IJASEM

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

BIOMETRIC BASED AUTHENTICATION FOR VEHICLE IGNITION SYSTEM

1.M CHANDRA RAO,2. H. NIKHITHA,3. M. SANTHOSHI PRAVALIKA,4. M. RAJASRI,5. B. SUSHMA

ABSTRACT: Biometric authentication is an emerging technology that has found its application in various domains. One of the domains that have recently gained attention is vehicle ignition. This technology is used to prevent unauthorized access to the vehicle and ensure that only the authorized driver can start the vehicle. The biometric authentication system typically uses a combination of physiological and behavioral traits to identify the driver, such as facial recognition, fingerprint scanning, iris recognition, voice recognition, and gait analysis. This paper aims to provide an overview of the biometric authentication system for vehicle ignition, including the advantages, disadvantages, and challenges of implementing such a system. The paper also discusses the different biometric modalities that can be used for authentication, the algorithms used for recognition, and the security aspects of the system. The results show that biometric authentication for vehicle ignition has the potential to increase the security of the vehicle and prevent theft. However, there are still some technical and social challenges that need to be addressed before this technology can be widely adopted.

Keywords: Biometric authentication, Ignition, Fingerprint Scanning, Aurdino, Wifi Module.

INTRODUCTION

Biometric authentication for vehicle ignition is a security measure that uses a person's unique physical characteristics to verify their identity before allowing them to start a vehicle. This technology involves the use of sensors and software to analyse a person's biometric data, such as fingerprints, facial recognition, voice recognition, or iris recognition. Biometric authentication for vehicle ignition is becoming increasingly popular in modern vehicles as it provides a high level of security against theft and unauthorized use. By using biometric authentication, vehicle owners can ensure that only authorized drivers are able to start and operate their vehicles, preventing theft, and enhancing the safety and security of both the vehicle and its occupants. Biometric authentication is a technology that has become increasingly popular in recent years due to its accuracy and security in identifying individuals. Biometric authentication involves using unique physical characteristics, such as fingerprints, iris patterns, or facial features, to verify a person's identity. This technology has been widely used in many industries, including finance, healthcare, and security, and it is now being adopted in the automotive industry as well. In particular, biometric authentication is

1.ASSISTANT PROFESSOR,2,3,4&5 UG SCHOLAR
DEPARTMENT OF IOT, MALLA REDDY ENGINEERING COLLEGE FOR WOMEN, HYDERABAD

being used for vehicle ignition to enhance the security and convenience of the driving experience. With biometric authentication, drivers can unlock their car, start the engine, and drive without the need for traditional keys or key fobs. Instead, the car recognizes the driver's unique biometric information and grants access to the vehicle. Biometric authentication for vehicle ignition is designed to prevent car theft and improve overall security. It provides a level of protection that traditional key-based systems cannot offer, as biometric authentication requires the driver's unique physical characteristics to be present for access to be granted. This means that even if a thief gains access to the car, they will not be able to start the engine without the driver's biometric data. Furthermore, biometric authentication provides a more convenient way to access and start the car. Drivers no longer have to carry traditional keys or fobs, which can be lost or stolen. Instead, all they need is their biometric data, which is unique to them and cannot be replicated.

A. Objectives:

• The main objective of this project is to provide authentication access to start the vehicle by using authenticated driver's fingerprint.

• It helps the owner to identify the driver based on the Live Camera Feed.

• In addition to that with the help of GPS, one can easily find out the location of the vehicle in case of misuse or if the vehicle gets stolen

B. Applications:

• Automotive sectors.

• Industries, factories, and high security facilities.

• Corporate and small-scale sectors.

C. Advantages:

• Provides a high level of security compared to traditional methods.

• It eliminates the risk of stolen as the user's biometric data cannot be duplicated

or replicated. • Convenient and fast method of authentication.

• Used for driver identification and monitoring.

II. LITERATURE SURVEY There are various existing models that are being implemented individually. All these models are implemented as a single unit. The data collected from these models are being updated frequently in the database, which can be viewed by the owner. Hence this system provides more information about the driver. The history of the driver can be verified during the payment times. Also, the data security added in this project is more helpful to secure the system from the hacker using SHA-1 & SALT algorithm. The proposed system can be added with more features and can be used as an assist for the government transportation. [1] In this paper, a low cost and efficient embedded vehicular speed detecting system is presented. The work aimed at implementing the better results by comparing the existing methods such as FFT, DSP and LASAR based techniques. The output was more accurate with no other moving objects in the surrounding. In reality, the radar will not measure the actual velocity when the vehicle is not travelling [2] This paper gives review on vehicle speed detection technique using different approaches. Different approaches are edge extraction, object tracking, motion vector technique, absolute, centroid method and background image subtraction. The processing is done in MATLAB. By using any of these methods, traffic can be controlled, and vehicle speed detection will be maintained. [3] This work presents an integrated vehicle tracking framework using roadside lidar data. Vehicle clusters were detected from the raw point clouds using a three-step schema in the first instance. Afterward, a centroid-based tracking procedure was applied to identify clusters for each vehicle. [4] Estimating

and classifying vehicle speed are crucial problems in VDs used to gather traffic data in an ITS. However, as noted in Section I, per-vehicle speed estimation by side looking single-beam microwave detection is generally inaccurate or unsupported. In addition, collecting reliable length data from these detectors is impossible because of the noisy speed estimates provided by conventional data aggregation for single beam detectors. [5] Studied multiple technologies used for speed violation detection like Radar Based Technology, Laser Light System, Average speed computer System, Vision Based System etc. Each of them suffers from the problem like Less Accuracy, don't work in bad weather or light condition, High Cost, Limited Range, Line of sight, problem to Focus on a particular vehicle etc. So, we need a system that can be automatically operated with good accuracy, work even in bad weather and light condition and identify the vehicle uniquely with its type to calculate the average speed for different types of vehicles. [6] This work deals with the field of video surveillance systems. These systems can be used in many application areas: security of the premises, detection of accidents, fires, robotics, object recognition. The video is the media treated in such systems. Among the most important steps in video surveillance systems the motion detection. This step involves the detection of moving objects in video sequences captured by the surveillance camera. The motion detection stage is among the most studied problems in the field of video analysis where many research works focus on this problem.[7] Automobile Anti-theft System Based on GSM and GPS Module has the functions of remote monitoring; high sensitivity responding and observation location of automobile online. The system has good properties of security integrate with traditional warning system of automobile. The system can develop deeply and add other functions such as Internet of Things. The system can achieve networking

between two automobiles or among many automobiles because NRF24L01 module adopted. So other automobiles can receive the warning information if one automobile alarm. It is good to find the lost automobile. [8]

Arduino Board

The Arduino is a family of microcontroller boards to simplify electronic design, prototyping and experimenting for artists, hackers, hobbyists, but also many professionals. People use it as brains for their robots, to build new digital music instruments, or to build a system that lets your house plants tweet you when they're dry. Arduinos (we use the standard Arduino Uno) are built around an ATmega microcontroller — essentially a complete computer with CPU, RAM, Flash memory, and input/output pins, all on a single chip. Unlike, say, a Raspberry Pi, it's designed to attach all kinds of sensors, LEDs, small motors and speakers, servos, etc. directly to these pins, which can read in or output digital or analog voltages between 0 and 5 volts. The Arduino connects to your computer via USB, where you program it in a simple language (C/C++, similar to Java) from inside the free Arduino IDE by uploading your compiled code to the board. Once programmed, the Arduino can run with the USB link back to your computer, or stand-alone without it — no keyboard or screen needed, just power

Fingerprint Module
Description

KY-M6 Fingerprint module adopts optic fingerprint sensor, which consists of high-performance DSP and Flash.

KY-M6 Fingerprint Sensor Module is able to conduct fingerprint image processing, template generation, template matching, fingerprint searching, template storage, etc. Compared with similar products from other suppliers, KY-M6 proudly boasts of following features:

1. Proprietary Intellectual Property

Optic fingerprint enrollment device, KY-M6 hardware as well as fingerprint algorithm are all developed by KeyPower Security.

2. Wide Application Range of Fingerprints with Different Quality

Self-adaptive parameter adjustment mechanism is used in the course of fingerprint enrollment. This ensures good image quality for even dry or wet fingers, thus it has wider application range.

3. Immense Improved Algorithm

KY-M6 Fingerprint algorithm is specially written according to optic imaging theory. The algorithm is good for low-quality fingers due to its excellent correction and tolerance features.

4. Flexible Application

User can easily set KY-M6 Module to different working modes depending on complexity of application systems. User can conduct secondary development with high efficiency and reliability.

5. Easy to Use and Expand

It is not necessary for user to have professional knowledge in the field of fingerprint verification. User can develop powerful fingerprint verification application systems with the command set provided by KY-M6.

6. Low Power Consumption

Sleep/awake control interface makes KY-M6 suitable for occasions that require low power consumption.

7. Different Security Levels

User can set different security level according to different application environment.

8. Application

KY-M6 can be used on all fingerprint verification systems, such as Safety cabinet, door lock, Complicated door-guard system, Fingerprint IC card Identification Terminal, Fingerprint identification and verification system associated with PC.

CONCLUSION In conclusion, biometric authentication for vehicle ignition is a promising technology that offers several benefits. It can significantly enhance the security of the vehicle, prevent unauthorized access and theft, and improve the user experience by eliminating the need for physical keys or passwords. Biometric authentication systems are becoming increasingly sophisticated and reliable, with many options available, including fingerprint, facial recognition, and voice recognition. However, it is important to note that biometric authentication for vehicle ignition is not without its limitations and challenges. The technology can be expensive to implement and may require significant changes to the vehicle's design and infrastructure. There are also concerns about the accuracy and reliability of biometric authentication systems, particularly in adverse weather conditions or when users are wearing

masks or other facial coverings. Despite these challenges, biometric authentication for vehicle ignition is a promising technology that has the potential to revolutionize the way we interact with our vehicles. As the technology continues to evolve and improve, we can expect to see more widespread adoption in the automotive industry in the coming years.

FUTURE WORK

• Integration with multiple biometric modalities: Currently, most biometric authentication systems for vehicle ignition rely on a single modality, such as fingerprint or facial recognition. However, integrating multiple modalities, such as fingerprint and iris recognition, can improve the accuracy and security of the system.

• Robustness to environmental conditions: Biometric authentication systems can be affected by various environmental conditions, such as changes in lighting or temperature. Future work could focus on developing systems that are robust to these conditions, ensuring that they work reliably in all circumstances.

• Privacy and data security: Biometric data is highly sensitive, and ensuring its privacy and security is crucial. Future work could focus on developing secure storage and transmission methods for biometric data, as well as developing protocols for ensuring that the data is only used for the intended purpose.

• User experience and acceptance: Biometric authentication systems can be inconvenient or uncomfortable for users, which can lead to resistance or non-adoption. Future work could focus on improving the user experience and making the systems more user-friendly and accessible.

• Interoperability: Biometric authentication systems for vehicle ignition could benefit from interoperability with other systems, such as those used for access control or payment systems. Future work could focus on developing standards and protocols that enable interoperability between different biometric authentication systems.

REFERENCES

[1] "Authenticated Access Control for Vehicle Ignition System by Drivers License and Fingerprint Technology."Arwa M. Ali ,Dr. Heisum M. Awad ,Ibrahim K. Abdalgader, (2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)).

[2] "FaceIgnition: An automatic anti-theft and key less solution for vehicles" , Tushar Dang, Vanshita gupta, Diljot singh Wadia., (2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), March 17– 18, 2021, Amity University Dubai)

[3] "IoT based Smart Vehicle Ignition and Monitoring System ", Dr. Fathima Jabeen, Sudhir Rao Rupanagudi, Varsha G Bhat.

[4] " Driver Authentication for Smart Car Using Wireless Sensing", Xuejun Tan, Bir Bhanu, Yingqiang Lin.

[5] "Implementation of Vehicle Security System using GPS,GSM and Biometric ", Mridhula Ramesh, Akruthi S, Nandhini K, Meena S, Joseph Gladwin S, and Rajavel R.

[6] "Study on Biometric Authentication Systems, Challenges and Future Trends: A Review", Krishna Dharavath, F. A. Talukdar, R. H. Laskar

[7] "Selecting a Reference High Resolution for Fingerprint Recognition Using Minutiae and Pores" , David Zhang, E, Feng Liu, Qijun Zhao,Guangming Lu,and Nan Luo .

[8] Hu Jian-ming, Li Jie,Li Guang-hui Tianjin University of Technology and Education Tianjin, China, "Automobile Anti-theft System Based on GSM and GPS Module" , 2012 Fifth International Conference on Intelligent Networks and Intelligent Systems.