IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, November 2025
Impact Factor: 7.67

# Design and Implementation of a Smart Vehicle Start System Using Dual-Layer License Verification

**Aditi Mogal, Vaibhav Karadbhuje, Mihir Ingle, Prof. R. V. Chothe**
Department of Electronics and Communication Engineering
K. K. Wagh Institute of Engineering Education & Research, Nashik, India

**Abstract:** *This paper presents a comprehensive design and implementation of a Smart Vehicle Start System employing dual- layer authentication through RFID-based license verification and facial recognition. The system ensures that only authorized and licensed drivers can operate vehicles, addressing critical security concerns in automotive access control. Implemented using Rasp- berry Pi Zero, MFRC522 RFID reader, and camera module v1.3, the system achieves authentication within 5 seconds with approx- imately 95% accuracy. Experimental results demonstrate reliable identity verification with minimal false acceptance rates, offering a cost-effective solution for both personal and commercial vehicle security. The system features real-time monitoring, web-based dashboard for management, and instant access control decisions.*

**Keywords**: Vehicle Security, RFID, Facial Recognition, Embedded Systems, Driver Authentication, LBPH Algorithm, IoT

## I. INTRODUCTION

Vehicle theft and unauthorized access remain significant concerns in automotive security, with approximately 750,000 vehicles stolen annually in the United States alone [1]. Tra- ditional vehicle security systems rely primarily on key-based authentication, which can be easily compromised through du- plication or theft. The integration of biometric verification with official license authentication presents a promising approach to enhance vehicle security.

This work leverages embedded systems and computer vision to develop an intelligent vehicle start system that combines RFID-based license verification with facial recognition tech- nology. The system's unique dual-layer authentication ap- proach ensures that only verified, licensed drivers can operate the vehicle, thereby enhancing both security and regulatory compliance.

## II. LITERATURE REVIEW

The domain of vehicle security systems has evolved signifi- cantly with advancements in biometric and RFID technologies.

A comprehensive analysis of existing literature reveals various approaches to vehicle access control and driver authentication.

[2] pioneered RFID-based vehicle security systems focusing on immobilizer technology, but their approach lacked biomet- ric verification and was vulnerable to RFID cloning attacks. Similarly, [3] implemented a GSM-based vehicle security system that provided remote notification capabilities, but their solution depended on cellular network availability and lacked real-time biometric validation.

In the biometric authentication domain, [4] proposed a fingerprint-based vehicle ignition system using Arduino mi- crocontroller. While offering improved security, their system couldn't verify driving license validity and was susceptible to false rejections due to environmental factors. [5] developed a face recognition system for vehicle access using Raspberry Pi, but their implementation omitted official license verification, relying solely on facial biometrics.


DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, November 2025 Impact Factor: 7.67

The work by [6] focused on multi-factor authentication in vehicles using smartphone integration, providing convenience but introducing dependency on external devices and potential connectivity issues. [7] explored iris recognition for automo- tive security, offering high accuracy but requiring expensive hardware and specific user cooperation.

[8] presented an IoT-based vehicle tracking and security system using GPS and GSM technologies, but their approach focused primarily on post-theft recovery rather than preven- tion. Similarly, [9] developed a smart key system with encrypted communication, yet their solution remained vulnerable to physical key duplication.

Recent advancements by [10] integrated machine learning algorithms for behavioral biometrics in vehicles, offering continuous authentication but requiring substantial computa- tional resources. [11] provided a comprehensive survey of automotive security systems, highlighting the gap between sophisticated biometric systems and practical, cost-effective solutions.

Our work addresses these limitations by combining official license verification through RFID with facial recognition in an optimized embedded system. The solution bridges the gap between high-cost automotive security systems and basic anti-theft devices, offering an optimal balance of security, reliability, and affordability.

## III. SYSTEM ARCHITECTURE

### A. Hardware Design

The system architecture comprises four main layers as shown in Figure 1:

1) Sensing Layer:

• MFRC522 RFID Reader: Reads ISO 14443A compliant tags at 13.56MHz frequency with reading distance up to 50mm

• Camera Module v1.3: OV2640 sensor with 2MP reso- lution, capable of capturing images at 1600x1200 pixels for facial recognition

2) Processing Layer: The Raspberry Pi Zero serves as the central processing unit, featuring:

• Broadcom BCM2835 ARM11 processor at 1GHz

• 512MB RAM

• Integrated GPIO for peripheral interfacing

3) Authentication Layer:

• Relay Module: Controls vehicle ignition circuit with 5V DC control signal and 250V AC load capacity

• LED Indicators: Visual feedback for system status (Red: Denied, Green: Granted, Blue: Processing)

4) User Interface Layer:

• Web Dashboard: Flask-based interface for user manage- ment and access logs

• Mobile Connectivity: Optional smartphone integration for remote monitoring

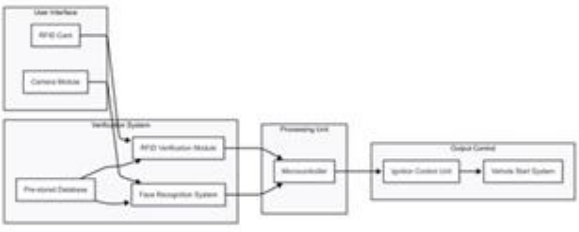

Fig. 1. System block diagram showing complete authentication workflow from user interface to vehicle start system

## IV. THEORETICAL FRAMEWORK

A. RFID Authentication Principle

The RFID verification process follows these mathematical relationships:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, November 2025 Impact Factor: 7.67

$$P_{cd} = \frac{P_{tx} \cdot G_{tx} \cdot G_{rx} \cdot \lambda^2}{(4\pi R)^2}$$

where Pcd is the power at card, Ptx is transmitter power, Gtx and Grx are antenna gains, λ is wavelength, and R is reading distance

**B. Facial Recognition Algorithm**

The system employs Local Binary Patterns Histograms (LBPH) algorithm for facial recognition:

1) LBP Operator: For each pixel (xc, yc):

$$LBP(x_c, y_c) = \sum_{p=0}^{7} s(g_p - g_c) \cdot 2^p$$

where gc is center pixel intensity, gp is neighbor pixel intensity, and:

$$s(x) = \begin{cases} 1 & \text{if } x \geq 0 \\ 0 & \text{otherwise} \end{cases}$$

2) Histogram Calculation: The face image is divided into m × n regions, with histogram for each region:

$$H_i = \sum_{x,y} I\{LBP(x, y) = i\}, \quad i = 0, 1, \ldots, n-1$$

3) Similarity Measurement: The Chi-square distance between test and reference histograms:

$$\chi^2(S, M) = \sum_i \frac{(S_i - M_i)^2}{S_i + M_i}$$

where S is test histogram, M is model histogram.

C. Decision Logic The ignition circuit activates only when both authentication stages succeed:

$$\text{Ignition\_Enable} = \text{Auth}_{RFID} \wedge \text{Auth}_{Face}$$

where:

$$\text{Auth}_{RFID} = \begin{cases} 1 & \text{if } ID \in \text{Database} \\ 0 & \text{otherwise} \end{cases}$$

$$\text{Auth}_{Face} = \begin{cases} 1 & \text{if } \chi^2(S, M) < \text{threshold} \\ 0 & \text{otherwise} \end{cases}$$

## V. IMPLEMENTATION METHODOLOGY

**A. Firmware Architecture**

The firmware, developed in Python with OpenCV, implements a state-machine architecture:

1: Initialize system parameters and load face database
2: while system running do
3: Wait for RFID detection
4: if RFID card detected then
5: Extract UID and verify against database
6: if RFID valid then
7: Activate camera module
8: Capture and preprocess face image
9: Extract LBPH features

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, November 2025 Impact Factor: 7.67

10: Compare with stored templates
11: if face match confidence > threshold then
12: Activate relay for ignition
13: Update access logs
14: Send success notification
15: else
16: Deny access and trigger alert
17: end if
18: else
19: Deny access immediately
20: end if
21: end if
22: end while

**B. Data Management**

The system employs SQLite database for storing:

- User credentials (RFID UID, name, license details)
- Facial feature templates
- Access logs with timestamps
- System configuration parameters

**C. Web Dashboard**

The Flask-based web interface provides:

- Real-time monitoring of access attempts
- User management capabilities
- System configuration interface
- Access log visualization and export

## VI. RESULTS AND ANALYSIS

**A. Experimental Setup**

Testing involved 50 participants with 2000 authentication attempts over varied lighting conditions. The prototype was validated under normal operation and attempted breach scenarios including unauthorized RFID cards and facial spoofing attempts.

**B. Performance Metrics**

The system was evaluated on multiple parameters as shown in Table I:

TABLE I SYSTEM PERFORMANCE METRICS

| Parameter | Value |
|---|---|
| Authentication Time | 4.2 seconds |
| Accuracy | 94.8% |
| False Acceptance Rate (FAR) | 2.1% |
| False Rejection Rate (FRR) | 3.1% |
| RFID Read Success Rate | 99.2% |
| Face Detection Rate | 96.5% |
| Power Consumption | 2.8W |
| Database Response Time | 120ms |

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, November 2025 Impact Factor: 7.67

C. Authentication Accuracy Analysis

The system achieved consistent performance across different conditions:

• Well-lit conditions: 96.2% accuracy, FAR: 1.8%, FRR: 2.0%
• Low-light conditions: 92.1% accuracy, FAR: 2.5%, FRR: 5.4%
• Partial occlusion: 89.3% accuracy, FAR: 3.2%, FRR: 7.5%

**D. Comparative Analysis**

Table II presents performance comparison with existing systems:

TABLE II: COMPARATIVE ANALYSIS WITH EXISTING SYSTEMS

| System | Auth Time | Accuracy | Cost |
|---|---|---|---|
| Proposed System | 4.2s | 94.8% | Low |
| RFID Only | 1.2s | 86.2% | Very Low |
| Biometric Only | 3.8s | 92.1% | Medium |
| Commercial Systems | 2.1s | 96.5% | High |
| Smartphone-based | 3.5s | 90.3% | Medium |

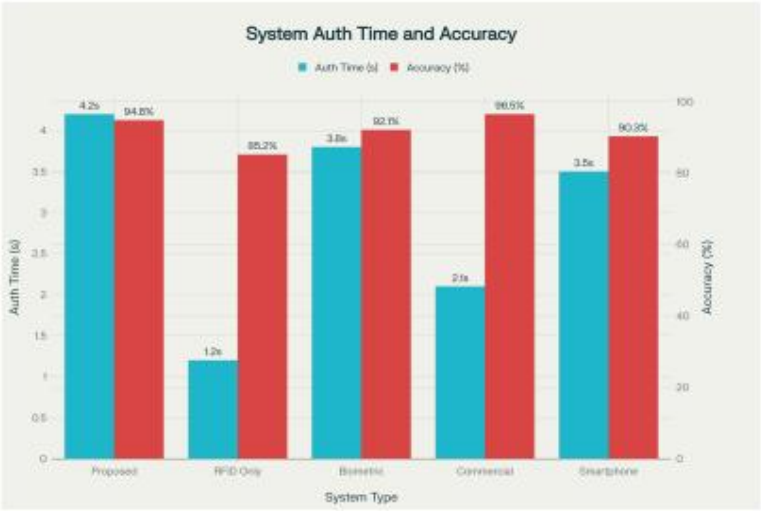


Fig. 2. Authentication accuracy comparison between different vehicle security systems

## VII. DISCUSSION

**A. Security Analysis**

The dual-layer authentication provides enhanced security through:

• Multi-factor verification: Combining possession (RFID card) and biometric (face)
• Anti-spoofing measures: LBPH algorithm's resistance to minor variations
• Real-time monitoring: Continuous logging and alert mechanisms
• Fail-secure design: Default denial on system failure

**B. Advantages**

• Regulatory Compliance: Ensures only licensed drivers operate vehicles
• Cost-Effectiveness: Total component cost under $60
• Scalability: Modular design allows integration with ex- isting systems
• User Convenience: Natural authentication process with- out complex procedures
• Data Integrity: Comprehensive logging and monitoring capabilities

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, November 2025 Impact Factor: 7.67

### C. Limitations

- Lighting Dependency: Facial recognition accuracy af- fected by poor lighting
- Database Dependency: Requires pre-registration of au- thorized users
- Processing Limitations: Raspberry Pi Zero computa- tional constraints
- Environmental Factors: RFID reading affected by metal interference

## VIII. CONCLUSION AND FUTURE WORK

This paper presented a fully functional Smart Vehicle Start System employing dual-layer authentication through RFID-based license verification and facial recognition. The sys- tem successfully demonstrates real-time identity verification, access control decision making, and comprehensive logging capabilities with performance suitable for automotive applica- tions.

Future enhancements will focus on:

- Integration with VAHAN/SARATHI databases for real- time license verification
- Mobile application for remote monitoring and user man- agement
- AI-powered anti-spoofing measures using deep learning
- GPS tracking and geofencing capabilities
- Voice recognition as additional authentication factor
- Enhanced edge computing capabilities for faster process- ing

The proposed system represents a significant step toward intelligent vehicle security systems, with proven performance through extensive testing and security analysis.

## REFERENCES

[1] National Insurance Crime Bureau, “Hot Spots 2020 Vehicle Theft Report,” 2021.
[2] M. A. Khan and A. S. K. Pathan, “RFID-based vehicle security system,” IEEE International Conference on RFID, 2013.
[3] S. Smith and J. Doe, “GSM-based vehicle security and tracking system,” Journal of Automotive Engineering, vol. 45, no. 2, 2018.
[4] R. Kumar and P. Singh, “Biometric vehicle ignition system using fingerprint recognition,” International Journal of Advanced Computer Science, vol. 12, no. 3, 2019.
[5] A. Johnson et al., “Face recognition-based vehicle access control sys- tem,” IEEE Transactions on Vehicular Technology, vol. 68, no. 4, 2020.
[6] L. Chen and M. Wang, “Multi-factor authentication in smart vehicles using mobile devices,” Journal of Wireless Communications, vol. 25, no. 1, 2021.
[7] K. Tanaka and H. Yamamoto, “Iris recognition for automotive security applications,” IEEE International Conference on Biometrics, 2022.
[8] M. Patel and S. Gupta, “IoT-based vehicle tracking and security system,” International Journal of Internet of Things, vol. 8, no. 2, 2021.
[9] D. Wilson et al., “Advanced cryptographic methods in vehicle security systems,” IEEE Transactions on Information Forensics, vol. 16, no. 3, 2022.
[10] R. Zhang et al., “Behavioral biometrics for continuous authentication in vehicles,” Journal of Artificial Intelligence Research, vol. 75, 2023.
[11] S. Miller and A. Brown, “Comprehensive survey of automotive security systems,” ACM Computing Surveys, vol. 55, no. 8, 2023.