Face Recognition Based Anti-Theft Car System Using Arduino Uno

Prof. Madhusudan Singh
Dept. of Electrical Engineering
Delhi Technological University
Delhi, India

Prof. Anil Singh Parihar
Dept. of Computer Science and Engineering
Delhi Technological University
Delhi, India

Utsav Agarwal
Dept. of Electrical Engineering
Delhi Technological University
Delhi, India

Tanishq Harit
Dept. of Electrical Engineering
Delhi Technological University
Delhi, India

Utkarsh Singh
Dept. of Electrical Engineering
Delhi Technological University
Delhi, India
utkarshsingh_

***Abstract*—This paper presents an Arduino Uno based Face Recognition Car Security and Safety System aimed at enhancing vehicle security through bio metric authentication. The system utilizes Python programming language along with various modules including face recognition, cv2, numpy, smtblib, and serial for software implementation. The Face recognition algorithm is employed for facial recognition, ensuring accurate and reliable identification of individuals attempting to access the vehicle, granting entry only to authorized users. Once inside the vehicle, a secondary facial recognition system ensures that only authorized individuals can start the car's engine. In the event of unauthorized access attempts, the engine remains immobilized, and an alert notification is promptly sent to the owner's phone via email. Additionally, the paper details the hardware prototype consisting of components such as the L298N motor driver, Arduino UNO board, batteries, and DC motors. Integration of hardware and software components demonstrates the practical implementation of the system, showcasing its effectiveness in real-world scenarios. The Arduino UNO Based Face Recognition Car Security and Safety System offers a comprehensive solution to mitigate unauthorized access to vehicles, ensuring the safety and security of both the vehicle and its occupants.**

***Index Terms*—Face Recognition, Arduino Uno, OpenCV, Python, DC Motors**

I. Introduction

In recent years, the security of vehicles has emerged as a critical concern, prompting a quest for innovative solutions to thwart unauthorized access and enhance safety measures. In this context, we introduce a novel Face Recognition System designed to bolster automotive security through bio metric authentication. Distinguished from conventional approaches, our system embodies several unique characteristics. Firstly, it offers a low-cost solution by leveraging affordable hardware components and open-source software, making advanced security measures accessible to various small-scale applications. Moreover, our system exhibits exceptional adaptability, empowered by customised software modules capable of recognizing diverse facial profiles and executing tailored responses for authorized users. This flexibility ensures its efficacy in addressing the dynamic security needs of different environments. Despite its robust capabilities, our system maintains a compact footprint, facilitating deployment in space-constrained environments without compromising performance. Its small form factor enhances compatibility with existing security infrastructure, enabling seamless integration into automotive environments. Embracing the principles of open-source development, our system harnesses widely adopted tools such as OpenCV and Python, fostering accessibility, transparency, and community collaboration. This ethos not only promotes continual improvement but also cultivates a vibrant ecosystem of developers contributing to its refinement. In this paper, we present a comprehensive exploration of our Face Recognition System, elucidating its architectural design, implementation methodology, and performance evaluation. Through empirical validation and comparative analysis, we showcase the efficacy and versatility of our system in addressing the security challenges prevalent in contemporary automotive environments.

II. Literature Review

In the paper "Face Recognition by using Support Vector Machines" authored by Guodong Guo [1], the author emphasizes the importance of a face recognition system's ability to adapt to various changes in face images. These changes can stem from differences in illustration style and viewing direction, posing a challenge to accurate recognition. Two key issues are identified: firstly, determining which features to utilize in representing a face image, considering variations in view, illumination, and facial expressions. Secondly, establishing an effective classification method for new face images based on the selected representation.

In Timo Ahonen's paper titled "Face Description with Local Binary Patterns - Application to Face Recognition" [2], the author explores the utilization of local binary patterns for face image representation, focusing on texture features and

addressing challenges such as face misalignment. However, the algorithms employed in this approach are noted to be less efficient.

In the publication ”Face Recognition System for Accessing Automobile using GSM and Embedded Technology” [3] by K. K. Dube, the security system’s primary goal is to deter vehicle theft and ensure car safety by thwarting potential theft methods. Driver authentication is accomplished through a facial recognition system, which verifies the user’s identity as an authorized individual permitted access to the system. Upon detecting a person within the parked vehicle, the system captures an image using the onboard camera and compares the recognized face with authorized user images stored in the database.

In the paper titled ”Vehicle Security Systems using Face Recognition based on Internet of Things” [4] by Mohammed Kayed and Ahmed A. Elngar, a system named VSS-IoT (Vehicle Security System using IoT) is proposed. The authors employed a hybrid mechanism combining Haar cascade and PCA algorithms for face recognition and detection. As outlined in the paper, their system integrates embedded devices, IOT technologies, and biometric techniques. Additionally, the authors describe the system as straightforward.

III. Methodology

The system captures live video from the webcam and loads sample images of authorized individuals. It then encodes the faces in the sample images for comparison with detected faces in the live video stream. Detected faces are compared with the known face encodings to determine if they match any authorized individuals. If a match is found, the individual’s name is displayed. If no match is found, an alert email is sent and printed in the console. Additionally, the system sends signals to an Arduino board to control security mechanisms such as engine activation or immobilization.

The code continuously loops to capture video frames, detect faces, perform recognition, and take appropriate actions based on the recognition results. Pressing ’q’ on the keyboard terminates the program. This methodology ensures vehicle security by actively monitoring and identifying individuals attempting to access the vehicle, thereby preventing unauthorized entry or theft.

A. Software Libraries Used

- Open cv: Open cv is an open source library and is usually used for image processing.
- Face Recognition: Recognize and manipulate faces from Python or from the command line, built using dlib’s state-of-the-art face recognition.
- SMTP lib: It is used for sending emails via the Simple Mail Transfer Protocol.
- Serial: The serial library in Python facilitates serial communication between the computer and external devices.
- NumPy: NumPy is a Python library for numerical computations, particularly optimized for array operations and mathematical functions.

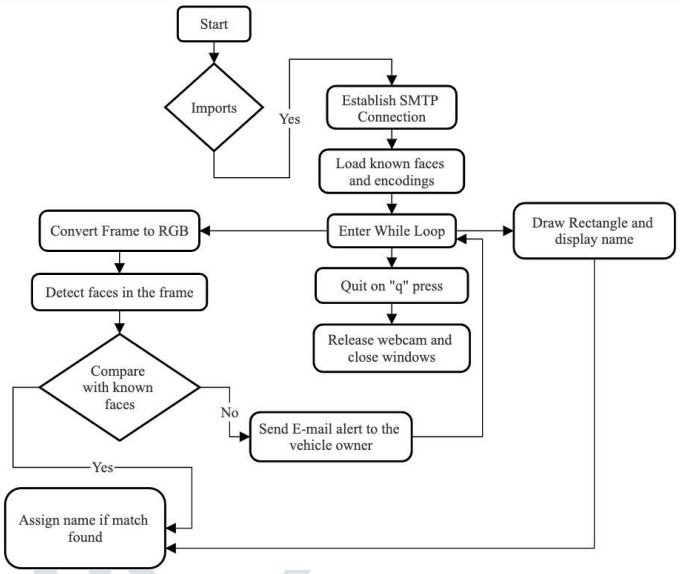


Fig. 1: Methodology Flowchart

B. Hardware Components

- Arduino Uno Micro-controller Board :
  The Arduino Uno micro-controller board serves as the brain of the security system, orchestrating the interaction between various hardware components such as the L298N motor driver, batteries, and DC motors.. Its significance lies in its ability to process data, execute commands, and control peripheral devices with remarkable precision. Equipped with an ATmega328P micro-controller, the Arduino Uno offers an extensive array of digital and analog pins, allowing seamless interfacing with sensors, actuators, and other electronic modules.
  Programming the Arduino Uno involves writing code in C/C++, facilitated by the user-friendly Arduino Integrated Development Environment (IDE). This programming environment simplifies the development process, enabling even novice programmers to create complex algorithms for tasks such as facial recognition, image processing, and motor control.

Fig. 2: Arduino Uno Micro-Controller Board

- L298N Motor Driver :
  The L298N motor driver is a crucial component responsible for controlling the DC motors integrated into the security system. Its primary function is to provide bidirectional control of two motors simultaneously, enabling precise manipulation of speed and direction. The motor driver operates on the principle of an H-bridge configuration, allowing it to reverse the polarity of the motor terminals to change direction.
  Interfacing the L298N motor driver with the Arduino Uno involves connecting control pins from the microcontroller to specific input pins on the motor driver. Through these connections, the Arduino Uno sends PWM (Pulse Width Modulation) signals to regulate motor speed and digital signals to control motor direction. Additionally, the L298N motor driver incorporates current sensing and protection mechanisms to prevent overheating and damage to the motors.

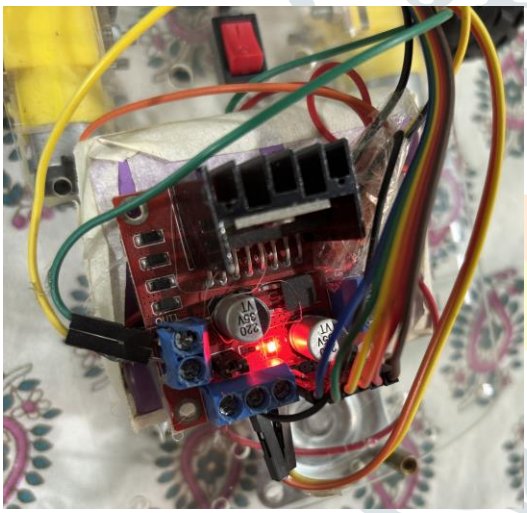


Fig. 3: L298N Motor Driver

- DC Motors :
  DC motors are the mechanical workhorses of the security system, responsible for actuating various components such as, engine ignition mechanisms and other movable parts. These motors are chosen for their simplicity, reliability, and ease of control. Brushed DC motors, in particular, are commonly employed due to their straightforward operation and cost-effectiveness.
  The selection of DC motors is based on several factors, including torque requirements, speed characteristics, power consumption, and physical size constraints. Depending on the specific application within the security system, different types and sizes of DC motors may be employed to ensure optimal performance and efficiency.

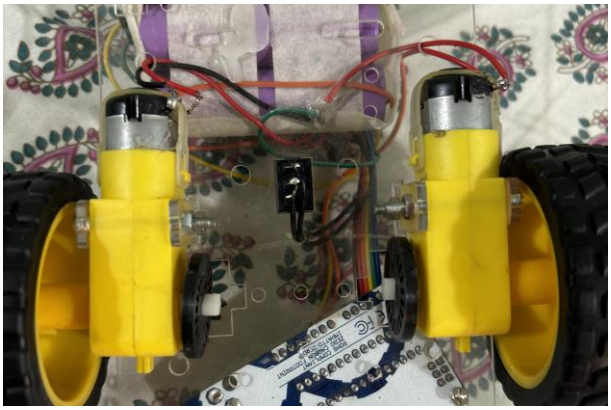
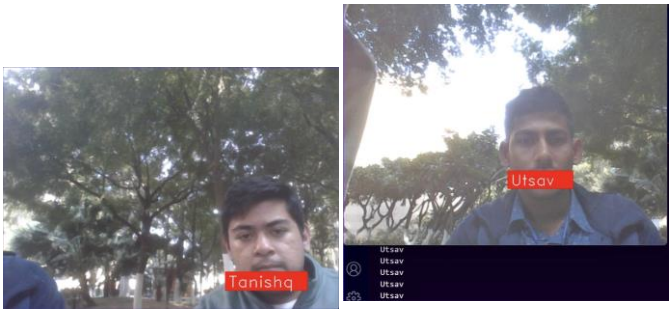


Fig. 4: DC Motors for Motoring

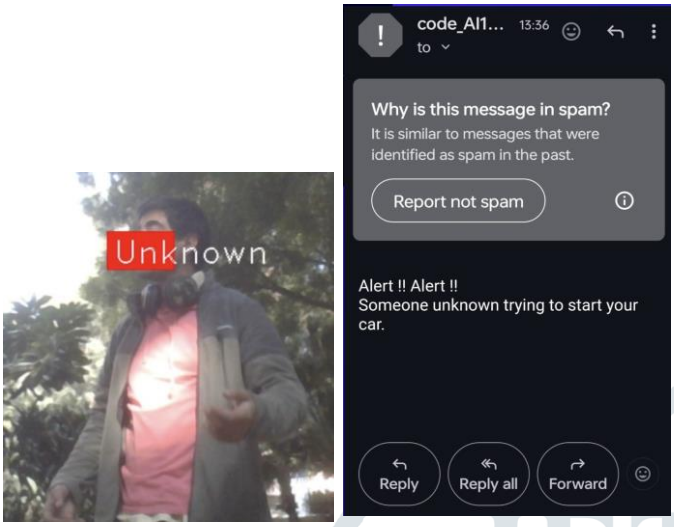
- Integration and Practical Application :
  The integration of hardware components involves establishing seamless communication between the Arduino Uno, the L298N motor driver, and the DC motors. This process begins with the physical connection of wires and cables, ensuring proper alignment of pins and terminals to facilitate data exchange and power transmission.
  Once the hardware components are interconnected, software protocols are implemented to enable coordinated operation and control. For instance, the Arduino Uno executes code to capture images from a webcam, analyze facial features using a predefined algorithm, and send commands to the L298N motor driver based on the recognition results.
  Testing and validation procedures are conducted to assess the functionality, reliability, and performance of the integrated system. This includes conducting stress tests, evaluating response times, and verifying the accuracy of bio-metric authentication. Any issues or discrepancies encountered during testing are meticulously addressed through iterative refinement and troubleshooting.

IV. Software Results



(a) Tanishq (b) Utsav

Fig. 5: Known Faces



(a) Unknown Person Detected (b) Alert Mail Sent to Owner

Fig. 6: Unknown Face

V. Unique Selling Points

1. Low-Cost Solution: Our system is built using low-cost hardware components and open-source software, which makes it an affordable solution for small-scale applications. This is in contrast to many commercial face recognition systems that can be quite expensive.

2. Flexibility: Our system is highly customizing and can be easily adapted to suit different applications. For example, we can modify the software to recognize different types of faces or to trigger different outputs when an authorized user is detected.

3. Integration with ARDUINO UNO: Our system is built on the ARDUINO UNO platform, which is a popular choice for hobbyists and DIY enthusiasts. By using an ARDUINO UNO board, we can easily add other sensors or actuators to our system, such as a temperature sensor or a buzzer.

4. Compact Size: Our system can be built in a small form factor, making it suitable for applications where space is limited. For example, we can integrate our system with a small lock or a security camera.

5. Open-Source Software: Our system uses open-source software such as OpenCV and Python, which allows other developers to modify and improve the software. This can help to foster a community of developers who can contribute to the project and make it better over time.

VI. Conclusion

In conclusion, our research project aimed to bolster vehicle security with a machine learning-based system. By harnessing face recognition technology, our goal was to enhance automobile security and minimize theft risks. Our system functioned by capturing images of individuals attempting to access the car, permitting entry solely to authorized users. We employed an advanced face recognition method utilizing libraries like OpenCV, NumPy, Serial, and SMTP, with the core face recognition library leveraging dlib's cutting-edge technology. This library boasts an impressive accuracy of 99.38 percent on the Labeled Faces in the Wild benchmark, ensuring dependable identification of authorized users. Additionally, we demonstrated the effectiveness of our system through a hardware prototype, incorporating components such as Arduino Uno and L298N motor driver. This exhibition underscored the practical implementation and real-world applicability of our security solution, offering a seamless and user-friendly approach to vehicle access and security. Furthermore, we integrated face recognition to start the car's motor, further enhancing overall security and user experience. The integration of a hardware prototype further reinforced the viability and strength of our approach, highlighting its potential for practical deployment in real-world scenarios.

References

[1] Guodong Guo, Stan Z Li, and Kapluk Chan "Face recognition by support vector machines" (2000). IEEE Conference Publication — IEEE Xplore. https://ieeexplore.ieee.org/document/840634 - School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore

[2] Ahonen, T., Hadid, A., Pietika¨inen, M. (2004). "Face Recognition with Local Binary Patterns". In Lecture notes in computer science (pp. 469–481). https://doi.org/10.1007/978-3-540-24670-1-36 - Machine Vision Group, Infotech OuluPO Box 4500, FIN-90014 University of Oulu, Finland

[3] IRJET- Face Recognition based Anti -Theft System using Raspberry Pi. Issuu. https://issuu.com/irjet/docs/irjet-v8i1249/1. Published February 10, 2021.

[4] Elngar AA, Kayed M. Vehicle Security Systems using Face Recognition based on Internet of Things. https://www.semanticscholar.org/paper/Vehicle-Security-Systems-using-Face-Recognition-on-Elngar-Kayed/6decdaa4362cd381f7f7748f0999a19e331a00e8citing-papers. Published 2020.

[5] Penki, R., Somasekhar, D., Thota, J. K. (2024). "ADVANCED VEHICLE SECURITY SYSTEM USING BIOMETRIC VISUALS" - Department of Electronics and Communication Engineering, Chaitanya College of Engineering, JNTU-GV University, Vishakhapatnam, India