Grenze International Journal of Engineering and Technology, January Issue

Smart Vehicle Starter System using Face Recognition and Raspberry Pi Pico W

Ch. Kranthi Rekha[1], Mohammad Afrin[2], Karra Meenakshi[3] and Malga Anand[4]
[1]Assistant Professor, Department of Electronics and Communication Engineering, Vignana Bharathi Institute of Technology, Hyderabad, India
Email: kchennaboina20@gmail.com
[2-4]Students, Department of Electronics and Communication Engineering, Vignana Bharathi Institute of Technology, Hyderabad, India
Email: afrinmohammad317@gmail.com, karrameenakshi212@gmail.com, anandmalga@gmail.com

***Abstract*— Face detection technology is used in an Internet of things-based vehicle starter system. The requirement for facial recognition to start the engine improves vehicle security. A camera the driver's face is captured by the module and sent for validation. When detection and matching are successful, the Raspberry Pi Pico W receives an instruction from the system that turns on the relay module to start the car's engine. By preventing unwanted access, the system offers a safe and practical way to start cars. It can identify several authorized users and be tailored to meet the needs of a particular vehicle. the study shows how the Internet of Things may improve car security and build smarter, safer automobiles.**

***Index Terms*— Real VNC viewer, face detection, facial recognition, and vehicle security.**

I. Introduction

The integration of IoT and AI has transformed vehicle security. Traditional ignition systems are vulnerable to theft. A face-detection-based vehicle starter system addresses these challenges. It uses a Pico Zero W microcontroller and relay. This smart system leverages facial recognition technology. A camera captures and analyzes facial features. Only pre- registered individuals can start the vehicle. The Pico Zero W manages data and controls the relay.

It's a compact and Wi- Fi-enabled microcontroller. The system is efficient and reliable. The relay module activates the vehicle's starter motor. The Pico Zero W allows for remote monitoring and cloud data storage. The system is highly scalable and adaptable. It's a cost-effective IoT setup for vehicle security. Biometric authentication enhances security. The system reflects a shift towards smarter vehicles. Real-time data and intelligent control drive this shift. The system can be customized for specific vehicles. It recognizes multiple authorized users.

It's suitable for cars, trucks, and motor cycles. The system provides an additional layer of security. It can be integrated with existing security systems. IoT enhances vehicle security and convenience. The project demonstrates IoT's potential in vehicle security. It's a step towards smarter and more secure vehicles. Facial recognition secures vehicle ignition. The project can be further developed. It's applicable in automotive and transportation industries. IoT innovation drives modern vehicle security. The system prevents vehicle theft and unauthorized access.

Grenze ID: 01.GIJET.12.1.347

II. LITERATURE SURVEY

Our vehicle security system is designed by learning from several research studies to make it both strong and depend-able. One major inspiration comes from Verma et al., who developed an iris-based door security system using OpenCV and Raspberry Pi. This shows how biometric authentication can provide reliable security. In our system, we use an ESP32-CAM module with infrared support so that it can detect the iris even in low-light conditions—like in-side a car. This makes user identification more accurate and secure.
Another idea we built on comes from Rathi et al., who created a real-time intruder detection and alert system using GSM and GPS. Based on their concept, our system can track the vehicle's live location if someone tries to break in. The GPS coordinates are automatically sent to the owner's mobile phone through the GSM module, allowing for a quick response and a higher chance of recovering the vehicle.
We also took inspiration from Patel et al., who explored multimodal biometric vehicle security systems that combine face and iris recognition. Similarly, our system uses both facial and iris recognition for double-layered authentication. This dual-factor method reduces false access and provides better protection against identity spoofing or fake entries.
For communication and alerts, we were influenced by Sharma et al., who showed how the SIM800L GSM module can be used for real-time notifications. In our setup, the SIM800L module sends an instant message to the owner's phone with the vehicle's GPS location and a warning—like "INTRUDER DETECTED"—if someone fails the authen-tication process. This ensures the owner is immediately informed and can take quick action to secure the vehicle.

III. PROPOSED METHODOLOGY

The smart vehicle ignition system is designed to make starting a vehicle safer and easier.
Instead of using a regular key, it uses face detection to identify the authorized driver.
A small but powerful controller, the Raspberry Pi Pico Zero W, runs the whole system.
When the driver approaches, a camera captures their face and checks it with stored images.
If the system recognizes the face, it allows the ignition to start the vehicle.
This removes the need for physical keys and prevents unauthorized access.
The Pico Zero W acts as the brain, handling the camera input and facial recognition process.
It also controls a relay module, which works like a switch to power the starter motor.
Only after successful face verification does the relay activate the ignition.
The Pico Zero W's wireless capability allows for future upgrades like remote control or cloud storage.
The facial recognition feature is powered by artificial intelligence for accurate results.
It continuously compares real-time images with the stored authorized faces.
If a match is found, the ignition is triggered instantly and safely.
By combining AI and IoT technologies, the system offers smart and reliable vehicle operation.
Overall, it's a cost-effective and advanced solution that can make vehicles more secure and modern.

IV. DESIGN CONSIDERATIONS

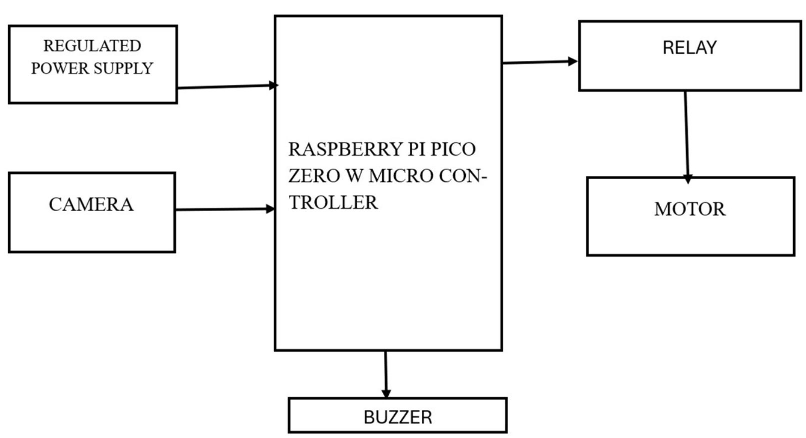

Fig 1

A. Hardware Components

- Microcontroller or Processor: Select a microcontroller or processor capable of handling camera input and network-ing, supporting peripherals like cameras, relays, and sensors.
- Power Supply: Ensure a stable power supply with sufficient current for all components, including voltage regula-tors if battery-powered.
- Camera Module: Choose a camera module compatible with the microcontroller, with sufficient resolution and frame rate for reliable face detection.
- Relay Module : Use a relay module to control high-current loads like the vehicle starter motor, matching the vehi-cle system voltage.
- Connectivity Hardware Include Wi-Fi or Bluetooth modules for IoT features external modules for better range if needed.

B. Software Considerations

- Operating System or Runtime Environment: Use a Linux- based OS for Raspberry Pi or bare-metal code/RTOS for microcontrollers depending on complexity.
- Face Detection Algorithm: Utilize OpenCV haar cascades, deep learning optimizing for real-time performance and accuracy.
- Communication Protocols: Employ MQTT, HTTP, or TCP/IP for remote commands and status updates, securing communication with encryption like TLS.
- Control Logic and Workflow: Implement logic to check for face authentication, enable the relay if authorized, and start the vehicle, including fallback or emergency stop logic.
- Error Handling and Feedback: Provide user feedback via buzzer, LED.

V. IMPLEMENTATION

The implementation of a vehicle anti-theft system using face recognition involves several key components, including an face camera, microcontroller. The system works by enrolling authorized users' face images, capturing and com-paring iris images to authenticate users, and controlling the vehicle's ignition system via the relay module. The face recognition algorithm involves image preprocessing, feature extraction, and template matching to ensure accurate authentication.

- Camera scanning device captures user's face image.
- Image is processed and compared to pre-stored face templates.
- If match is found, system sends signal to enable vehicle's ignition system.
- Vehicle can only be started by authorized users with matching face profiles.
- This system provides a secure, convenient, and eliminating the need for physical keys or passwords.

The vehicle anti-theft system using iris recognition provides a highly secure and reliable solution for preventing un-authorized access and theft. By utilizing advanced iris scanning technology, the system accurately identifies and authenticates users, ensuring that only authorized individuals can start and operate the vehicle. This technology elim-inates the need for physical keys, passwords, or other traditional security methods, offering a convenient and user-friendly experience. With its robust security features and advanced biometric technology, the vehicle anti-theft sys-tem using iris recognition is an effective solution for protecting vehicles from theft and unauthorized access.

VI. WORK FLOW

A. Face Enrollment

- Collect images of authorized faces using OpenCV
- Train and save the captured images

B. Face Detection and Recognition

- Camera captures frames continuously
- Each frame is compared with known face encodings
- If a match is found, send a signal to Raspberry Pi Pico W

C. Communication with Pico W

- Pico W runs Micro Python script
- Listens to incoming Wi-Fi signals When valid signal is received, it activates GPIO pin

D. Relay and Motor Control

- GPIO pin turns ON the relay
- Relay powers the motor (e.g., opens a door or turns a device)
- After some time, motor is turned OFF

E. When authorized person's face is recognized, a signal is sent to Pico W.

F. Pico W turns on a relay, starts a motor that simulates the vehicle ignition.

G. Vehicle can be programmed to stay ON for a fixed time or until another signal is received.

VII. RESULT AND DISCUSSION

The project successfully demonstrates the development of a smart vehicle starter system that combines biometric security and convenience using the Raspberry Pi Pico W and face detection technology. The system uses a camera to capture the driver's image and smart algorithms to recognize authorized users. This means the vehicle can be started without a physical key, making it both safer and more convenient. It also supports multiple drivers, allowing the system to recognize each one and adjust settings based on their preferences.

This innovation shows great potential for use in modern and future vehicles, especially smart and autonomous cars. By using face detection, the system ensures that only registered individuals can start the vehicle, reducing the risk of theft or unauthorized access. The use of the compact Raspberry Pi Pico W makes the design small, efficient, and cost-effective, which is ideal for real-world use.

Overall, this project highlights how technology can make vehicles smarter and more secure. It blends artificial intelligence, biometrics, and IoT to create a more personalized and safe driving experience. With its focus on both security and convenience, this system could play a big role in the future of vehicle access and control.

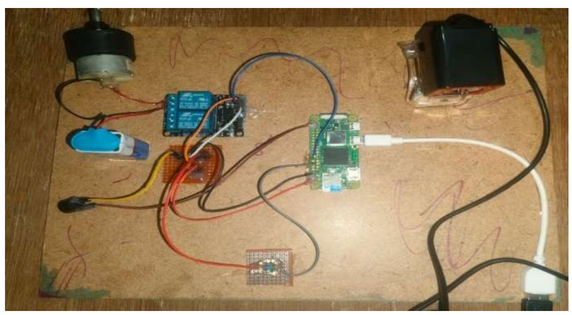

Fig 1. Architecture

Fig 2. Output results

VIII. CONCLUSION

The proposed Face Recognition-Based Vehicle Starting System using Raspberry Pi Pico W successfully demonstrates a secure, intelligent, and contactless ignition mechanism for modern vehicles. By integrating OpenCV-based facial recognition with MicroPython-driven relay and motor control, the system ensures that only authorized users can access and start the vehicle, thereby significantly enhancing security and reducing the risk of theft or unauthorized use. The Raspberry Pi Pico W's built-in Wi-Fi enables efficient real-time communication between the recognition module and the ignition controller, making the system flexible, scalable, and adaptable for future IoT-based automotive applications. This research highlights the potential of combining biometric authentication, embedded hardware, and IoT communication to create a next-generation vehicle security framework that is cost-effective, reliable, and suitable for practical implementation in the automotive industry.

FUTURE SCOPE

- Cloud-Based Monitoring: Use Firebase or IoT platforms to log vehicle access attempts and maintain user logs/history.
- Multi-Layer Authentication: Implement dual authentication using facial recognition and fingerprint/PIN code for added security.
- GPS and Geo-Fencing: Combine with GPS modules to restrict vehicle access to specific locations.
- Voice Command Integration: Add voice command control (via Google Assistant or Alexa) for hands-free access in future smart car models.
- AI-based Driver Detection: Use AI models to recognize specific driving behavior and restrict access based on user profiles.

REFERENCES

[1] A. Kumar and A. Passi, "Comparison and combination of iris matchers for reliable personal authentication," Pat-tern Recognition, vol. 43, no. 3, pp. 1016–1026, Mar. 2010.

[2] R. P. Wildes, "Iris recognition: an emerging biometric technology," Proceedings of the IEEE, vol. 85, no. 9, pp. 1348–1363, Sep. 1997.

[3] J. Daugman, "How iris recognition works," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 21–30, Jan. 2004.

[4] A. Tiwari and A. Sharma, "Vehicle ignition control system using iris recognition," International Journal of Com-puter Applications, vol. 115, no. 19, pp. 1–5, Apr. 2015.

[5] P. Sharma and P. Jindal, "Design and Implementation of a Biometric Vehicle Anti-theft System Using Iris Recog-nition," International Journal of Advanced Research in Computer Science, vol. 9, no. 2, pp. 163–167, Mar.–Apr. 2018.

[6] K. U. Kyaw and M. M. Lwin, "Biometric authentication system using iris recognition for security," 2018 IEEE Conference on Computer Applications (ICCA), Yangon, Myanmar, 2018, pp. 208–212.

[7] S. R. Dubey and A. A. Malik, "Iris based biometric system using Raspberry Pi and OpenCV," 2019 5th Interna-tional Conference on Signal Processing, Computing and Control (ISPCC), Solan, India, 2019, pp. 249–254.

[8] A. A. Paul, S. K. Harit, and B. N. Chatterji, "A study on real-time iris recognition system using OpenCV and its implementation on embedded platforms," International Journal of Biometrics, vol. 12, no. 1, pp. 22–39, 2020.

[9] H. Proença and L. A. Alexandre, "Iris recognition: On the segmentation of degraded images acquired in the visi-ble wavelength," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 32, no. 8, pp. 1502–1516, Aug. 2010.

[10] K. Lakshmi and B. P. Rani, "Implementation of Smart Security System Using Iris Recognition," International Journal of Engineering Research & Technology (IJERT), vol. 9, no. 8, pp. 179–183, Aug. 2020.