Advanced Vehicle Locking System Using Facial Recognition

Bhushan Dive
Electronics Engineering
Yeshwantrao Chavan College of Engineering
Nagpur, India.
bhushandive43@gmail.com

Vedant Gaherwar
Electronics Engineering
Yeshwantrao Chavan College of Engineering
Nagpur, India.
vedant.phoenix07@gmail.com

Pratham Karmarkar
Electronics Engineering
Yeshwantrao Chavan College of Engineering
Nagpur, India.
prathamkarmarkar09@gmail.com

Spruha Kango
Electronics Engineering
Yeshwantrao Chavan College of Engineering
Nagpur, India.
spruhakango942@gmail.com

Aditya Nimje
Electronics Engineering
Yeshwantrao Chavan College of Engineering
Nagpur, India.
adsne19@gmail.com

Access control systems are crucial for vehicle security. This study presents an innovative method employing a Raspberry Pi-based system integrated with face-api.js, along with dlib libraries, to establish a secure vehicle access control system. Facial recognition algorithms are utilized for user authentication, adding an extra level of security. Any unauthorized access prompts an alert to the administrator, improving real-time monitoring and response capabilities.

I. INTRODUCTION (*HEADING 1*)

The advent of sophisticated technology has revolutionized various aspects of our daily lives, including the way we approach vehicle security. As the number of vehicles on the road continues to rise, ensuring their safety becomes an imperative concern. Traditional methods of securing vehicles, such as key-based systems and electronic locks, while effective to some extent, are susceptible to breaches and unauthorized access. This underscores the necessity for advanced and reliable access control systems that leverage cutting-edge technologies.

II. Problem Statement

The limitations of conventional car security systems have become increasingly evident in the face of evolving security threats. Instances of unauthorized access and vehicle theft persist, emphasizing the need for innovative solutions. Recognizing faces as a means of identification, a concept popularized by advancements in facial recognition technology, presents an intriguing avenue for enhancing vehicle security. Integrating this technology into a secure access control system can potentially address the vulnerabilities associated with traditional methods.

A. Objectives

This research endeavours to rectify the limitations of current vehicle access control systems by proposing and implementing a comprehensive solution. The primary objectives are threefold: firstly, to design a robust system utilizing the Raspberry Pi as the core platform; secondly, to integrate advanced face recognition technology using the face-api.js library, contributing to accurate user identification; and thirdly, to establish a notification mechanism that promptly alerts administrators in the event of unauthorized access. The accomplishment of these objectives is anticipated to significantly contribute to the progression of secure vehicle access control systems. The subsequent sections will intricately explore the methodology employed, delve into the intricacies of the system architecture, and present detailed insights into the research outcomes. By adopting a holistic approach and embracing emerging technologies, this research aspires to set new benchmarks in vehicular access control security. Through innovative strategies and exploration of cutting-edge technologies, we aim to pave the way for enhanced security measures and foster advancements in the domain of vehicular access control.

III. PREVIOUS SOLUTIONS

The Idea of secure access to personal vehicles is not new and has been implemented in various ways for a long time. Although the security of these mechanisms varies. We will take a look at some of these mechanisms.

A. Key Based Systems

Historically, key-based systems have been the cornerstone of personal vehicular access. This straightforward mechanism involves the use of physical keys to unlock and start a vehicle. While simple, this approach is prone to vulnerabilities such as key loss, theft, or unauthorized duplication. These simple systems have a lot of problems with it. As it is very easy to duplicate and forge a fake key, the security provided by these systems is very weak.

B. RFID (Radio Frequency Identification Devices) Cards

RFID cards have gained popularity as a convenient means of vehicular access control. These cards utilize radio-frequency

signals to communicate with a reader installed in the vehicle. While RFID systems offer improved security compared to traditional keys, they are not immune to issues such as card cloning or interception of RFID signals. Additionally, the physical nature of the cards poses a risk of loss or theft and effectively renders them as a simple key based system.

C. Electronic Fobs and Remote Controls

Electronic fobs and remote control devices have become commonplace for unlocking and starting vehicles. These systems often employ rolling code technology to enhance security. However, vulnerabilities such as signal interception and relay attacks have been demonstrated, raising concerns about the robustness of these access control mechanisms.

D. Biometric Authentication

Some innovative approaches to personal vehicular access involve biometric authentication methods. Fingerprint recognition and iris scanning systems have been explored to replace traditional key-based or card-based systems. While biometric authentication provides a more unique and personalized method of access, concerns related to accuracy, environmental conditions, and the potential for spoofing have been raised.

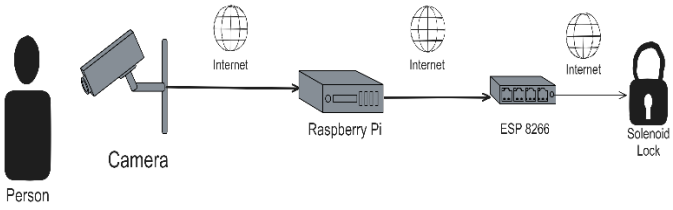
E. Emerging Technologies

Recent advancements in technology have given rise to smart access systems, including smartphone-based applications and digital key solutions. These systems leverage Bluetooth, NFC (Near Field Communication), or other wireless communication protocols to establish a secure connection between the user's device and the vehicle. While these technologies offer the convenience of remote access and digital keys, cybersecurity challenges, device compatibility, and dependency on battery-powered devices are aspects that require consideration.

IV. PROPOSED SOLUTION

A. Hardware Setup

Our proposed secure vehicle access control system centres around a Raspberry Pi-based architecture. A handheld device, seamlessly integrated into the vehicle's interior, incorporates a Raspberry Pi 4B with an attached high-resolution camera module. This compact setup is designed for versatility, fitting into any car model. The handheld device is strategically wired into the car's ignition system, forming a cohesive unit.



B. Software Implementation

The software stack harnesses the capabilities of face-api.js for robust facial detection and authentication. Face-api.js, an advanced JavaScript library for face recognition, stands as a cornerstone in our system's development. This library integrates essential functionalities for facial analysis, detection, and recognition, offering a comprehensive and efficient solution. Through the power of face-api.js, our system benefits from advanced algorithms that enable accurate identification and real-time performance. Python scripts continue to play a vital role in orchestrating the seamless interaction between hardware components, ensuring the unified functionality of the system.

C. Face Recognition Algorithms

The core strength of our system resides in the advanced face recognition algorithm. Utilizing the face-api.js library, our algorithm taps into the robust detection algorithms embedded within this powerful library. Face-api.js provides state-of-the-art face detection and recognition capabilities, enhancing the system's proficiency in identifying facial features accurately.

Harnessing the power of deep learning models integrated into the face-api.js library, our algorithm excels in detecting and recognizing facial features with remarkable precision. This approach ensures reliable performance even under diverse lighting conditions and varying facial angles, contributing to the system's effectiveness in real-world scenarios. The use of face-api.js not only streamlines the implementation but also capitalizes on the library's continuous development and refinement, ensuring our system remains at the forefront of facial recognition technology.

D. Authentication Process

As a user approaches the vehicle, the system initiates the authentication process. The camera captures facial features, and the face recognition algorithm compares the captured image with pre-registered facial data. If a match is confirmed, the system grants access to the vehicle, enabling the ignition system. In cases of unauthorized attempts, the backend system comes into play.

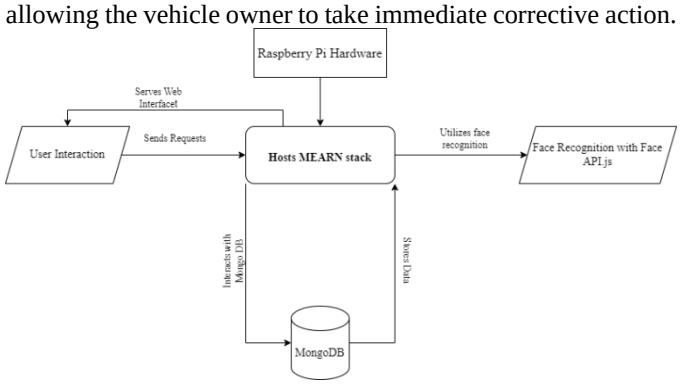
E. Notification System

The backend system, developed using Express.js and the MERN (MongoDB, Express.js, React, Node.js) stack, is responsible for handling security incidents. Upon detecting an unauthorized access attempt, the backend system swiftly

triggers a notification. This notification is sent to the vehicle owner's designated device, providing real-time information about the security breach. The integration of this notification system enhances the system's responsiveness and aids in immediate corrective action.

F. System Architecture

The architecture of our system is designed for seamless functionality. The camera captures facial images, which are processed by the Raspberry Pi using the face recognition algorithm. Successful authentication triggers vehicle access, while unauthorized attempts activate the backend notification system. This secure communication ensures prompt alerts, allowing the vehicle owner to take immediate corrective action.



G. Security Measures

To fortify the security of our solution, we have implemented robust encryption protocols for both storing and transmitting facial data. Continuous monitoring of the system's health, coupled with regular updates and patches, ensures the system's reliability and resilience against potential vulnerabilities.

H. User Friendly Interfaces

The system features a user-friendly interface for administrators. This interface facilitates the registration of new users, allowing the easy management of authorized individuals. Additionally, the interface provides comprehensive insights into system performance and security incidents, contributing to a streamlined user experience.

V. CONCLUSION

The proposed solution synergizes the capabilities of Raspberry Pi and leverages the face-api.js library, providing a dynamic foundation for a secure and efficient vehicle access control system. This amalgamation of hardware and cutting-edge facial recognition technology transcends the limitations inherent in traditional access methods, offering an enhanced level of vehicular security. Subsequent sections will meticulously delve into the implementation details, results, and discussions, presenting a thorough analysis of the system's functionality and performance. This shift to face-api.js marks a strategic choice in pursuit of more advanced and flexible facial recognition capabilities, reflecting our commitment to staying at the forefront of emerging technologies in vehicular access control.

REFERENCES

[1] S. Mohanasundaram, V. Krishnan and V. Madhubala, "Vehicle Theft Tracking, Detecting And Locking System Using Open CV," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 2019, pp. 1075-1078, doi: 10.1109/ICACCS.2019.8728460.

[2] V. S. Katti, D. Sweshitha, S. Mahendra and S. M. Akash, "Anti-Theft Face Recognition and Alcohol Detection Car Ignition System," 2023 IEEE Women in Technology Conference (WINTECHCON), Bangalore, India, 2023, pp. 1-6, doi: 10.1109/WINTECHCON58518.2023.10277468.

[3] S. fasiuddin, S. Omer, K. Sohelrana, A. Tamkeen and M. A. Rasheed, "Real Time Application of Vehicle Anti Theft Detection and Protection with Shock Using Facial Recognition and IoT Notification," 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2020, pp. 1039-1044, doi: 10.1109/ICCMC48092.2020.ICCMC-000194.