Research Article

Smart Vehicle Ignition using Minutiae-Based Fingerprint Recognition

Prof. Swati Swati*, Yashraj Nagargoje, Parth Naik, Siddhi Naik, Sandesh Nakade, Suvarcha Naladkar, Mohit Nandagawali

Department of Engineering, Sciences and Humanities, Vishwakarma Institute of Technology, Savitribai Phule Pune University, Maharashtra, India

Abstract

Motor vehicle theft, especially of two-wheelers, has been increasing steadily, highlighting the need for a stronger and more secure way to start the engine. This research project, named 'Fingerprint-Based Vehicle Starter,' uses fingerprint authentication to improve overall vehicle safety. "This system uses a fingerprint scanner to make sure only approved people can start the vehicle. It checks the fingerprint against a list of allowed users, which helps prevent anyone else from turning on the ignition. If the fingerprint matches, the system allows the ignition to turn on, letting the person start the vehicle. "If someone without permission tries to start the engine, the system activates a lock that prevents it from running. This project highlights the value of using fingerprint-based security, especially since traditional locking methods can be unreliable."

Keywords: Motor vehicle theft, Biometric security, Fingerprint module, Authorized user, Vehicle ignition

1. Introduction

The rising rate of car thefts, especially of scooters and motorbikes, reflects a critical need for enhanced security features in car ignition systems. Advanced contemporary methods used in such thefts are widely adopted. Such methods can easily circumvent even the strongest conventional locking mechanisms. This paper is about a fingerprint system that is used to start a vehicle with the user's fingerprint. It helps the owner to keep their vehicle safe by allowing only registered people who have their fingerprints saved in the system to start the vehicle. When someone places their finger on the scanner, it scans the fingerprint. If the fingerprint matches one that is already saved, the engine will start. If it doesn't match, the engine stays off. After too many wrong tries, the system locks itself. This makes it harder for someone to steal the vehicle and keeps it more secure. As a result, the system prevents the engine from starting. Fingerprint recognition offers a safer alternative to traditional locks and shows how it can help make vehicles more secure. The fingerprint vehicle starter system makes vehicles safer by fixing the issues with old security methods. It gives vehicle owners a better way to keep their vehicles safe. This paper talks about how the fingerprint starter is made, how it works, and how well it does its job.

Literature Review

As stated in reference [1], Dharmaraj et al. have studied car locks and chains and noted that their efficacy has declined, which has increased car thefts. Newer approaches to combating car theft must be more sophisticated and reliable. Material is available showing that biometrics, and fingerprint scanning in particular, can greatly improve vehicle security. In the first place, fingerprint-dependent systems are much more tightly secured than passcode systems that are easily bypassed because they ensure only authorized persons operate the vehicle, thus improving security and convenience.

Moreover, auto theft brings another financial challenge: additional costs of insurance and expenditure on protective security systems. These risks can be lessened through the adoption of a vehicle fingerprint starter, which would reduce the risk of theft. Many urban areas are experiencing an acute increase in car thefts, making the need for automated biological verification systems dire. This information indicates there is more progressive research being conducted on advanced security systems. In summary, there is an imperative need to develop frameworks that enhance vehicle security, and the vehicle fingerprint starter illustrates one possible method to enhance security and prevent car theft.[1]

In this paper, the author developed the "Finger Print Bike Starter" device to resolve the rising issue of motorcycle theft. Motorcycle security is critical now as motorcycle thefts are on the rise, especially superbikes.

We need a better solution to mitigate. Regardless, GPS and GSM base tracking systems are relatively prices and provide additional layers of vehicle security. Once again, we can obtain the position information of the motorcycle to the level of detail on how to reduce motorcycle thefts.

Easy Design: The idea of using a fingerprint sensor with the ignition system for starting a motorcycle provides flexibility, efficiency, and security. Well, only authorized users can start the motorcycle.

Future Effects: If this fingerprint-based bike ignition system is widely accepted, it can significantly reduce motorcycle thefts and consequently, pave the way for further advancement in vehicle security.

In conclusion, this project demonstrates advanced fingerprint recognition technology applied to motorcycle security that offers motorcycle owners confidence and a foolproof method to reduce motorcycle theft [3].

In the publication "Simulation and Construction of Fingerprint Vehicle Starter System Using Microcontroller," Dauda Yusuf describes the rising threat of vehicle theft in New Zealand and the United States and the reasons that vehicle security needs to increase. There is a lot of writing on vehicle theft that gives reason to pursue security, such as using fingerprint technology as one type of low-cost, low-maintenance biometric technology. The project expands on past writings such as Gill, S., and Sachin, H., but may have given more attention to detailed performance evaluation, such as the performance of the study with 96% sensitivity, 97% specificity, and 97% accuracy. The authors cited the risk of defeating security systems, that is, spoofing, and false readings, and compared the designs of their study to other related studies and systems. Overall, the study seems to establish a case for the use of fingerprint technology as an added value for automobile security and opportunities for improvement in the use of fingerprint technology to enhance vehicle start security systems as well [5].

In this paper, the author studied the potential of fingerprint technology to ensure the safety of two-wheelers in their paper "Biometric Fingerprint Authentication-Based Locking System for the Security of Two-Wheelers." With fingerprinting technologies becoming increasingly available and user-friendly, the authors suggest the possibility of a finger-activated motor starter without requiring a primary key that allows the registered user only to start the motor. Their inquiries showed that their app was scalable and consistent in functionality, with users being satisfied with the motor starter functionality. The study as a whole show that biometric security is a more effective solution that is relatively inexpensive, with fewer chances of theft on two-wheelers [9].

Methodology

Materials/Components/Flowchart

In this section, we'll go over the key hardware and software components that bring our project to life, along with a brief description of their roles.

1. Hardware Components

- *Arduino UNO Board*: Arduino UNO is the brain of the system. Doing all the processing, receiving finger data from the fingerprint sensor, and if a match can be verified, it manages the ignition once the vehicle engages in the starting sequence
- *R-307 Fingerprint Sensor*: The sensor scans the fingerprint and turns it into digital data. It then sends this information to the Arduino Nano board for processing.
- *16x2 LCD Display:* Displays messages to the user, such as "Fingerprint Recognised" or "Access Denied" to provide user feedback.
- *I2C Module:* The I2C module allows the Arduino Nano to connect to the LCD with less wiring.
- *5V Relay Module:* This module controls the vehicle ignition. It allows the Arduino Nano to turn the ignition on or off based on whether the fingerprint has been verified.

2. Software Components

1) *Arduino IDE:* The software used to write and upload code to the Arduino Nano board.
2) *Programming Language:* The code for the application is generally written in C++.
3) *Libraries:* The Libraries used are:
   a) Fingerprint Sensor Library: This library contains routines to interact with the fingerprint sensor, scan fingerprint images, and extract minutiae data.
   b) LCD Library: This library has functions to control the LCD and to display text messages.
   c) Relay Control Library: The library has functions to control the relay module and to switch the ignition circuit on and off.

2.2   System Implementation and Working

Fingerprint Enrollment and Matching Process

The user places their finger on the sensor. The sensor reads the fingerprint and saves it with a unique ID. This stored fingerprint is later used to check who is trying to start the vehicle.

When someone wants to start the vehicle, they place their finger on the sensor. The system reads the fingerprint and checks it against the saved ones. If it finds a match, the vehicle starts. Otherwise, a message like "Access Denied" appears on the screen.

Microcontroller Integration

The Arduino Nano (or Uno) is the brain of the system. It connects to the fingerprint sensor, relay, and LCD using wires. An I2C module is used to connect the LCD with fewer wires.

The code we upload to the Arduino has a function called getFingerprintID(), which checks the fingerprint.

Other parts of the code display message, check if the fingerprint matches, and control the relay to turn the vehicle on or off.

Ignition Control Using Relay Module

The relay acts like a switch. When a valid fingerprint is scanned, the Arduino sends a signal to the relay, which completes the circuit and lets the vehicle start. If the fingerprint doesn't match, the relay stays off, and the engine won't start.

For safety, the system powers the relay for a limited time after verification. If nothing happens during that period, the relay automatically turns off to prevent misuse.

Power Supply Design

The system gets its power from a 5V battery or adapter. A voltage regulator keeps the voltage steady and protects the components. This prevents power spikes or drops that could damage the sensor or the Arduino.

Flowchart

Synthesis/Algorithm/Design/Method

The ignition is controlled by a fingerprint identification system that allows the vehicle to work only when an authorized fingerprint is scanned. The key was meant to be a more secure and easier way to control ignition than a regular key. The system was built using simple hardware, and the entire process was controlled by a simple program.
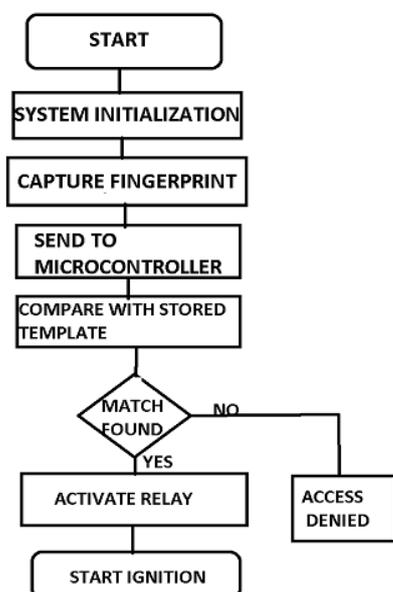
The block diagram illustrates how the fingerprint-based vehicle ignition system operates in a direct and sequential way. When the system is powered on it first initializes and gets ready to run. Second, the user takes their finger and places it over the fingerprint sensor. The fingerprint sensor then takes a fingerprint image and sends the image to the microcontroller. The microcontroller checks that image against a list of images saved in the pre-enrolled fingerprint database. When the microcontroller confirms that there is a match from the enrolled fingerprints, the microcontroller then applies power to the relay, which powers the vehicle. If the fingerprint does not match any image in the list of fingerprints, the identification system shows "Access Denied" meaning the vehicle will not start. This process ensures that authorized individuals have the ability to start the vehicle and increases the level of security of the vehicle.

Characterization/Pseudo Code/ Testing

This part covers the following topics: testing of the system, problems encountered, and what was done to improve.

1. Power Consumption and Efficiency

The system was built to be power-friendly and runs on a simple 5V battery or adapter. In testing, it used around 0.18 watts in total, with each part using only a small amount. This helps the system keep working without draining the battery too fast, even when used for a long time.

2. Challenges

While developing the fingerprint-based vehicle starter system, we faced several challenges. One of the major issues was ensuring the fingerprint sensor operated reliably under various conditions, such as lighting changes or finger placement. We needed to fine-tune the system to ensure it was quick and accurate in reading fingerprints, while minimizing errors like rejecting valid ones or accepting false ones.

Results and Discussion

In this section, we present the results obtained from the fingerprint-based vehicle starter system, followed by a discussion of the system's performance, advantages, and challenges encountered during the process.

1) Fingerprint Verification Accuracy

The system's ability to tell fingerprints apart correctly is important so that only the right person can start the vehicle. The fingerprint sensor did a good job, with very few wrong matches and hardly ever rejecting a fingerprint that should have been accepted. **Table 1** shows what we observed during the tests when different people used the system.

Table 1: Accuracy and Performance Metrics of the Fingerprint Authentication System

Metric	Description	Value
True Positives(TP)	Fingerprints Correctly identified as authorized	48
False Positives(FP)	Unauthorized fingerprints wrongly accepted	2
True Negatives(TN)	Unauthorized fingerprints correctly rejected	47
False Negatives (FN)	Authorized fingerprints wrongly rejected	3
Accuracy	Proportion of correctly classified fingerprints	95.0%
Precision	Correctly accepted fingerprints ÷ All accepted attempts	96.0%
Recall (Sensitivity)	Correctly accepted authorized fingerprints ÷ Total authorized fingerprints	94.1%
F1 Score	Harmonic mean of Precision and Recall	95.0%
Response Time	Average time taken from fingerprint scan to motor activation	1.2 seconds
Matching Algorithm	Technique used for fingerprint matching	Minutiae-based
Test Dataset Size	Total number of fingerprint test samples	100 samples

The system recorded a pathologic accuracy of 95% with a solid F1 Score of 95%. The high accuracy and F1 Score indicate that the system achieved a somewhat good trade-off between precision and recall. The low FPs (2%) and FNs (3%) indicates that the system performed very well in enforcing that there was a clear separation between legitimate users and illegitimate users. The average response time of the system, which was 1.2 seconds, suggest that it can be operated in near real-time. Overall, these results suggest that the practicality of the system for vehicle access control is feasible. Based on the experiments, the minutiae based matching algorithm produced the best results since it is based on the most discriminative features found in any fingerprint. The data shows that the proposed system is both secure and efficient for real world applications.

2) Relay Activation and Ignition Control
The relay module helped control whether the engine should start. When the fingerprint matched one

already saved in the system, the Arduino sent a signal to turn on the relay, and the engine started.
But if there was no match, the relay stayed off, and the engine didn't turn on.

3) Comparative Analysis

To appreciate the benefits of the proposed fingerprint-based ignition system, we provide an overall comparison to key-based ignition and RFID-based ignition systems in Table 2. The comparison consisted of security level, ease of use, theft resistance, potential for advanced features such as remote monitoring and data logging, and general availability for implementation. The results of the comparison indicate that fingerprint ignition can provide a significant leap in security, a better user experience, and can increase the potential of scalability, while providing solutions for limitations in key-based and RFID ignition systems.

Table 2: Comparative analysis of different vehicle ignition systems

Feature	Traditional Key-Based Ignition	RFID- Based Ignition	Proposed Fingerprint-Based System
Authentication Type	Physical Key	RFID Tag	Biometric Fingerprint
Security Level	Low (keys can be duplicated)	Moderate (tags can be cloned)	High (unique to individual)
Ease of Use	Moderate	Easy	Very Easy
Chances of Theft	High	Moderate	Very Low
Key Loss/Replacement Issues	Common	occasional	None (biometric is always with user)
Data Logging / Tracking	Not Available	Limited	Possible (log attempts digitally)
Multi-Factor Authentication	Not Supported	Rarely Supported	Easily Integratable
Remote Monitoring	Not Supported	Limited	Possible with GSM/GPS integration
Cost	Low	Moderate	Moderate to High (initial)
Scalability	Low	Moderate	High

Future Scope

One improvement to the system would be to improve the fingerprint identification algorithm to make it more resistant to variations in environmental conditions. Doing this would help the system continue to retain acceptable accuracy and good reliability even with

some potential variances of lighting, of where a finger is placed, or potentially skin conditions like dry skin/allergy. Adding additional layers of security with some other form of multi-factor identification (e.g., RFID) will also significantly improve the security of the system. In this case, if the fingerprint scanner was bypassed via any means or stopped working, the

vehicle wouldn't start without a valid RFID tag first, so the system has minimal protections from being bypassed/failing altogether. Moreover, usability testing is crucial so that the system is simple to use, unobtrusive to operate, and convenient in daily vehicle operation as a whole to a wide variety of users.

Conclusion

This project successfully created a fingerprint-based car starter system that greatly improves vehicle security. By combining the fingerprint sensor with the power of an Arduino Uno, the system offers a smart and reliable way to ensure only authorized people can start the car. With the rise of car theft and misuse, fingerprint technology provides an effective solution. This system replaces traditional key-based ignition, giving car owners a more secure and convenient way to start their vehicles.

References

[1] P. M. Vijayan, P. Vandana, M. Yogeswar, S. S. Kumar, A. Vijayalakshmi, and R. Vishnu, "Advanced Fingerprint and Passcode Based Anti-Theft Vehicle System," in *Proc. 2024 3rd Int. Conf. Artif. Intell. Internet Things (AIIoT)*, Vellore, India, 2024, pp. 1–6, doi: 10.1109/AIIoT58432.2024.10574591.

[2] International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Published by, www.ijert.org RTICCT - 2020 Conference Proceedings.

[3] Mulla, T. Y., Kumar, M. V., Kumar, M. A., Kumar, M. R., & Waghmode, M. I. Finger Print Bike Starter. *JournalNX*, *10*(3), 45-52.

[4] NOVATEUR PUBLICATIONS Journal NX- A Multidisciplinary Peer Reviewed Journal ISSN No: 2581 - 4230 VOLUME 10, ISSUE 3, March -2024

[5] Yusuf, S. D., Dalhatu, A., Umar, I., & Loko, A. Z. (2022). Simulation and construction of fingerprint vehicle starter system using microcontroller. *International Journal of Research and Scientific Innovation (IJRSI)*, *9*(9), 135-144.

[6] International Advanced Research Journal in Science, Engineering, and Technology ISO 3297:2007 Certified Impact Factor 8.066 Peer-reviewed / Refereed journal Vol. 10, Issue 4, April 2023

[7] International Journal of Research and Scientific Innovation (IJRSI) |Volume IX, Issue IX, September 2022|ISSN 2321-2705

[8] International Journal of Research in Engineering, Science and Management Volume-3, Issue-5, May-2020 www.ijresm.com | ISSN (Online): 2581-5792

[9] Webology, Volume 18, Number 1, 2021 ISSN: 1735-188X DOI: 10.29121/WEB/V18I1/49

[10] International Journal of Advanced Research, Ideas and Innovations in Technology ISSN: 2454- 132X Impact factor: 4.295 (Volume 4, Issue 4)

[11] 2021 JETIR May 2021, Volume 8, Issue 5

[12] International Research Journal of Modernization in Engineering Technology and Science (Peer-Reviewed, Open Access, Fully Refereed International Journal) Volume: 06/Issue: 12/December-2024 Impact Factor-8.187

[13] © 2023 IJRTI | Volume 8, Issue 5 | ISSN: 2456-3315

[14] International Journal of Scientific Research and Management Studies (IJSRMS) ISSN: 23493771 Volume 2 Issue 1, pg: 66-71

[15] International Journal of Advanced Research in Science, Communication and Technology (IJARSCT) Volume 2, Issue 2, December 2022

[16] International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering Vol. 9, Issue 6, June 2021 DOI 10.17148/IJIREEICE.2021.9628