Anti-Theft Vehicle Starter on Face Detection

Aryan Garud*1, Prathamesh Nalawade*2, Sumedh Gaikwad *3,

Navin Wanare *4, Vishnukant Panchal*5, Prof. P.B Nagawade*6

*1,2,3,4,5,6Electrical Department, TSSM BSCOER POLY, Pune, Maharashtra, India.

*6Prof., Department of Electrical Engineering, TSSM's BSCOER Poly Narhe Pune, Maharashtra, India.

ABSTRACT

The increasing vulnerability of conventional vehicle security systems, such as physical keys and keyless entry mechanisms, has necessitated the development of more secure and intelligent authentication solutions. This paper presents the design and implementation of a face recognition-based vehicle ignition system using a Raspberry Pi platform. The proposed system integrates computer vision, machine learning, and embedded hardware to enable a secure, keyless vehicle access mechanism. A USB camera captures real-time facial images of the user, which are processed using OpenCV and deep learning-based facial recognition algorithms to extract unique biometric features. These features are compared against a pre-trained database of authorized users using classification techniques such as k-Nearest Neighbors (k-NN) or Support Vector Machines (SVM).

Upon successful authentication, the system activates the vehicle ignition through GPIO-controlled motor driver circuitry, while unauthorized access attempts are denied and logged for security purposes. The system also supports alert mechanisms and can be extended with IoT-based notifications. The implementation demonstrates reliable performance under standard conditions, offering enhanced security, user convenience, and scalability compared to traditional systems. However, challenges such as varying lighting conditions, facial obstructions, and potential spoofing attacks are identified. The proposed solution highlights the feasibility of deploying low-cost, AI-enabled embedded systems for real-time automotive security applications and paves the way for future advancements in smart vehicle technologies.

Keywords: Face Recognition, Vehicle Security, Raspberry Pi, Computer Vision, Machine Learning, Biometric Authentication, OpenCV, Embedded Systems, IoT, k-NN, SVM, Smart Vehicle Technology

I. INTRODUCTION

The rapid advancement of automotive technology has significantly improved user convenience and vehicle functionality; however, it has also introduced new security challenges. Conventional vehicle access systems, including mechanical keys and remote keyless entry, are increasingly vulnerable to theft, duplication, and electronic hacking. As a result, there is a growing demand for more secure, intelligent, and user-friendly authentication mechanisms. Biometric-based systems, particularly face recognition, have emerged as a promising solution due to their uniqueness, non-intrusive nature, and ease of integration with modern embedded platforms.

Face recognition technology, powered by recent developments in computer vision and machine learning, enables real-time identification and verification of individuals based on distinct facial features. With the availability of low-cost yet powerful hardware such as Raspberry Pi, it has become feasible to deploy such intelligent systems in practical applications. The integration of OpenCV libraries and deep learning-based models allows efficient detection, feature extraction, and classification of facial data, making it suitable for real-time embedded implementations.

This paper presents the design and implementation of a face recognition-based vehicle ignition system using a Raspberry Pi. The proposed system replaces traditional ignition mechanisms with a biometric authentication approach, ensuring that only authorized users can start the vehicle. A camera module captures live facial images, which are processed through a machine learning pipeline to verify identity against a pre-trained database. Upon successful authentication, the system triggers the ignition mechanism via hardware interfacing, while unauthorized attempts are denied and logged.

The proposed system aims to enhance vehicle security, eliminate the dependency on physical keys, and provide a scalable platform for future smart vehicle applications. Additionally, the work highlights the challenges associated with real-time facial recognition, such as variations in lighting conditions, facial occlusions, and processing limitations of embedded systems. Overall, this research demonstrates the potential of combining artificial intelligence with embedded hardware to develop cost-effective and reliable automotive security solutions.

II. METHODOLOGY

1. System Initialization
   - Raspberry Pi boots and loads the operating system.
   - Required libraries (OpenCV, face recognition, NumPy, GPIO) are initialized.
   - Pre-trained facial encodings of authorized users are loaded into memory.
2. Image Acquisition
   - A USB camera continuously captures real-time video frames.
   - Frames are processed at regular intervals for efficient computation.
3. Face Detection
   - OpenCV-based algorithms (Haar Cascade or HOG) detect the presence of a face in each frame.
   - The detected face region is extracted for further processing.
4. Pre-processing
   - The extracted face image is resized and normalized.
   - Noise reduction and grayscale conversion (if required) are applied to improve accuracy.
5. Feature Extraction
   - A deep learning model generates a numerical feature vector (face embedding) representing unique facial characteristics.
   - These embeddings are invariant to lighting and minor facial variations.
6. Face Recognition / Classification
   - The generated embedding is compared with stored embeddings of authorized users.
   - Classification algorithms such as k-Nearest Neighbors (k-NN) or Support Vector Machine (SVM) are used.
   - A confidence threshold determines whether the match is valid.
7. Decision Making
   - Authorized User: If the match exceeds the threshold, access is granted.
   - Unauthorized User: If no match is found, access is denied and optionally logged.
8. Hardware Control (Ignition System)
   - On successful authentication, Raspberry Pi sends a HIGH signal via GPIO pins.
   - This signal activates the motor driver (L298N), which powers the DC motor (simulating vehicle ignition).
9. Security & Logging
   - Unauthorized attempts are recorded with timestamps.
   - Optional alert mechanisms (buzzer, LED, or GSM notification) can be triggered.
10. Training Phase (Offline Setup)

- Multiple images of authorized users are captured.
- Data is pre-processed and used to train the recognition model.
- Generated embeddings are stored in the system database for future matching.

III. BLOCK DIAGRAM

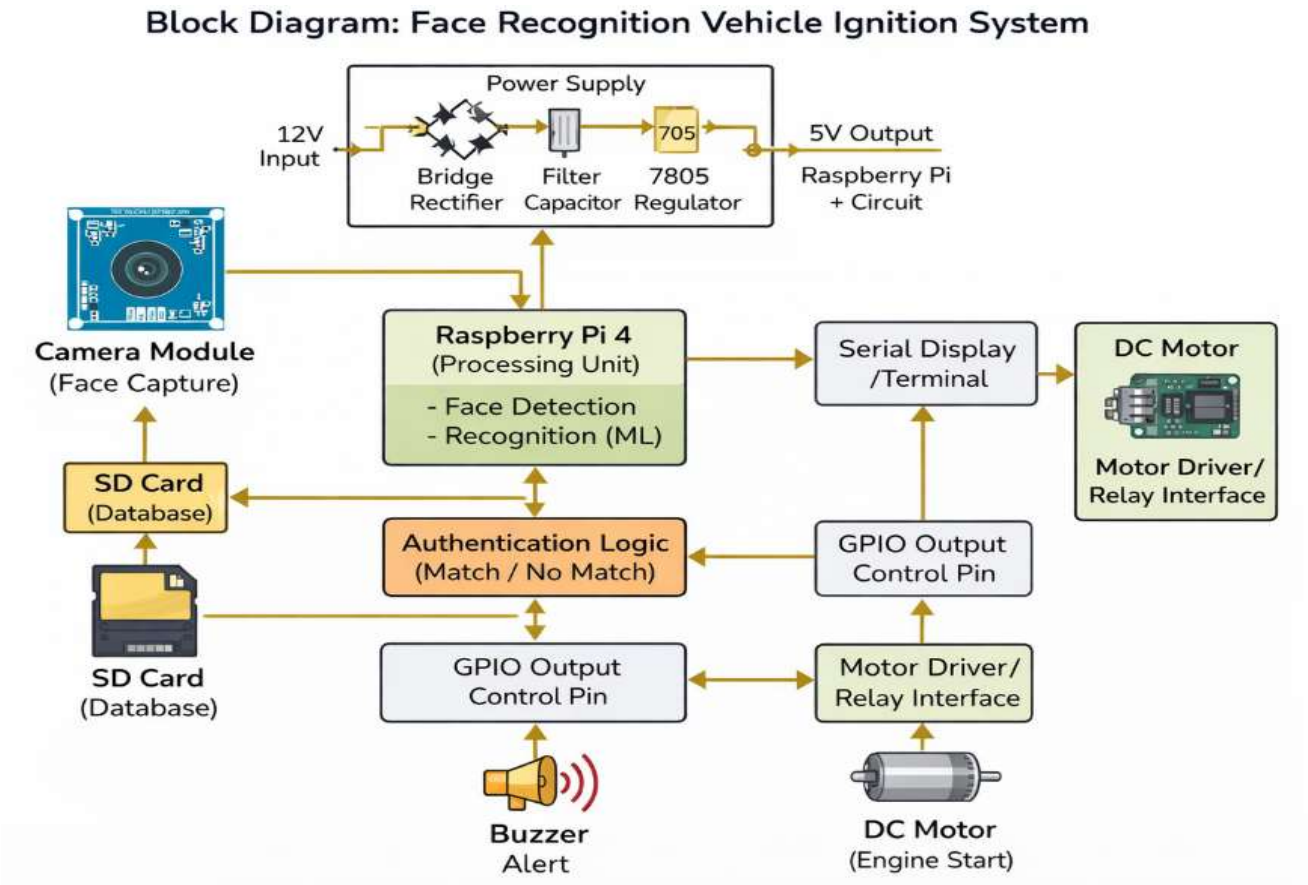

Fig: -Face recognition Vehicle Ignition System

Explanation of Each block

- Power Supply (Bridge Rectifier + Filter + 7805 Regulator): Converts 12V input to stable 5V DC required for Raspberry Pi and circuits.
- Camera Module (Face Capture): Captures real-time images of the user for facial recognition.
- SD Card (Database): Stores trained facial data and system-related files.
- Raspberry Pi 4 (Processing Unit): Processes images and performs face detection and recognition using ML algorithms.
- Authentication Logic (Match / No Match): Compares detected face with stored data and decides access permission.
- GPIO Output Control Pin: Sends control signals from Raspberry Pi to external hardware components.
- Serial Display / Terminal: Displays system status such as access granted or denied.
- Motor Driver / Relay Interface: Acts as a switch to control high-power motor using low-power GPIO signals.
- DC Motor (Engine Start): Simulates vehicle ignition by running when access is granted.
- Buzzer Alert: Produces sound alerts during unauthorized access attempts.

IV. MODEL

Fig. Hardware model

V. OBJECTIVE

To design and develop a secure vehicle ignition system using face recognition technology.
To eliminate the need for traditional keys and enhance vehicle security through biometric authentication.
To implement real-time face detection and recognition using Raspberry Pi and OpenCV.
To allow only authorized users to start the vehicle based on facial verification.
To integrate hardware components (motor driver, DC motor, buzzer) with embedded control.
To provide alerts and logging for unauthorized access attempts.
To develop a cost-effective and scalable smart vehicle security solution.

VI. CONCLUSION

The proposed face recognition-based vehicle ignition system successfully demonstrates a secure and intelligent alternative to conventional key-based mechanisms. By integrating computer vision, machine learning, and embedded hardware using Raspberry Pi, the system ensures that only authorized users can access and start the vehicle. The implementation highlights the feasibility of real-time facial recognition on a low-cost platform while maintaining acceptable accuracy and response time.The system enhances vehicle security, improves user convenience, and eliminates risks associated with key theft or duplication. Additionally, features such as access logging and alert mechanisms further strengthen the overall reliability of the system. However, certain challenges such as varying lighting conditions, facial obstructions, and potential spoofing attacks need to be addressed for real-world deployment. Overall, this work proves that AI-based biometric authentication can be effectively applied to automotive security systems. With further improvements like liveness detection, cloud connectivity, and system optimization, the proposed model can be extended into a robust, scalable solution for next-generation smart vehicles.

VII. REFERENCES

[1] P. Viola and M. J. Jones, "Rapid Object Detection using a Boosted Cascade of Simple Features," *Proc. IEEE CVPR*, 2001.

[2] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "DeepFace: Closing the Gap to Human-Level Performance in Face Verification," *Proc. IEEE CVPR*, 2014.

[3] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering," *Proc. IEEE CVPR*, 2015.

[4] K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, "Joint Face Detection and Alignment using MTCNN," *IEEE Signal Processing Letters*, 2016.

[5] K. He, X. Zhang, S. Ren, and J. Sun, "Deep Residual Learning for Image Recognition," *Proc. IEEE CVPR*, 2016.

[6] C. Cortes and V. Vapnik, "Support-Vector Networks," *Machine Learning Journal*, 1995.

[7] T. Cover and P. Hart, "Nearest Neighbor Pattern Classification," *IEEE Transactions on Information Theory*, 1967.

[8] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Transactions on Circuits and Systems*, 2004.

[9] D. A. Patterson and J. L. Hennessy, *Computer Organization and Design: The Hardware/Software Interface*, Morgan Kaufmann, 2013.

[10] M. Chen, S. Mao, and Y. Liu, "Big Data: A Survey," *Mobile Networks and Applications*, 2014.