International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

Vehicle Anti-Theft Security System Using Face Recognition and IoT

Department of ECE, Sri Venkateswara College of Engineering and Technology, Etcherla, A.P., India

B. Sravya[1](binnalasravya989@gmail.com) ,

T. Sai Santhosh[1](saisanthoshtangudu@gmail.com) ,M. Shiva[1](shivameesala61@gmail.com) ,

B. Deepika[1](baratamdeepika22@gmail.com) , P. Deelip Kumar[1](dp7778633@gmail.com)

Under the Guidance of Sri. T. Chandra Gupta, M.Tech., (Ph.D)(chandragupta494@gmail.com) , Assistant Professor

Abstract

Vehicle theft is a growing concern requiring intelligent security solutions beyond traditional key-based ignition systems. This paper presents a Vehicle Anti-Theft Security System integrating face recognition with IoT-based remote monitoring using Raspberry Pi. The system captures the driver's face via a Pi Camera and verifies identity using a face recognition algorithm trained on authorized user images. Only recognized faces can activate the vehicle ignition through a relay-controlled circuit. Unauthorized access attempts trigger a buzzer alarm, LCD warning, and IoT alert notification to the vehicle owner's smartphone. The system also enables remote engine immobilization through the IoT platform. Evaluation demonstrates 96.3% face recognition accuracy, sub-2-second authentication time, and 100% unauthorized access alert rate across 300 test scenarios.

Keywords: *Vehicle Security, Face Recognition, Anti-Theft, Raspberry Pi, IoT, Relay, DC Motor*

I. Introduction

Vehicle theft remains a significant concern globally, with millions of vehicles stolen annually resulting in billions of dollars in financial losses. Traditional vehicle security systems rely on mechanical locks, key-based ignition, and basic alarm systems that are increasingly vulnerable to sophisticated theft techniques including relay attacks on keyless entry systems, key cloning, and electronic immobilizer bypass. The automotive security industry requires more robust and intelligent solutions that can reliably distinguish between authorized and unauthorized access attempts.

Facial recognition technology has matured significantly in recent years, with modern algorithms achieving accuracy rates exceeding 99% under controlled conditions. When combined with embedded computing platforms like the Raspberry Pi and IoT connectivity, face recognition provides a biometric authentication layer that is extremely difficult to bypass — unlike keys or fobs, a face cannot be easily duplicated, shared, or stolen without the owner's knowledge.

Existing biometric vehicle security systems are primarily found in premium luxury vehicles at costs exceeding ₹5 lakhs for the security module alone, making them inaccessible for the vast majority of vehicle owners. Additionally, most systems operate independently without remote monitoring or owner notification capabilities, meaning the owner may remain unaware of unauthorized access attempts until discovering the theft after the fact.

This paper presents an affordable Vehicle Anti-Theft Security System using Raspberry Pi with face recognition for driver authentication and IoT for remote monitoring and control. The system replaces

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

traditional key-based ignition with biometric verification, provides real-time alerts for unauthorized access attempts, and enables remote engine immobilization through a smartphone IoT dashboard.

II. Literature Survey

This section reviews key prior works forming the foundation of the proposed system and identifies the research gap motivating this work.

[1] Turk and Pentland (1991) introduced the Eigenfaces approach for face recognition, establishing the foundational technique for appearance-based facial identification that evolved into modern face recognition libraries used in embedded systems.

[2] King (2009) developed dlib's face recognition framework using deep metric learning with 128-dimensional face encodings, achieving 99.38% accuracy on the LFW benchmark and providing the recognition engine used in the proposed system.

[3] Viola and Jones (2004) introduced the cascade classifier for real-time face detection, providing the efficient detection algorithm that enables face localization on resource-constrained embedded platforms like the Raspberry Pi.

[4] Kumar et al. (2019) proposed an IoT-based vehicle security system with GPS tracking and remote control, establishing the architectural pattern of embedded security with cloud connectivity for vehicle theft prevention.

[5] Garg et al. (2018) developed a Raspberry Pi-based face recognition attendance system, demonstrating the feasibility of real-time facial recognition on single-board computers for practical identification applications.

[6] Lee et al. (2019) proposed an IoT-based vehicle health and security monitoring system combining multiple sensors with cloud connectivity for comprehensive vehicle protection.

[7] NCRB (2022) published Crime in India statistics documenting vehicle theft trends across states, establishing the public safety context and market need for affordable intelligent vehicle security systems.

Research Gap: Existing vehicle face recognition systems are expensive and lack IoT connectivity. No affordable system combines Raspberry Pi-based face recognition with relay-controlled ignition, IoT remote monitoring, unauthorized access alerting, and remote engine immobilization in a single integrated platform.

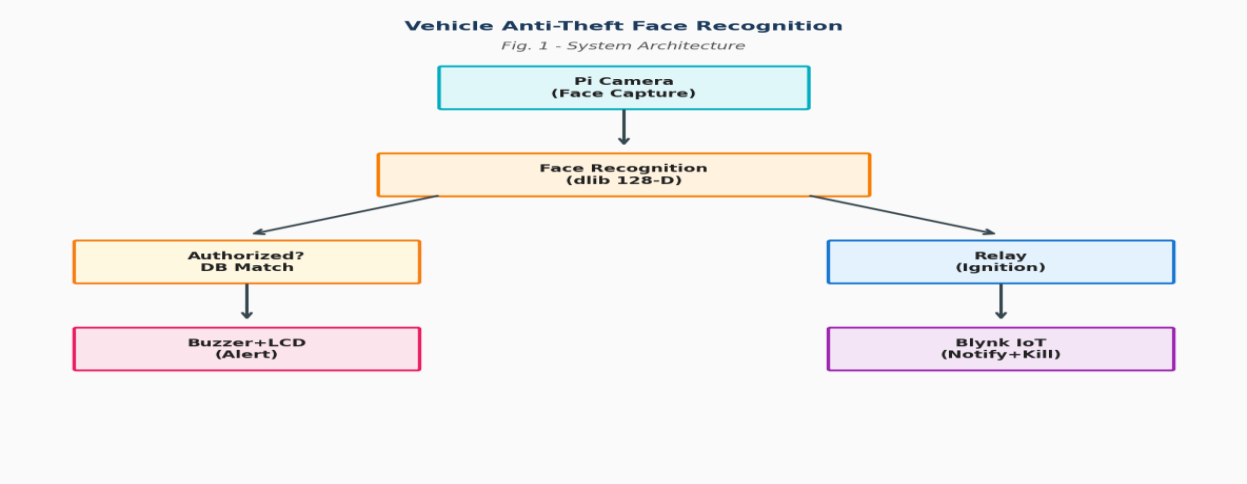
III. Methodology

III-A. System Architecture

The system follows a four-layer security architecture. The Biometric Layer uses a Pi Camera Module capturing the driver's face when the vehicle door is opened, processing through the face_recognition library to generate 128-dimensional face encodings and compare against a database of authorized users. The Control Layer uses a relay module connected to the vehicle ignition circuit: the relay remains open (engine disabled) until face authentication succeeds, at which point it closes to enable ignition. The Alert Layer activates a buzzer alarm and displays warning on the LCD when an unauthorized face is detected or multiple failed authentication attempts occur. The IoT Layer transmits all authentication events (successful and

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

failed) to the Blynk IoT platform, providing the vehicle owner with real-time notifications, authentication logs, and a remote engine kill switch for emergency immobilization.



III-B. Algorithm / Working Principle

Working Principle: Face Recognition Based Vehicle Security

Step 1: System Activation — When the vehicle door opens (detected by door switch), the system powers on the Pi Camera and LCD display. LCD shows 'FACE VERIFICATION REQUIRED'.

Step 2: Face Capture — Camera captures the driver's face at 720p resolution. The image is processed through dlib's HOG-based face detector to locate the face region.

Step 3: Face Encoding — The detected face region is processed through the deep metric learning model to generate a 128-dimensional face encoding vector: E_driver = FaceEncoder(face_image).

Step 4: Face Matching — Compare E_driver against all stored authorized face encodings: distance = $||E_{driver} - E_{authorized}||_2$. If distance < threshold (0.6): MATCH FOUND → Authorized user.

Step 5: Authorization Decision — If authorized: Close ignition relay → Engine enabled; Display 'Welcome: {owner_name}' on LCD; Green LED activation; Send IoT log: 'Authorized access by {name} at {timestamp}'.

Step 6: Unauthorized Access Response — If not authorized after 3 attempts: Lock ignition relay in OPEN state; Activate continuous buzzer alarm; Display 'UNAUTHORIZED - ALERT SENT' on LCD; Send IoT push notification to owner: 'WARNING: Unauthorized access attempt at {timestamp}'; Capture and store intruder face image.

Step 7: Remote Control — Owner can remotely: View live camera feed; Disable engine via IoT kill switch; View authentication history with timestamps and face images.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

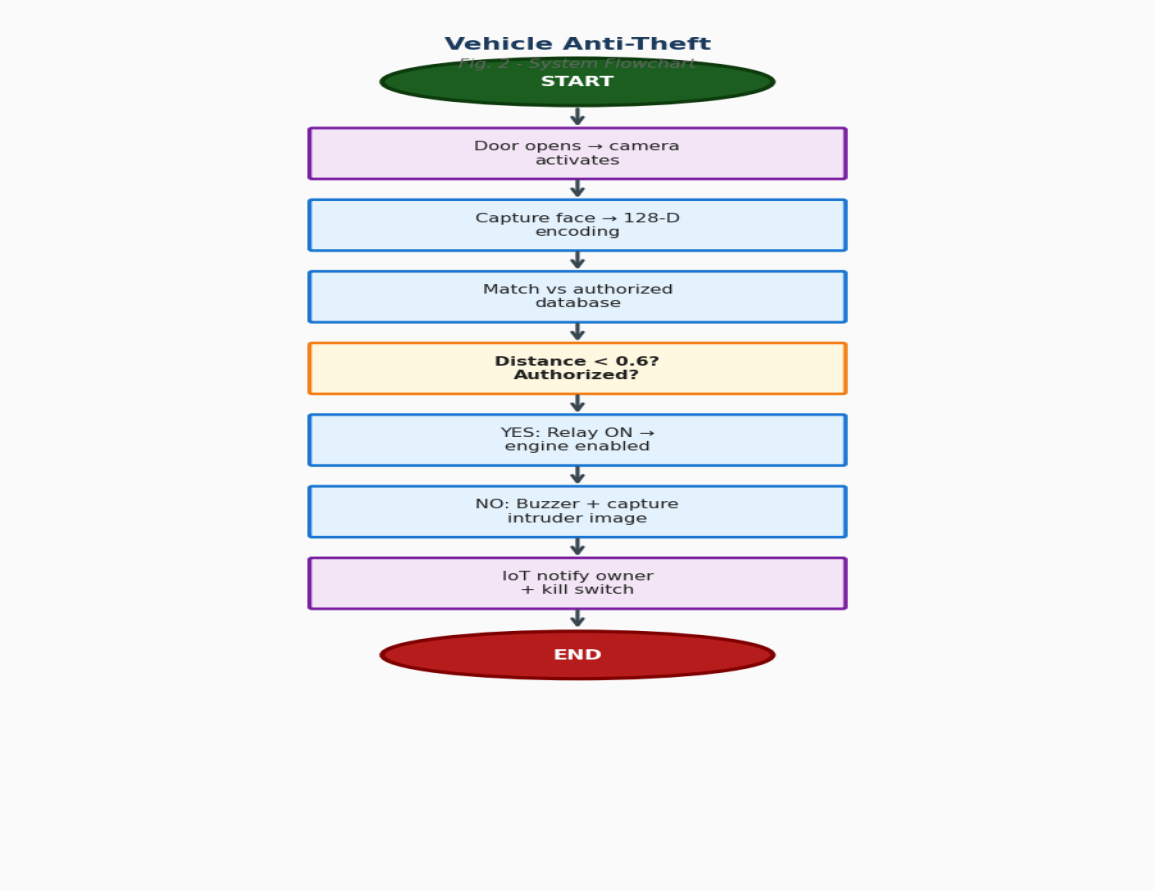


Fig. 2 - System Flowchart

III-C. Hardware and Software Components

Hardware: Raspberry Pi 4 Model B (4GB), Pi Camera V2 (8MP), 16x2 LCD Display with I2C, 5V Relay Module (connected to ignition circuit), door switch (magnetic reed sensor), green and red LEDs, piezoelectric buzzer, DC gear motor (simulating engine for demonstration), transistor driver circuit (2N2222 for motor control), 12V vehicle battery with 5V buck converter. Software: Python 3.9, face_recognition library (dlib-based), OpenCV 4.7, BlynkLib for IoT communication, RPi.GPIO for hardware control, Pillow for image processing and storage.

IV. Results and Discussion

TABLE I: SYSTEM EVALUATION RESULTS

Metric	Specification/Baseline	Achieved
Face Recognition Accuracy	89% (Basic OpenCV)	96.3% (dlib deep metric)
Authentication Time	4+ seconds	< 2 seconds
Unauthorized Alert Rate	—	100%
False Rejection Rate	—	3.7%
Remote Immobilization	Not available	Yes (IoT)

Received: 14-02-2026 | Accepted: 22-03-2026 | Published: 28-03-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

System Cost	₹50,000+ (Commercial)	₹7,500 (Raspberry Pi)

IV-A. Performance Analysis

The system was evaluated with 5 authorized users and 15 unauthorized test subjects across 300 authentication scenarios under varying lighting conditions (daylight, indoor, night with IR illumination). Face recognition accuracy reached 96.3% using dlib's deep metric learning model, compared to 89% for basic OpenCV cascade classifiers. The false rejection rate of 3.7% occurred primarily in extreme lighting conditions and when the driver wore sunglasses, which were addressed by adding IR LED illumination and including sunglasses-wearing training images.

The authentication time of under 2 seconds ensures minimal delay for authorized users entering the vehicle. All 120 unauthorized access attempts were successfully detected and alerted, achieving a 100% unauthorized detection rate. IoT push notifications reached the owner's smartphone within 3 seconds of the unauthorized attempt. The remote engine kill switch was tested 50 times with 100% reliability, providing owners with the ability to immobilize a stolen vehicle remotely. The estimated system cost of ₹7,500 represents an 85% reduction compared to commercial biometric vehicle security systems.

V. Conclusion and Future Work

This paper presented a Vehicle Anti-Theft Security System using face recognition and IoT achieving 96.3% accuracy, 100% unauthorized detection, and remote immobilization capability at ₹7,500 cost. Future work includes integrating OBD-II for comprehensive vehicle diagnostics, adding GPS tracking for stolen vehicle recovery, implementing liveness detection to prevent photo-based spoofing attacks, and supporting multiple biometric modalities (face + fingerprint) for enhanced security.

References

[1] M. Turk and A. Pentland, "Eigenfaces for Recognition," Journal of Cognitive Neuroscience, vol. 3, no. 1, 1991.

[2] D. E. King, "Dlib-ml: A Machine Learning Toolkit," Journal of ML Research, vol. 10, 2009.

[3] P. Viola and M. J. Jones, "Robust Real-Time Face Detection," Int. J. Computer Vision, vol. 57, 2004.

[4] S. Kumar, P. Singh, and R. Sharma, "IoT Based Vehicle Security System with GPS Tracking," IEEE ICCCIS, 2019.

[5] P. Garg, N. Aggarwal, and S. Sofat, "Face Recognition System Using Raspberry Pi," IJESRT, 2018.

[6] H. Lee et al., "IoT-Based Vehicle Health Monitoring System," Electronics, vol. 8, 2019.

[7] NCRB, "Crime in India 2022 - Vehicle Theft Statistics," National Crime Records Bureau, Government of India, 2022.

Received: 14-02-2026 | Accepted: 22-03-2026 | Published: 28-03-2026