Vehicle Security: Raspberry PI Based Vehicle Starter on Face Detection

Mrs. MASEEHA BANU [1], DUSHYANTH H M [2], HARSHAN H R [3], VARUN KUMAR C K [4], VINAY N V [5]

[1] *Assistant. Professor, Dept. of Information Science & Engineering, Rajeev Institute of Technology, Hassan*
[2] *Information Science & Engineering, Rajeev Institute of Technology, Hassan*
[3] *Information Science & Engineering, Rajeev Institute of Technology, Hassan*
[4] *Information Science & Engineering, Rajeev Institute of Technology, Hassan*
[5] *Information Science & Engineering, Rajeev Institute of Technology, Hassan*

---***---

Abstract - The "Raspberry-Pi Based Vehicle Starter on Face Detection" project integrates facial recognition technology with biometric authentication to improve vehicle security. The system uses a camera module to take real-time facial photographs, which are then processed by OpenCV and machine learning algorithms on a Raspberry Pi, which serves as the central processing unit. The ignition system is activated by an electronic relay circuit upon successful recognition, allowing only authorized individuals to start the car. Unauthorized attempts are recorded, and for further security, alarms can be issued by SMS or email. By doing away with real keys, this creative method lowers the possibility of theft and unwanted entry. The technology guarantees an affordable, scalable, and user-friendly solution for contemporary vehicle security by combining embedded systems, computer vision, and the Internet of Things. The project intends to improve ease and safety by offering a workable, dependable, and clever substitute for conventional vehicle entry techniques.

Key words: camera vision, image processing, guidance system, and face recognition.

1. INTRODUCTION

Since conventional techniques like physical keys and keyless entry systems are becoming more and more susceptible to theft, copying, and hacking, vehicle security is a major worry. Biometric authentication, especially facial recognition, offers a safe and automated way to solve these security issues. In order to improve security, do away with physical keys, and automate car access, this project introduces a Raspberry Pi-based vehicle starter system that combines computer vision and the Internet of Things. The solution makes sure that only authorized individuals may start the car by employing machine learning algorithms for authentication and a camera module to take real-time facial images. Access is blocked and the owner may receive an alert if an unidentified face is found.

Grade I: Vehicle theft is a serious worldwide issue since millions of cars are stolen annually as a result of antiquated security measures. Conventional security solutions like RFID-based entry systems and keys are vulnerable to hackers, loss, and duplication. Using facial recognition technology based on machine learning for vehicle access control provides a cutting-edge, effective, and extremely safe substitute. Only authorized persons are able to start automobiles thanks to this system, which increases security and lowers the danger of theft. It also offers a smooth user experience by removing typical annoyances related to misplaced or stolen keys.

Grade II: Artificial intelligence and deep learning have greatly increased the precision and effectiveness of car access control systems. Convolutional Neural Networks (CNNs), Haar cascades, and Support Vector Machines (SVMs) are used in this project's facial recognition methods to verify users. By doing away with the need for conventional access methods, the system increases security, decreases human error, and automates the vehicle startup procedure. The automatic classification and verification approach ensures a safe yet user-friendly car ignition system by providing faster and more dependable results than human authentication systems.

Grade III: Beyond merely providing security, machine learning-powered car authentication systems also support intelligent automation and customized vehicle control. The technology may alter climate control, seat settings, and driving preferences according to the recognized driver by examining user data and facial recognition trends. Furthermore, remote monitoring and access management are made possible by cloud-based authentication, which enables car owners to permit or deny access through a mobile application. Improved fleet management, intelligent transportation, and customized car experiences are made possible by these AI-driven developments.

Grade IV: Beyond only individual users, machine learning-powered car security has an impact on the automobile industry's accessibility and economic efficiency. Users may remotely assess and manage vehicle security by combining AI-driven access control with mobile applications, greatly lowering the need for physical key replacements. By guaranteeing that only authorized personnel are able to operate the vehicles, this technology can further improve security in ride-sharing and automobile rental businesses. Digital access control solutions can improve transparency and efficiency in vehicle security management by streamlining legal and insurance claims procedures.

Using AI-based authentication systems like CNN, SVM, and KNN guarantees quick, safe, and intelligent vehicle access control as the automotive sector adopts smart security solutions. Future developments like GPS-based tracking, fingerprint identification, and voice authentication will increase security while enhancing usability. By laying the groundwork for next-generation vehicle security, this invention opens the door to intelligent and networked transportation systems. Future developments like GPS-based monitoring, voice authentication, and fingerprint recognition will strengthen security protocols while simultaneously providing a smooth and customized user experience. Vehicles can be remotely monitored and controlled by combining biometric authentication with real-time location tracking. This enables owners to lock, unlock, or even disable their vehicles in the event of theft or unwanted access.

2. LITERATURE REVIEW

A literature review is a crucial step in the software development process since it offers information on current studies and advancements in car security systems. This section outlines important research that shaped the creation of the facial recognition-based vehicle starter system based on the Raspberry Pi. The integration of biometric authentication in automobile security was examined by Singh et al. (2023), who emphasized the benefits of facial recognition over conventional key-based systems. Their research showed how face identification models driven by AI enhance the prevention of auto theft by lowering the dangers of key duplication and illegal entry. The study made clear how urgently real-time facial authentication technologies that guarantee quick and precise user verification are needed.

Kumar et al.'s (2023) study concentrated on facial recognition using deep learning for safe access control. Convolutional neural networks (CNNs) and Haar cascades were used in their suggested approach to accurately detect and classify faces. The findings supported the promise of computer vision in car security by showing improved authentication accuracy and decreased false acceptance rates.

A comparative analysis of CNN, SVM, and KNN algorithms for vehicle security applications was carried out by Patel and Ramesh (2022). According to their research, CNN-based models performed better on face recognition tasks than conventional machine learning methods. In order to enhance real-time driver authentication, they underlined the significance of feature extraction techniques and dataset variety.

Chitra et al. (2023) presented a hybrid AI model for real-time facial recognition in automotive applications that combines CNNs with conventional ML techniques. Their methodology addressed frequent issues in real-world deployments by increasing detection accuracy under a range of illumination and environmental conditions.

3. SYSTEM DESIGN

Existing system:

Physical keys, RFID-based access, and keyless entry technologies are the mainstays of conventional car security systems. Despite their widespread use, these techniques have a number of drawbacks. While keyless entry systems are vulnerable to hacking efforts and relay attacks, physical keys can be misplaced, stolen, or copied. Furthermore, conventional car access techniques are becoming less and less dependable due to security flaws including signal interception and hot wiring.

.

While some contemporary security systems incorporate remote locking or PIN-based authentication, these solutions still rely on human interaction and lack real-time biometric verification. Although some cars now have fingerprint-based ignition systems, their usefulness is restricted by environmental factors that might alter recognition accuracy and sensor degradation.

Proposed system:

Through facial recognition-based identification, the suggested solution combines deep learning, computer vision, and the Internet of Things to improve vehicle security. The system uses K-Nearest Neighbors (KNN), Convolutional Neural Networks (CNNs), and Support Vector Machines (SVM) to automate real-time driver authentication and guarantee that only authorized users can start the car. The technology uses a methodical process, first acquiring images via a camera module and then employing sophisticated feature extraction techniques to discover and recognize faces. As the central computing unit, the Raspberry Pi manages real-time picture analysis and manages a relay module that, after successful authentication, turns on the car's ignition. Unauthorized access attempts are recorded, and the owner can be notified via email or SMS notifications.

4. METHODOLOGY

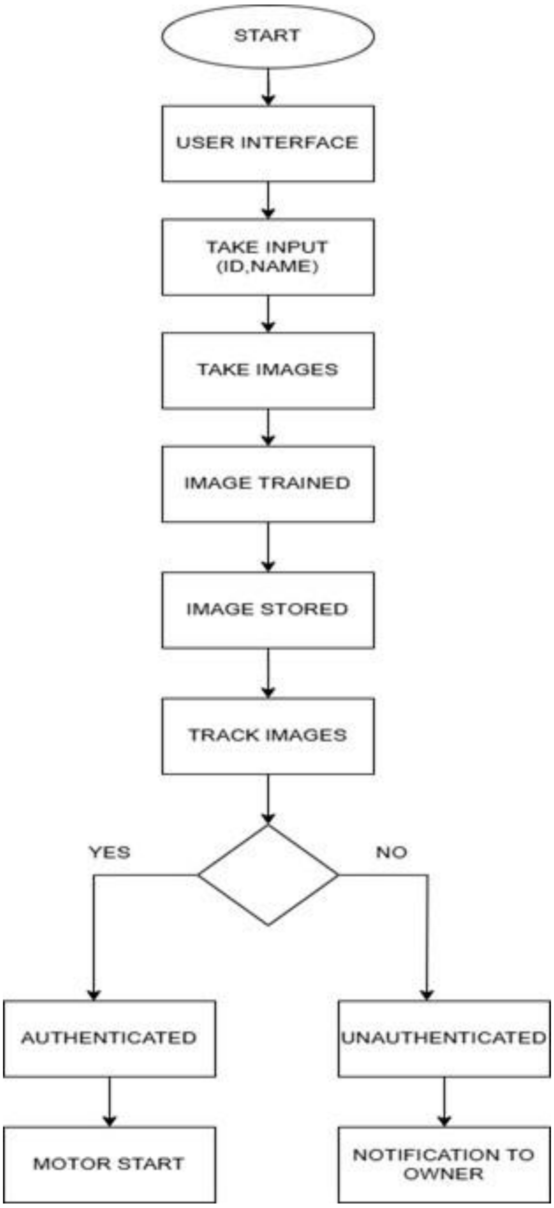

Figure 1: Dataflow Diagram

For safe vehicle authentication, the suggested solution integrates deep learning, computer vision, and the Internet of Things using an organized methodology. A camera module attached to a Raspberry Pi is used to acquire photographs at the start of the procedure, taking real-time pictures of the user's face. Convolutional Neural Networks (CNNs), Support Vector Machines (SVM), and K-Nearest Neighbors (KNN) are used for face identification and recognition after these photos have undergone preprocessing using OpenCV for noise reduction and feature extraction. To guarantee that only authorized users can start the car, the Raspberry Pi activates the ignition system by triggering a relay module upon successful authentication. The system records any attempt at unauthorized access and has the ability to notify users via SMS or email. Users may adjust access control and keep an eye on authentication logs in real time with the Graphical User Interface (GUI). With the possible addition of voice recognition, multi-factor authentication, and mobile-based remote access, the system guarantees scalability while improving user ease and overall security.

5. CONCLUSIONS

The Raspberry Pi-Based Vehicle Starter System is a cutting-edge security solution that uses machine learning and deep learning to improve facial recognition and vehicle identification. A secure and smooth vehicle access mechanism is ensured by the system's efficient detection and verification of authorized users through the application of classification algorithms including Convolutional Neural Networks (CNNs), Support Vector Machines (SVM), and K-Nearest Neighbors (KNN). Physical keys are no longer necessary thanks to the incorporation of AI-driven face recognition, greatly lowering the possibility of theft and unwanted entry. By automating the authentication process and integrating IoT to provide remote access control and real-time monitoring, the system also enhances security. This experiment shows how smart car security systems driven by AI have the potential to revolutionize automotive safety. Multi-factor authentication, voice recognition, fingerprint scanning, and GPS-based tracking are examples of future developments that will improve vehicle security and accessibility even more while opening the door for intelligent and networked transportation systems.

6. FUTURE DIRECTIONS

Future developments in the Raspberry Pi-Based Vehicle Starter System have the potential to greatly improve user ease, security, and accessibility. Users will be able to manage vehicle security from any location thanks to the creation of mobile applications for remote vehicle access, monitoring, and authentication management. To further enhance security, telematics and IoT integration can provide automatic lock/unlock capabilities, real-time vehicle tracking, and theft alarms. To further improve access control, multi-factor authentication techniques including voice recognition, fingerprint scanning, and PIN verification can be used**.** AI-driven anomaly detection, which detects suspicious activity and unauthorized access attempts and sends out proactive security notifications, may also be a future development. Additionally, data-driven insights for fleet management, usage monitoring, and security audits can be made easier with integration with cloud-based analytics. These developments will help smart car security systems advance, guaranteeing a safer, smarter, and more connected automotive future.

REFERENCES

[1] Bhand Nishigandha Padmakar, Kolse Pooja Ravindra, Bankar Akash Dnyaneshwar, Anap Sachin Dattatray, and Chitte Pankaj Pramod (2021). Face-Detection-Based Vehicle Starter Using Raspberry Pi. [Name of Journal/Conference]

[2] Raj Kamal (Year). Principles of Internet of Things Architecture & Design. McGraw Hill Schooling.

[3] Andreas Willig and Holger Karl (2005). Wireless Sensor Network Architectures and Protocols. Wiley & Sons, John.

[4] Leonidas J. Guibas and Freng Zhao (2007). An approach to information processing for wireless sensor networks. Elsevier.

[5] Daniel Minoli, Taieb Znati, and Kazem Sohraby (2007). The technology, protocols, and applications of wireless sensor networks. Wiley & Sons, John.