Raspberry Pi-based dual authentication system for vehicle security

Ms. Komal Ananda Palande, Prof. Mr. Santosh Dattatray Kale
Electronics and Telecommunication Engineering, SHIVNAGAR VIDYA PRASARAK MANDAL College of Engineering, Malegaon (BK) Malegaon, India

***Abstract*— The proposed system combines two-factor authentication using biometric fingerprint recognition and real-time image verification to establish a comprehensive security solution. Only after both the fingerprint and image checks are validated does the system trigger the relay, allowing access to the vehicle. In cases of failed authentication, the system activates a buzzer to notify nearby individuals of a potential intrusion attempt, while the display provides feedback, showing an "Access Denied" message. This dual authentication approach mitigates the risks associated with single-point verification methods, significantly reducing vulnerability to unauthorized access attempts. Designed with scalability in mind, this project demonstrates a practical and effective solution for vehicle security, integrating biometric and visual verification technologies. This system can be further expanded or adapted for various security applications, providing a versatile framework for modern security needs.**

Keywords—Dual Authentication; Raspberry Pi; Camera, Fingerprint

1. INTRODUCTION

With the increasing sophistication of vehicle theft methods, the need for more advanced security systems has become paramount. Traditional vehicle access controls, such as keys or remote fobs, are increasingly vulnerable to attacks like key cloning, relay attacks, and lock manipulation. To overcome these vulnerabilities, this project introduces a dual authentication security system for vehicles, incorporating both biometric fingerprint recognition and real-time image verification. The use of dual authentication elevates the security standard by ensuring that access to the vehicle is only granted to verified, authorized users, minimizing the risk of unauthorized entry. This layered approach to security addresses the limitations of single-point authentication methods, making the vehicle significantly more secure against modern threats.

The Raspberry Pi was chosen due to its computational capabilities, ease of integration with multiple sensors and modules, and support for complex software programming. This microcontroller acts as a bridge between the system's input and output devices, including a fingerprint sensor, camera module, display, buzzer, and relay.

The first layer of authentication utilizes a fingerprint sensor, which scans and verifies the user's unique biometric data. Biometric security is widely regarded as one of the most reliable forms of authentication, as fingerprints are unique to each individual and difficult to replicate. The second layer of authentication is where a camera module captures a real-time image of the user. This image verification stage adds security measures by enabling visual confirmation of the user's identity, which could be used for further analysis or as a deterrent for unauthorized individuals.

In addition to the authentication modules, the system includes a display, buzzer, and relay to enhance user interaction and provide feedback on authentication attempts. The display plays a critical role by providing visual feedback to the user, indicating the status of the authentication process. For instance, messages such as "Authentication Successful" or "Access Denied" can inform users of their access status in real time. If authentication fails at any stage, the system activates a buzzer, alerting those nearby to a potential security breach. This auditory alert adds an extra layer of deterrence against unauthorized access. Finally, a relay controls the locking mechanism of the vehicle, which is only activated upon successful dual authentication. This relay setup ensures that even if one layer of security is compromised, access is only granted if both layers are verified.

1.1 PROBLEM STATEMENT:

In recent years, the rise in vehicle theft has exposed the limitations of conventional security mechanisms, which often rely on single-factor authentication methods such as keys, PIN codes, or remote keyless entry. These traditional methods, though widely used, have shown significant vulnerabilities. Techniques like key cloning, relay attacks, and lock picking allow criminals to bypass these systems with relative ease.

Additionally, traditional security solutions fail to account for personalized and adaptive security. A physical key, for instance, can be used by anyone who possesses it, meaning it does not truly verify the user's identity. PIN codes and remote fobs can be lost, stolen, or even hacked, leaving vehicles vulnerable to unauthorized individuals. This lack of identity-specific verification is a fundamental weakness, as it allows anyone with access to the key to bypass security. The absence of user-specific verification not only compromises vehicle security but also diminishes user trust in the system's ability to protect against unauthorized access.

OBJECTIVE:

The primary objective of this project is to develop a Raspberry Pi-based dual authentication system that enhances vehicle security by integrating biometric and visual verification methods.

Specific Goals Include:

- Develop a Dual Authentication Security System
- Utilize Cost-Effective and Readily Available Hardware
- Implement Real-Time Monitoring and Feedback Mechanisms
- Securely Control Vehicle Access Using a Relay Mechanism
- Strengthen the Vehicle's Security Framework Through Multi-Layered Protection
- Provide a User-Friendly Interface and Experience

2. LITERATURE REVIEW

1. "Autonomous Vehicle: Security by Design" in IEEE Transactions on Intelligent Transportation Systems on Date of Publication: 30 June 2020 by Authors Mr. Anupam Chattopadhyay, Mr. Kwok-Yan Lam and Mr. Yaswanth Tavva are Senior Members, IEEE. Said it as Security of (semi)-autonomous vehicles is a growing concern, first, due to the increased exposure of the functionality to potential attackers; second, due to the reliance of functionalities on diverse (semi)-autonomous systems; third, due to the interaction of a single-vehicle with myriads of other smart systems in urban traffic infrastructure.. We attempt to identify the core issues of securing an AV.

2. "Security challenges in vehicular cloud computing" in IEEE Transactions on Intelligent Transportation Systems on Date of Publication: 03 September 2012 by authors Mr. Gongjun Yan, Mr. Stephan Olariu and Ms. Michele C. Weigle are said that In a VC, underutilized vehicular resources including computing power, storage, and Internet connectivity can be shared between drivers or rented out over the Internet to various customers. Clearly, if the VC concept is to see a wide adoption and to have significant societal impact, security and privacy issues need to be addressed. The main contribution of this work is to identify and analyze a number of security challenges and potential privacy threats in VCs.

3. "Connected Vehicles' Security from the Perspective of the In-Vehicle Network" in IEEE Network on 04 June 2018 by Authors Xiangxue Li and Yu Yu are said that Connected vehicles are generally equipped with many (dozens of, or even hundreds of) electronic and intelligent devices so that drivers can gain a more comfortable driving experience. Despite their numerous benefits, these technological developments have also created serious safety/security concerns.

4. "A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs)" in IEEE Transactions on Intelligent Transportation Systems on 07 June 2021 by Authors Mr. Xiaoqiang Sun, Mr. F. Richard Yu and Ms. Peng Zhang are said that As the general development trend of the automotive industry, connected and autonomous vehicles (CAVs) can be used to increase transportation safety, promote mobility choices, reduce user costs, and create new job opportunities.

3. SYSTEM IMPLEMENTATION

BLOCK DIAGRAM

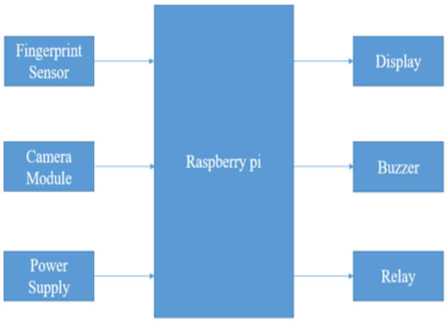


Figure 3.1 : Block Diagram

WORKING MODE:

The block diagram illustrates the components and flow of operation in a Raspberry Pi-based dual authentication system designed for vehicle security. At the centre of the diagram is the Raspberry Pi acts as the control hub, coordinating input from the fingerprint sensor and camera module, and managing output through the display, buzzer, and relay module. The combination of biometric and visual verification creates a robust dual authentication system that provides enhanced vehicle security, effectively deterring unauthorized access and theft. This setup ensures that access is only granted when both authentication methods confirm the user's identity, making it a reliable and advanced solution for vehicle security.

4. COMPONENTS DESCRIPTIONS

Raspberry pi :

The Raspberry Pi 4 is the latest product in the Raspberry Pi range, boasting an updated 64-bit quad core processor running at 1.4GHz with built-in metal heatsink, USB 3 ports, dual-band 2.4GHz and 5GHz wireless LAN, faster (300 mbps) Ethernet, and PoE capability via a separate PoE HAT. This version comes with 1GB of RAM, but we also have versions with 2 and 4 GB if youlike.

Specifications:

Model-Raspberry Pi 4 Model-B

Processor- Broadcom BCM2711, quad-core Cortex-A72 (ARM v8) 64-bit SoC @ 1.5GHz

RAM Memory - 1 GB LPDDR4 SDRAM

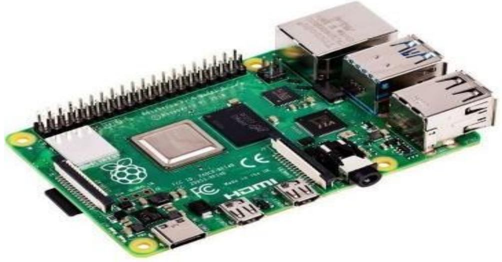


Figure 4.1: Raspberry pi

Fingerprint Sensor :

R307 is a finger print sensor module with TTL UART interface. The user can store the finger print data in the module and can configure it in 1:1 or 1: N mode for identifying the person.The FP module can directly interface with 3v3 Microcontroller.

The R307 fingerprint module has two interface TTL UART and USB2.0, USB2.0 interface can be connected to the computer; RS232 interface is a TTL level, the default baud rate is 57600 , can be changed, refer to a communication protocol ; can And microcontroller, such as ARM, DSP and other serial devices with a connection, 3.3V 5V microcontroller can be connected directly.

Features:-

- Supply voltage: DC 4.2 ~ 6.0V
- Fingerprint image input time: <0.3 seconds
- Matching method: Comparison method (1: 1)
- Search method (1: N)
- Characteristic file: 256 bytes
- Template file: 512 bytes
- Storage capacity: 1000 pieces
- Storage environment: Temperature: -40 ℃- +85 ℃Relative humidity: <85% H (no condensation)

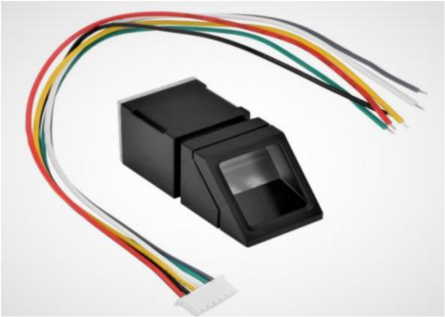


Figure 4.2: Fingerprint Sensor

Camera Module:

This full functionality Webcam can deliver smooth and detailed high-quality video. With bright, crystal clear footage and vibrant colors, make your video chat or online conference session, a wonderful experience. Audio quality is also immaculate.

Specifications:

Brand - Zebion

Model Name: Tiger Eye

Type - Web camera

Dimensions - L 5.3 x B 6.5 x H 4.3 cm

Image Sensor - CMOS

Video resolution - 640 x 480 (30 FPS)

Cable length - 1.58 Meter

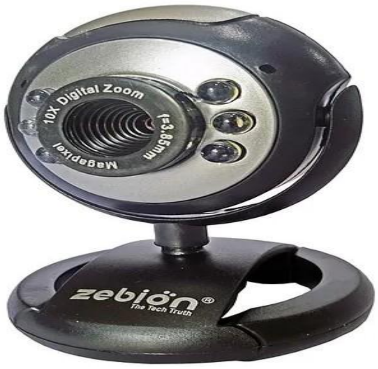


Figure 4.3: L293d

Buzzer:

This is Small PCB Mountable 5V Passive Buzzer-10 Pcs. It is great to add Audio Alert toyour electronic designs. It operates on 5V supply, uses a coil element to generate an audibletone.

Specifications

- Input Voltage(Max.) : 5V
- Resistance: 42 Ω
- Resonance Frequency: 2048 Hz
- Body Size : 12 x 8mm
- Pin Pitch: 6mm

4.5 Relay:

A single-channel relay is an electronic switch that can be controlled by a low-power electrical signal, such as the output from an raspberry pi. By using an single-channel relay module, you can control high-voltage or high-power devices, such as lights, motors, and appliances, from your computer or mobile device. In this blog, we will explore how a relay works, how to interface a single-channel relay with an Arduino Uno, and demonstrate a simple example of how to use the 5v relay module to control a lamp.

Specifications:

Relay Type: Low Level Trigger
Logic Input: 3.3 ~ 5
Trigger Voltage (VDC): 5
Switching Voltage (VAC): 250@10A
Switching Voltage (VDC): 30@10A

Figure 4.5: Relay

4.6 LCD :

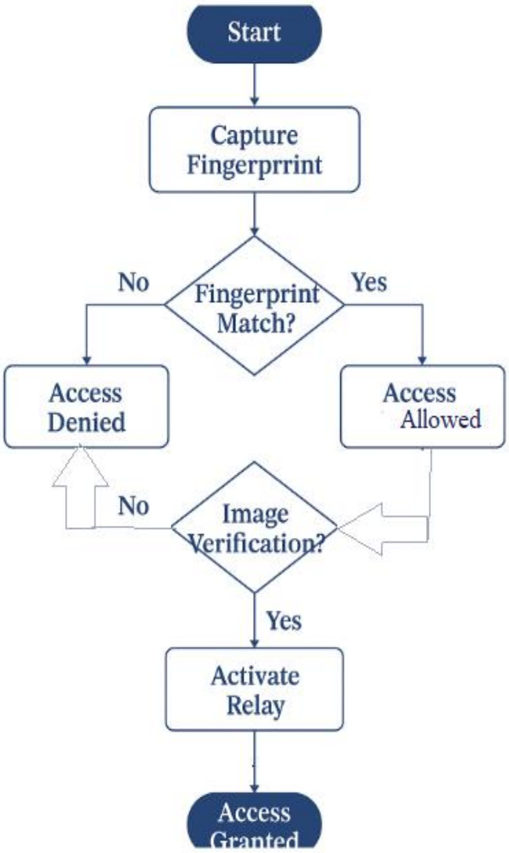
This is LCD 1602 Parallel LCD Display that provides a simple and cost-effective solution for adding a 16×2 White on Liquid Crystal Display into your project. The display is 16 character by 2line display has a very clear and high contrast white text upon a blue background/backlight. This is great blue backlight LCD display. It is fantastic for Arduino based project. This LCD1602 LCD Display is very easy to interface with Arduino or Other Microcontrollers.

Specifications:

- Arduino IIC/I2C interface was developed to reduce the IO port usage on Arduino board
- I2C Reduces the overall wirings.
- 16 characters wide, 2 rows
- Interface: I2C
- Interface Address: 0x27
- Character Color: White
- Supply voltage: 5V

Fig 4.6 LCD

Flowchart:



Result:

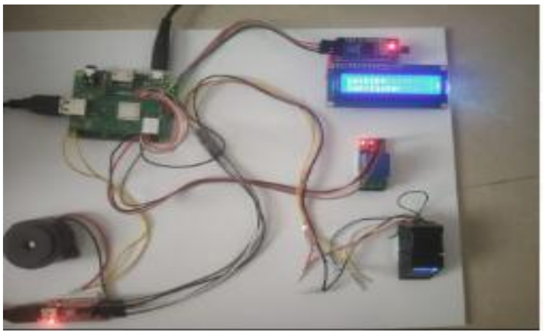


Fig. Result of Dual Authentication System

ADVANTAGES AND FUTURE SCOPE

5.1 ADVANTAGES:

- Enhanced Security: By using both fingerprint and face recognition, the system creates a dual-layer authentication method. This makes it significantly harder for unauthorized users to gain access, as both biometric credentials need to match.
- User-Friendly: Biometrics are quick and convenient, allowing authorized users to unlock their vehicle without the hassle of keys or remembering a PIN.
- Scalability: The system can register multiple users with individual biometric profiles, making it ideal for families or fleet vehicles where multiple people need access.
- Cost-Effective: Leveraging the Raspberry Pi and readily available sensors, this solution is affordable compared to many proprietary vehicle security systems.
- Low Power Consumption: The Raspberry Pi and its components are designed for energy efficiency, making it practical for long-term operation in a vehicle without draining the battery.
- Customizable: This system can easily integrate additional features, such as remote alerts, GPS tracking, or even IoT connectivity.

5.2 DISADVANTAGES:

- Limited Processing Power: The Raspberry Pi, while versatile, may struggle with real-time face recognition if processing power or memory is limited, potentially causing delays in authentication.
- Security Vulnerabilities: While secure, consumer-grade biometric systems may still be susceptible to spoofing attacks, like using high-resolution photos for face recognition or fake fingerprints.
- Privacy Concerns: Storing biometric data raises privacy issues and requires careful handling to prevent unauthorized access or data misuse.
- Complex Setup: Setting up and maintaining this system requires technical expertise.

5.3 APPLICATIONS:

The integration of dual biometric authentication using fingerprint and face recognition can significantly improve security and convenience in various sectors. Here are some key applications:

- Vehicle Security:
- Car Rental Services:
- Ride-sharing and Carpooling:
- Government and Law Enforcement Vehicles:
- Luxury and High-End Vehicles:
- Corporate and VIP Transport:
- Public Transportation Systems:
- Valet Services:
- Automated Parking and Self-Driving Cars:
- Industrial and Commercial Vehicles:

5.4 FUTURE SCOPE:

The future scope of a Raspberry Pi-based dual authentication security system for vehicles is promising, especially as biometric and embedded technologies continue to evolve. With advancements in Raspberry Pi processing power and more sophisticated machine learning algorithms, future versions of this system could achieve faster and more accurate authentication, making it feasible for broader adoption in real-world scenarios. Integrating AI-driven algorithms could also enhance biometric accuracy, improving the system's resilience against environmental factors such as lighting or fingerprint condition.

CONCLUSION

In conclusion, a Raspberry Pi-based dual authentication system for vehicle security offers a robust and innovative approach to protecting vehicles through the combined use of fingerprint and face recognition. This dual-layer biometric method strengthens security, making it much harder for unauthorized individuals to gain access while providing a convenient, user-friendly experience for vehicle owners. By leveraging affordable hardware and open-source technologies, this system provides an accessible and scalable alternative to traditional security measures.

REFERENCES

[1] Sadagopan, Vinoth Kumar, Upendran Rajendran, and Albert Joe Francis authored the paper titled "Design of an Anti-theft Control System Using Embedded Systems," which was presented at the 2011 IEEE International Conference on Vehicular Electronics and Safety.

[2] Pawar, M.R., and Rizvi, I. (2018). "Development of an IoT-Based Embedded

System for Vehicle Security and Driver Monitoring." In Proceedings of the Second International Conference on Inventive Communication and Computational Technologies (ICICCT), IEEE.

[3] Manjunath, T. K., Andrews SamrajMaheswari, and Chidaravalli Sharmila authored a paper titled "Locking and Unlocking of Theft Vehicles Using CAN," which was presented at the 2013 International Conference on Green High Performance Computing.

[4] Mukhopadhyay, D., et al. (2018). "Exploring the Development of an IoT-Driven Approach for Vehicle Security." In Proceedings of the 2018 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS) (pp. 1 6). IEEE.

[5] Ramadan, M. N., Al-Khedher, M. A., and Al Kheder, S. A. published a paper titled "Intelligent vehicle security and tracking system" in the International Journal of Machine Learning and Computing in 2012 (Volume 2, Issue 1).

[6] Jesudoss, A., Vybhavi, R., & Anusha, B. (2019). "Smart Helmet Design for Accident Avoidance." In Proceedings of the 2019 International Conference on Communication and Signal Processing (ICCSP). IEEE.

[7] S. Ajaz, M. Asim, M. Ozair, M. Ahmed, M. Siddiqui, and Z. Mushtaq presented a paper titled "Autonomous Vehicle Monitoring Tracking System" at SCONEST 2005, which was published in the conference proceedings spanning pages 1-4 in 2005.

[8] Joseph A. O'Sullivan and Robert Pless contributed to the article titled "Advances in Security Technologies: Detection, and Target Imaging, and Anomaly Biometric Recognition," which was published in the International Volume of the Microwave Symposium IEEE/MTT-S in 2007.