



SMART SECURITY SYSTEM FOR VEHICLE ANTI-THEFT

Anjana R,

*Department of Electronics and Communication Engineering,
National Engineering College, Kovilpatti.*

Padma Preethi R

*Department of Electronics and Communication Engineering,
National Engineering College, Kovilpatti.*

Sujitha J,

*Department of Electronics and Communication Engineering,
National Engineering College, Kovilpatti.*

Mrs.S.Karthika,

*Department of Electronics and Communication Engineering,
National Engineering College, Kovilpatti.*

Abstract- In today's culture, the demand for automobiles has been constantly increasing. At the same time, the theft of these vehicles is on the rise. This project is used to validate the user's identification and provide security to the vehicle. Biometrics is crucial in verifying the user's identification and ensuring high levels of security, preventing the car from being stolen. Unlike other authentication techniques such as passwords, email verification, or fingerprint verification, this one does not need the use of a password. According to security, only authorized persons are likely to unlock the doors using fingerprint recognition. Due to the existence of a fingerprint sensor on the doors, only authorized individuals are permitted to access the vehicle. The role of face recognition follows, which is utilized to validate the user's identification. A camera is used inside the vehicle to record the user's image and compare it to recorded data. It compares the information to a database to find a match.

Keywords- Arduino microcontroller, Anti-theft, Fingerprint recognition, Face recognition.

I. INTRODUCTION

Security has become a big worry in the current environment. Everyone has a car, and that vehicle's safety is in threat. As the number of vehicles on the road rises, so does the possibility of a vehicle being stolen. It's also simple to get into the higher-priced high-end autos. As a result, the proposed effort will contribute to the development of a high-level security system for all types of vehicles.

The purpose of this project was to eliminate keys as a typical method of starting an automobile and to verify the user's identity before starting it. One of the fastest-growing industries in the car business. Biometric-based security is currently used by almost all automotive manufacturers. The use of biometrics is justified since it has a very minimal chance of being replicated. Automobiles have previously been fitted with a variety of commercial security features. We've incorporated fingerprint recognition and face recognition to verify the user's identity. Researchers were able to create false fingerprints that fooled many gadgets despite putting in a lot of work. For years, the security of fingerprint-based authorization has been a matter of passionate debate. You must first submit your fingerprint information for the door lock to work. The door will then match the fingerprint to the stored data every time someone enters. If the fingerprints match, the door will open. Face recognition has a few advantages. It's straightforward in that no physical touch is necessary to be recognized or identified. As a result, face recognition is one of the most rapidly evolving fields in biometrics. In this project's hardware and software setup, fingerprint recognition and face recognition are both used.

To prevent the automobile from starting, anti-theft security systems require real-time recognition, robust door control, and a solid security system. This study develops an anti-theft car protection system to address the drawbacks of completely autonomous driving.

II. LITERATURE REVIEW

This concept uses fingerprint recognition and facial recognition technologies to unlock the doors of automobiles, ensuring vehicle security. These two circumstances allow the user to start the vehicle's ignition. Similarly, protecting our valuables from intruders through the window, as well as the towing issue. This survey gives an overview of the many studies that have been conducted before in order to complete the project.

"A Prototype of a Fingerprint Based Ignition Systems in Vehicles," by Omidiora E. O. Fakolujo O. A. Arulogun O. T. and Aborisade D. O., discusses the creation of a car using fingerprint identification to open the doors instead of using traditional techniques of utilizing keys to enter the vehicle[15].

"Smart Security System Utilizing Face Recognition on Raspberry Pi," by Fahim Faisal and Syed Akhter Hossain, discusses the design of using face recognition to identify people and allow verified persons to ignite automobiles[9].

"Smart Car Security System For Defending Against Collaborative Attacks By Malware," by Chandra Shekar Ramaiah, Dr.S.Asif Hussain, S.Zahid Hussain, and Yahya Al Balushi, has explored the concept to enable only authorized users to enter the vehicle and avoid theft and intrusions[4].

III. METHODOLOGY

The goal of this project is to develop a theft-prevention anti-theft automobile security system. This security system makes use of the Arduino Uno microprocessor. Figure 1 shows a working block schematic of the anti-theft vehicle security system.

When the fingerprint is correct, the doors will be unlocked, and the security of individual verification will be increased. It is difficult to start the engine without first opening the door if the fingerprint is wrong. If the face recognized matches the database, the engine can be initiated in the next phase of validating the user's identity. The engine will not start if the face does not match the database.

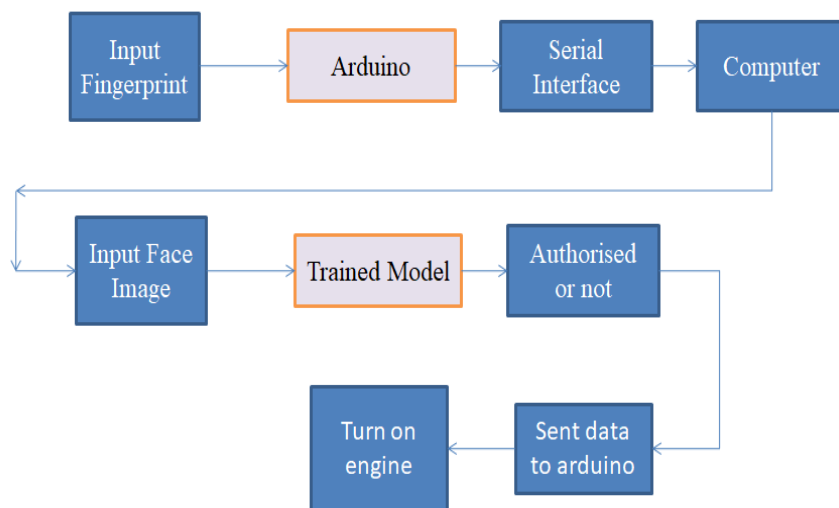


Fig.1. Block Diagram of the vehicle security system

IV. CIRCUIT DIAGRAM

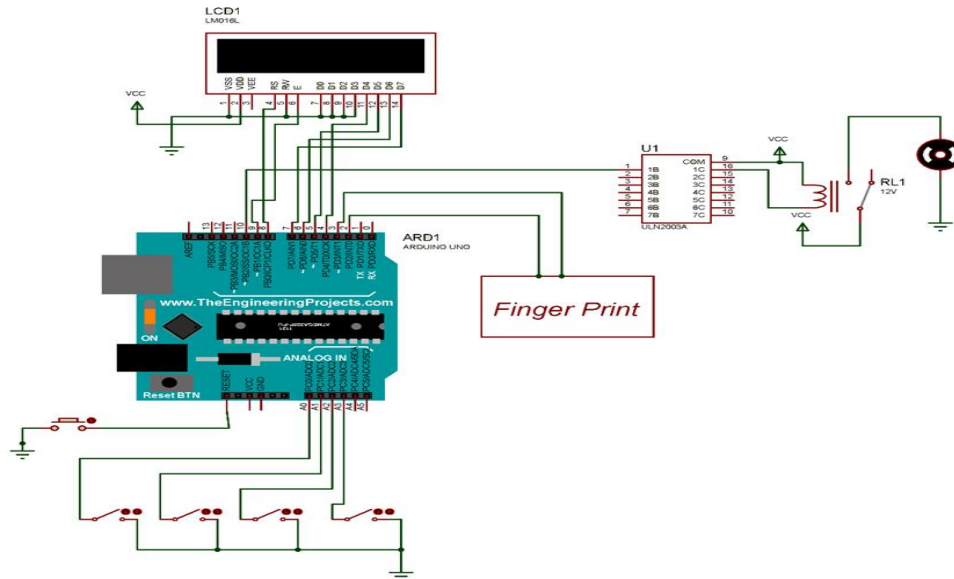


Fig.2. Circuit diagram of anti-theft vehicle security system

The Fingerprint Sensor Module collects imprints of the fingers or thumbs for use as a system input. Enroll/Back, Delete/OK, UP, and Down are the four push buttons we're using here. The enroll key is used to both register fresh finger imprints and return to the prior function. When a user wants to enroll a fresh finger, they must first press the enroll key, following which the LCD will ask for the ID or place where the fingerprint output should be kept. If the user does not choose to proceed at this time, he or she can return to the previous screen by pressing the enroll key again (this time the enroll key behaves as the Back key). The enroll key so conducts both the enrollment and the back operation. When a user enrolls a new finger, extra two keys, UP/MATCH and DOWN/MATCH, must be used to select the finger ID or location (which also has a double function) The user must now press the DEL/OK key to proceed with the provided ID or Location (this time this key functions like OK). The UP/DOWN keys can also be used to match fingerprints.

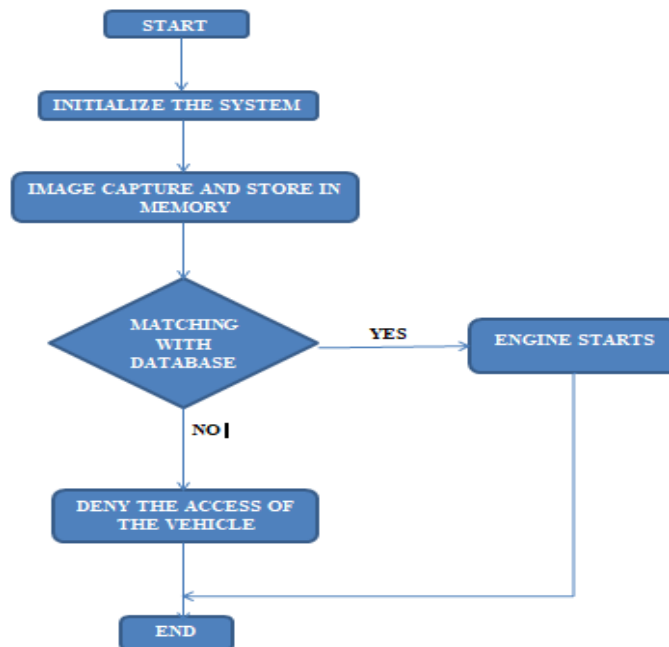


Fig.3. Flow Chart of Face Recognition

During the facial recognition process, the machine first takes the image and saves it in memory. It compares that image to the other photos in the database. The engine can start the car if the image matches the database. If it does not match, the user is denied the car.

IV. ALGORITHM

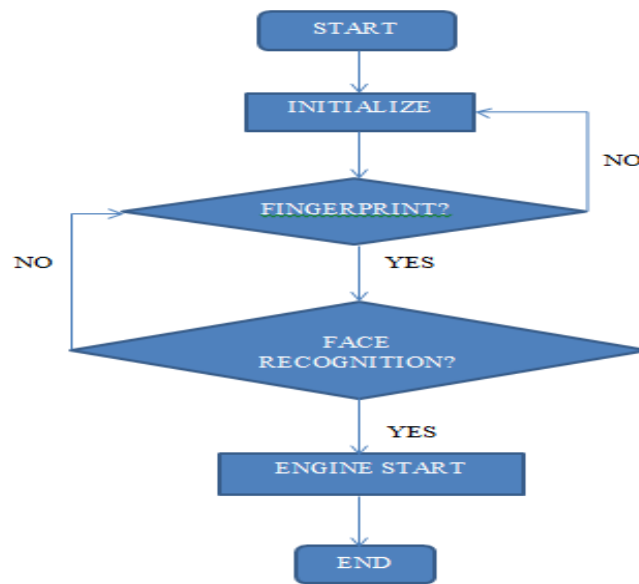


Fig.3. Flowchart of the Entire Vehicle Security System

After the fingerprint has been established, it must be verified. After the fingerprint is recognized, the door is unlocked. If the fingerprints aren't identical, the procedure starts over. It asks for your face to start the vehicle's engine when you unlock the door. When the captured face matches the data in the database, the vehicle's engine begins.

V. RESULT ANALYSIS

The output of this security system is the LCD and the engine, hence there is no graphical representation. Figure 4 shows the overview of the vehicle security system.

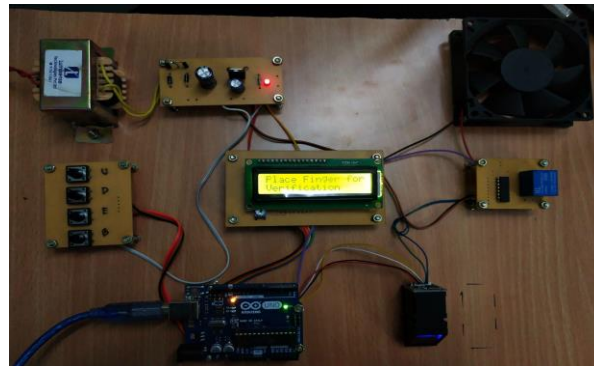


Fig.4 Overview of the system



Fig.4(a)



Fig.4(b)



Fig.4(c)

Figure 4(a) depicts the LCD at the beginning of the vehicle security process. A message appears in Fig.4(b) when the fingerprint is recognized. The display in Fig.4(c) is ready for facial recognition.

At first, the LCD panel displays "Place finger for verification." The notification "Found Match" shows if the fingerprints match; otherwise, the message "Not Found" appears, and the users are refused admission to the automobile. When the fingerprint is identified, the LCD panel displays "Waiting for facial recognition." The engine will start running if the face detected by the camera matches. The engine will not start if this is not done. The fingerprint must be matched once again to switch off the engine. As a consequence, this security system delivers a high level of protection to the system.

VI. CONCLUSION

Proper use becomes increasingly vital as technology progresses and becomes more incorporated into daily life. As the world evolves toward the usage of smart applications and more autonomous systems replace the current ones, the proposed method might provide image-based authentication. This device is the most dangerous to thieves since any effort to get unauthorized access to the vehicle's engine or ignition system results in the vehicle's engine and ignition system being deactivated. However, owing to several constraints, including cost, equipment availability, and interface complexity, establishing an anti-theft security system for vehicle protection that meets all of the necessary criteria is not feasible. All needed functionalities for creating the anti-theft security system could not be integrated due to these limits.

As a result, this anti-theft security system will necessitate some further work in the future: Using Voice Recognizing technology, the vehicle's door may be opened by the owner's voice. This device, which employs a very sensitive vibration technology, can also be used in accident avoidance systems. If an accident occurs, the location of the nearest hospitals and police station will be broadcast. By tracking the location of cars, this technology can assist improve traffic systems. As a result, this anti-theft security system will necessitate some further work in the future: Using Voice Recognizing technology, the vehicle's door may be opened by the owner's voice. This device, which employs a very sensitive vibration technology, can also be used in accident avoidance systems. If an accident occurs, the location of the nearest hospitals and police station will be broadcast. By tracking the location of cars, this technology can assist improve traffic systems.

REFERENCES

- [1]. Y. Faridah, W M Amir Asyraf W Abdul Rahman, "Car alarm detection device", Institute of Electrical and Electronics Engineers, 978-1-5090-1543-6/16/\$31.00 ©2016 IEEE.
- [2]. Abdellah El Mekki, Afaf Bouhoute, and Ismail Berrada, "Improving Driver Identification for the Next Generation of In-vehicle Software Systems", [IEEE Transactions on Vehicular Technology](#) (Volume: 68, Issue: 8, Aug. 2019).
- [3]. Mithileysh Sathiyarayanan, Santosh Mahendra and Rajesh Babu Vasu, "Smart Security System for Vehicles using Internet of Things (IoT)", Institute of Electrical and Electronics Engineers, 978-1-5386-5657-0@2018 IEEE.
- [4]. Chandra Shekar Ramaiah, Dr.S.Asif Hussain, S.Zahid Hussain, Yahya Al Balushi, "Smart Vehicle Security System For Defending Against Collaborative Attacks By Malware", Institute of Electrical and Electronics Engineers, 978-1-4673-9584-7©2016 IEEE.
- [5]. Chandra Shekar Ramaiah, Dr.S.Asif Hussain, S.Zahid Hussain, Yahya Al Balushi, "Design and Implementation of Microcontroller Based Anti-Theft Vehicle Security System using GPS, GSM and RFP", Institute of Electrical and Electronics Engineers, 978-1-5386-8279-7©2018 IEEE.
- [6]. A.Anusha, Syed Musthak Ahmed, "Vehicle Tracking and Monitoring System to Enhance the Safety and Security Driving using IOT", Institute of Electrical and Electronics Engineers, 978-1-5090-6266-9 © 2017 IEEE.
- [7]. Kingshuk Mukherjee, "Anti-Theft Vehicle Tracking and Immobilization System", Institute of Electrical and Electronics Engineers, 978-1-4799-5912 ©2014 IEEE.
- [8]. Chandra Shekar Ramaiah, Dr.S.Asif Hussain, S.Zahid Hussain, Yahya Al Balushi, "Smart Vehicle Security System For Defending Against Collaborative Attacks By Malware", Institute of Electrical and Electronics Engineers, 978-1-4673-9584-7©2016 IEEE.
- [9]. Fahim Faisal, Syed Akhter Hossain, "Smart Security System Using Face Recognition on Raspberry Pi", Institute of Electrical and Electronics Engineers, 978-1-7281-2741-5©2019 IEEE.
- [10]. Prabal Deep Das, Sharmila Sengupta, "Proposing the systems to provide protection of vehicles against theft and accident", IEEE International Conference On Recent Trends In Electronics Information Communication Technology, May 20-21, 2016, India.
- [11]. Amritha Nag, Nikhileendra J N, Mrutyunjay Kalmath, "IOT Based Door Access Control Using Face Recognition", Institute of Electrical and Electronics Engineers, 978-1-4799-5912-9 ©2014 IEEE.
- [12]. Prabal Deep Das, Sharmila Sengupta, "Proposing the systems to provide protection of vehicles against theft and accident", IEEE International Conference On Recent Trends In Electronics Information Communication Technology.
- [13]. Ajinkya Kawale, "Fingerprint-based locking system", International Journal of Scientific & Engineering Research, Volume 4, No 5, pp.899 -900, May-2013.
- [14]. Arpit Agrawal and Ashish Patidar, "Smart Authentication for Smart Phones", International Journal of Computer Science and Information Technologies, Vol. 5, No4, pp.4839-4843, 2014.

- [15]. Omidiora E. O. Fakolujo O. A. Arulogun O. T. and Aborisade D. O, "A Prototype of a Fingerprint Based Ignition Systems in Vehicles", European Journal of Scientific Research, Vol.62, No.2, pp. 164- 171,2011.
- [16]. Prashant Kumar R., Sagar V. C. Santosh S, SiddharthNambiar, "Two Wheeler Vehicle Security System", International Journal of Engineering Sciences & Emerging Technologies, Volume 6, No. 3, pp. 324-334,2013.
- [17]. Karthikeyan.A and Soundarya. J, "Fingerprint Based Ignition System", International Journal Of Computational Engineering Research, Vol. 2, Issue No.2, pp. 236-243. 2012.
- [18]. Benjamin Sliwa, Nico Piatkowski, and Christian Wietfeld, "The Channel as a Traffic Sensor: Vehicle Detection and Classification Based on Radio Fingerprinting", Ieee Internet Of Things Journal, VOL. 7, NO. 8, August 2020.
- [19]. Yijie Xun, Jiajia Liu, Nei Kato, Yongqiang Fang, and Yanning Zhang, "Automobile Driver Fingerprinting: A New Machine Learning-Based Authentication Scheme", IEEE Transactions On Industrial Informatics, VOL. 16, NO. 2, February 2020.
- [20]. Junaid Ahsenali Chaudhry, Kashif Saleem, Mamoun Alazab, Hafiz Maher Ali Zeeshan, Jalal Al-Muhtadi, and Joel J. P. C. Rodrigues, "Data Security Through Zero-Knowledge Proof and Statistical Fingerprinting in Vehicle-to-Healthcare Everything (V2HX) Communications", IEEE Transactions On Intelligent Transportation Systems, VOL. 22, NO. 6, JUNE 2021.