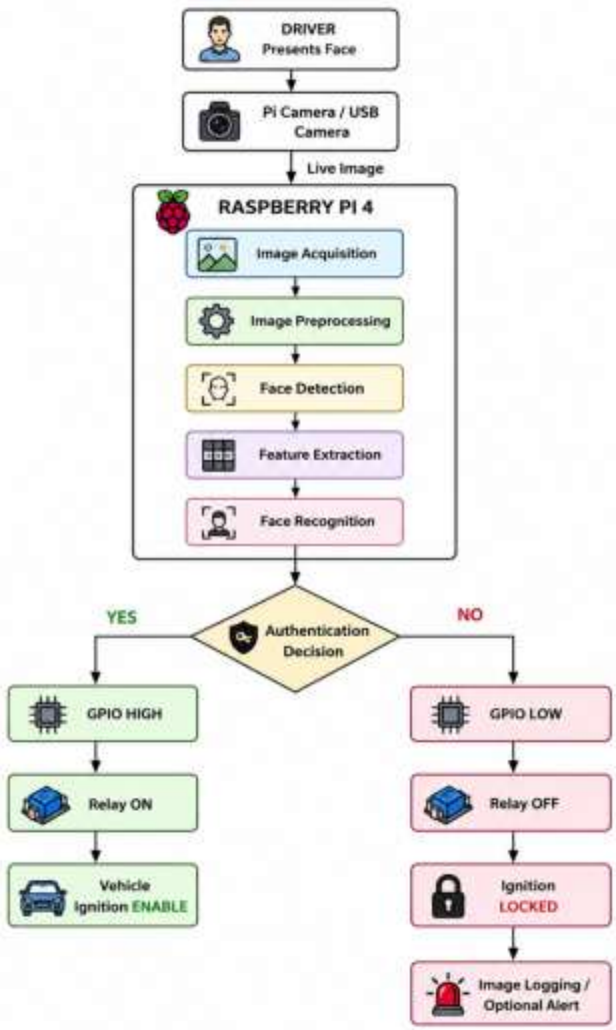

Figure 1 The overall architecture of the proposed system

The camera captures the driver's face and transfers the image to the Raspberry Pi 4. The Raspberry Pi performs preprocessing and face detection. Once the facial region is identified, the recognition module extracts facial features or embeddings and compares them with registered authorized-user information. If the detected driver satisfies the authentication criterion, the Raspberry Pi generates a GPIO control signal. The signal activates the relay interface, thereby enabling the vehicle ignition mechanism. If authentication fails, the relay remains inactive and the ignition remains locked.

The Raspberry Pi 4 acts as the central controller. Its functions include camera interfacing, image processing, face detection, feature extraction, recognition, authentication, GPIO control, relay operation, and security logging. Local processing is particularly beneficial for vehicle applications because the authentication decision does not have to depend completely on continuous Internet connectivity. The local architecture also reduces the dependency on remote processing for the basic access-control operation.

A Pi Camera or USB camera can be used for facial image acquisition. The camera is positioned to capture the driver's face during the authentication process. During registration, multiple images of an

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

authorized driver can be captured under different orientations and illumination conditions. These samples are processed and their facial representations are stored in the authorized-user database. During authentication, live frames are acquired and passed to the detection and recognition pipeline. Factors such as camera distance, illumination, facial orientation, spectacles, expression, and partial occlusion can affect recognition performance. The proposed system maintains facial information corresponding to registered users. During registration, facial images are acquired and processed to generate features or embeddings. During authentication, the representation generated from the live image is compared with the stored representations. The database can support multiple authorized drivers, allowing the system to be extended to fleet vehicles, institutional vehicles, rental vehicles, or shared transportation systems.

IV. METHODOLOGY

The registration process establishes the facial information required for subsequent authentication. The procedure consists of Starting the Raspberry Pi, Initializing the camera, Capturing multiple images of the authorized driver, Preprocessing the captured images, Detecting the facial region, Extracting facial features or embeddings and Storing the resulting facial representation in the local database. Multiple images are preferable because they allow the registered representation to account for changes in facial orientation and illumination. The project report specifies grayscale conversion, resizing, normalization, face detection, and feature extraction as part of the registration process.

The captured image is prepared before recognition. The preprocessing stage may include resizing, grayscale conversion, normalization, noise reduction, and facial-region extraction. Preprocessing reduces unnecessary variations in the input and provides a consistent representation to the face-detection and recognition stages.

The system identifies the facial region from the acquired image. Haar Cascade can be used as a computationally efficient detector. The processing sequence consists of camera-frame acquisition, grayscale conversion, face detection, and facial-region extraction. A DNN-based detector can be substituted when improved detection robustness is required. Once the facial region is detected, the system extracts features suitable for identity verification. Depending on the implementation, the system can employ LBPH descriptors, Dlib facial embeddings, or lightweight deep-learning models. For an embedding-based implementation, the facial representation generated from the live image is compared with representations stored in the authorized-user database. Euclidean distance or cosine similarity can be used as the comparison mechanism. The recognition threshold should be experimentally selected using genuine and impostor samples. A threshold that is too permissive may increase false acceptance, whereas an overly restrictive threshold may increase false rejection.

The authentication module produces one of two decisions: Authorized: The detected facial representation sufficiently matches an enrolled user. Unauthorized: No registered user satisfies the authentication criterion. For an authorized user, the Raspberry Pi enables the GPIO output and activates the relay. For an unauthorized user, the relay remains OFF and the ignition remains locked.

The GPIO interface connects the software authentication decision to the relay-control circuit. The relay acts as the switching interface between the Raspberry Pi and the ignition-control demonstration circuit.

When an unauthorized face is detected, the proposed system maintains the ignition in the locked state. An image of the attempted user can additionally be captured and stored as a security record. The architecture can be extended to send an alert through email, SMS, or an IoT/cloud service. This provides an additional security layer beyond simply rejecting the authentication attempt.

V. EXPERIMENTAL IMPLEMENTATION AND RESULTS

A prototype was designed using Raspberry Pi 4, a camera, OpenCV-based image processing, Haar Cascade face detection, and a GPIO-controlled relay. The experimental objective was to demonstrate the relationship between visual detection and physical access control. The camera captures live frames and transfers them to the Raspberry Pi. The image is converted into an appropriate format and processed using the Haar Cascade classifier. When a face is detected, the prototype generates an authorization output and activates the relay. When no face is detected, the relay remains inactive and the ignition-control interface remains locked. The implementation demonstrates the feasibility of combining camera-based computer vision with embedded hardware control. However, the supplied implementation code must be distinguished from the complete proposed recognition architecture. The code included in the project report detects the presence of a face and immediately sets the relay GPIO HIGH; it does not compare the detected face with an authorized-user database. Consequently, the present prototype should be described as a face-detection-based access-control demonstration, while authorized identity recognition represents the intended enhanced implementation.

Table 1. Functional behavior of the proposed system

Test Condition	Face Detection	Authentication	Relay	Ignition
Authorized user	Detected	Successful	ON	Enabled
Unauthorized user	Detected	Failed	OFF	Locked
No face	Not detected	Not performed	OFF	Locked

The prototype verifies the fundamental interaction between the camera, Raspberry Pi, face-detection process, GPIO output, and relay interface. The Raspberry Pi performs local processing and generates the hardware-control decision. The principal functional advantage is that the system does not stop at detecting or identifying a face. The authentication decision is intended to directly control physical vehicle access. This provides a clear relationship between biometric verification and vehicle-start authorization.

The system also provides an extensible mechanism for unauthorized-access logging. When authentication fails, an image can be captured and stored. The event can subsequently be transmitted through an optional email, SMS, or IoT service. This feature can be particularly useful in vehicles where repeated unauthorized attempts need to be recorded for subsequent analysis. The source report explicitly proposes image logging and optional notification functionality.

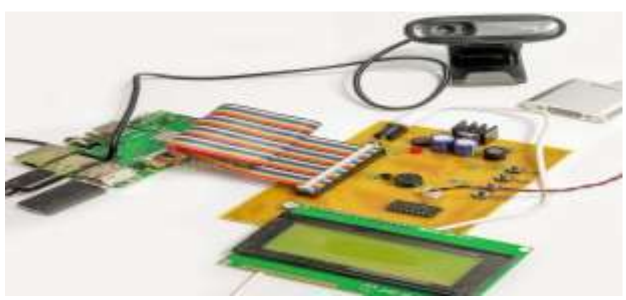

Figure 2 Experimental Output

VI. CONCLUSION

This paper presented a Raspberry Pi-based intelligent vehicle starter system that integrates computer vision, biometric authentication, embedded processing, and relay-based vehicle access control. The proposed architecture uses a camera to acquire the driver's facial information and a Raspberry Pi 4 to perform image processing, face detection, recognition, authentication, and hardware control. The central concept is to establish a direct connection between driver authentication and vehicle ignition authorization. A successfully authenticated driver is permitted to activate the ignition-control interface, whereas an unauthorized driver is denied access. The system additionally provides the possibility of security-event logging and remote notification. The prototype demonstrates the feasibility of implementing camera-based access control and relay operation using Raspberry Pi and OpenCV. However, the supplied prototype code currently implements face detection rather than complete authorized-user recognition. Therefore, the next stage of development should integrate a validated facial-recognition model and authorized-user database before claiming biometric identity authentication performance. With the addition of lightweight deep-learning recognition, liveness detection, quantitative evaluation, and automotive-grade hardware isolation, the proposed architecture can evolve into a more robust intelligent vehicle-security platform.

REFERENCES

[1] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2001.

[2] G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, "Labeled Faces in the Wild: A database for studying face recognition in unconstrained environments," University of Massachusetts, Amherst, Technical Report 07-49, 2007.

[3] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2015.

[4] R. Ranjan *et al.*, "Deep learning for face recognition: A critical analysis," arXiv preprint arXiv:1605.02863, 2016.

[5] D. E. King, "Dlib-ml: A machine learning toolkit," *Journal of Machine Learning Research*, vol. 10, pp. 1755–1758, 2009.

[6] A. Rahman, M. R. Islam, and M. S. Hossain, "IoT-based smart home security system using Raspberry Pi and cloud computing," *International Journal of Computer Applications*, vol. 182, no. 43, pp. 20–26, 2021.

[7] S. Zhang, X. Zhu, Z. Lei, H. Shi, X. Wang, and S. Z. Li, "S^3FD: Single shot scale-invariant face detector," *Proceedings of the IEEE International Conference on Computer Vision*, 2017.

[8] S. Kumar and R. Mehta, "Face-recognition-based vehicle ignition using embedded controller," *International Journal of Engineering Research & Technology*, vol. 11, no. 5, pp. 1–6, 2022.

[9] Raspberry Pi Foundation, "Raspberry Pi 4 Model B Technical Documentation," 2019.

[10] M. Turk and A. Pentland, "Eigenfaces for recognition," *Journal of Cognitive Neuroscience*, vol. 3, no. 1, pp. 71–86, 1991.