Fingerprint Sensor-Based Vehicle Starter Using Arduino

[1]Dr.B.JogeswaraRao, [2]J.varsha, [3]M.Vaibhav, [4]D.Varsha, [5]G.Vijayashimha
[1]Professor, [2,3,4,5] UG Students
Department of Computer Science and Engineering
MallaReddy University, Maissamaguda, Kompally, Medchal-Malkajgiri District, Hyderabad -500100, Telangana State

Abstract

Vehicle security is a growing concern, with traditional key-based ignition systems being susceptible to theft, duplication, and unauthorized access. This paper proposes a biometric-based vehicle ignition system using fingerprint authentication to ensure that only authorized individuals can start the vehicle. The system is developed using an Arduino Uno microcontroller, an R307 fingerprint sensor, five push buttons for fingerprint management, an I2C LCD display, an L298N motor driver, and a DC motor to simulate vehicle ignition. The integration of biometric security eliminates the risk of key duplication and unauthorized use, providing an efficient and secure method of vehicle access. This paper discusses the system's design, working principle, hardware implementation, and future improvements for real-world applications.

Keywords: Arduino Uno, R307 FPS, L298N, LCD

1. Introduction:

Vehicle theft remains a critical issue worldwide, with conventional ignition systems offering limited security. Traditional keys and RFID-based access methods can be duplicated, while password-protected systems are vulnerable to hacking or unauthorized disclosure. In contrast, biometric authentication, particularly fingerprint recognition, offers a high level of security since fingerprints are unique and difficult to forge. The proposed system eliminates the need for physical keys by integrating a fingerprint-based vehicle starter mechanism, ensuring that only authorized individuals can access and operate the vehicle.

The system uses an Arduino Uno as the central controller, an R307 fingerprint sensor for biometric authentication, an I2C LCD display for user interaction, and an L298N motor driver to control a DC motor, which simulates the vehicle's engine. The fingerprint authentication process is managed through five push buttons that allow users to enroll, delete, and manage stored fingerprints. By combining security, automation, and ease of use, this system provides a practical and cost-effective solution for vehicle protection.

Objectives

1. To develop a biometric authentication system for vehicle ignition.
2. To integrate an FPS module with an Arduino Uno for fingerprint enrollment and verification.
3. To enhance vehicle security by allowing only authorized users to start the vehicle.
4. To provide user feedback through an LCD and buzzer.
5. To implement a motor driver circuit to control the ignition system.

Problem Statement:

Vehicle theft is a growing concern, and traditional security measures such as mechanical locks and RFID-based systems are not entirely foolproof. Unauthorized access and key duplication pose significant risks. A fingerprint-based vehicle starter system addresses these issues by ensuring only registered users can start the vehicle, enhancing security and ease of use.

2. Literature Review:

Various vehicle security technologies have been developed to prevent unauthorized access, including RFID-based keyless entry, PIN/password-based authentication, and smart card systems. However, these methods have limitations, such as susceptibility to hacking, loss of access credentials, or duplication risks. Biometric authentication, particularly fingerprint recognition, facial recognition, and iris scanning, has gained attention due to its uniqueness and reliability.

Several research studies have explored the implementation of fingerprint-based ignition systems. Some designs integrate GSM modules for remote authentication, while others utilize Bluetooth or IoT-based mechanisms for added security. Compared to RFID and password-based security, fingerprint authentication is more robust, ensuring that access is granted only to pre-registered users. However, challenges such as fingerprint recognition failures in extreme environmental conditions (e.g., dirt, moisture) and system response time must be addressed for real-world implementation.

3. System Architecture and Components

3.1 System Architecture:

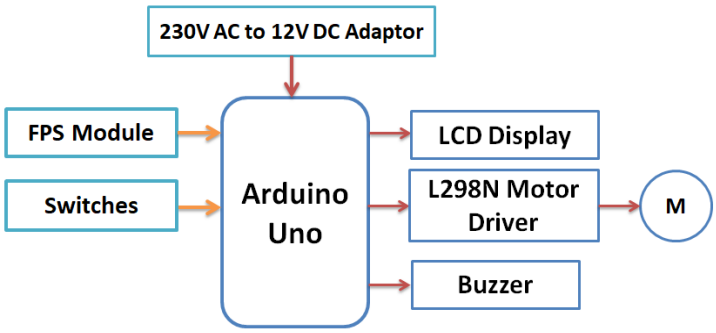

Fig 3.1 System Architecture

3.2 Hardware Components:

The system consists of the following key components:

- **Arduino Uno**: The Arduino Uno is a microcontroller board based on the ATmega328P. It features 14 digital input/output pins, 6 analog inputs, a 16 MHz quartz crystal, a USB connection, a power jack, and a reset button.

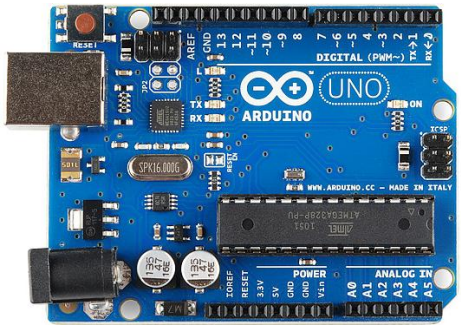

Fig. 3.2.1 Arduino Uno Board

It serves as the brain of the system, processing data from the R307 fingerprint sensor and controlling outputs such as the LCD display and motor driver. The board is programmed using the Arduino IDE with embedded C/C++ language. It operates at 5V and is widely used due to its ease of programming, open-source nature, and extensive library support for interfacing various sensors and modules.

- **R307 Fingerprint Sensor**: The R307 fingerprint sensor is a biometric module that captures, stores, and verifies fingerprints. It features an optical scanning mechanism, ensuring high accuracy and fast recognition.

Fig 3.2.2. R307 FPS Module

The module has a flash memory that can store up to 1000 fingerprint templates and communicates with Arduino via a serial UART interface (TX, RX pins). The sensor captures an image, converts it into a digital template, and compares it with stored data for authentication. It provides real-time verification in less than one second, making it ideal for security applications such as vehicle ignition, door locks, and access control systems.

- **Push Buttons (5 units)**: The system includes five push buttons for controlling the fingerprint sensor's functionalities. Each button has a dedicated role, such as enrolling a new fingerprint, deleting stored fingerprints, verifying authentication, resetting the system, and manually overriding the ignition process. These buttons send high or low (digital) signals to the Arduino, triggering predefined actions based on the user's input. They are simple, cost-effective, and durable components that provide an interactive interface for users to manage fingerprint data efficiently. Their compact size and straightforward wiring make them ideal for integrating into small security-based electronic projects.
- **I2C LCD Display:** The I2C 16x2 LCD display is used to provide real-time system feedback and

status messages to the user. It simplifies wiring by using only two pins (SDA and SCL) for communication, reducing the number of required connections compared to a standard parallel LCD.

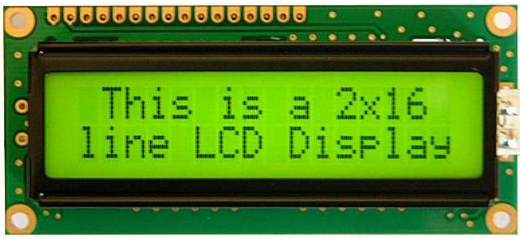

Fig 3.2.3. I2C LCD Display

The display shows instructions such as “Place Finger,” “Access Granted,” “Access Denied,” and “System Ready”, enhancing user experience. It operates on 5V power and can display alphanumeric characters, making it suitable for embedded systems. The display improves usability by ensuring clear interaction between the user and the fingerprint authentication system.

- **L298N Motor Driver:** The L298N motor driver is a dual H-Bridge driver IC used for controlling the DC motor in the system. It operates at 5V logic and 12V motor voltage, handling currents up to 2A per channel. The Arduino sends PWM (Pulse Width Modulation) signals to the driver, regulating motor speed and direction.

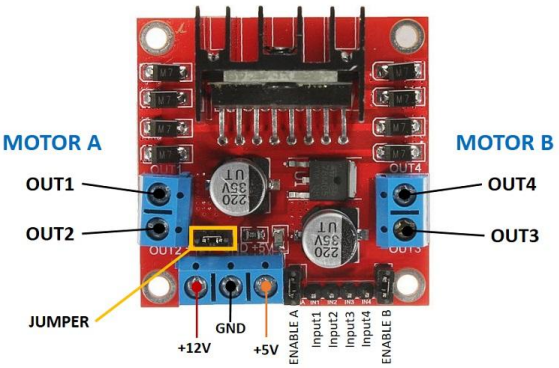

Fig. 3.2.4. L298N Motor Driver

When an authorized fingerprint is detected, the L298N enables motor operation, simulating the vehicle ignition process. It provides features like thermal shutdown, overcurrent protection, and independent motor control, making it ideal for motorized applications in robotics, automation, and security systems.

- **DC Motor:** The DC motor in this project represents the vehicle’s engine, turning on only when an authorized fingerprint is recognized. It converts electrical energy into mechanical motion using magnetic fields and brushes.

Fig 3.2.5. DC Motor with Wheel

The motor’s speed and direction are controlled via the L298N motor driver using PWM signals from the Arduino. It operates on 6V-12V and is commonly used in embedded systems due to its high efficiency, easy control, and fast response time. The motor’s activation upon successful authentication demonstrates how biometric access can be used to control vehicle ignition securely and effectively.

3.3 Software and Programming

The system is programmed using:

- Arduino IDE: Used for coding and compiling the microcontroller firmware.
- Embedded C Programming: Implements fingerprint recognition, motor control, and LCD display interactions.
- Adafruit Fingerprint Library: Handles communication between the Arduino and the R307 fingerprint sensor.

4. Working Principle

The fingerprint-based vehicle starter system operates as follows:

- System Initialization: When powered on, the system initializes the fingerprint sensor, LCD display, and motor driver. The LCD displays "System Ready."
- Fingerprint Enrollment: Using dedicated push buttons, authorized users can enroll their fingerprints into the R307 sensor's memory. The stored templates are used for future authentication.
- User Authentication: To start the vehicle, the user places their finger on the R307 sensor. The system compares the scanned fingerprint with stored templates.
- Access Granting: If the fingerprint matches, the LCD displays "Access Granted," and the L298N

motor driver activates the DC motor, simulating vehicle ignition.

- ☞ Access Denial: If an unregistered fingerprint is detected, the LCD displays "Access Denied," and the motor remains off.
- ☞ Fingerprint Management: Users can delete or re-enroll fingerprints using push buttons, ensuring flexibility in user access control.

5. Structural Diagrams

1. Class Diagram

A class diagram illustrates the interaction between different system components, such as the Arduino, FPS module, LCD, motor driver, and buzzer.

2. Component Diagram

A component diagram showcases the hardware interconnections:

- **Arduino Uno** – Central controller for processing authentication.
- **FPS Module** – Captures and verifies fingerprints.
- **Switches** – Used for enrollment and authentication.
- **LCD Display** – Shows system status and authentication results.
- **L298N Motor Driver** – Controls the ignition system.
- **Buzzer** – Provides feedback on authentication success or failure.

Behavioral Diagrams

1. Use Case Diagram

- **User Enrollment** – The user registers a fingerprint using the FPS module.
- **Authentication** – The system verifies the fingerprint before starting the vehicle.
- **Ignition Control** – If authenticated, the motor driver starts the vehicle.
- **Failure Handling** – If authentication fails, the buzzer alerts the user.

2. Sequence Diagram

1. The user presses the switch for fingerprint enrollment.
2. The FPS module captures and stores the fingerprint in the database.
3. The user attempts to start the vehicle.
4. The FPS module compares the input fingerprint with stored data.
5. If matched, the Arduino signals the L298N motor driver to start the motor.
6. If mismatched, the buzzer activates, and the system denies access.

6. Results and Discussion

The system was tested under various conditions to evaluate its efficiency, accuracy, and reliability. Key findings include:

- ☞ High Recognition Accuracy: The fingerprint sensor demonstrated a high success rate in recognizing authorized users while rejecting unauthorized ones.
- ☞ Fast Response Time: The system processed fingerprint authentication in under 1 second, ensuring a seamless user experience.
- ☞ Enhanced Security: Unlike traditional keys, the biometric authentication method significantly reduces unauthorized access risks.
- ☞ User-Friendly Interface: The I2C LCD display provided clear and informative messages, making the system easy to operate.
- ☞ Limitations: Some challenges were identified, such as reduced recognition accuracy when the user's finger was dirty or wet. Future improvements could involve integrating multiple biometric modalities for increased reliability.

7. Results:

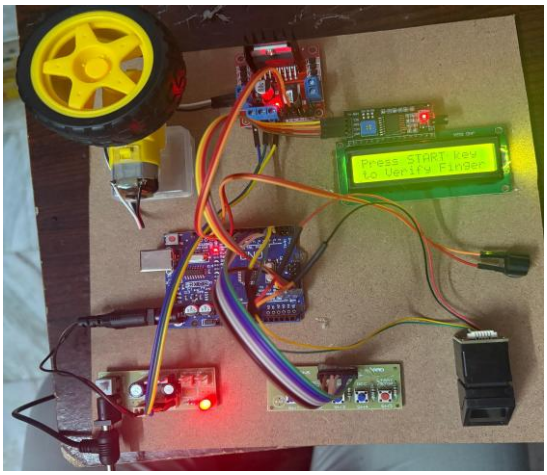

Fig 7.1. System Waiting for Verify the Finger

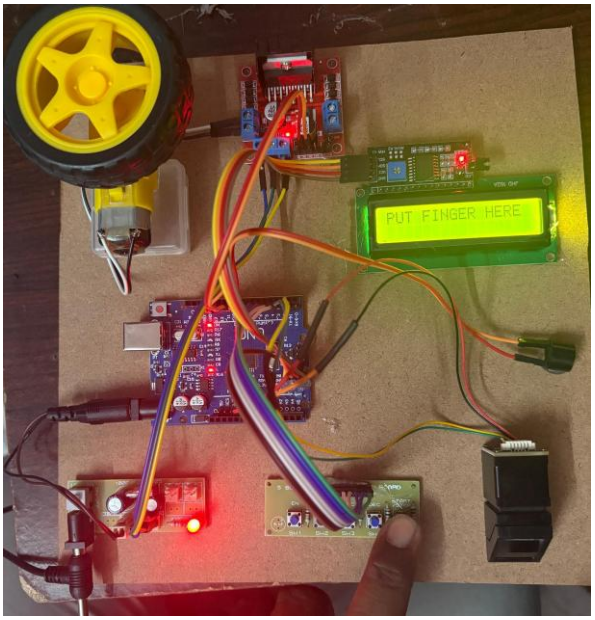

Fig 7.2. System Verify the user Finger

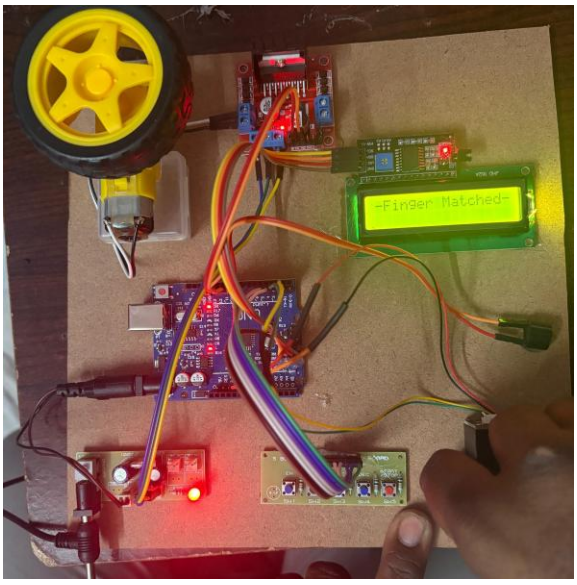

Fig 7.3. Finger Matched

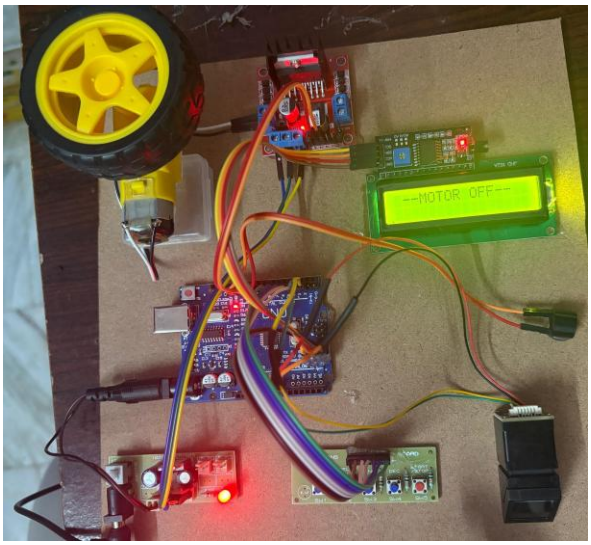

Fig 7.4. Motor Off

7. Future Enhancements

Although the system provides enhanced security, it can be further improved by incorporating additional features such as:

- GSM Module Integration: Allowing remote vehicle access through SMS-based authentication.
- GPS Module: Tracking vehicle location in real time in case of unauthorized access or theft attempts.
- IoT Connectivity: Enabling users to monitor and control vehicle ignition via a smartphone app.
- Facial Recognition: Adding an additional layer of security for multi-factor authentication.
- Voice-Based Authentication: Allowing users to start the vehicle using voice commands for convenience.

Conclusion:

This paper presents a fingerprint sensor-based vehicle starter system using Arduino, providing a secure and efficient alternative to traditional key-based ignition. The use of biometric authentication ensures that only authorized individuals can start the vehicle, significantly reducing theft risks. The system integrates an Arduino Uno, R307 fingerprint sensor, push buttons, an I2C LCD display, an L298N motor driver, and a DC motor, demonstrating a practical and reliable approach to vehicle security.

The results indicate that fingerprint authentication is a highly effective method for vehicle access control, offering improved security, fast response time, and ease of use. While the system performs well under normal conditions, future enhancements such as IoT integration, GSM-based remote control, and additional biometric features could further enhance its applicability. The proposed system is cost-effective, easy to implement, and ideal for modern vehicle security applications.

REFERENCES:

[1] Amit Saxena, "IGNITION BASED ON FINGERPRINT RECOGNITION" was published in the International Journal of Scientific Research and Management Studies (IJSRMS) Volume 2 Issue1.

[2] Prashant Kumar R. "TWO-WHEELER VEHICLE SECURITY SYSTEM" appeared in the December 2013 issue of the International Journal of Engineering Sciences & Emerging Technologies, Volume 6, Issue 3.

[3] Bhumi Bhatt, "Smart Vehicle Security System Using GSM & GPS" June 2015 issue of the International Journal of Engineering and Computer Science.

[4] K. A. Amusa "DESIGN OF AN SMS-ENABLED CAR SECURITY SYSTEM" Volume 2 of the International Journal of Science and Technology, November 2012.

[5] Roopam Arora "FINGERPRINT THE ENGINE AND TURN IT ON" Volume IX, Issue X, October 15, International Journal of Computer Engineering and Applications.