PROJECT PROPOSAL

VEHICLE - SMART ENGINE LOCK SYSTEM USING BIOMETRIC AUTHENTICATION (FACE RECOGNITION AND FINGERPRINT)

Batch 17 (PT) - 2024

Name	: M. R. M. Rashid
Field	: Automotive Engineering
Reg. No.	: ENGSC/BEng/PT Wlv 300 /24-01/0017
Date of submission	: 20th of December, 2024

Individual Innovation Project – BEng –Batch 17		
Project	Topic:	Vehicle - Smart engine lock system using biometric authentication (Face recognition and Finger print)
Supervisor Details	Name:	M. J. M. Anees
	*Designation:	Software Engineering Lead
	*Place of work:	Riyadh, Saudi Arabia
	*Qualifications:	BSc. Eng (Hons) UOM
	*email:	anees.jenawfer@gmail.com
	*Tel:	+94 77 400 9678
Student Details	Name:	M. R. M. Rashid
	Reg. No.:	ENGSC/BEng/PT Wlv 300 /24-01/0017
	Field:	Atomotive Engineering
	Contact Tel. No.	+94 77 909 6462

INTRODUCTION

Vehicle security has become a major concern with the rise of car thefts and unauthorized access. Traditional methods such as key fobs, PIN codes, or physical locks have proven to be vulnerable to technological advances that enable hacking or theft. To counter these vulnerabilities, a more advanced and secure solution is required. This proposal outlines the development of a Vehicle - Smart Engine Lock System that utilizes biometric authentication methods - specifically face recognition and fingerprint scanning to enhance security and convenience for vehicle owners. By leveraging these advanced technologies, this system ensures that only authorized users can start and operate the vehicle, offering a higher level of protection than conventional locking mechanisms.

The proposed Vehicle - Smart Engine Lock System incorporates two primary biometric authentication methods: face recognition and fingerprint scanning. These technologies work in tandem to verify the identity of the vehicle owner or authorized users before granting access to the vehicle's engine. This multi-layered authentication process will make it nearly impossible for unauthorized individuals to bypass the system and gain access to the vehicle.

AIMS AND OBJECTIVES

The primary aim of the **Vehicle - Smart Engine Lock System** is to provide an advanced, secure, and user-friendly solution for vehicle authentication and engine access. By utilizing cutting-edge biometric technologies - specifically facial recognition and fingerprint scanning, the system aims to replace traditional key-based entry systems, offering a highly secure and seamless experience for vehicle owners.

Objectives:

- **Enhance Vehicle Security:**
  - The system's main objective is to provide a higher level of security than traditional key fob or PIN-based systems by using unique biometric identifiers (face and fingerprint) that are difficult to replicate. This minimizes the risk of theft or unauthorized vehicle access.
- **Create a Seamless User Experience:**
  - The system will be designed for ease of use, allowing authorized users to start and operate their vehicle without the need for physical keys or fobs. The goal is to create a hands-free, hassle-free experience that enhances user convenience while maintaining high security.
- **Create a Scalable Solution:**
  - The system should be adaptable to a range of vehicles, from personal cars to commercial fleets. The objective is to offer a versatile solution that can be scaled for different vehicle types and fleet management systems, enabling businesses to adopt the technology for security purposes.
- **Foster Market Innovation:**
  - Finally, the project aims to position the vehicle with biometric authentication as a leading innovation in automotive security. By providing a solution that integrates advanced biometric authentication, the system will enhance the vehicle's appeal, increase its market value, and set a new standard for security.

Through these aims and objectives, the project seeks to revolutionize vehicle security by introducing a secure, seamless, and efficient way to authenticate users and unlock engine access.

METHODOLOGY

Literature Review:

Biometric authentication has become increasingly popular in various industries due to its ability to provide a higher level of security and convenience compared to traditional password or key-based systems. In recent years, the automotive sector has been exploring the integration of biometrics for vehicle security, with a focus on technologies like **facial recognition** and **fingerprint scanning**. This literature review examines existing research and innovations in vehicle security systems, with an emphasis on biometric authentication, and discusses their relevance to the proposed **Smart Vehicle Engine Lock System**.

The research paper "Biometric Authentication for Automobiles" (Karumudi et al., 2019) explores the integration of biometric technologies into the automotive industry to enhance security, personalization, and convenience. It reviews various biometric modalities such as fingerprints, facial recognition, iris scanning, voice recognition, and electrocardiogram (ECG), emphasizing their application in vehicle access, ignition control, and in-car services like payments and user-specific settings. The paper highlights the advantages of biometrics in preventing theft, enabling secure car sharing, and monitoring driver health and behavior, while addressing challenges such as environmental factors, data security, and system integration. It underscores the potential of biometrics to replace traditional keys and pave the way for seamless, user-centric automotive experiences, proposing future work in exploring emerging modalities and multimodal systems.

The study (Kiruthiga & Latha, 2014) explores advancements in biometric technologies for vehicle security, emphasizing fingerprint recognition due to its reliability and unique identification capabilities. Conventional security systems, including RFID-based mechanisms and GPS tracking, face limitations such as susceptibility to theft, signal degradation, and high dependency on environmental conditions. Fingerprint biometrics is proposed as a superior alternative, offering reduced False Acceptance Rates (FAR) and False Rejection Rates (FRR) through minutiae-based techniques for feature extraction. Additionally, related studies reviewed in the paper highlight methods like Gabor filters, Principal Component Analysis (PCA), and Local Binary Patterns (LBP) to improve accuracy and reduce errors in fingerprint recognition systems. The integration of these

biometric methods into embedded systems for vehicle security underscores their potential to enhance theft prevention and user authentication across various applications, including banking and robotics.

The research paper **"**Biometric Authentication**"** provides a comprehensive overview of biometric authentication, highlighting its significance as a secure alternative to traditional methods like passwords and PINs. Biometric systems leverage unique physical and behavioral traits, including fingerprints, facial recognition, iris patterns, and gait analysis, to authenticate users. These methods are increasingly adopted in diverse domains such as smartphones, banking, and high-security facilities due to their accuracy and resistance to forgery. However, the study acknowledges potential vulnerabilities, such as biometric spoofing and privacy concerns, emphasizing the need for advancements in liveness detection and multi-modal approaches. The review discusses recent innovations like behavioral biometrics and edge-based systems, which enhance security and user convenience. Despite its challenges, biometric authentication is positioned as a pivotal technology in the evolving landscape of secure identification (Misini & Lajçi, 2022).

The research paper "Biometric Authentication for Vehicle Security System Using Raspberry Pi", delves into multi-factor biometric authentication for vehicle security, integrating facial recognition, fingerprint sensors, and keypad passwords to provide robust theft prevention. Leveraging the computational capabilities of Raspberry Pi, the system synchronizes these methods for seamless operation and enhanced security. Literature highlights the efficiency of biometric technologies in vehicle protection, noting the distinct advantages of face recognition for non-intrusive access and fingerprints for precise identification. Complementary systems, such as ultrasonic sensors for anti-lift detection and servo motor-based wheel locking, further solidify the defense mechanism. Previous works, including RFID-based systems, underscore limitations such as susceptibility to theft and technological malfunctions, which this paper addresses by employing advanced biometric and anti-theft measures (Sudarshan et al., 2024).

"Vehicle Security System" (Reddy et al., 2020) explores an IoT-based solution to enhance vehicle safety and security. The proposed system integrates accident detection and theft control mechanisms, ensuring timely notifications to emergency services and the vehicle owner's contacts

during accidents. Utilizing components like Arduino, GSM, and GPS modules, it provides real-time alerts and allows remote ignition control to counter thefts. This system improves upon existing technologies by addressing limitations such as delayed emergency responses and lack of vehicle control during thefts. The authors highlight the system's potential to significantly improve road safety and vehicle security.

Biometric authentication, especially through **facial recognition** and **fingerprint scanning**, offers promising solutions to enhance vehicle security by providing a more secure and convenient alternative to traditional methods. Combining multiple biometric methods further strengthens the system, making unauthorized access significantly more difficult. However, challenges such as data privacy, system reliability, and the need for backup access mechanisms remain important considerations. As technology advances, the integration of **AI**, **machine learning**, and improved biometric sensors will further enhance the effectiveness and user experience of biometric-based vehicle security systems.

System Design:

I. **Biometric Authentication Components**

- **Facial Recognition Module:** The facial recognition component utilizes high-resolution cameras placed inside or around the vehicle, such as on the dashboard or near the rearview mirror. The cameras will capture detailed images of the user’s face upon approach. Advanced algorithms will then analyze the facial features, including the distance between eyes, shape of the nose, and structure of the face, comparing them against a pre-registered database of authorized users. Facial recognition offers an added layer of convenience as it can operate without physical contact, ensuring a hands-free experience for the user.
- **Fingerprint Recognition Module:** Complementing the facial recognition system, the fingerprint scanning module will be integrated into various parts of the vehicle, such as the door handle, dashboard, or ignition panel. The fingerprint scanner will capture the fingerprint pattern of the user and compare it with the data stored in the system. This provides an additional layer of security and ensures that even if the face recognition system is bypassed, fingerprint authentication remains a reliable security check.

II. Secure Database Management

The biometric data of authorized users will be stored in a secure, encrypted database. The data can be stored either locally in the vehicle's onboard system. All biometric data will be encrypted with the highest standards of security to protect the privacy of users. Additionally, users will be able to update or manage their biometric data via the vehicle's interface, allowing for ease of access and updates.

III. Access Protocol

To ensure a robust authentication process, the system will implement a dual authentication approach, requiring both face recognition and fingerprint scanning. The engine will remain locked unless both authentication methods confirm the identity of the authorized user. This redundancy reduces the likelihood of unauthorized access. This flexibility allows for customized experiences for multiple drivers within the same vehicle.

IV. Authentication Process

The authentication process is designed to be seamless and efficient, providing the user with a convenient experience while maintaining a high level of security.

- ***Step 1: Approach the Vehicle*** – The system detects the proximity of the user through sensors embedded in the vehicle. As the user approaches, the authentication system activates.
- ***Step 2: Face Recognition Scan*** – The system uses an infrared-enabled camera to scan the user's face, ensuring that the facial recognition system works under various lighting conditions, including low light or night-time settings.
- ***Step 3: Fingerprint Scan*** – Once the facial recognition confirms the user's identity, the system prompts the user to place their finger on the fingerprint scanner for further verification.
- ***Step 4: Engine Lock Release*** – If both authentication methods match the stored data, the system will send a signal to release the engine lock, allowing the user to start and operate the vehicle.
- ***Step 5: Emergency Override*** – In case of system malfunction, failure to recognize the biometric data, or if the user is unable to authenticate, the system will provide a backup solution such as a manual key or password override mechanism for emergency access.

V. Safety Features

The system is to be designed with advanced safety features to prevent unauthorized access and protect against spoofing or hacking attempts.

- ***Anti-Spoofing Measures:*** To prevent spoofing, the face recognition module includes infrared sensors that detect depth and ensure that the system is scanning a real, live face rather than a photo or video. Similarly, the fingerprint scanner includes liveness detection technology, which checks for signs of a real finger, such as heat or moisture, to prevent the use of fake prints.
- ***Multiple Failed Attempts Protocol*:** To further safeguard against unauthorized access, the system includes a protocol for handling multiple failed authentication attempts. After a set number of unsuccessful tries (e.g., five consecutive failures), the system will temporarily disable further authentication attempts and send an alert to the vehicle owner. This feature ensures that brute force attacks are effectively thwarted.

VI. User Experience

The system is designed to provide an intuitive, seamless, and user-friendly experience.

- ***User Registration Process:*** Registering biometric data for the first time is a simple process, through the vehicle's onboard system. The process will guide the user through steps to capture their facial features and fingerprints securely. Once registered, the user will be able to authenticate and start the vehicle without the need for physical keys or fobs.

TIMELINE

	2024	2025										
	DEC	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV
TASK												
Planning & Proposal submission												
Market Research & Literature reveiw												
System Design & Architecture Development												
Hardware & Software Procurement												
Biometric Technology Integration												
Prototype Development (Hardware + Software)												
System Testing (Unit Testing & Integration Testing												
Data Privacy & Security Implementation												
Emergency Override System Development												
Final System Testing & Debugging												
Documentation & User Manual Preparation												
Final Project Review & Deployment												
Project Presentation & Handover												

REFERENCES

i. Karumudi, B. R., Gist, P., Shahzad, M. Q., & Wagner, G. M. (2019). *Biometric authentication for automobiles* [Research proposal]. Syracuse University. DOI: 10.13140/RG.2.2.17735.85929

ii. Kiruthiga, N., & Latha, L. (2014). A Study of Biometric Approach for Vehicle Security System Using Fingerprint Recognition. *International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)*, 1(2).

iii. Misini, E., & Lajçi, U. (2022). Biometric Authentication. Retrieved from https://www.researchgate.net/publication/371567274.

iv. Sudarshan, T. B. R., Rohini, H. N., Priyanka, N., Ankitha, V., & Hullamani, R. M. (2024). Biometric Authentication for Vehicle Security System Using Raspberry Pi. *International Journal of Advanced Research in Computer and Communication Engineering, 13*(5), 170-177. DOI: 10.17148/IJARCCE.2024.13524.

v. Reddy, N. C. S., Rao, M. S., Thota, R. R., & Reddy, Y. H. (2020). Vehicle Security System. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 9(3), 2266–2269. https://doi.org/10.35940/ijitee.l3247.019320