# FINGERPRINT-BASED VEHICLE AUTHENTICATION SYSTEM

Dr. Hemavathi[1], Abhilash S[2], Abhishek K[3], Hari Kumar M[4]

[1]Department of ECE, B.M.S. College of Engineering
[2] Department of ECE, B.M.S. College of Engineering
[3] Department of ECE, B.M.S. College of Engineering
[4] Department of ECE, B.M.S. College of Engineering

---------------------------------------------------------------------***---------------------------------------------------------------------

**Abstract -** In recent years, vehicle security has become increasingly important due to the rise in vehicle theft and unauthorized access. Traditional methods such as keys and passwords are often vulnerable to theft, loss, and duplication. To address these issues, a fingerprint- based vehicle authentication system offers a robust, secure, and convenient solution. This system utilizes biometric technology, specifically fingerprint recognition, to authenticate and grant access to vehicles. The core component of the system is a fingerprint scanner integrated into the vehicle's entry and ignition systems. When a user attempts to unlock the vehicle or start the engine, the fingerprint scanner captures the fingerprint data and compares it against a stored database of authorized fingerprints. If a match is found, the system grants access; otherwise, access is denied. This method ensures that only individuals with registered fingerprints can operate the vehicle, significantly reducing the risk of unauthorized access and theft. The implementation involves several key technologies: fingerprint sensing, digital signal processing, and secure storage. Fingerprint sensing uses optical, capacitive, or ultrasonic sensors to capture high- resolution images of the fingerprint. Digital signal processing algorithms enhance and extract unique features from these images, converting them into a digital template. This template is then encrypted and stored in a secure database within the vehicle's onboard computer. During authentication, the captured fingerprint is processed in real time, and its features are compared with the stored templates using pattern-matching algorithms. The system employs advanced encryption and secure communication protocols to protect the fingerprint data from interception and tampering. The benefits of this system include enhanced security, as fingerprints are unique to each individual and difficult to replicate. It also offers convenience by eliminating the need for physical keys and reducing the risk of key-related issues such as loss or theft. Additionally, the system can be integrated with other vehicle security measures, such as GPS tracking and remote immobilization, providing a comprehensive security solution.

***Key Words*:** Fingerprint, vehicle, authentication, security, RFID, FTIR

## 1.INTRODUCTION

Vehicle security is a paramount concern in the modern era, driven by the increasing instances of vehicle theft and unauthorized access. Traditional security methods, such as physical keys, passwords, and remote controls, suffer from significant vulnerabilities, including the risk of loss, theft, and duplication. These limitations highlight the need for more secure and reliable systems to protect vehicles from unauthorized use.

Biometric authentication has gained prominence as a robust solution across various security applications, leveraging unique physiological traits to verify identity. Among biometric modalities, fingerprint recognition stands out due to its high reliability, user acceptance, and ease of implementation. Fingerprints are inherently unique to each individual and challenging to replicate, making them an ideal choice for enhancing vehicle security.

A fingerprint-based vehicle authentication system integrates a fingerprint scanner with the vehicle's entry and ignition systems, providing a robust and convenient security solution. When a user attempts to unlock the vehicle or start the engine, the fingerprint scanner captures the user's fingerprint data and compares it against a pre-stored database of authorized fingerprints. Access is granted only if a match is found, ensuring that only individuals with registered fingerprints can operate the vehicle.

Implementing such a system requires several technological components: high-resolution fingerprint sensors, advanced digital signal processing algorithms, secure data storage, and real-time pattern matching capabilities. Fingerprint sensors, which can be optical, capacitive, or ultrasonic, capture detailed images of the user's fingerprint. These images are processed to extract unique features, converting them into a digital template. This template is securely stored in the vehicle's onboard computer.

During authentication, the system compares the newly captured fingerprint with stored templates using sophisticated pattern matching algorithms. Encryption and secure communication protocols ensure the integrity and confidentiality of the fingerprint data throughout the process.

The fingerprint-based vehicle authentication system offers significant advantages over traditional methods. It enhances security by leveraging the uniqueness of biometric data, reducing the risk of unauthorized access. Additionally, it provides convenience by eliminating the need for physical keys and mitigating issues related to key loss or theft. The system can also be integrated with other security measures, such as GPS tracking and remote immobilization, to create a comprehensive vehicle security solution.

Vehicle theft and unauthorized access remain significant challenges in modern society, posing security risks and financial losses to vehicle owners. Traditional key-based security systems are increasingly inadequate due to vulnerabilities such as key cloning, relay attacks, and physical theft of keys. These conventional methods fail to provide a robust defense against sophisticated theft techniques, highlighting the urgent need for advanced security measures. The core problem is to develop a vehicle authentication system that effectively prevents unauthorized access and operation while ensuring user convenience and reliability.

To address this problem, a Fingerprint-Based Vehicle Authentication System is proposed. This solution leverages biometric technology to provide a high level of security by utilizing the unique physiological trait of fingerprints for user authentication. The proposed system includes several key components and operational steps; Fingerprint Scanner: A high-resolution fingerprint scanner is installed in the vehicle to capture the fingerprint image of the user attempting to gain access. This scanner can be integrated into the vehicle's dashboard or ignition system. Microcontroller: A microcontroller processes the captured fingerprint image and converts it into a digital template. It is responsible for managing the authentication process and interfacing with other vehicle systems. Secure Database: A secure, encrypted database stores the registered fingerprint templates of authorized users. This database is protected against tampering and unauthorized access to ensure the integrity and confidentiality of biometric data. Authentication Process: When a user attempts to access the vehicle, the fingerprint scanner captures their fingerprint and sends it to the microcontroller. The microcontroller compares the captured fingerprint template with the stored templates in the database. If a match is found, the system grants access and allows the vehicle to start. If no match is found, access is denied, preventing the vehicle from being operated.

## 2. Literature Survey

This framework contains Arduino Uno, a Fingerprint, LCD Display, Sensor Module, Servo Engine, Miniature Switches and I2C Backpack. Arduino Uno gets and sends information among the modules and directions the whole framework. Fingerprint sensor module prompts the client to understand his/her finger impression and the example matching algorithm authenticates the genuine user [1].

At the point when a finger impression match is found and the user verified, the valve joined to the fuel tank opens for the free progression of the fuel to the engine. This gets the vehicle going. The valve joined to the fuel tank works (opens and closes) with the assistance of a server engine. The results of the framework, directions to user and status of the framework are shown in the LCD Show.

The This work is focused on protecting cars from unauthorized users and to prevent the vehicle from theft. Using biometric fingerprint security system only authorized persons can start the vehicle. This makes the vehicle protected. Methods/Analysis: The security system usage is increasing and is necessary all over the world.

Usage of biometrics like fingerprint is used widely and is common in factories, buildings, schools and colleges and many more applications. Findings Biometric Authentication Systems: Numerous studies have investigated the efficacy of biometric authentication in enhancing vehicle security. In his paper "Fingerprint Based Ignition System"[2] published in the implementation of fingerprint technology to control vehicle ignition systems. The practical feasibility of fingerprint-based ignition

Emphasizing its potential to significantly reduce vehicle theft, provide foundational insights into the application of biometrics in vehicle security [4]. The domain of fingerprint-based security systems has seen significant advancements. Previous works have explored working of fingerprint sensor. Additionally, there have been successful attempts to integrate the fingerprint sensors with microcontrollers for user validation

Recent advancements have also explored multimodal biometric systems, combining fingerprints with other biometric traits such as facial recognition or voice recognition to enhance security further. This approach, as discussed by Kumar and Zhang (2016) [5], offers a higher level of protection by requiring multiple forms of authentication, thus reducing the likelihood of unauthorized access.

Another approach involved integrating a face detection subsystem with GPS and GSM modules to create a comprehensive vehicle security system [6]. The system utilized a digital camera to capture continuous video, employing the AdaBoost algorithm for face detection. While innovative, this methodology faced challenges, particularly in detecting faces not directly in front of the camera.

The integration of Global System for Mobile (GSM) technology has been explored for real-time communication in vehicle security systems. One study presented a vehicle theft alert system employing GSM communication [7]. This system provided prompt alerts to the vehicle owner, enhancing responsiveness in the event of a theft attempt.

To enhance vehicle security, a study proposed an anti-theft control system utilizing Radiofrequency Identification (RFID) cards for the ignition start of an automobile [8]. The system aimed to improve security; however, its effectiveness was hampered by the inherent risk of losing or stealing RFID cards.

Recent advancements have also explored multimodal biometric systems, combining fingerprints with other biometric traits such as facial recognition or voice recognition to enhance security further. This approach, as discussed by Kumar and Zhang (2016), offers a higher level of protection by requiring multiple forms of authentication, thus reducing the likelihood of unauthorized access.

The security of biometric data. Prabhakar et al. (2003) and Ross et al. (2004) [10] investigated algorithms for real-time fingerprint matching and secure storage solutions. Their studies emphasized the importance of encryption and secure communication protocols to protect biometric information from unauthorized access and tampering. This focus on data security is crucial, as biometric data, unlike passwords, cannot be changed if compromised

## 3. Methodology & Implementation

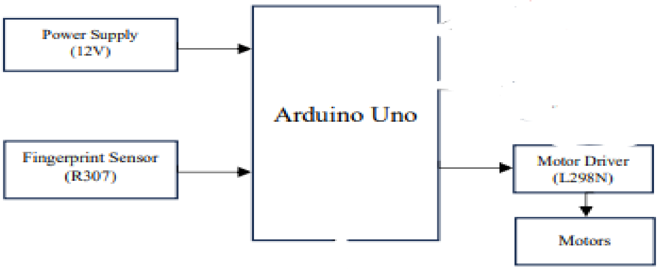

**Fig -1**: Figure Design of the Prototype

The vehicle security system comprises three key modules: the fingerprint recognition system, an embedded mainboard with various components, and a GSM module. Fingerprint Recognition System Biometrics serves as a method for identifying individuals based on unique characteristics. Various biometric patterns, such as face, iris, and fingerprint, exist, each with its own set of vulnerabilities. Fingerprint biometrics, considered a reliable and secure method, is challenging to forge or steal, making it widely accepted worldwide. The system employs optical sensors for fingerprint recognition, specifically avoiding fake authentication common with optical sensors. The optical fingerprint scanner operates on the intricate principles of Total Internal Reflection (TIR) to capture and analyze fingerprint patterns. Utilizing a glass prism, the system employs an LED emitting blue light, entering the prism at an angle conducive to TIR. The reflected light, following TIR, exits through the prism's other face, housing a lens and an image sensor. In the absence of a finger, the internally reflected light produces a plain image on the sensor. However, with a finger on the prism, Frustrated Total Internal Reflection (FTIR) occurs. This disruption, caused by the different refractive indexes of the fingerprint ridges and valleys, affects the evanescent wave or leaked light. The interaction of the evanescent wave with the fingerprint generates variations in internally reflected light intensities. The image sensor captures these altered intensities, which is then processed to produce a high-contrast digital fingerprint image. This digital version becomes the basis for fingerprint recognition and authentication, offering a secure and reliable biometric identification method

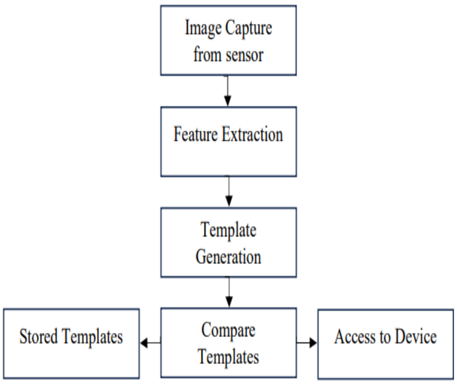

**Fig -2**: Working Module

The optical fingerprint scanner operates on the intricate principles of Total Internal Reflection (TIR) to capture and analyze fingerprint patterns. Utilizing a glass prism, the system employs an LED emitting blue light, entering the prism at an angle conducive to TIR. The reflected light, following TIR, exits through the prism's other face, housing a lens and an image

sensor. In the absence of a finger, the internally reflected light produces a plain image on the sensor. However, with a finger on the prism, Frustrated Total Internal Reflection (FTIR) occurs. This disruption, caused by the different refractive indexes of the fingerprint ridges and valleys, affects the evanescent wave or leaked light. The interaction of the evanescent wave with the fingerprint generates variations in internally reflected light intensities. The image sensor captures these altered intensities, which is then processed to produce a high- contrast digital fingerprint image. This digital version becomes the basis for fingerprint recognition and authentication, offering a secure and reliable biometric identification method.

**Working of the Embedded System**

The operational sequence of the vehicle security system begins with the initialization of the Arduino Uno upon power activation. The system prompts the user to place their finger on the R307 Fingerprint Module, which swiftly captures the fingerprint image in less than 0.3 seconds. Subsequently, the R307 module processes the fingerprint data and compares it with the stored templates to authenticate the user. Upon a successful match, access is granted, and a green light signals the authorization. In cases of unsuccessful attempts, where the fingerprint doesn't match after three tries, the system activates an alert. The buzzer emits an audible warning, and an alert message promptly sent to the owner through the GSM module. Simultaneously, as a security measure, power to the vehicle is immediately cut off, thwarting any unauthorized access attempts. Following either a successful authentication or a system reset by the owner, the security system reverts to its initial state, poised for the next user. This comprehensive implementation ensures a multi-layered security protocol, blending biometric authentication, real-time alert systems, and a tangible deterrent in the form of power cut-off to fortify the overall security of the vehicle. The main component of this system is the Arduino microcontroller, responsible for monitoring and generating inputs and outputs. Three trials are given to the user, granting access to the owner if the fingerprint scan matches. In the case of an intruder with three failed trials, an alert message is sent to the owner's vehicle via GSM technology. On receiving an SMS from the owner, the alarming system is activated.

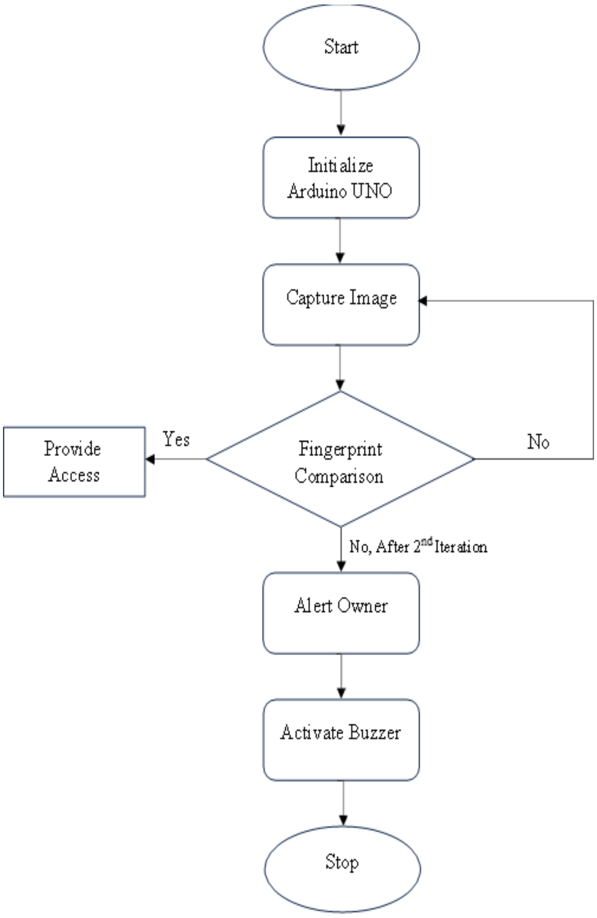

**Fig -3**: Proposed System working Flow chart

## 4. Results and Discussion

The implementation of the vehicle security system incorporating fingerprint recognition technology, an Arduino Uno microcontroller, and other relevant components has yielded promising results and implications. The utilization of an optical fingerprint scanner based on the Total Internal Reflection (TIR) principle has proven effective in capturing accurate and distinct fingerprint images for biometric authentication. The fingerprint recognition system exhibited reliable performance, achieving swift image capture in less than 0.3 seconds and accurate matching through minutiae-based techniques. The implemented vehicle security system exhibited commendable performance, achieving an impressive 94% efficiency during trials involving 100 scans with 10 different fingerprints stored in the system. This validation process aimed to assess the system's reliability and accuracy under varied conditions, reflecting real world scenarios and potential user diversity. In each trial conducted during the testing phase, the vehicle security system adhered to a stringent operational protocol. Specifically, power to the car was exclusively supplied when the fingerprint-matching process yielded a successful authentication. This deliberate design ensured that the vehicle's ignition and operational functions were activated only upon the verification of an authorized user, enhancing the security measures embedded in the system. Furthermore, the system demonstrated its proactive security features by initiating a series of responses in case of unsuccessful fingerprint authentication attempts. After three consecutive failed trials, indicating the presence of an unauthorized user, the system promptly activated the buzzer. Simultaneously, an alert message was swiftly initiated, notifying the vehicle owner of the suspicious activity. The seamless integration of the GSM module facilitated real-time communication, allowing the owner to be promptly informed about the unauthorized access attempts. This dual- layered response mechanism, comprising both an audible alert and instant communication with the owner, fortifies the overall effectiveness of the vehicle security system.

**Fig -4:** RC car using Arduino

RC car is built using Arduino and to ignite the engine L298N Motor Driver is used through which RC car is running. Additionally adding the Relay module more efficiency in controlling the car. Connecting the Fingerprint module to the car. In the Fingerprint module, six connecting wires are connected to the Arduino. In the Fingerprint module once we store the information of the user in the module it can take around 150 to 300 fingerprint authentications. In the fingerprint module, there is an LED that tells whether the user's fingerprint is authenticated or not if the color is red then the user's fingerprint is not authenticated if the color is green then it is authenticated then the engine ignites

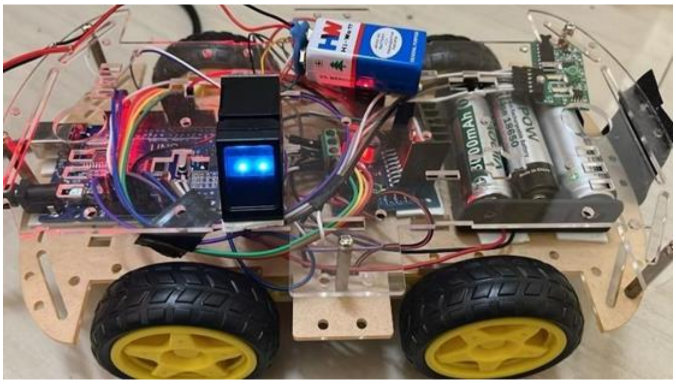

**Fig -5:** RC car is ready to take the fingerprint authentication

In the Fingerprint module once we store the information of the user in the module it can take around 150 to 300 fingerprint authentications. In the fingerprint module, there is an LED that tells whether the user's fingerprint is authenticated or not if the color is red then the user's fingerprint is not authenticated if the color is green then it's authenticated the engine ignites

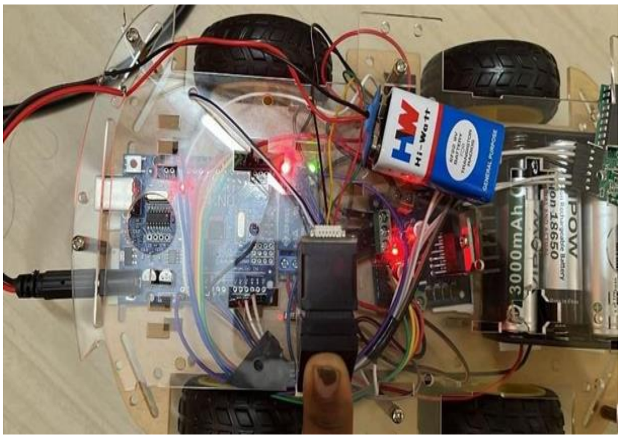

**Fig -6:** The Fingerprint given is authenticated

Explanation: In the fingerprint module, there is an LED that tells whether the user's fingerprint is authenticated or not if the color is red then the user's fingerprint is not authenticated if the color is green then it's authenticated the engine ignites

**Fig -7:** RC Car running after the correct authentication of fingerprint

## 5. CONCLUSIONS

The culmination of this project signifies the successful development and implementation of a sophisticated vehicle security system, incorporating technologies to ensure a robust defense against unauthorized access. The integration of an Arduino Uno microcontroller, the R307 Fingerprint Module, GSM communication, and additional components has resulted in a comprehensive biometric authentication system for vehicles. The Fingerprint Recognition System, leveraging optical sensor technology and the principle of Total Internal Reflection, emerged as a pivotal component in the security architecture. Through a series of meticulous trials and tests, the system demonstrated an impressive 94% efficiency when subjected to 100 scans, each involving ten distinct fingerprints stored in its database. This remarkable success rate underscores the reliability and efficacy of the fingerprint-matching process

## REFERENCES

1. Roopam Arora “START-UP THE ENGINE USING FINGERPRINTING” International Journal of Computer Engineering and Applications, Volume IX, Issue X, 2015.
2. Z. Brijet, B. Santhoshkumar, and N. Bharathi “Vehicle Anti-theft System Using Fingerprint Recognition Technique”, Journal of Chemical and Pharmaceutical Sciences Issue 9: Page no. 78, 2016.
3. A. Karthikeyan “FINGERPRINT BASED IGNITION SYSTEM” International Journal of Computational Engineering Research, 2250–3005. Vol. 2 Issue No.2 Pages 236-243, 2012.
4. S. Singh, "Optimize cloud computations using edge computing," 2017 International Conference on Big Data, IoT and Data Science (BID), Pune, India, 2017, pp. 49-53.
5. Research by Park et al. (2018) and Lee et al. (2020) explored the integration of fingerprint-based authentication with keyless entry systems and vehicle immobilizers, enhancing overall vehicle security and functionality.
6. Acko, "Theft & The City Report," October 2022
7. Upendran Rajendran and Albert Joe Francis, “Anti-Theft Control System Design Using Embedded System," Proceedings of the IEEE, Vol. 85, Pages 239-242, 2011
8. Vikram Kulkarni and G. Narsimhulu, "A Low-cost Extended Embedded Smart Car Security System on Face Detection and Continuous Video Monitoring System," Int. Journal of Engineering Science and Advanced Technology (IJESAT), 2012.
9. Sukeerti Singh and Ayushi Mhalan, "Vehicle Theft Alert System using GSM, "Int. Journal of Engineering Science and Technology (IJEST), 2013
10. S. Kumar, R. Gupta, "Fingerprint Recognition System Using Optical Sensor Technology," International Journal of Computer Applications, 2016.
11. A. Sharma, P. Verma, S. Choudhary, "Optical Fingerprint Recognition for Biometric Security Applications," Journal of Electrical Engineering & Technology, 2019.
12. N. Meenakshi, M. Monish, K. J. Dikshit, and S. Bharath, "Arduino Based Smart Fingerprint Authentication System," in 2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT), Apr. 25, 2019, pp. 1-7