International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Face Recognition System Based Car Security System

Tipparti Anil Kumar[1], Y Prithvi Murthy [2], Ch Yashwanth Goud [3], N Harsha Vardhan[4]

[1,2,3,4]Department of Electronics and Communication Engineering, CMR Institute of Technology, Hyderabad, Telangana, India, 501401

ABSTRACT:
Modern car security systems have been developed as a result of the growing demand in the automotive sector for increased convenience and security. In order to provide safe access management and authentication for cars, this paper suggests a face recognition system-based auto security system that makes use of facial recognition techniques. When a match is detected, the system uses computer vision algorithms to identify and detect the faces of approved drivers, enabling the car to be unlocked and started without any issues. In order to convert near infrared face images into their corresponding visible images, we develop a nir-vis image translation model. Using two distinct nir databases of face images, the pre-trained face embedding model is applied to present the evaluation performances. The proposed system offers improved security by eliminating the need for traditional key-based systems and providing a robust biometric-based authentication mechanism. Anti-spoofing procedures are also integrated to guarantee the system's dependability and defense against fraudulent attempts. One of the disadvantages of the current systems is that not everyone finds it comfortable to have to memorize their password for certain systems. An RFID card is another device that has been developed to verify the identification of the user. Hackers have the ability to modify RFID data and substitute it with their own. Certain systems utilize fingerprints to verify an individual's identity. The primary reasons for the low adoption of biometric fingerprint locks are their expensive cost and the potential for falsified or damaged fingerprints. Certain systems identify an obstruction ahead of the car, sound an alert, tell the driver to pull over, but do nothing to actually avoid the obstruction. Through tests and assessments, the usefulness and practicability of the suggested system are shown, highlighting its potential as a workable option for safe and practical access management in automotive settings

Keyword: Face recognition, Auto security system, NIR-VIS image translation, Biometric authentication, Anti-spoofing procedures, Automotive access management

INTRODUCTION:

Artificial intelligence has been evolving quickly in the last few years. These days, it's evident that self-driving cars and self-serve supermarkets have been developed. Computer vision and artificial intelligence are closely related fields. Humans use their vision to adapt to and comprehend the settings they are in, whereas computer vision attempts to replicate human vision by using electronics to detect and interpret

images. Not only does computer vision function as an eye, but it also has to respond. It must be endowed with the capacity to recognize, detect, and interpret pictures in a manner similar to that of human vision.

Fig. 1 Vehicle Thefts in Various cities of India in 2020

Theft, duplication, and unauthorized access are growing threats to conventional key-based or card-based security systems. Innovative and reliable access control solutions that provide increased security and guarantee car owners' convenience are required to solve these concerns. The existing car security systems predominantly rely on traditional methods such as physical keys, key fobs, or RFID cards for access control which can be problematic at times.

A viable option for safe access control and authentication is face recognition technology. face recognition systems are able to recognize people precisely by using computer vision algorithms and deep learning techniques to analyze each person's distinctive face traits. Because face recognition is based on human face feature information and is capable of operating in a variety of environments, it is regarded as a good biometric approach for car security and alarm systems . As a result, the majority of face recognition algorithms were created with a higher rate of discrimination in mind.

People can be recognized without their knowledge thanks to the more user-friendly face recognition system.

The following are some benefits of the face recognition technique for car security:

- From the moment one sits down, it is efficient, comfortable, and senses.
- It is inexpensive and can be used in addition to the current techniques.
- Minimal user interaction is needed to access this security measure.
- Does not require the user to be active

The goal of a car security system is to deter vehicle theft and guarantee vehicle safety by preventing potential theft routes. Using a face recognition system to confirm that a user is an authorized user with access to the ignition system is one way to ensure driving authenticity.

LITERATURE REVIEW:

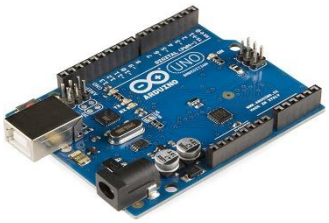
There have been valued assets and prized belongings since the invention of the vehicle. Cars became less of a luxury and more commonplace, which made people leave them unattended and open to theft. Consequently, the requirement to make them secure and impenetrable grew. The earliest automobile antitheft device is said to have been a detachable steering wheel, created by Leach Automobile in 1900. To discourage thieves, the driver was supposed to take off the steering wheel after driving and take it with

them. 1914 saw the introduction of power locks on high-end Scripps-Booth vehicles. Ford originally implemented keyless entry on a few models in 1980. The driver would need to enter a 5-digit code on a keypad above the driver's side door in order to unlock the vehicle. In 1984, Nissan would launch a comparable system.

BLOCK DIAGRAM:

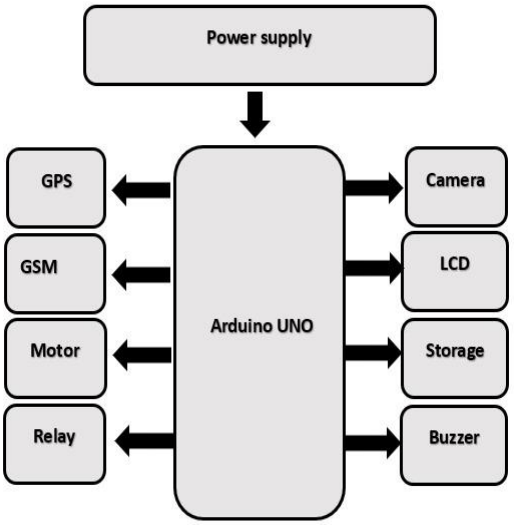
The main components of the block diagram are

- **ARDUINO**



The Arduino is a family of microcontroller boards to simplify electronic design, prototyping and experimenting for artists, hackers, hobbyists, but also many professionals.

- **POWER SUPPLY**



We require a power supply to provide power to the components i.e., a reliable power source to ensure continuity in system.

- **GSM**

Global System for Mobile communication is a cellular network used by mobile phones. It uses GSM SIM 900 to alert the authority of mal-activities or unrecognized individual

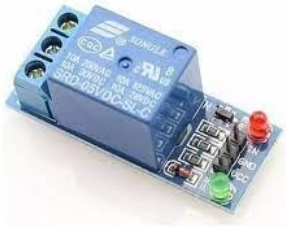
- **MOTOR**

A dc motor converts electrical energy to mechanical energy, conductors. The input of a DC motor is current/voltage and its output istorque(speed)

- **LCD**

A liquid crystal display (LCD) is a thin, flat display device made up of any number of color or monochrome pixels arrayed in front of a light source or reflector

- **Arduino Relay Module**



Hobbyists often use a relay module with Arduino in their projects. An Arduino is a microcontroller board that is widely popular in DIY electronics projects. The relay module, when paired with an Arduino, can control various appliances and devices.

- **Esp32 wroom 32**

ESP32-WROOM-32 is a powerful, generic Wi-Fi+BT+BLE MCU module that targets a wide variety of applications, ranging from low-power sensor networks to the most demanding tasks, such as voice encoding, music streaming and MP3 decoding

METHODOLOGY:

This project suggests a sophisticated facial recognition authentication mechanism. Robust and effective apps utilize a real-time verification system. A sophisticated algorithm is used for authentication in face detection and recognition systems. The image of the occupant of the vehicle, positioned correctly in front of the driver's seat, is captured by the camera. After obtaining the person's photograph, the algorithm attempts to identify the face.It gathers a diverse dataset of facial images for training the recognition model. Includes various lighting conditions, angles, and facial expressions. The normalize and resize images to ensure consistency for betterment Apply face detection to locate and extract faces from images. Implement liveness detection mechanisms to differentiate between live faces and still images, preventing spoofing attacks.Techniques may include analyzing facial movements, checking for blinking, or employing 3D face reconstruction. Develop an intuitive and user-friendly interface for system configuration and monitoring, providing feedback to users during the recognition process. Implementing a secure and efficient database results in storing facial templates of authorized users in any amount of number Regularly updating the database allows us to include new users or remove revoked access. Implementation of a backup mechanism, alternative methods like lock so that there occurs no problems or delay in case of face recognition failure. Provide detailed documentation for system setup, maintenance, and troubleshooting. Provide detailed documentation for system setup, maintenance .Remember to tailor these processes to the specific needs and limits of the car security system you're creating.. Implement liveness detection mechanisms to differentiate between live faces and still images, preventing spoofing attacks. Techniques may include analyzing facial movements, checking for blinking, or employing 3D face reconstruction.

CONCLUSION:

To sum up, the auto security system that utilizes facial recognition technology presents a viable way to improve vehicle security and access management. The suggested solution overcomes the shortcomings of conventional vehicle security systems and offers a number of advantages by utilizing cutting-edge facial recognition algorithms and computer vision techniques. Since facial recognition is used for authentication rather than physical keys or cards, the system removes the weaknesses related to key duplication and theft. In addition to improving the vehicle's overall security, this greatly lowers the possibility of unwanted entry. Furthermore, the incorporation of anti-spoofing methods guarantees the system's resilience against fraudulent endeavors, including manipulating the face recognition algorithm with photos or masks. The system's security is further enhanced by the use of liveness detection and powerful facial feature analysis, which enable precise differentiation between real people and attempted spoofing. The system's real-time performance makes access management quick and easy, giving users a responsive and effective experience. After a successful face recognition identification, the driver can start the engine, unlock the doors, and deactivate the immobilizer thanks to the interaction with the current car systems, which facilitates seamless coordination and operation. The suggested system prioritizes data privacy and protection, guaranteeing safe storage and encryption of biometric data. By adhering to privacy laws and putting strong data protection measures in place, the system fosters user confidence in the management of personal data. All things considered, the facial recognition system-based auto security system provides a dependable, practical, and cutting edge technology solution for vehicle access management. It makes automobiles more secure, lowers the possibility of unwanted access, and makes vehicle owners' lives easier. The system's accuracy can be improved, its capacity to handle different environmental circumstances may be increased, and rigorous testing and validation in real-world settings can be the main

goals of future research and development. The facial recognition system-based vehicle security system may develop further and help progress automotive security technology by tackling these issues.

ACKNOLEDGMENT:

For their period of inspiration, we are very grateful to Dr. M. Janga Reddy, Director, Dr. B. Satyanarayana, Principal, and Dr. K. Niranjan, Head of Department of Electronics and Communication Engineering, CMR Institute of Technology, Hyderabad**.**

We are grateful to Dr. T. Anil Kumar, Professor of ECE Dept at CMR Institute of Technology in Hyderabad, for his consistent guidance, encouragement, and moral support during the project.

REFERENCES:

1. E. Learned-Miller, G. B. Huang, A. RoyChowdhury, H. Li, and G. Hua, "Labeled faces in the wild: A survey," in Advances in face detection and facial image analysis. Springer, 2016, pp. 189–248.
2. S. Marcel, M. Nixon, and S. Li, "Handbook of biometric antispoofing-trusted biometrics under spoofing attacks," Advances in Computer Vision and Pattern Recognition. Springer, 2014.
3. "Information technology Biometric presentation attack detection Part 1: Framework." International Organization for Standardization, Standard, Jan. 2016.
4. A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: a public database and a baseline," in Biometrics (IJCB), 2011 international joint conference on. IEEE, 2011, pp. 1–7.
5. Rattani, A., & Sridhar, V. (2014). Vision-based driver drowsiness detection system for intelligent vehicles: A review. IEEE Transactions on Intelligent Transportation Systems, 15(2), 760-776.
6. Vapnik, V. (1995). The nature of statistical learning theory. Springer Science & Business Media.
7. Ojala, T., Pietikäinen, M., & Harwood, D. (1996). A comparative study of texture measures with classification based on featured distributions. Pattern Recognition, 29(1), 51-59.
8. Han, J., Shao, L., Xu, D., & Shotton, J. (2015). Enhanced computer vision with Microsoft Kinect sensor: A review. IEEE Transactions on Cybernetics, 45(10), 2013-2025.
9. Li, S. Z., & Jain, A. K. (2011). Handbook of face recognition. Springer Science & Business Media. Huang, D.,
10. Wang, Y., Wang, L., & Tan, T. (2011). A face recognition algorithm based on multiple facial features fusion. Pattern Recognition, 44(11), 2637-2645.
11. Zhang, Z., He, R., & Tan, T. (2016). A practical anti-spoofing method for face recognition with liveness detection. In European Conference on Computer Vision (pp. 238-253).
12. Springer. Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4-20
13. I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in Proceedings of the 11th International Conference of the Biometrics Special Interest Group, no. EPFL-CONF-192369, 2012.
14. Z. Boulkenafet, J. Komulainen, and A. Hadid, "Face antispoofing based on color texture analysis," in Image Processing (ICIP), 2015 IEEE International Conference on. IEEE, 2015, pp. 2636–2640.
15. R. Ramachandra and C. Busch, "Presentation attack detection methods for face recognition systems: a comprehensive survey," ACM Computing Surveys (CSUR), vol. 50, no. 1, p. 8, 2017.