iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

FINGERPRINT VEHICLE STARTER

MEREDDY NIKHILESH REDDY,
P VAMSHI
UG Students, J.B Institute of Engineering and Technology,
Moinabad, RangaReddy, Telangana

ABSTRACT
The fingerprint vehicle starter project aims to enhance vehicle security and convenience by implementing a system that allows users to start their vehicles using fingerprint recognition. This involves integrating a fingerprint sensor into the vehicle's ignition system. Users register their fingerprints, and the system authenticates them during the start-up process. This technology adds an extra layer of security beyond traditional key-based systems and can prevent unauthorized access to the vehicle. The project may include aspects such as fingerprint sensor integration, biometric data storage, and communication with the vehicle's ignition system to enable a seamless and secure user experience. Additionally, considerations for robustness, reliability, and user-friendly design are likely integral to the development of this project.

INTRODUCTION
In recent years, vehicle security has become a major concern due to the increasing incidents of car theft. Traditional vehicle ignition systems that rely on mechanical keys or remote key fobs are vulnerable to theft and unauthorized access. To address this issue, biometric authentication methods, particularly fingerprint recognition, offer a highly secure and user-friendly alternative for vehicle ignition.
This paper presents a Fingerprint Vehicle Starter System using Arduino UNO, which ensures that only authorized users can start the vehicle. The system integrates a fingerprint sensor, I2C LCD display, relay module, and DC motor to simulate the vehicle engine. The Arduino UNO acts as the central processing unit, managing fingerprint authentication and controlling the ignition process. When an authorized fingerprint is detected, the system activates the relay, allowing the engine (DC motor) to start. If authentication fails, the system remains locked, preventing unauthorized access.
The proposed system enhances vehicle security by eliminating the risk of stolen or duplicated keys. Additionally, it offers a cost-effective, efficient, and reliable solution that can be implemented in automobiles, motorcycles, and other transport vehicles. With the increasing adoption of biometric technology, the fingerprint-based vehicle starter system represents a significant step toward smart and secure transportation systems.

LITERATURE SURVEY
Recent studies have focused on developing fingerprint-based vehicle starter systems to enhance security. These systems typically involve the use of a fingerprint sensor connected to a microcontroller, which processes the fingerprint data and controls the vehicle's ignition system. Various algorithms, such as minutiae extraction and pattern matching, are employed to accurately verify the user's fingerprint. Several prototypes and implementations have been reported in the literature:
- Adebisi et al. (2017) designed a fingerprint-based ignition system using an ATmega328 microcontroller. Their system demonstrated high accuracy in fingerprint recognition and successfully prevented unauthorized access to the vehicle.
- Singh et al. (2019) developed a similar system using an ARM Cortex-M3 microcontroller. Their system included additional features such as remote vehicle control via a mobile application, showcasing the versatility of microcontroller-based implementations.
- Ali et al. (2021) proposed an advanced fingerprint vehicle starter system that integrated GPS tracking and GSM modules for real-time vehicle monitoring and alerting in case of unauthorized access attempts.

Challenges and Limitations Despite the advantages, several challenges remain in the implementation of fingerprint vehicle starter systems. Environmental factors, such as dirt or moisture on the fingerprint sensor, can affect the accuracy of fingerprint recognition. Additionally, the system's response time and reliability are crucial for user

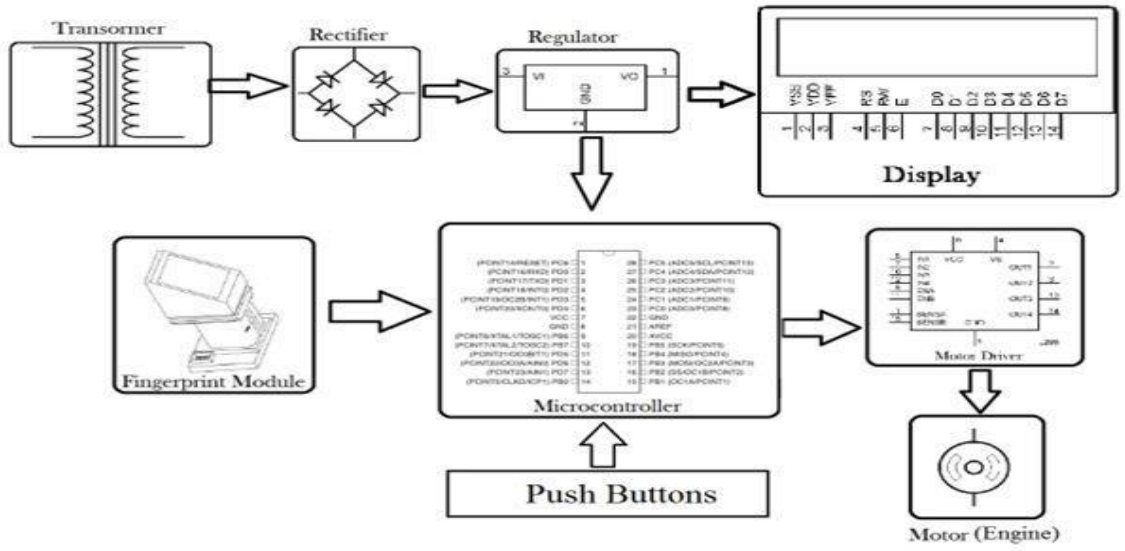
iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

acceptance. Research continues to address these challenges by improving sensor technology and optimizing fingerprint recognition algorithms.

Future Directions Future research may focus on enhancing the robustness of fingerprint vehicle starter systems through the integration of multi-modal biometric systems, combining fingerprint recognition with facial recognition or iris scanning for added security.

Conclusion Fingerprint vehicle starter systems offer a secure and reliable solution to prevent unauthorized vehicle access. Microcontroller-based implementations provide the necessary processing power and flexibility to integrate biometric security features into modern vehicles. As technology advances, these systems are expected to become more sophisticated, addressing existing challenges and offering enhanced security features.

PROPOSED SYSTEM



The given block diagram represents a biometric-based motor control system, likely utilizing a fingerprint module for authentication. Here's an explanation of its key components and working principle:

System Overview:

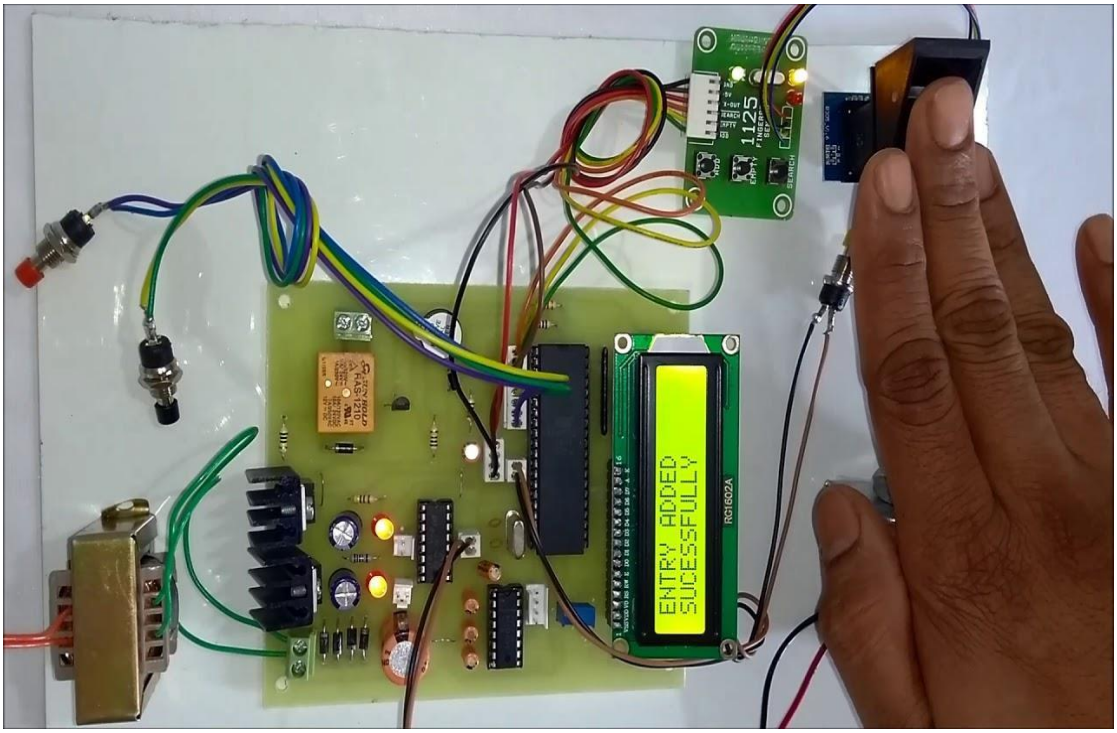
This system is designed to operate a motor (or engine) using fingerprint recognition. It involves various electronic components such as a transformer, rectifier, voltage regulator, microcontroller, fingerprint module, push buttons, display, and motor driver.

Working Principle:

1. When a user places their fingerprint on the Fingerprint Module, it scans and verifies the identity.
2. The Microcontroller processes the input and determines whether the fingerprint matches the stored data.
3. If authentication is successful, the Microcontroller signals the Motor Driver to turn on the motor.
4. The Display Unit provides visual feedback to the user.
5. The Push Buttons can be used to reset or manually control the system if needed.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

RESULTS



CONCLUSION

Arduino fingerprint launcher. This design ensures the safety of the vehicle. Uses a biometric system. This project is used to start a vehicle with only fingerprints. If you insert your right finger, only the vehicle starts and the owner receives a text message that the vehicle has started successfully. The owner is an unauthorized person trying to start the vehicle.

FUTURESCOPE

The Fingerprint Vehicle Starter system has significant potential for future advancements, integrating modern technology trends to enhance security, efficiency, and user convenience. Below are some key areas of future development:

1. Integration with IoT and Smart Connectivity
   - Vehicles can be connected to a cloud-based system that allows owners to register and manage fingerprints remotely.
   - Integration with mobile applications to provide remote authentication and engine start/stop via smartphones.
   - Real-time tracking and monitoring of vehicle access logs through IoT-based platforms.
2. Artificial Intelligence (AI) and Machine Learning (ML)
   - AI-based fingerprint recognition can improve accuracy and reduce false rejection rates.
   - ML algorithms can analyze driver behavior and suggest security enhancements.
   - Multi-modal biometric authentication (fingerprint + facial recognition) for increased security.
3. Advanced Security Features
   - Anti-theft Mechanism: If an unauthorized user attempts to start the vehicle, the system can alert the owner via SMS or app notifications.
   - Geofencing: Prevents the vehicle from being started in unauthorized locations.
   - Emergency Access Control: Owners can grant temporary access to family members or friends remotely.
4. Multi-Factor Authentication

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

- Combining fingerprint scanning with voice recognition, retina scanning, or PIN codes for enhanced security.
- Use of RFID/NFC technology along with fingerprint authentication for dual security layers.

5. Automotive Industry Adoption
   - Future self-driving cars can utilize fingerprint authentication for personalized settings and driver profiles.
   - Automakers can incorporate this system into high-end and commercial vehicles to reduce car theft.
   - Integration into electric vehicles (EVs) to provide secured access and prevent unauthorized usage.
6. Blockchain-Based Vehicle Security
   - Blockchain can store fingerprint authentication logs securely to prevent data tampering.
   - Allows for decentralized and secure access management across multiple users (e.g., rental or shared vehicles).
7. Customizable User Experience
   - Vehicles can automatically adjust seat positions, mirrors, climate control, and infotainment settings based on recognized fingerprints.
   - Different users (family members or fleet drivers) can have personalized access permissions.
8. Government and Law Enforcement Applications
   - Used for official or military vehicles where only authorized personnel can start the engine.
   - Law enforcement agencies can use fingerprint authentication to track stolen vehicles.
9. Wireless and Contactless Biometric Authentication
   - Contactless fingerprint scanning using ultrasonic or infrared sensors for faster and cleaner authentication.
   - Wearable biometric authentication where the user's smartwatch or biometric ring can serve as an alternative key.
10. Cost-Effective and Mass Production
    - As fingerprint sensors become more affordable, mass production and implementation in budget vehicles will become feasible.
    - Future vehicles may completely replace traditional keys with fingerprint-based ignition systems.

REFERENCES

1. Omidiora E. O. "A Prototype of a Fingerprint Based Ignition Systems in Vehicles" European Journal of Scientific Research ISSN 1450-216X Vol.62 No.2 (2011), pp. 164 171.
2. "Arduino- Introduction". Arduino.cc
3. GSM Global system for mobile communication ". 4G Americas, Retrieved 2014-03-22.
4. Karthikeyan.a "FINGERPRINT BASED IGNITION SYSTEM" International Journal Of Computational Engineering Research / ISSN: 2250–3005