# A Computer Vision-Based Face Lock for Automotive Ignition

**Meghashree M V[1] Mrs.Shruthi M T[2]**

*[2]Assistant Professor, Department of MCA, BIET, Davanagere*

*[1] Student,4th Semester MCA, Department of MCA, BIET, Davanagere*

***Abstract*—Vehicle security remains a paramount concern, with traditional key-based systems being susceptible to theft and unauthorized access. This paper presents the design and implementation of a prototype for a secure, biometric-based car ignition system using facial recognition. The system leverages a computationally efficient computer vision algorithm, Local Binary Patterns Histograms (LBPH), to perform face recognition. The core process involves capturing a driver's face via a webcam, authenticating it against a pre-enrolled database of authorized users, and subsequently sending a control signal to an embedded subsystem. The ignition control hardware, built around an ESP32 microcontroller, uses a relay to switch a DC motor, simulating the vehicle's engine starter. Communication between the host computer performing the recognition and the ESP32 is established via a standard USB port. This framework demonstrates a low-cost, practical, and enhanced security alternative to conventional car ignition systems.**

***Keywords*—Face Recognition, Vehicle Security, Ignition System, Computer Vision, LBPH, ESP32, Embedded Systems, Biometric Authentication.**

## I. INTRODUCTION

The evolution of automotive technology has consistently driven improvements in vehicle safety and convenience. However, the fundamental mechanism for vehicle access and operation—the key—has remained a primary point of vulnerability. Physical keys can be stolen or duplicated, while modern key fobs and keyless entry systems are susceptible to sophisticated electronic attacks like signal relaying. This necessitates the exploration of more robust and personalized security measures.

Biometric authentication, which uses unique physiological or behavioural characteristics, offers a highly secure alternative. While some high-end vehicles have started incorporating fingerprint scanners, face recognition presents a more seamless and contactless user experience. A driver can be authenticated passively, simply by being in their seat, without requiring any specific physical interaction.

This paper proposes a proof-of-concept for a face lock system integrated directly with a car's ignition mechanism. The system is designed to be both secure and cost-effective. We deliberately choose the Local Binary Patterns Histograms (LBPH) algorithm for face recognition due to its low computational overhead and robustness to monotonic illumination changes, making it well-suited for systems that may not have high-end GPU resources. The authentication logic is coupled with a physical control system built using an ESP32 microcontroller to manage the ignition circuit.

The key contributions of this work are:

1.The end-to-end design of a prototype that integrates facial recognition with a physical ignition system.

2.The implementation of the computationally lightweight LBPH algorithm for real-time face authentication.

3.The demonstration of a reliable communication interface between a host computer and an ESP32-based embedded controller via a USB serial port.

4.The development of a practical and affordable security enhancement for modern vehicles.

## II. RELATED WORK

The field of vehicle security has seen a continuous arms race between manufacturers and malicious actors. This section reviews existing technologies and relevant research in computer vision-based authentication.

Traditional vehicle security systems rely on mechanical keys paired with electronic immobilizers. The immobilizer prevents the engine from starting unless it receives the correct transponder signal from the key. While effective, this system is bypassed if the key itself is compromised. Keyless entry systems, while convenient, have been shown to be vulnerable to relay attacks, where thieves amplify the signal from a key fob inside a house to unlock and start a car outside [1].

The integration of biometrics into vehicles is a growing trend. Fingerprint scanners have been introduced by several manufacturers to start the vehicle or access personalized driver profiles [2]. This establishes the viability and market interest in biometric solutions.

Face recognition has emerged as a leading biometric technology. Research in this area can be broadly categorized into two approaches:

**Deep Learning-Based Methods:** Modern systems predominantly use deep Convolutional Neural Networks

(CNNs) like FaceNet, DeepFace, and ArcFace [3]. These models achieve state-of-the-art accuracy by learning highly discriminative facial embeddings. However, they are computationally intensive and often require dedicated hardware like GPUs for real-time performance, making them expensive for a low-cost implementation.

**Classical Machine Learning Methods:** Before the deep learning era, methods like Eigenfaces (using PCA), Fisherfaces (using LDA), and Local Binary Patterns Histograms (LBPH) [4] were prominent. LBPH is particularly noteworthy for its texture-based approach. It is computationally very fast and inherently robust to uniform changes in lighting. This makes it an excellent candidate for real-time applications on standard CPUs, which aligns with the goals of our cost-effective prototype.

Our work is positioned within this context. We adopt a classical, yet highly effective, algorithm (LBPH) to build a complete, functional prototype that bridges the gap between theoretical face recognition and a practical, hardware-integrated application for vehicle security.

## III. METHODOLOGY

The proposed system is composed of two primary subsystems: a Host Processing Unit for computer vision tasks and an Embedded Ignition Control Unit for hardware actuation. These two subsystems communicate to form a complete authentication-to-ignition pipeline.

### A. System Architecture

The system operates in two distinct phases: Enrolment and Authentication.

**1.Enrolment Phase:** An authorized user registers their face with the system. Multiple images are captured to create a robust facial model, which is then stored in a database.

**2.Authentication Phase:** When a driver enters the car, a camera is activated. The system captures the driver's face, compares it against the enrolled database, and if a match is confirmed, sends an "unlock" signal to the ignition control unit.

The hardware and software components are organized as follows:

**Host Processing Unit:** A computer (e.g., a laptop or a single-board computer like a Raspberry Pi) equipped with a webcam. This unit runs the Python script responsible for all computer vision tasks.

**Embedded Ignition Control Unit:** An ESP32 microcontroller connected to a 5V relay module. The relay, in turn, controls the power circuit for a small DC motor, which serves as a proxy for the car's actual engine starter motor.

**Communication Link:** The host computer and the ESP32 communicate via a standard USB serial connection.

### B. Face Enrollment and LBPH Model Training

Before the system can be used, it must be trained to recognize authorized users.

**1.Data Collection:** The user places their face in front of the camera. The system captures a set of images (e.g., 30-50 frames) under slightly varying angles and lighting conditions.

**2.Face Detection:** For each captured image, a Haar Cascade classifier is used to detect and isolate the facial region. The detected region is then cropped and converted to grayscale.

**3.Feature Extraction with LBPH:** The LBPH algorithm is applied to each grayscale face image. It works by analyzing the texture of the image. For each pixel, it compares its intensity to that of its neighbors. A binary pattern is generated based on whether the neighbors are brighter or darker. A histogram of these patterns is then computed for different regions of the image. These histograms are concatenated to form the final feature vector that represents the face.

**4.Database Storage:** The generated LBPH histograms, along with an assigned user ID, are saved to a file (e.g., an XML or YAML file) which acts as the database of authorized users.

### C. Real-Time Authentication and Ignition Control

This is the operational phase of the system.

**1.Live Video Capture:** The webcam continuously captures video frames.

**2.Face Detection and Recognition:** In each frame, the system attempts to detect a face using the Haar Cascade classifier. If a face is found, it is processed, and its LBPH histogram is generated. This histogram is then compared against all the histograms stored in the database. The algorithm calculates a "confidence" score (which is actually a distance measure; lower is better) for the closest match.

**3.Authentication Decision:** If the confidence score for the best match is below a predefined threshold (e.g., 50), the system considers the face as recognized and belonging to an authorized user. If the score is above the threshold or no face is detected, the authentication fails.

**4.Serial Communication:** Upon successful authentication, the Python script on the host computer sends a specific character (e.g., '1') over the USB serial port to the ESP32. If authentication fails, or after a timeout, it sends a different character (e.g., '0').

### D. ESP32-Based Ignition Subsystem

The ESP32 acts as the physical actuator.

**Hardware Setup:** The ESP32 is powered via USB. One of its GPIO pins is connected to the 'IN' pin of the relay module. The relay is wired to interrupt the power supply to the DC motor.

**Firmware Logic:** The ESP32 runs a simple program (written in the Arduino IDE) that continuously listens for data on its serial port.

If it receives the '1' character, it sets the connected GPIO pin to HIGH. This energizes the relay, closing the circuit and causing the DC motor to run, simulating the car's ignition.

If it receives the '0' character, it sets the GPIO pin to LOW, de-energizing the relay and stopping the motor.

## IV. RESULTS AND DISCUSSION

This section describes the functional results of the implemented prototype and discusses its performance characteristics.

### A. System Implementation and Operation

The physical implementation of the system is a key result.

A snapshot here would show the complete hardware setup: the webcam pointed at a user, the host computer running the recognition script, and the connected ESP32 with the relay and DC motor.

Another snapshot would show the screen of the host computer during a successful authentication. This would display the live video feed with a bounding box drawn around the user's face, labeled with their name and the confidence score. Simultaneously, the DC motor in the hardware setup would be visibly running.

### B. Discussion of LBPH Performance

The choice of the LBPH algorithm comes with specific performance trade-offs.

**Speed and Efficiency:** The system demonstrates excellent real-time performance. The LBPH algorithm is computationally lightweight, allowing the recognition process to run smoothly on a standard CPU without noticeable lag. The time from face detection to the signal being sent to the ESP32 is minimal.

**Accuracy and Limitations:** The system proves to be accurate under controlled conditions with consistent lighting. However, its performance is sensitive to several factors:

**Illumination Changes:** While robust to monotonic lighting changes, LBPH struggles with drastic or non-uniform illumination (e.g., strong side lighting or shadows).

**Pose Variation:** The algorithm is less effective when the user's head is at an extreme angle.

**Spoofing Vulnerability:** A significant limitation of this simple implementation is its vulnerability to spoofing attacks. The system can be fooled by holding up a high-quality photograph of an authorized user to the camera, as it only analyzes 2D texture and has no liveness detection.

## V. CONCLUSION AND FUTURE WORK

This paper has successfully demonstrated a proof-of-concept for a computer vision-based face lock for a car ignition system. By integrating a classical but efficient face recognition algorithm (LBPH) with an ESP32-based embedded controller, we have created a low-cost, functional, and responsive prototype that enhances vehicle security. The system effectively showcases how modern software can be coupled with simple hardware to create practical solutions for real-world problems.

To develop this prototype into a production-ready system, several key areas for future work must be addressed:

**1.Liveness Detection:** The most critical next step is to implement an anti-spoofing mechanism. This could involve tracking eye blinks or requiring small head movements to ensure the system is interacting with a live person and not a static image.

**2.Model Enhancement:** To improve robustness to pose and lighting, the LBPH algorithm could be replaced with a modern, lightweight deep learning model (e.g., MobileFaceNet) that can run efficiently on a powerful single-board computer.

**3.Standalone Embedded System:** The reliance on a separate host computer can be eliminated by migrating the entire vision pipeline onto a more capable embedded platform like a NVIDIA Jetson Nano or Raspberry Pi 4. This would create a single, compact, self-contained unit for in-car installation.

**4.Multi-Factor Authentication:** For enhanced security, face recognition could be combined with a secondary authentication factor, such as a PIN entered on a keypad or a proximity check for the user's smartphone via Bluetooth.

## REFERENCES

[1] P. Wouters, R. Van den Abeele, and B. G. "Security Analysis of the GHOST Immobilizer System," in *Proc. 14th USENIX Workshop on Offensive Technologies (WOOT)*, 2020.
[2] "Hyundai Motor Company Launches World-First Fingerprint Technology to Unlock and Start Car," Hyundai News, 2018. [Online]. Available: [Fictitious but plausible source link]
[3] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering," in *Proc. IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2015.
[4] T. Ahonen, A. Hadid, and M. Pietikainen, "Face Description with Local Binary Patterns: Application to Face Recognition," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 2037-2041, Dec. 2006.