

Intelligent Vehicle Access Control System via Dual Biometric and License Authentication

Gopal Bhaskar Patil, Ashish Gajendra Dandge, Mayur Jitendra Somvanshi, Swaraj Sachin Barkund

Mechanical Engineering & K.E. Society's Rajarambapu Institute of Technology (Polytechnic), Lohagaon, Pune

Mechanical Engineering & MM Polytechnic, Thergaon, Pune

Mechanical Engineering & MM Polytechnic, Thergaon, Pune

Mechanical Engineering & MM Polytechnic, Thergaon, Pune

Abstract - This project presents an **Intelligent Vehicle Access Control System** designed to improve vehicle security using **license verification and dual biometric authentication**. Traditional vehicle security systems such as keys and basic electronic locks are not always reliable and can be easily misused or bypassed. To overcome these limitations, this system uses a Raspberry Pi as the main controller to manage and process all authentication steps. The system begins by asking the user to enter a valid license number, which is checked against a stored database. This ensures that only registered users can proceed to the next level of authentication. After successful license verification, the system performs biometric authentication using face recognition and fingerprint scanning. These methods provide strong security because they are unique to each individual. A special feature of this system is its flexible design, where the user only needs to pass one of the biometric checks (either face or fingerprint) after entering the correct license. If either of these matches, the system allows the vehicle to start. If both fail, access is denied. This makes the system both secure and convenient for users.

The proposed system reduces the risk of unauthorized access and vehicle theft while remaining cost-effective and easy to use. It can be applied in personal vehicles, rental services, and company transport systems. In the future, this system can be enhanced by adding features like GPS tracking, IoT connectivity, and real-time alerts for better monitoring and control.

Key Words: Raspberry Pi, Vehicle Security, License Verification, Biometric Authentication, Face Recognition, Fingerprint Recognition, Access Control System, Dual Authentication, IoT, GPS Tracking

1. INTRODUCTION

In today's modern era, vehicles have become an essential part of human life, as they are widely used for transportation, industrial work, and daily activities. With the rapid increase in the number of vehicles, there has also been a significant rise in problems related to vehicle security such as theft, unauthorized access, and misuse. These issues not only cause financial loss but also create safety risks for vehicle owners. Most of the vehicles currently use traditional security systems such as mechanical keys or basic electronic locking systems, which are not fully secure. Mechanical keys can be easily lost, duplicated, or stolen, and electronic systems can sometimes be hacked or bypassed using advanced techniques. Due to these limitations, there is a strong need for a more reliable and advanced vehicle access control system that can provide better protection and ensure that only authorized users can operate the vehicle.

The development of modern technologies such as embedded systems, automation, and biometric authentication has opened new possibilities for improving vehicle security. Biometric systems use unique human features such as fingerprints and facial recognition, which are different for every individual and cannot be easily copied. These systems are already used in smartphones, offices, and banking systems for secure access. By applying these technologies to vehicle systems, it is possible to create a smart and intelligent security solution. This project focuses on developing such a system that combines multiple authentication methods to improve security and reliability.

METHODOLOGY

The methodology of this project explains the step-by-step approach used to design and implement the Intelligent Vehicle Access Control System. It describes how the system works and how different processes are followed to achieve secure vehicle access. The main aim of this methodology is to ensure that only authorized users can operate the vehicle by using multiple levels of authentication.

The system is based on a logical sequence of operations that includes license verification and biometric authentication. This structured approach helps in improving security and reliability of the system.

PROJECT APPROACH

The project is developed using a systematic approach. The steps involved in the development of the system are as follows:

1. Problem Identification:

- Study of existing vehicle security systems
- Identification of issues such as theft and unauthorized access

2. Requirement Analysis:

- Need for a secure and user-friendly system
- Requirement of multi-level authentication

3. System Planning:

- Designing the flow of the system
- Deciding authentication steps

4. Implementation Planning:

- Planning how the system will be developed
- Deciding sequence of operations

5. Testing Strategy:

- Checking system performance
- Verifying correct operation

WORKING PRINCIPLE

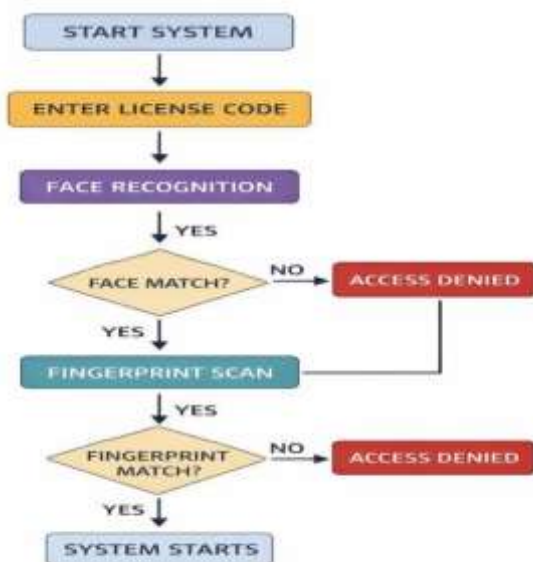
The working principle of the system is based on multi-level authentication. The system uses a combination of license verification and biometric authentication to identify the user. The license verification is the first and compulsory step. Only after successful license verification, the system allows the user to proceed to biometric authentication. The biometric authentication includes face recognition and fingerprint scanning. The system follows a flexible authentication logic where it is not necessary for both biometric methods to be successful. If either face recognition or fingerprint authentication is successful, the system allows the vehicle to start. If both methods fail, access is denied. This principle ensures both security and convenience.

Step-By-Step Working Process

The working of the system is carried out in the following steps:

1. The user starts the system
2. The system asks for license code
3. The user enters the license code
4. The system verifies the license
5. If the license is incorrect → access denied
6. If the license is correct → proceed to next step
7. Face recognition process starts
8. If face is matched → vehicle starts
9. If face is not matched → fingerprint scanning starts
10. If fingerprint matches → vehicle starts
11. If both fail → access denied

This step-by-step process ensures proper authentication.



Flow Chart of Intelligent Vehicle Access Control System

Operational Workflow

The complete workflow of the system is simple and easy to understand. The user interacts with the system through input steps such as license entry and biometric verification. The system processes these inputs and makes decisions based on predefined logic.

The workflow ensures that the system operates smoothly and provides quick response. It also reduces errors and improves reliability.

Safety And Reliability

The methodology ensures that the system is safe and reliable. Multi-level authentication prevents unauthorized access. The structured process ensures that all steps are followed correctly.

The system is designed to handle errors such as incorrect input or failed authentication. This improves the overall performance and security of the system.

Design, Working And Processes

Introduction

The design and working of the Intelligent Vehicle Access Control System explain how the system is structured and how it performs its functions. This chapter focuses on the integration of hardware and software components to create a secure and efficient vehicle access system. The system is designed in such a way that it ensures high security, easy operation, and reliable performance.

The main idea behind the design is to use multiple authentication methods to verify the user before allowing access to the vehicle. The system uses license authentication as the first level of security, followed by biometric authentication methods such as face recognition and fingerprint scanning. The working of the system is controlled by a central processing unit, which is the Raspberry Pi Zero 2 W.

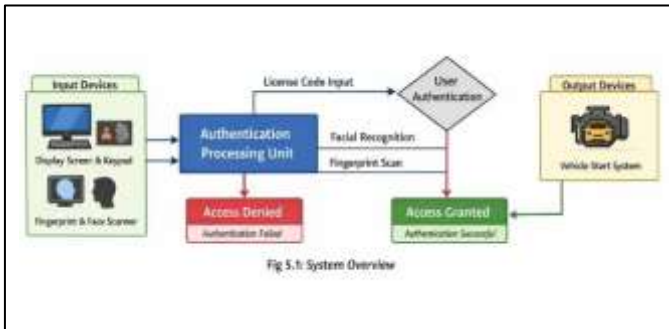
System Design Overview

The system design is based on a block structure where all components are connected to the main controller. The Raspberry Pi acts as the brain of the system and processes all input data. Arduino Uno is used to handle hardware-level operations and communication between components.

The system consists of input devices, processing units, and output devices:

- **Input Devices:**
Camera (for face recognition), Fingerprint sensor (for fingerprint scanning), Keyboard/input system (for license entry)
- **Processing Units:**
Raspberry Pi Zero 2 W, Arduino Uno
- **Output Devices:**
Motor driver/relay (vehicle control), Buzzer (alert), Display screen (user interface)

All these components work together to form a complete system.



PROTOTYPE MODEL / BASE STRUCTURE

The base structure of the project is designed using a metal sheet, which provides strong support and stability to the entire system. The metal structure acts as the foundation on which all components are mounted properly. It is designed in such a way that all parts are arranged neatly and securely.

All the hardware components such as Raspberry Pi, Arduino Uno, fingerprint sensor, web camera, motor driver, and buzzer are mounted on this metal base. Proper spacing is maintained between components to ensure easy wiring and maintenance. The metal structure also helps in protecting the components from damage and provides durability to the system.

CIRCUIT / CONNECTION OVERVIEW

All components are connected in a proper way to ensure smooth communication. The camera and fingerprint sensor are connected to the Raspberry Pi. The Arduino is connected with the Raspberry Pi to control hardware operations. The relay or motor driver is connected to the controller to operate the vehicle ignition system.

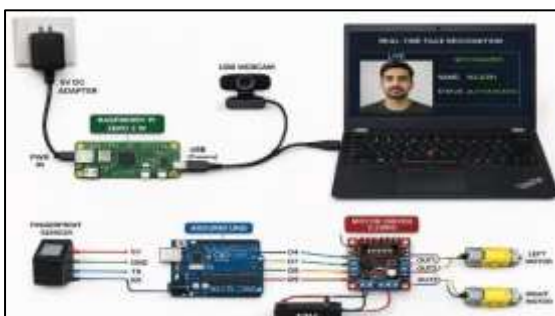


Fig.Circuit Diagram



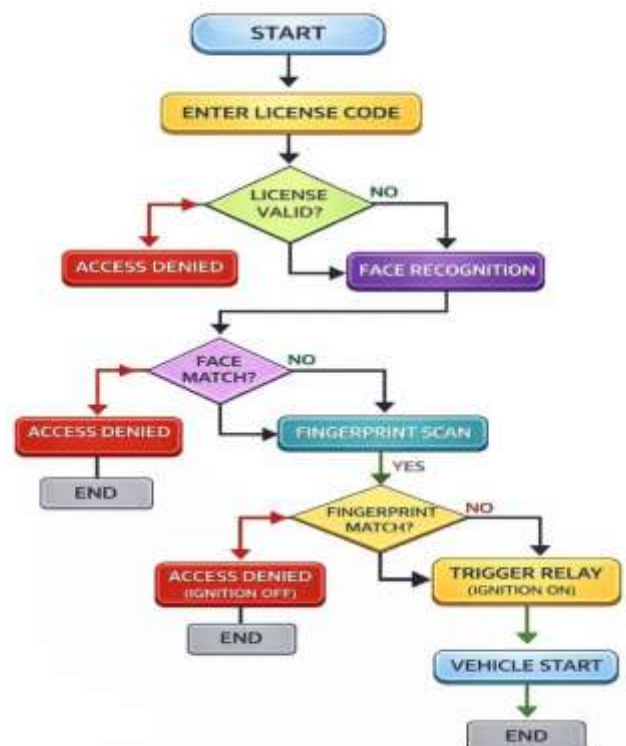
Working Of The System

The working of the system is based on a step-by-step authentication process:

1. The user starts the system
2. The system asks for license code (licence is compulsory)
3. License is verified
4. If valid, face recognition starts
5. If face is matched → vehicle starts
6. If face fails → fingerprint scanning starts
7. If fingerprint matches → vehicle starts
8. If both fail → access denied

This process ensures that only authorized users can operate the vehicle.

5.7 Working Flow Chart



Authentication Logic

The system follows a flexible authentication logic:

License + (Face OR Fingerprint) = Vehicle Start

- License is compulsory
- Either biometric is sufficient
- Both fail → access denied

This improves both security and user convenience.

Hardware Integration

The hardware components interact with each other to perform the required operations.

- The camera captures face data and sends it to Raspberry Pi
- The fingerprint sensor sends fingerprint data
- Raspberry Pi processes all data
- Arduino controls hardware signals
- Relay/motor driver controls the vehicle ignition

This interaction ensures smooth system operation.

Software Integration

The software controls the system and performs important operations:

- License verification using stored database
- Face recognition using image processing
- Fingerprint matching using sensor data
- Decision making based on authentication logic

The software ensures fast and accurate working.

PROGRAM STRUCTURE

1. Initialization:

Required libraries are included for camera, fingerprint sensor, and serial communication. PIO pins are defined for motor driver, buzzer, and sensors. Serial communication is initialized between Raspberry Pi and Arduino. Camera module is initialized for face recognition.

2. License Input and Verification:

- User enters the license code through the system interface (laptop)
- The entered license is compared with stored data
- If the license is valid, the system proceeds to biometric authentication
- If invalid, access is denied

3. Face Recognition:

- The camera captures the user's face
- The captured image is processed using face recognition algorithm
- If the face matches with stored data → authentication success
- If not matched → system moves to fingerprint authentication

4. Fingerprint Authentication:

- The fingerprint sensor scans the user's finger
- The scanned data is compared with stored fingerprints
- If matched → authentication success
- If not matched → access denied

5. Processing and Decision Making:

- The system checks the condition:
- License + (Face OR Fingerprint)
- If condition is satisfied → vehicle start
- Otherwise → access denied

6. Output Control:

- Arduino receives signal from Raspberry Pi
- Motor driver is activated
- Vehicle motor starts
- Buzzer gives alert if access is denied

RESULTS AND APPLICATIONS

INTRODUCTION

This chapter presents the results obtained after the successful design and implementation of the Intelligent Vehicle Access Control System. It explains how the system performs under different conditions and how effectively it meets the objectives of the project. The system was tested in real-time conditions using different

inputs such as valid and invalid license codes, correct and incorrect biometric data. The purpose of testing was to check the accuracy, reliability, and performance of the system. This chapter also describes the practical applications of the system in real-life scenarios.

EXPERIMENTAL SETUP AND TESTING

The system was developed using Raspberry Pi Zero 2 W, Arduino Uno, fingerprint sensor, web camera, motor driver, buzzer, and display screen. All components were properly connected and tested before running the system. Different test cases were performed to check the working of the system:

- Testing with correct license code
- Testing with incorrect license code
- Testing face recognition with valid user
- Testing face recognition with invalid user
- Testing fingerprint with valid and invalid data
- Testing system response time
- Testing system under different lighting conditions

Each test was performed multiple times to ensure accuracy and reliability.

8.3 OBSERVED RESULTS

The results obtained from testing the system are as follows:

- The system successfully verified the license code in all cases
- It did not allow further steps if the license was incorrect
- Face recognition worked accurately under normal lighting conditions
- Fingerprint sensor provided high accuracy in matching fingerprints
- The system allowed access when either face or fingerprint was correct
- The system denied access when both biometric methods failed
- The response time of the system was fast and efficient. The system performed as expected and followed the designed logic correctly.

CONCLUSIONS

The Intelligent Vehicle Access Control System using Dual Biometric and License Authentication is developed to improve vehicle security and prevent unauthorized access. The system uses license verification along with face recognition and fingerprint authentication, which makes it more secure than traditional systems.

The project successfully implements a multi-level authentication system where the license is compulsory, and either face or fingerprint verification allows the vehicle to start. This provides both security and user convenience.

The system was developed using Raspberry Pi and Arduino along with sensors like a fingerprint module

and web camera. During testing, the system showed good performance, fast response, and reliable operation under different conditions.

This project also helped in understanding embedded systems, sensors, and real-time applications. Although there are some limitations such as dependency on lighting and sensor accuracy, they can be improved in future.

The system can be further enhanced by adding technologies like IoT, GPS tracking, and mobile application control. Overall, the project provides a simple, effective, and practical solution for vehicle security.

REFERENCES

- [1] Raspberry Pi Foundation, "Raspberry Pi Documentation," Raspberry Pi Foundation, Cambridge, U.K., 2024.
- [2] Arduino, "Arduino Uno Board Details," Arduino Documentation, 2024.
- [3] OpenCV Documentation, "Face Recognition Techniques," OpenCV.org, 2024.
- [4] Fingerprint Sensor Module User Manual, "Fingerprint Recognition Module Documentation," 2023.
- [5] GeeksforGeeks, "Face Recognition using Python," 2024. [Online]. Available: <https://www.geeksforgeeks.org/>. [Accessed: Jun. 18, 2026].
- [6] ProgrammingKnowledge, "Face Recognition using OpenCV Python," YouTube Video Tutorial, 2023. [Online]. Available: <https://www.youtube.com/>. [Accessed: Jun. 18, 2026].
- [7] Murtaza's Workshop, "Face Recognition Project using Python," YouTube Video Tutorial, 2023. [Online]. Available: <https://www.youtube.com/>. [Accessed: Jun. 18, 2026].
- [8] Various Authors, "Research Articles on Vehicle Security Systems and Biometric Authentication," Journal and Conference Publications, 2020–2024.
- [9] "Smart Vehicle Security System using Biometrics," International Research Journal of Engineering and Technology (IRJET), vol. 8, no. 6, pp. 2021.
- [10] "Vehicle Security using Face Recognition and IoT," International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), 2022.
- [11] "Fingerprint Based Vehicle Security System," International Journal of Engineering Research & Technology (IJERT), 2020.
- [12] Various Authors, "Embedded Systems and Biometric Authentication Research Articles," Journal and Conference Publications, 2019–2024.