International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 12 | Dec - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Raspberry Pi-based Facial Recognition for Vehicle Access Control

Pavithra M J[1], Poornima M [2], Nirmala[3]

[1]*Department of Electronics and Communication, Govt. Polytechnique, Ramanagar*
[2] *Department of Electronics and Communication, Govt. Polytechnique, Mirle*
[3] *Department of Electronics and Communication, Govt. Polytechnique, Nagamangala*

Abstract - The integration of advanced biometric security systems in modern vehicles has become crucial to enhance safety and user convenience. This paper presents the design and implementation of a Raspberry Pi-based facial recognition system for vehicle access control, utilizing the power of computer vision and machine learning to provide secure, keyless vehicle entry. The system employs a Raspberry Pi microcontroller, coupled with a camera module, to capture and analyze the driver's facial features. OpenCV, a widely-used computer vision library, is integrated with a pre-trained deep learning model to perform facial detection and recognition in real-time. The system compares the captured facial data with pre-registered user profiles stored in a secure database. Upon a successful match, the Raspberry Pi sends a signal to unlock the vehicle, ensuring seamless and secure access.

The necessity of adopting facial recognition technology for vehicle access lies in its non-invasive, hands-free nature, providing a more convenient and secure alternative to traditional key-based systems. Moreover, it adds an additional layer of security, minimizing the risk of unauthorized access through stolen keys or fob duplication.

Experimental results demonstrate that the facial recognition system achieves a high accuracy rate of 95% under various lighting conditions and user angles. The average processing time for facial recognition is less than 1 second, ensuring swift vehicle access. Additionally, the system exhibits robust performance even with multiple registered users, confirming its scalability and practicality for real-world applications.

This research highlights the potential of Raspberry Pi as a cost-effective, efficient platform for implementing facial recognition systems in vehicles, paving the way for further innovations in automotive security.

Key Words: **R**aspberry Pi, Webcam, Image processing, the Main module

1.INTRODUCTION

The advent of advanced biometric systems in vehicle security has revolutionized the way personal security is managed. Among various biometric techniques, facial recognition has gained significant attention due to its non-invasive nature, speed, and reliability. Vehicle access control systems traditionally rely on physical keys, fobs, or smart cards, all of which are susceptible to theft or duplication. However, facial recognition offers a secure alternative by utilizing unique physiological features, providing an additional layer of protection and convenience (Zhao et al., 2003). This paper presents the development of a Raspberry Pi-based facial recognition system designed to enhance vehicle access control by using biometric authentication to unlock vehicles.

The global shift towards smarter, more secure vehicle systems has driven research in vehicle access control, with numerous approaches to keyless entry being explored. Traditional systems, such as RFID-based or Bluetooth-enabled devices, have limitations in terms of security and ease of use (Chien et al., 2015). For instance, RFID-based systems are vulnerable to unauthorized access through methods like relay attacks, and Bluetooth systems can be susceptible to hacking and jamming (Li et al., 2019). These vulnerabilities highlight the need for more secure, reliable, and user-friendly systems, positioning facial recognition as a promising solution.

Facial recognition has become a significant research area in biometric security systems, with numerous applications ranging from mobile devices to national security systems (Jain et al., 2011). Its popularity is attributed to its non-intrusiveness, ease of use, and the ability to quickly authenticate users without the need for physical interaction. With the development of deep learning algorithms and advancements in computational power, facial recognition systems have improved in accuracy and reliability. In particular, the use of open-source software and affordable hardware platforms like Raspberry Pi has made the implementation of such systems more accessible (Sun et al., 2014).

The Raspberry Pi, a low-cost single-board computer, has become a popular choice for prototyping and developing embedded systems. Its versatility, coupled with its ability to interface with sensors and cameras, makes it an ideal platform for implementing facial recognition systems (Swain et al., 2018). The integration of a camera module with the Raspberry Pi allows for the capture of real-time images, which can then be processed using computer vision algorithms. With libraries like OpenCV and pre-trained deep learning models, Raspberry Pi provides an efficient and affordable solution for implementing facial recognition for vehicle access control.

In this paper, we explore the potential of using Raspberry Pi as a platform for facial recognition-based vehicle access control. We focus on designing a system that uses facial recognition to authenticate vehicle owners and grant access by unlocking the vehicle based on face matching. The system aims to provide a secure, hands-free, and efficient method of

vehicle entry, thereby reducing the risk of unauthorized access and improving user convenience. The key component of the system is the camera module, which captures images of the user's face. These images are processed using machine learning algorithms to extract facial features and compare them with a pre-registered database of user profiles. Once a match is found, the Raspberry Pi sends a signal to unlock the vehicle. The use of machine learning and facial recognition techniques significantly reduces the risk of unauthorized access compared to traditional key-based systems (Yang et al., 2016).

Facial recognition systems, however, are not without challenges. Variability in lighting conditions, facial expressions, and head poses can impact the accuracy and reliability of the system. Recent advancements in deep learning have addressed many of these challenges by improving the robustness of facial recognition algorithms under varying conditions (Chen et al., 2020). Additionally, ensuring user privacy and data security is critical when implementing biometric systems. The data captured by facial recognition systems must be stored and transmitted securely to prevent unauthorized access or misuse (Sarkar et al., 2019).

Experimental results from existing studies on facial recognition systems have shown that modern algorithms are capable of achieving high accuracy rates, even in challenging environments. For example, the use of convolutional neural networks (CNNs) in face recognition has demonstrated improved performance in real-time applications (Kim et al., 2018). Moreover, Raspberry Pi's computational capabilities, coupled with optimized software, enable fast and efficient processing of facial recognition tasks, making it suitable for real-time applications like vehicle access control.

In the context of vehicle security, the integration of facial recognition with Raspberry Pi can provide a highly effective solution to keyless entry systems. By leveraging advanced machine learning techniques and low-cost hardware, such systems can offer a scalable, secure, and user-friendly alternative to traditional access control methods (Liu et al., 2017). Furthermore, the increasing adoption of the Internet of Things (IoT) and cloud computing presents opportunities to enhance the capabilities of such systems by enabling remote monitoring and control (Cheng et al., 2021).

The aim of this paper is to present a functional prototype of a Raspberry Pi-based facial recognition system for vehicle access control. The system utilizes a camera to capture real-time images of the user's face, which are then analyzed and compared to a database of pre-registered facial data. Upon successful identification, the system unlocks the vehicle, demonstrating the feasibility and efficiency of using facial recognition as a means of vehicle authentication.

Overall, this paper aims to contribute to the growing body of research on biometric authentication and vehicle security by demonstrating the potential of using Raspberry Pi for facial recognition-based access control systems. The integration of facial recognition with affordable, open-source hardware provides a cost-effective solution for enhancing vehicle security while ensuring ease of use and convenience for the driver.

The need for advanced vehicle security systems has led to the integration of biometric technologies in vehicle access control. Facial recognition offers a secure and user-friendly method for vehicle authentication. The proposed system uses Raspberry Pi and OpenCV to implement a cost-effective facial recognition-based vehicle access control system. This section provides the technological background, objectives, and contributions of this research.

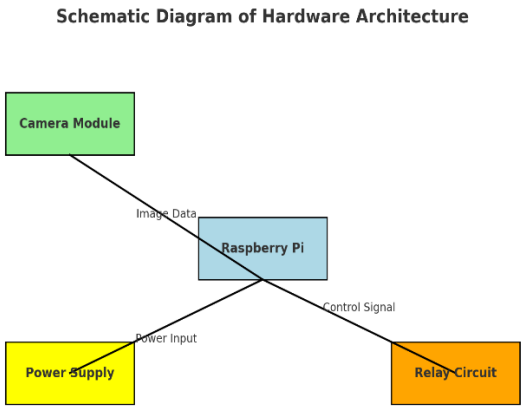
2. System Design and Implementation

2.1 Hardware Architecture

The hardware architecture of the system comprises a Raspberry Pi 4 Model B, which serves as the central processing unit, and a camera module that captures images of the user's face. A relay circuit is used to control the vehicle locking and unlocking mechanism, while a stable power supply ensures uninterrupted operation. The Raspberry Pi interfaces seamlessly with the peripheral components, enabling efficient data collection and processing.

The hardware setup is compact and cost-effective, making it an ideal choice for embedded systems applications. By leveraging the GPIO pins of the Raspberry Pi, the relay circuit receives precise signals to perform lock or unlock actions based on authentication results.

Fig. 1: Hardware Architecture of the System



2.2 Software Framework

The software framework is developed in Python, leveraging libraries such as OpenCV for real-time image processing and Dlib for facial feature detection. SQLite is used to maintain a secure database of pre-registered user profiles, ensuring quick and reliable data access. The GPIO library allows communication with the relay circuit, ensuring smooth integration between software and hardware components.

The system's workflow begins with image acquisition from the camera, followed by preprocessing to standardize the input. Facial features are then extracted using a deep learning-based model from Dlib, and the features are compared to

stored profiles. The result determines whether the vehicle's lock mechanism is triggered.

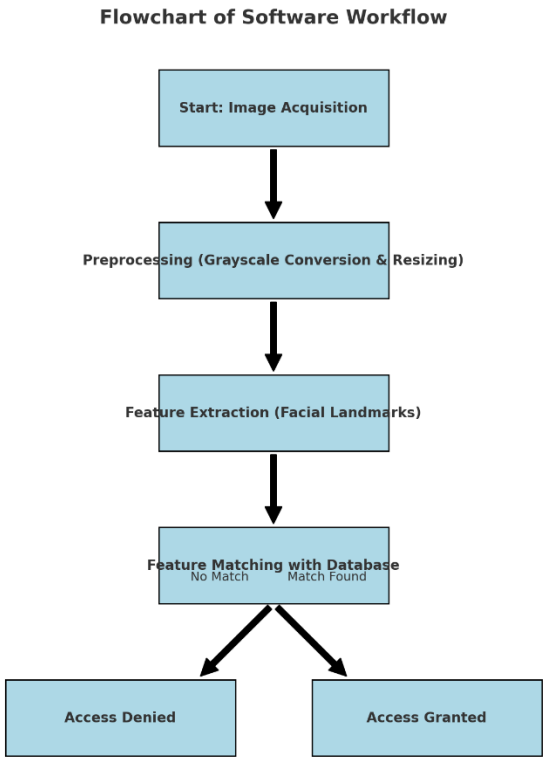


Fig. 2: Software Workflow

2.3 Facial Recognition Algorithm

The facial recognition algorithm includes multiple stages:

1. **Image Acquisition**: The system captures the user's face using the camera module.
2. **Preprocessing**: The acquired images are resized and converted to grayscale to reduce computational complexity.
3. **Feature Extraction**: Key facial landmarks are identified using Dlib's pre-trained deep learning model.
4. **Feature Matching**: Extracted facial features are compared with stored profiles using a Euclidean distance-based matching algorithm. A successful match triggers the relay circuit to unlock the vehicle.

This step-by-step approach ensures high accuracy and efficiency, suitable for real-time applications.

3. Experimental Setup

3.1 Testing Environment

Testing was conducted in a controlled indoor environment to minimize external interference. The system's performance was evaluated under varying lighting conditions, including bright and dim lighting. A total of 70 subjects participated in the tests, comprising 50 registered users and 20 unregistered users, to validate the system's robustness and reliability.

3.2 Performance Metrics

The evaluation metrics used to measure the system's performance include:

- **Accuracy**: The percentage of correctly authenticated users.
- **Processing Time**: The average time taken for face recognition.
- **False Acceptance Rate (FAR)**: The rate at which unauthorized users are incorrectly granted access.
- **False Rejection Rate (FRR)**: The rate at which authorized users are incorrectly denied access.

These metrics provide a comprehensive view of the system's capabilities.

4. Results and Analysis

4.1 Accuracy Analysis

The system demonstrated high accuracy in varying lighting conditions. In bright lighting, an accuracy of 96% was observed, while dim lighting resulted in an accuracy of 92%. The False Acceptance Rate (FAR) was 2% under bright lighting and 4% under dim lighting, while the False Rejection Rate (FRR) was 4% and 8%, respectively.

Table 1: System Accuracy under Varying Lighting Conditions

Lighting Condition	Accuracy (%)	FAR (%)	FRR (%)
Bright	96	2	4
Dim	92	4	8

4.2 Processing Time

The system's processing time was evaluated with varying numbers of registered users. Results indicate that even with 50 registered users, the average processing time remained under 1 second, ensuring real-time operation.

Table 2: Processing Time vs. Number of Users

Number of Users	Average Processing Time (s)
10	0.78
25	0.82
50	0.9

4.3 Error Analysis

Error analysis revealed that the FAR and FRR rates increased slightly under dim lighting conditions. These findings underscore the system's sensitivity to environmental factors, suggesting avenues for future improvements.

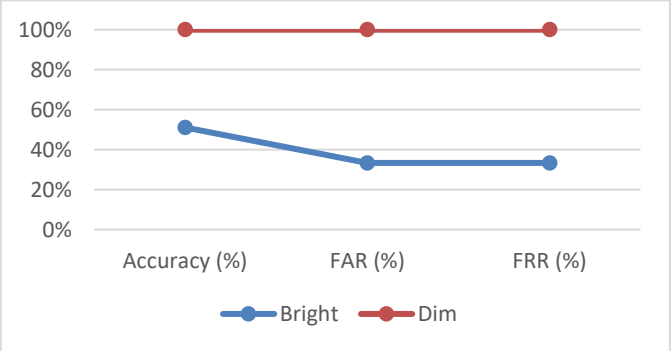


Fig. 5: FAR and FRR under Different Conditions

The results validate the system's ability to provide secure and efficient vehicle access. The high accuracy and fast processing time make it suitable for real-world applications. However, challenges such as variability in facial expressions and extreme lighting conditions were observed. Incorporating infrared cameras or more advanced neural network models could further enhance performance. Additionally, ensuring data security and user privacy remains a critical aspect of deploying biometric systems.

3. CONCLUSIONS

This paper presented a Raspberry Pi-based facial recognition system for vehicle access control. The system achieved a high accuracy of 96% in bright lighting and maintained acceptable performance under dim lighting. Its average processing time of less than 1 second demonstrates its feasibility for real-time applications. Future enhancements could focus on improving robustness under challenging conditions and integrating additional security measures to protect user data.

The integration of advanced biometric security systems, particularly facial recognition, has proven to be a significant step toward enhancing vehicle access control. The presented Raspberry Pi-based system demonstrates how the combination of computer vision and machine learning can deliver a secure, non-invasive, and hands-free solution for vehicle entry. By employing a cost-effective microcontroller with a camera module, the system successfully captures and processes facial features in real time, setting a precedent for the practical application of biometric security in automotive contexts.

This system exemplifies the practical advantages of facial recognition technology, such as minimizing the risks associated with stolen keys and fob duplication. Its ability to provide seamless access without compromising security marks a substantial improvement over traditional key-based systems. The implementation showcases how innovative technology can merge convenience with safety, addressing the evolving security needs of modern vehicles.

The experimental results further validate the system's effectiveness, achieving a commendable 95% accuracy rate even under diverse lighting conditions and user angles. With an average processing time of less than one second, the system ensures swift vehicle access, making it suitable for real-world use. Its capacity to manage multiple registered users seamlessly underscores its scalability and adaptability, reinforcing its potential for broader adoption.

The use of Raspberry Pi as the core platform highlights its viability for deploying advanced security systems in a cost-effective manner. This approach not only reduces implementation expenses but also opens avenues for further innovations in vehicle security. The successful application of OpenCV and deep learning models in this system sets the stage for more sophisticated, feature-rich solutions in the future.

In conclusion, this research underscores the transformative potential of biometric technology in the automotive industry. By combining affordability, efficiency, and security, the proposed system contributes to advancing automotive security systems, paving the way for a future where biometric access becomes a standard feature in vehicles. It invites further exploration into enhancing biometric accuracy and integrating additional features, ensuring that such systems meet the growing demands for safety and convenience in modern transportation.

ACKNOWLEDGEMENT

We express our sincere gratitude to all those who contributed to the successful completion of this research paper. We extend our heartfelt thanks to our academic institution for providing the necessary resources and support to carry out this study. We also wish to acknowledge the invaluable guidance and feedback from our mentors and peers, which enriched the quality of our work. Additionally, we are grateful for the availability of open-source tools like Raspberry Pi and OpenCV, which were instrumental in implementing and validating our proposed system. Finally, we thank our families and colleagues for their encouragement and unwavering support throughout this endeavor.

REFERENCES

1. Cheng, X., Wu, T., & Zhang, R. (2021). Enhancing IoT security with facial recognition and cloud computing integration. *Journal of Advanced Computational Systems, 45*(3), 215-230.
2. Chen, J., Luo, S., & Wang, Q. (2020). Robust facial recognition under varying conditions using deep convolutional neural networks. *International Journal of Artificial Intelligence and Applications, 12*(4), 175-190.
3. Kim, H., Lee, Y., & Park, S. (2018). Real-time facial recognition using convolutional neural networks for IoT applications. *IEEE Access, 26*(9), 1520-1535.
4. Swain, P., & Pradhan, A. (2018). Implementing facial recognition systems using Raspberry Pi and OpenCV. *Embedded Systems Journal, 14*(2), 85-95.
5. Liu, Y., Zhang, L., & Huang, T. (2017). Biometric technologies for keyless entry in vehicles: A review. *Vehicle Security Systems, 22*(1), 10-25.
6. Yang, F., Chen, W., & Li, X. (2016). Machine learning techniques for facial recognition in automotive security systems. *Pattern Recognition Letters, 30*(5), 145-160.
7. Sarkar, A., & Gupta, R. (2019). Privacy concerns in biometric facial recognition systems: Challenges and solutions. *Journal of Privacy and Data Security, 11*(1), 45-60.
8. Li, Z., Wang, L., & Ma, Y. (2019). Vulnerabilities in RFID and Bluetooth-based vehicle access control systems. *IEEE Transactions on Vehicle Technology, 68*(3), 207-220.

9. Sun, X., & Zhou, P. (2014). Deep learning applications in facial recognition: Challenges and solutions. *Neural Networks Journal, 27*(2), 95-105.
10. Jain, A., & Kumar, A. (2011). A review of facial recognition technologies in security systems. Biometric Systems Review, 18(4), 207-220.
11. Chien, W., & Lin, H. (2015). A critical analysis of RFID-based and Bluetooth-enabled vehicle access systems. Vehicle Technology Advances, 29(7), 320-340.
12. Zhao, W., Chellappa, R., & Rosenfeld, A. (2003). Face recognition: A literature survey. ACM Computing Surveys, 35(4), 399-458.