# Design of a Biometric Based Vehicle Security System for Theft Deterrence and Intruder Identity Communication

**By**

**Zekarias Girma Marie**

A Thesis Submitted to The Department of Mechanical Engineering

School of Mechanical, Chemical and Materials Engineering

**Presented in Partial Fulfillment of the Requirement for the Degree of Master of Science in Automotive Engineering**

## Office of Graduate Studies

## Adama Science and Technology University

June, 2024

Adama, Ethiopia

# Design of a Biometric Based Vehicle Security System for Theft Deterrence and Intruder Identity Communication

**By**

**Zekarias Girma Marie**

Advisor: Alemayehu Wakjira Huluka (Ph.D.)

A Thesis Submitted to The Department of Mechanical Engineering,

School of Mechanical, Chemical and Materials Engineering

**Presented in Partial Fulfillment of the Requirement for the Degree of Master of Science in Automotive Engineering**

## Office of Graduate Studies

## Adama Science and Technology University

June, 2024

Adama, Ethiopia

# DECLARATION

I declare that this Master's Thesis entitled "Design of a Biometric Based Vehicle Security System for Theft Deterrence and Intruder Identity Communication" is my original work. That is, it has not been submitted for the award of any academic degree, diploma or certificate in any other university. All sources of materials that are used for this thesis have been duly acknowledged through citation.

| Zekarias Girma Marie | | |
| --- | --- | --- |
| Name of student | Signature | Date |

# RECOMMENDATION

I, the advisor of this thesis, hereby certify that I have read the revised version of the thesis entitled "Design of a Biometric Based Vehicle Security System for Theft Deterrence and Intruder Identity Communication" prepared under my/our guidance by Zekarias Girma Marie submitted in partial fulfillment of the requirements for the degree of Master of Science in Automotive Engineering. Therefore, I recommend the submission of revised version of the thesis to the department following the applicable procedures.

| | | |
|---|---|---|
| Alemayehu Wakjira Huluka (Ph.D.) | | |
| Major Advisor | Signature | Date |
| | | |
| Co-advisor | Signature | Date |

# APPROVAL

I/we, the advisors of the thesis entitled "Design of a Biometric Based Vehicle Security System for Theft Deterrence and Intruder Identity Communication" and developed by Zekarias Girma Marie, hereby certify that the recommendation and suggestions made by the board of examiners are appropriately incorporated into the final version of the thesis.

| | | |
|---|---|---|
| Alemayehu Wakjira Huluka (Ph.D.) | | |
| Major Advisor | Signature | Date |
| | | |
| Co-advisor | Signature | Date |

We, the undersigned, members of the Board of Examiners of the thesis by Zekarias Girma Marie have read and evaluated the thesis entitled "Design of a Biometric Based Vehicle Security System for Theft Deterrence and Intruder Identity Communication" and examined the candidate during open defense. This is, therefore, to certify that the thesis is accepted for partial fulfillment of the requirement of the degree of Master of Science in Automotive Engineering.

| | | |
|---|---|---|
| | | |
| Chairperson | Signature | Date |
| | | |
| Internal Examiner | Signature | Date |
| Hailemariam Nigus (Ph.D) | | 11/6/2024 |
| External Examiner | Signature | Date |

Final approval and acceptance of the thesis is contingent upon submission of its final copy to the Office of Postgraduate Studies (OPGS) through the Department Graduate Council (DGC) and School Graduate Committee (SGC).

| | | |
|---|---|---|
| | | |
| Department Head | Signature | Date |
| | | |
| School Dean | Signature | Date |
| | | |
| Office of Postgraduate Studies, Dean | Signature | Date |

# ***ABSTRACT***

*Vehicle theft remains a significant issue, with over a million vehicles stolen in 2023 alone. This thesis adopts a comprehensive biometric-based vehicle security system designed to address these concerns by identifying the limitations of current security technologies, such as susceptibility to false alarms, dependency on physical keys, inability to prevent unauthorized engine starts, limited remote monitoring, and lack of intruder evidence. The proposed system seeks to overcome these limitations by integrating advanced biometric modalities, making the sophisticated security measure accessible beyond high-end luxury vehicles. The development process involved selecting suitable biometric modalities, optimizing the system for better accuracy, and enabling real-time communication through a dedicated Android application. A vital feature of the system is its ability to provide immediate notifications of unauthorized access attempts. When motion or vibration is detected, the system triggers an alarm, initiates a phone call, and captures images and fingerprints of the intruder, which are then sent to the vehicle owner via the app. The owner can also lock the engine and track the vehicle's location through the app. Additionally, a panic button is available to alert emergency responders in case of armed coercion. Fingerprint and face recognition were chosen for their accuracy, cost-effectiveness, availability, and adaptability. The R307S optical fingerprint module, tested across 310 scans, showed a specificity of 100%, sensitivity of 99.68%, and accuracy of 99.84%, with an average authentication time of 0.30 seconds. After undergoing hyper-parameter optimization in three stages, the CNN-based deep learning face recognition model was tested on 229 test images, and achieved a precision, recall, and f1-score of 99%, with an average detection time of 0.13 seconds. Hardware implementation utilized Arduino and Raspberry Pi 4B platforms, and the system was tested on a Nissan Diesel TD27 engine and a Jos-Hansen CAN dashboard training model to evaluate functionality. This biometric security system enhances vehicle safety and recoverability by providing prompt alerts and identification of intruders, serving as a deterrent to theft and aiding law enforcement. The study highpoints the necessity of advancing vehicle security technologies beyond conventional methods. By integrating intelligent biometric sensors and effective communication protocols, the proposed system significantly contributes to vehicle safety and the fight against vehicle-related crimes.*

***Keywords:*** *Android app, Biometric system, Face recognition, Fingerprint, Vehicle*

# ACKNOWLEDGMENT

Working on my thesis has been a fantastic voyage, one that I could not have done alone. Many people have supported and encouraged me along the journey, and I would want to thank everyone of them.

I am sincerely thankful to Leul Wujira, a Software Engineer at Addis Ababa University, for kindly sharing his time and skills with me. His knowledge and perspective were vital.

At the outset, I would want to express my gratitude to my advisers, Dr. Alemayehu Wakjira and Dr. Ramesh Babu, for their tremendous assistance, patience, and support throughout the procedure. Their combined opinions and guidance were important in molding this thesis and motivating me to do my best.

Finally, I'd want to thank all of the ASTU auto lab personnel’s Addis and Abiy for creating a stimulating and supportive academic atmosphere that has allowed me to pursue my research ambitions. Thank you for contributing to this thesis and making this experience unforgettable.

# DEDICATION

I would like to dedicate this thesis work to artist Tadesse Teshome, an aqua art specialist. The fruit of your fatherly advice has seasoned, and your unconditional support for education has paid off. You will always stay in my heart. I still miss your forehead kisses, though. May your soul rest in peace!!!

Zekarias Girma

# TABLE OF CONTENTS

# LIST OF ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| **AF** | : Activation Function |
| **BGRU** | : Bidirectional Gated Recurrent Unit |
| **BLoC** | : Business Logic Component |
| **BVSS** | : Biometric Vehicle Security System |
| **CAN** | : Controller Area Network |
| **CNN** | : Convolutional Neural Network |
| **CV** | : Computer Vision |
| **DPI** | : Dots Per Inch |
| **ECM** | : Engine Control Module |
| **ERR** | : Equal Error Rate |
| **FAR** | : False Acceptance Rate |
| **FDS** | : Face Detection System |
| **FN** | : False Negative |
| **FP** | : False Positive |
| **FPS** | : Fingerprint Sensor |
| **FRR** | : False Rejection Rate |
| **GAN** | : Generative Adversarial Network |
| **GPRS** | : General Packet Radio Service |
| **GPS** | : Global Positioning System |
| **GSM** | : Global System for Mobile Communications |

| | |
|---|---|
| **IDE** | : Integrated Development Environment |
| **IoT** | : Internet of Things |
| **IR** | : Infrared |
| **LED** | : Light Emitting Diode |
| **MMS** | : Multimedia Messaging Service |
| **MP** | : Mega Pixel |
| **NHTSA** | : National Highway Traffic Safety Administration |
| **NICB** | : National Insurance Crime Bureau |
| **ONS** | : Office for National Statistics |
| **OS** | : Operating system |
| **OTP** | : One Time Password |
| **PCB** | : Printed Circuit Board |
| **RFID** | : Radio Frequency Identification |
| **SIM** | : Subscriber Identity Module |
| **SMS** | : Short Message Service |
| **TN** | : True Negative |
| **TP** | : True Positive |
| **TTL** | : Time To Live |
| **UART** | : Universal Asynchronous Receiver/Transmitter |
| **UI** | : User Interface |

# LIST OF FIGURES

# LIST OF TABLES

# CHAPTER ONE

# INTRODUCTION

## 1.1 Background of the study

Vehicle theft remains a persistent threat worldwide, posing significant financial losses and safety risks to vehicle owners and communities. According to statistics from law enforcement agencies and insurance providers, millions of vehicles are stolen each year, with a substantial portion of them never recovered (National Insurance Crime Bureau (NICB), 2021). The prevalence of vehicle theft underscores the urgent need for robust security systems capable of deterring theft attempts and aiding in the identification and apprehension of perpetrators (Office for National Statistics (ONS), 2021).

According to the reporter (The Reporter, 2022), a police report showed that out of reported stolen cars in Ethiopia, 33% were unaccounted for, while 48% were found with missing parts, and 18% were being used by the thieves (New Bussiness Ethiopia, 2022).

Figure 1. 1 Car jacker in action (Police, 2023)

Conventional vehicle security systems, such as mechanical locks and immobilizers, have long been the primary line of defense against theft. While effective to some extent, these systems are susceptible to circumvention and exploitation by experienced thieves, as seen in figure 1. 1, using classy tools and techniques. As a result, there has been a growing demand for advanced security solutions capable of providing enhanced protection and peace of mind for vehicle owners.

In recent years, biometric technology has emerged as a promising solution for enhancing vehicle security. Biometrics, which involves the use of distinctive physical or behavioral features for authentication and identification, as shown in figure 1. 2, offers several advantages over conventional security measures (Konatham et al., 2023). By leveraging biometric modalities such as fingerprints, facial features, and iris patterns, vehicle security systems can achieve higher levels of accuracy, reliability, and convenience (Villa et al., 2018).

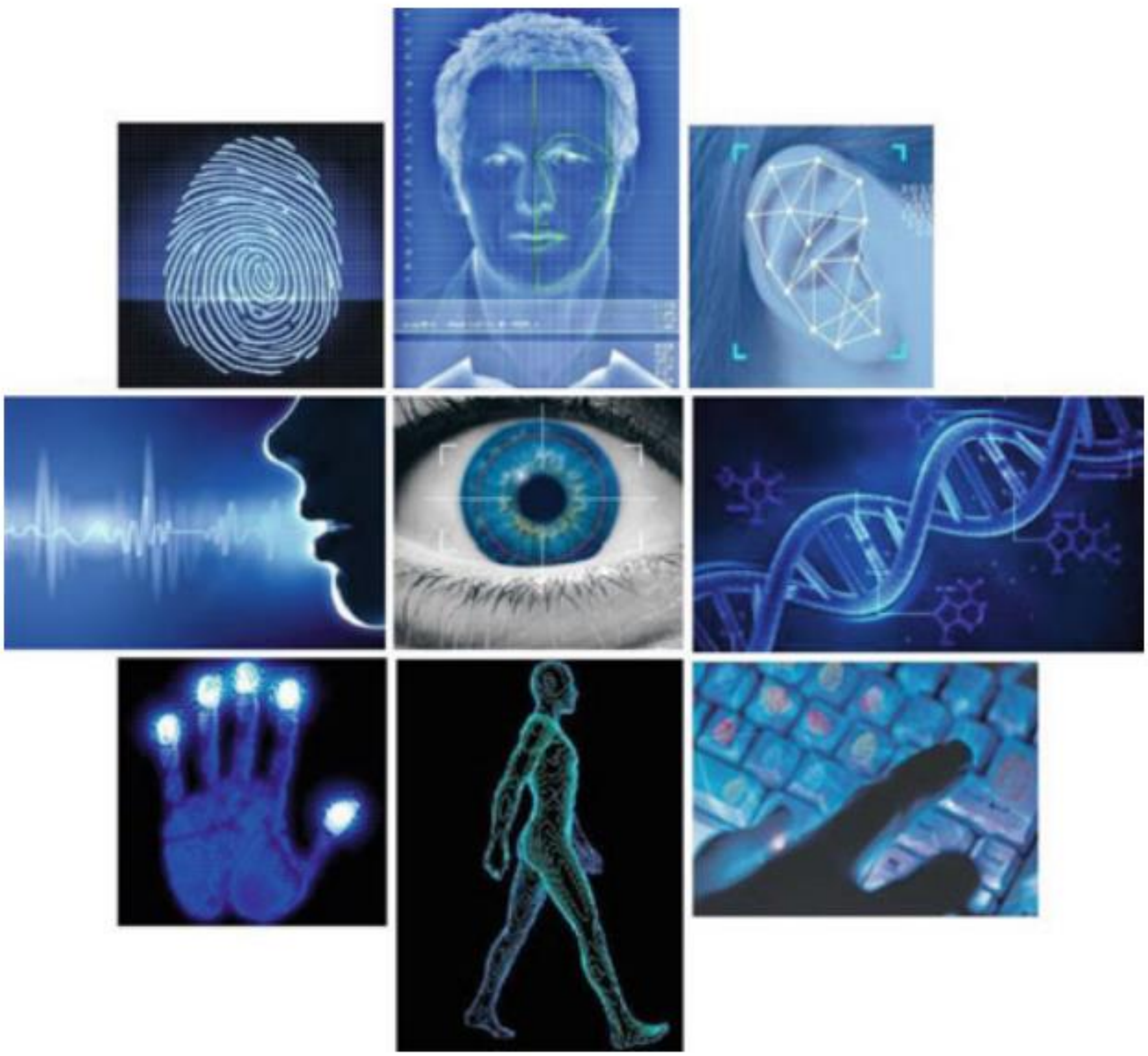

Figure 1. 2 Different biometric systems (Obaidat et al., 2018)

The integration of biometric technology into vehicle security systems represents a paradigm shift in the approach to vehicle protection. Unlike conventional security systems that rely on keys or electronic fobs for access control, biometric systems authenticate users based on their unique physiological or behavioral traits. This replaces the need for physical keys or access cards, lowering the likelihood of uninvited access and theft (Arora & Bhatia, 2022).

Existing biometric security systems, however, are predominantly confined to high-end luxury vehicles, limiting their accessibility to a privileged few who can afford it. The high cost of biometric technology, coupled with the complexity of integration into existing vehicle systems, has hindered widespread adoption across different vehicle types and models (F. Adebayo et al., 2015). As a result, there exists a substantial difference exists between the availability of modern security technologies and its accessibility to the general public.

Addressing this issue requires innovative research and development efforts aimed at democratizing access to biometric technology, making it more affordable and accessible to a wider audience. This thesis proposes a comprehensive biometric vehicle security system designed to bridge this gap and provide enhanced protection for vehicle owners across all socioeconomic backgrounds.

Central to the proposed system is its real-time communication capability, which enables immediate identification and notification of unauthorized access attempts. Upon detection of motion and shock events, the system activates an alarm, initiates a phone call, and captures images of the intruder, promptly transmitting them to the vehicle owner via a dedicated mobile application. Moreover, through the app, the owner can lock engine access and monitor the GPS coordinates of their vehicle with a single tap, further enhancing overall security.

By democratizing access to biometric technology and integrating it into existing vehicle systems, the proposed biometric vehicle security system holds the potential to significantly enhance both the safety and recoverability of valuable assets. By facilitating prompt identification of perpetrators, the system serves as a deterrent to theft and supports law enforcement efforts in combating vehicle-related crimes.

To sum up, the proposed biometric vehicle security system presents a significant potential in the advancement of vehicle security technology. Through its innovative design and implementation, this system aims to provide vehicle owners with enhanced protection and peace of mind, contributing to the reduction of vehicular theft and related crimes.

### 1.2 Problem Statement

The escalating issue of vehicle theft underscores the pressing need to improve conventional security measures with more advanced and effective solutions. Conventional vehicle security systems, predominantly reliant on alarms and central door locks, exhibit limitations that compromise their efficacy in preventing theft (Hans, 2015). One of the primary drawbacks of conventional systems is their inability to accurately identify intruders. Alarms triggered by these systems merely signal unauthorized access without providing critical identification details needed for law enforcement to apprehend perpetrators and recover stolen vehicles promptly (Akshay et al., 2018)(Anjana et al., 2022). Additionally, conventional alarms are prone to false triggers caused by innocuous events like passing animals or strong winds, leading to frequent false alarms that desensitize bystanders and undermine system reliability. Moreover, conventional systems heavily rely on physical keys or remote fobs for vehicle access, making them vulnerable to theft or unauthorized duplication (Bhargav et al., 2022). Once an intruder gains access to the vehicle, the conventional security measures often fail to prevent unauthorized engine start, allowing theft to proceed unchecked. While some conventional systems offer limited remote monitoring and control through smartphone apps for locking and unlocking (Zamin et al., 2022), they lack the sophistication required for real-time monitoring, intruder identification, and advanced security features provided by biometric-based systems.

Since most vehicles on the road are reliant on conventional vehicle security, they are becoming an easy prey and daylight car thefts are now becoming a common thing in Ethiopia (New Bussiness Ethiopia, 2022). Moreover, vehicle drivers are becoming endangered lately as armed robbers are now targeting ride chauffeurs, taking their lives in the theft process.

In contrast, biometric vehicle security systems leverage cutting-edge technologies such as fingerprint and face recognition for unique user authentication and precise intruder access denial.

By accurately verifying the sole identity of enrolled vehicle owners, biometric systems enable prompt alerts in the case of unauthorized access attempts and save intruder identity data, significantly enhancing conventional theft deterrence systems and supporting the process of lost vehicle recovery efforts. These advanced systems also facilitate seamless integration with smartphone applications, enabling convenient remote monitoring, location tracking, and immediate notification of security breaches.

The imperative to overcome the limitations of conventional vehicle security systems underscores the significance of advancing towards biometric-based solutions. This thesis work aims to address these challenges by designing an integrated biometric vehicle security system that not only deters theft effectively but also facilitates seamless intruder identification and real-time communication, ultimately enhancing overall vehicle security and safety. Through this research, the goal is to contribute to the development of comprehensive and technologically advanced solutions that protect vehicles and drivers against the rising threat of theft and unauthorized access.

## 1.3 Research questions

At the end of this thesis, the following research questions relevant to this research topic are to be answered:

- What are the practical implications of integrating biometric sensors in to existing vehicle security system?
- What type of technique can be used to enhance the biometric accuracy and speed of recognition in vehicular environment with varying conditions like light?
- How can an intruder data be seamlessly communicated while complying with existing standards?
- How effective is the designed biometric vehicle security system in reducing theft rates compared to existing security measures?

## 1.4 Objectives

### 1.4.1 General Objective

The primary objective of this thesis is to develop a vehicular biometric system that monitors vehicle security and deters theft attempts.

### 1.4.2 Specific Objectives

The following specific objectives are coined to realize the thesis work:

- To conduct systematic assessment of different biometric modalities and select a suitable modality for integration into vehicle security system.
- To develop a biometric vehicle security system for theft deterrence, owner authentication, and real-time monitoring.
- To test the developed biometric vehicle security system functionality through hardware implementation.

## 1.5 Scope of the thesis

It is important to note that this thesis will cover fingerprint and facial recognition, python programming, a panic/emergency button, a mobile app for real-time communication and hardware testing. Any other task will go beyond the precincts explicitly defined above.

## 1.6 Significance of the Study

The proposed biometric based system will contribute in the following aspects:

- The biometric security system enhances the protection of both the vehicle and its contents.
- The presence of a face-scanning camera may also serve as an additional security element by capturing images of the burglar during forced entries can assist law enforcement in apprehending the criminals.
- The panic/emergency button activation feature enhance driver's safety during armed theft attempts.
- The mobile app offers ease of use for the owner in monitoring his vehicle.
- The biometric security system can give the owner peace of mind about his vehicle.
- The suggested method might be a useful tool for major fleet management organizations such as importers, ride-sharing platforms, meter taxis, and rentals.

As a result, the suggested biometric system has positive implications for vehicle security, owner satisfaction, and the public in general.

### 1.7 Organization of the thesis

Following the completion of **Chapter 1**, **Chapter 2** introduces a summary of related works. This chapter includes various author works intertwined to biometric security systems utilizing fingerprint and face recognition.

**Chapter 3** describes the tools, circuitries and methodologies used in this thesis work. It affords an overview of the overall software and hardware tools employed and entertains the system design employed. This chapter also outlines the system topology, subsystem schematics and performance evaluation involved in the development of the system.

**Chapter 4** shows experimental findings, discussions, and contributions in this thesis.

**Chapter 5** provides conclusions and recommendations for future endeavors utilizing biometric methods.

Overall, this thesis aims to make a substantial contribution to the development of vehicle security systems using biometric approaches, and the chapters given here represent the rigor and depth of study involved to accomplish this goal.

# CHAPTER TWO

# LITERATURE REVIEW

This part of the thesis seeks to shed light on prior scholarly efforts to improve automotive security through the use of biometric technologies. The first portion discusses the various biometric technologies used for security objectives. The next section discusses the limits of each biometric modality. The next topic mentioned is the use of biometric technology for vehicle security, followed by real-time communication techniques. The last section provides a summary of the literature and identifies any gaps.

## 2.1 Vehicle Theft Related Statistics and the Need for Biometric Security

Vehicle theft is a significant and persistent issue worldwide, posing substantial economic losses and safety risks to individuals, businesses, and communities. Understanding the magnitude of this problem is crucial for highlighting the necessity of implementing robust security measures, such as biometric systems, to combat theft effectively.

Other victims are not as lucky, a 2020 police report showed that out of 211 reported stolen cars, 70 were unaccounted for, while 102 were found with missing parts, and 39 were being used by the thieves. Police reports show that organized crime in Addis Ababa, which was relatively the safest city in Africa, is now increasing. Crimes such as armed bank robberies and daylight car theft are now becoming common in Addis Ababa (The Reporter, 2022). Addis Ababa Police Commission recorded 211 car theft in the capital, Addis Ababa, Ethiopia in the nine months' period of the 2019 Ethiopian fiscal year. Out of the 211 stolen cars, 70 are not found, 102 are found with missing parts, while 39 are found being used by the. The Commission is facing challenges in capturing stolen cars as most of the cars are sold in border areas where conflicts are prevalent. (New Bussiness Ethiopia, 2022).

According to statistical data from various sources, including law enforcement agencies, insurance companies, and research organizations, vehicle theft rates vary significantly across different regions and countries. In the United States, for example, the National Highway Traffic Safety Administration (NHTSA) reported over 750,000 vehicle thefts in 2022 alone (National Highway

Traffic Safety Administration (NHTSA), 2022). This alarming statistic represents not only a significant economic burden due to the loss of vehicles but also a safety concern as stolen vehicles can be used in other criminal activities or pose risks to public safety.

Similarly, in Europe, vehicle theft rates have remained a pressing issue, with data from Europol indicating a concerning trend in organized theft rings targeting high-value vehicles. Countries such as the United Kingdom, Germany, and Italy have experienced substantial losses due to vehicle theft, as presented in figure 2. 1, prompting increased efforts to address this issue through legislative measures and technological solutions (Europol, 2020).

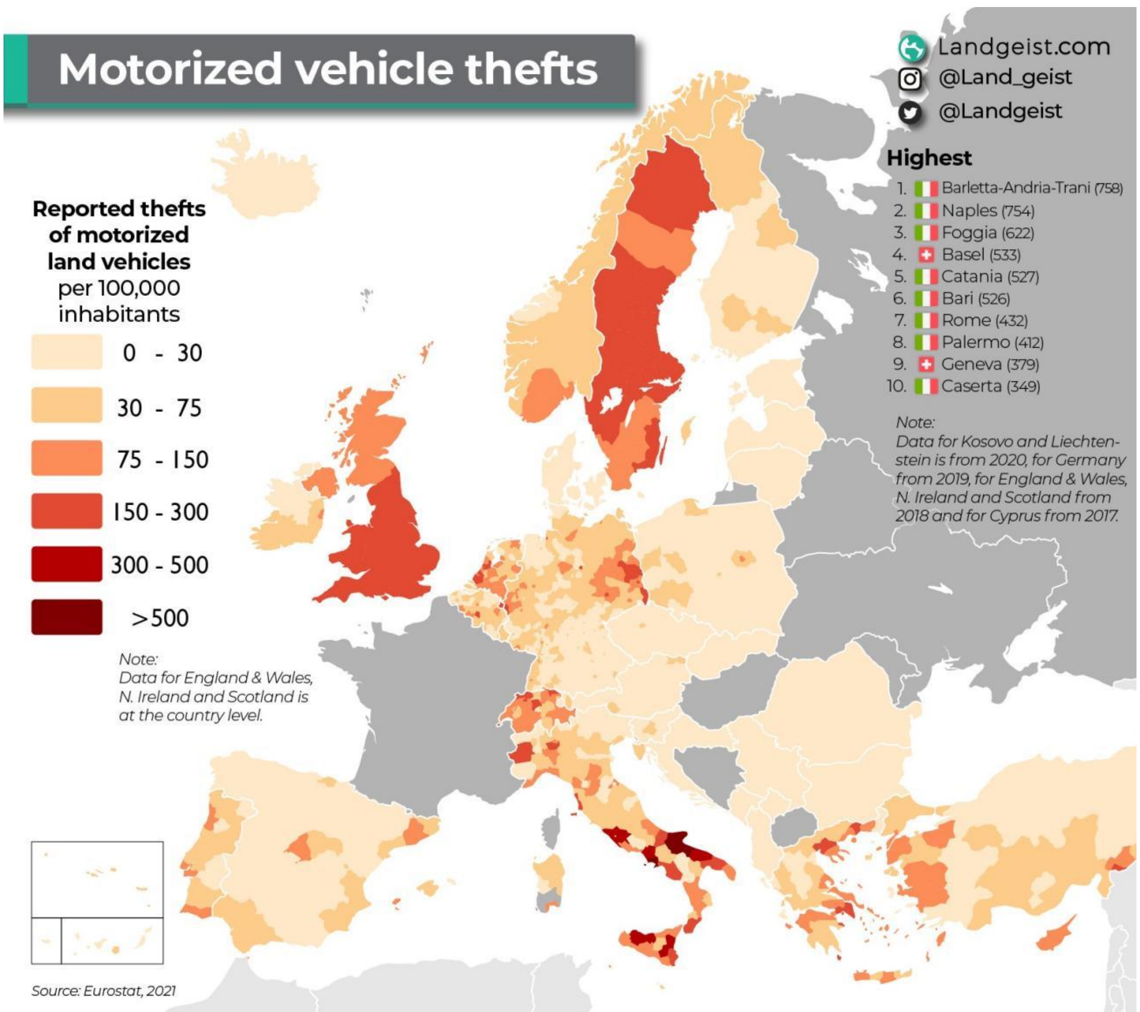


Figure 2. 1 Car theft rate in Europe (Landgeist, 2024)

Beyond North America and Europe, vehicle theft is also prevalent in other regions such as Asia, where densely populated urban areas and inadequate security infrastructure contribute to the vulnerability of vehicles. Countries like India and China have reported significant numbers of vehicle theft incidents, highlighting the need for comprehensive security solutions to protect vehicle owners' assets and enhance public safety (Saritha & Arun, 2018).

The economic impact of vehicle theft extends beyond the direct loss of vehicles. Insurance companies bear a significant financial burden due to payouts for stolen vehicles, leading to higher premiums for policyholders and increased operating costs for insurance providers (Konatham et al., 2023). Moreover, businesses reliant on transportation and logistics face disruptions and financial losses when their vehicles are stolen, affecting productivity and profitability.

In addition to economic losses, vehicle theft also poses safety risks to individuals and communities. Stolen vehicles can be used in other criminal activities such as smuggling, trafficking, or even terrorist attacks. Moreover, unauthorized access to vehicles can compromise personal safety if intruders gain access to sensitive information or valuables left inside the vehicle (Dhir et al., 2010).

The need for biometric security solutions arises from the limitations of conventional anti-theft measures such as mechanical locks, alarms, and immobilizers. While these measures provide some level of deterrence, determined thieves can bypass them using various techniques such as lock picking, hacking, or using counterfeit keys (Villa et al., 2018).

Biometric vehicle security systems offer a more robust and reliable approach to theft deterrence by leveraging unique physiological or behavioral characteristics of individuals for authentication and access control. By requiring biometric authentication for vehicle access, these systems significantly reduce the risk of unauthorized entry and theft (Dhir et al., 2010).

In a nutshell, vehicle theft statistics underscore the urgent need for effective security solutions to mitigate economic losses and safety risks associated with this crime. Biometric vehicle security systems represent a promising technological advancement in this regard, offering enhanced protection against theft.

### 2.2 Biometric Vehicle Security System

Biometric vehicle security systems represent a cutting-edge approach to enhancing security in the automotive industry. By leveraging unique physiological or behavioral characteristics shown in figure 2. 2, such as fingerprints and facial features, these systems provide robust authentication and access control mechanisms (Villa et al., 2018).

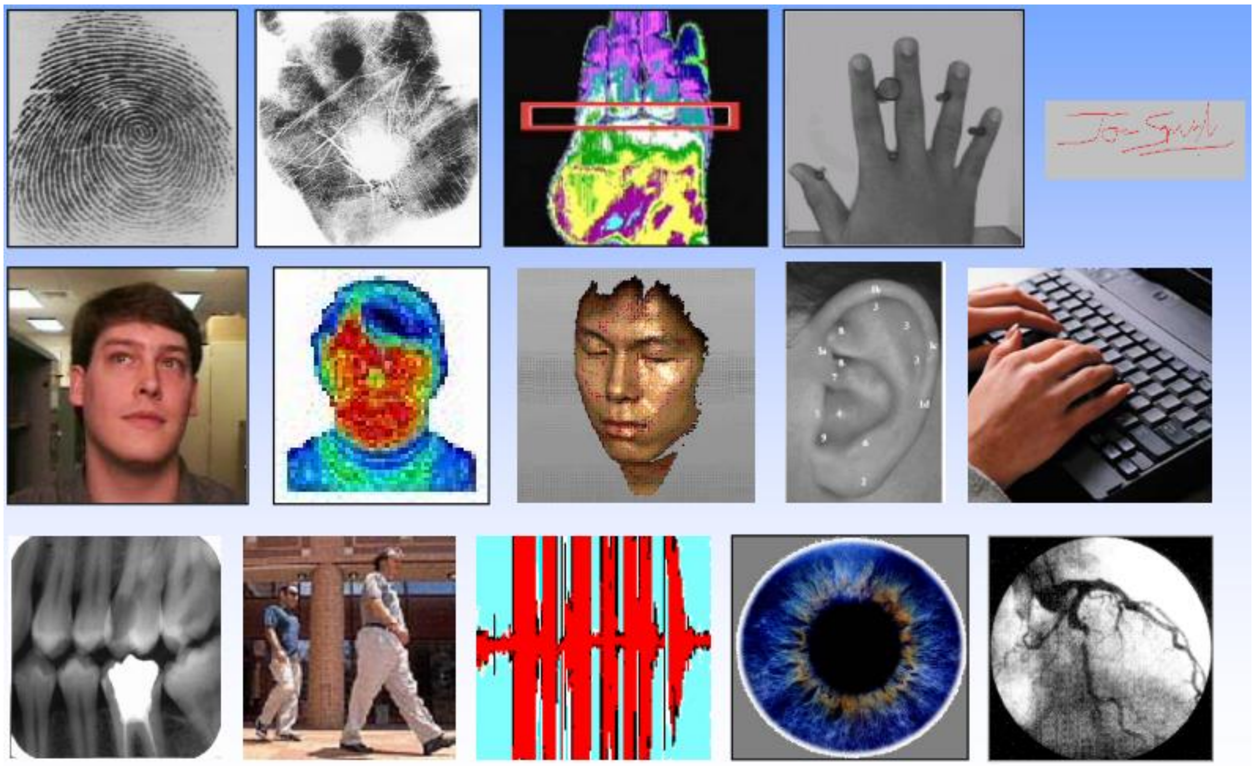

Figure 2. 2 Types of biometric modalities (Wirtz, 2004)

The next section explores the working principle, detailed architectures, and performance comparisons of two primary biometric modalities used in vehicle security: fingerprint and face recognition (Khan et al., 2005).

#### 2.2.1 Definition and Types of Biometric Vehicle Security Systems

Biometric vehicle security systems utilize biometric technologies to verify the identity of individuals attempting to access vehicles, see figure 2. 3. The two most common biometric modalities employed in these systems are fingerprint and face recognition.

- **Fingerprint Recognition:** involves capturing and analyzing the unique patterns present in an individual's fingerprints. These patterns, known as minutiae, include ridge endings, bifurcations, and ridge dots, which are used to create a unique fingerprint template for each individual. Fingerprint recognition systems typically consist of a fingerprint sensor, image processing software, and a database for storing and comparing fingerprint templates (Francesco Turroni, 2012). Hyundai was the first to adopt this to the Santa Fe model, as shown in figure 2. 3.

Figure 2. 3 Hyundai Santa Fe with the first automobile fingerprint (Hyundai, 2018)

- **Face Recognition:** Face recognition technology identifies individuals based on facial features captured by cameras installed within the vehicle. Facial recognition algorithms analyze various facial characteristics, such as the distance between eyes, nose, and mouth, to create a unique facial signature for each individual. Face recognition systems typically include image capture devices, feature extraction algorithms, and matching algorithms for comparing facial signatures with stored templates (Sardar et al., 2024).

### 2.2.2 Detailed Architecture of Biometric Vehicle Security Systems

Fingerprint recognition architecture is arranged as follows (Rafay et al., 2019):

- **Fingerprint Sensor:** The system begins with the capture of a fingerprint image using a fingerprint sensor. This sensor may be capacitive, optical, or ultrasonic, depending on the technology employed.
- **Image Processing Software:** The captured fingerprint image is processed to extract key features or minutiae, such as ridge endings and bifurcations.
- **Template Creation:** The extracted features are used to create a unique fingerprint template for the individual, which is stored in a database.

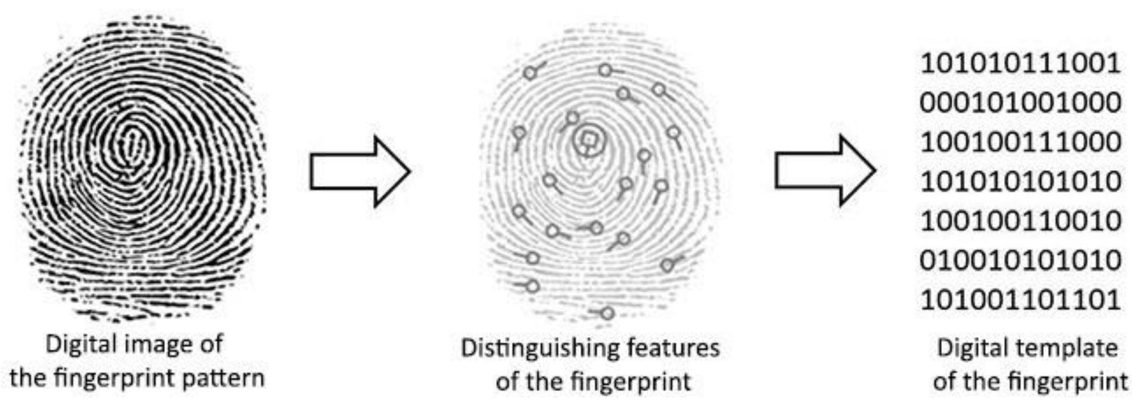


Figure 2. 4 Fingerprint digital template generation (Bayometric, 2024)

- **Matching Algorithm:** When an individual attempt to access the vehicle, their fingerprint is captured and compared against the stored templates using a matching algorithm.
- **Access Control:** If the captured fingerprint matches any of the stored templates within a predefined threshold, access to the vehicle is granted. The details can be seen in figure 2. 5.

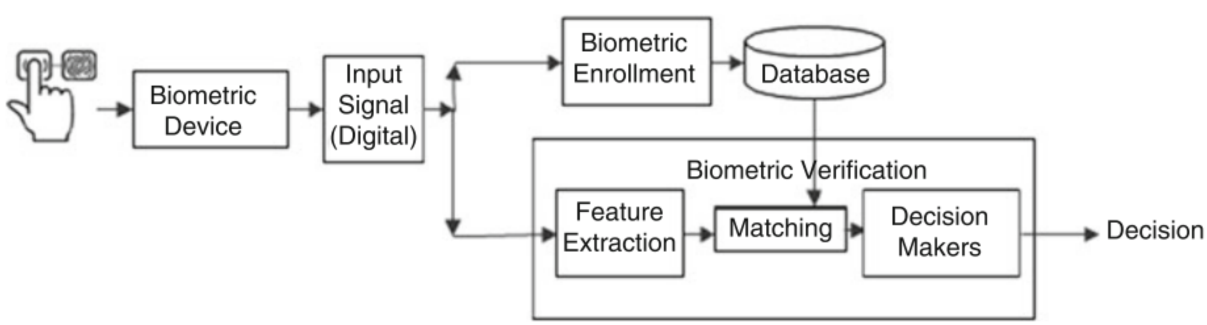


Figure 2. 5 Biometric authentication architecture (Obaidat et al., 2018)

Regarding the working principle, different types of fingerprint sensors are available namely optical, capacitive and ultrasonic type as presented in figures 2. 6, 2. 7 and 2. 8, respectively.

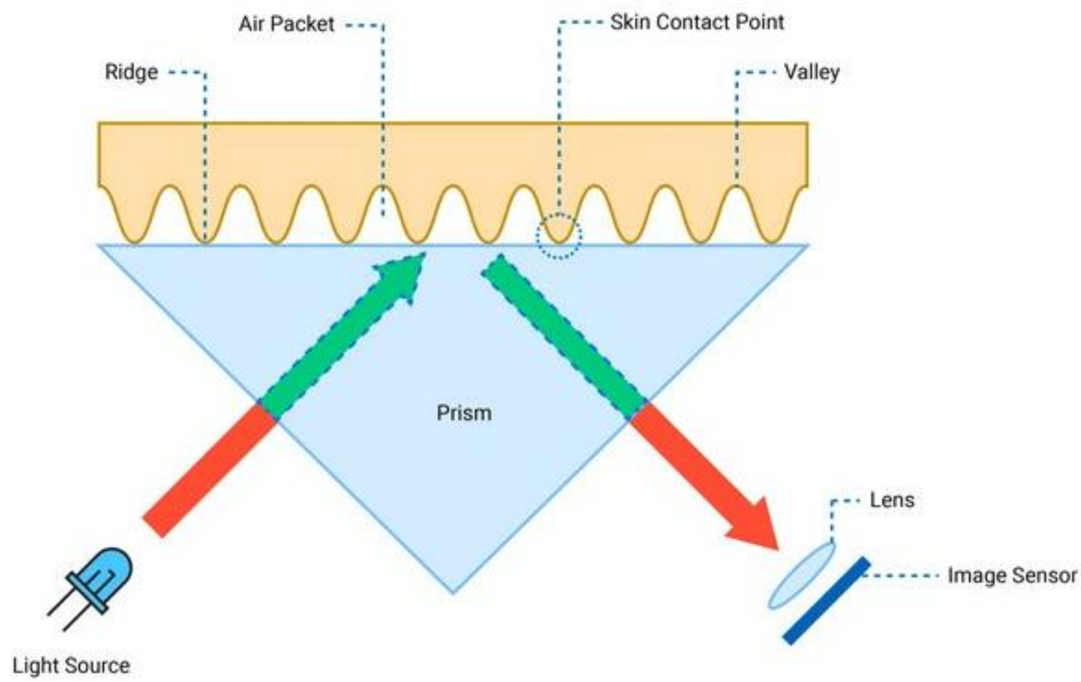


Figure 2. 6 Optical fingerprint sensor (Adafruit, 2024)

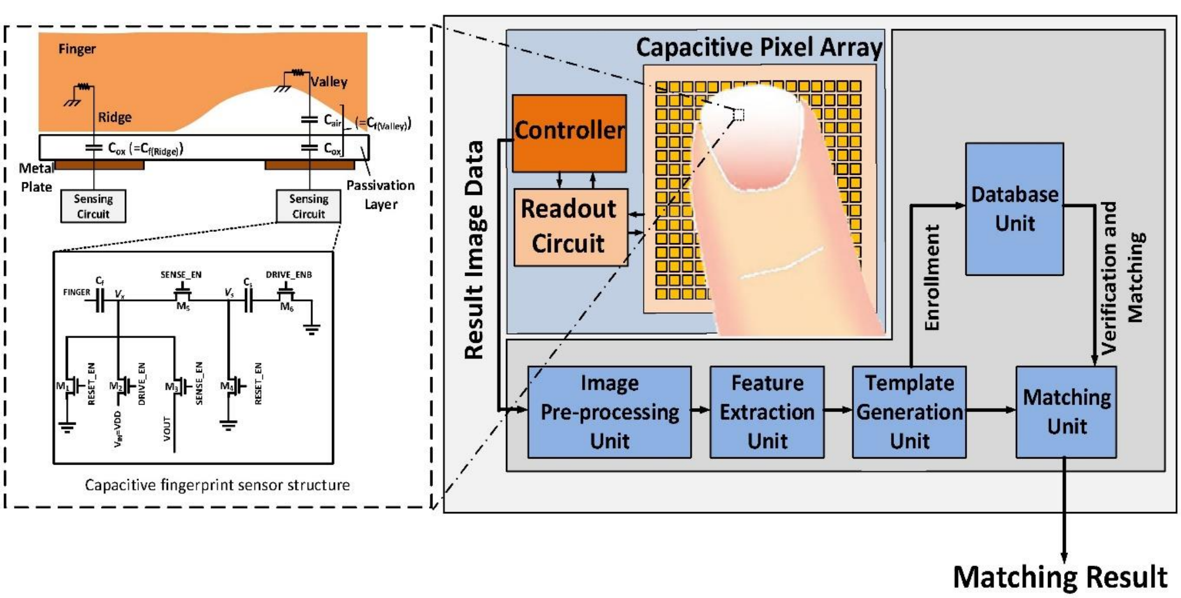


Figure 2. 7 Capacitive fingerprint sensor (MDPI, 2018)

The optical sensor in figure 2. 6 uses light to capture fingerprint pattern. While the capacitive sensor in figure 2.7 relies on static electricity on fingertips. Yet, the ultrasonic type in figure 2. 8 emits ultrasonic sound wave and listen to the echo bounce to determine the fingerprint in 3D.

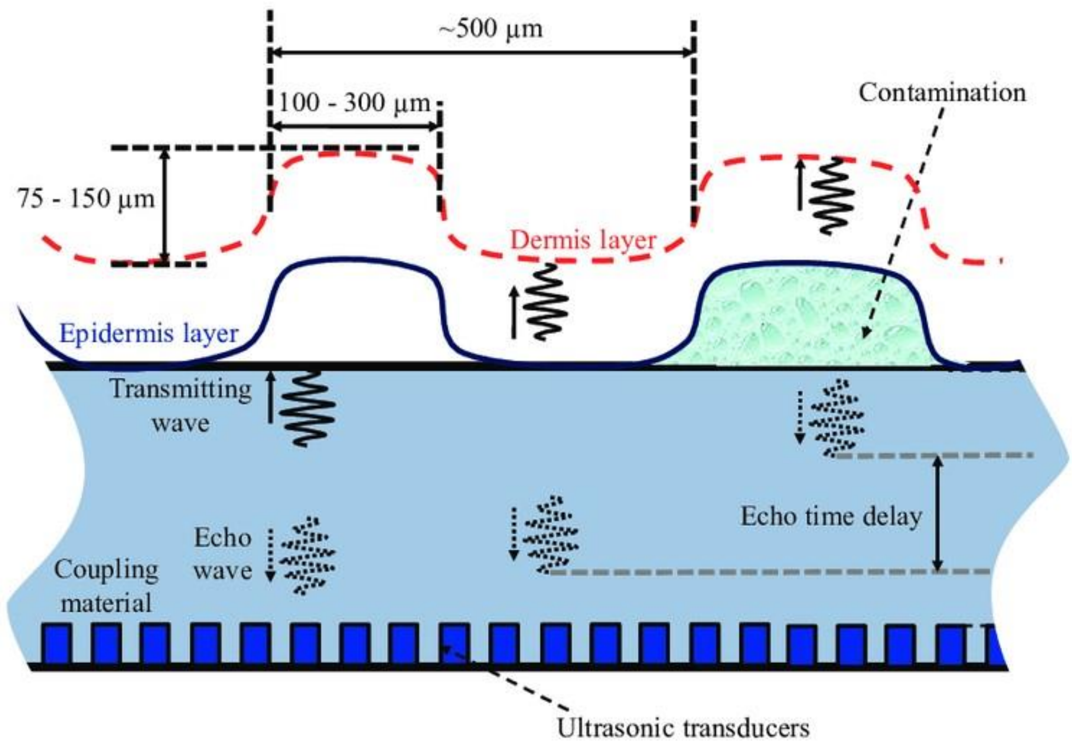


Figure 2. 8 Ultrasonic fingerprint sensor (ResearchGate, 2015)

Face recognition architecture is arranged as follows (Zamin et al., 2022):

- **Image Capture Devices:** Facial recognition systems utilize cameras installed within the vehicle to capture images of individuals attempting to access the vehicle.
- **Feature Extraction Algorithms:** These algorithms analyze the captured facial images to extract key features such as the position of eyes, nose, mouth, and facial contours. See the neural network algorithm in figure 2. 9.
- **Facial Signature Creation:** The extracted features are used to create a unique facial signature or template for each individual.
- **Matching Algorithms:** When an individual attempt to access the vehicle, their facial signature is compared against the stored templates using matching algorithms.
- **Access Control:** If the captured facial signature matches any of the stored templates within

a predefined threshold, access to the vehicle is granted.

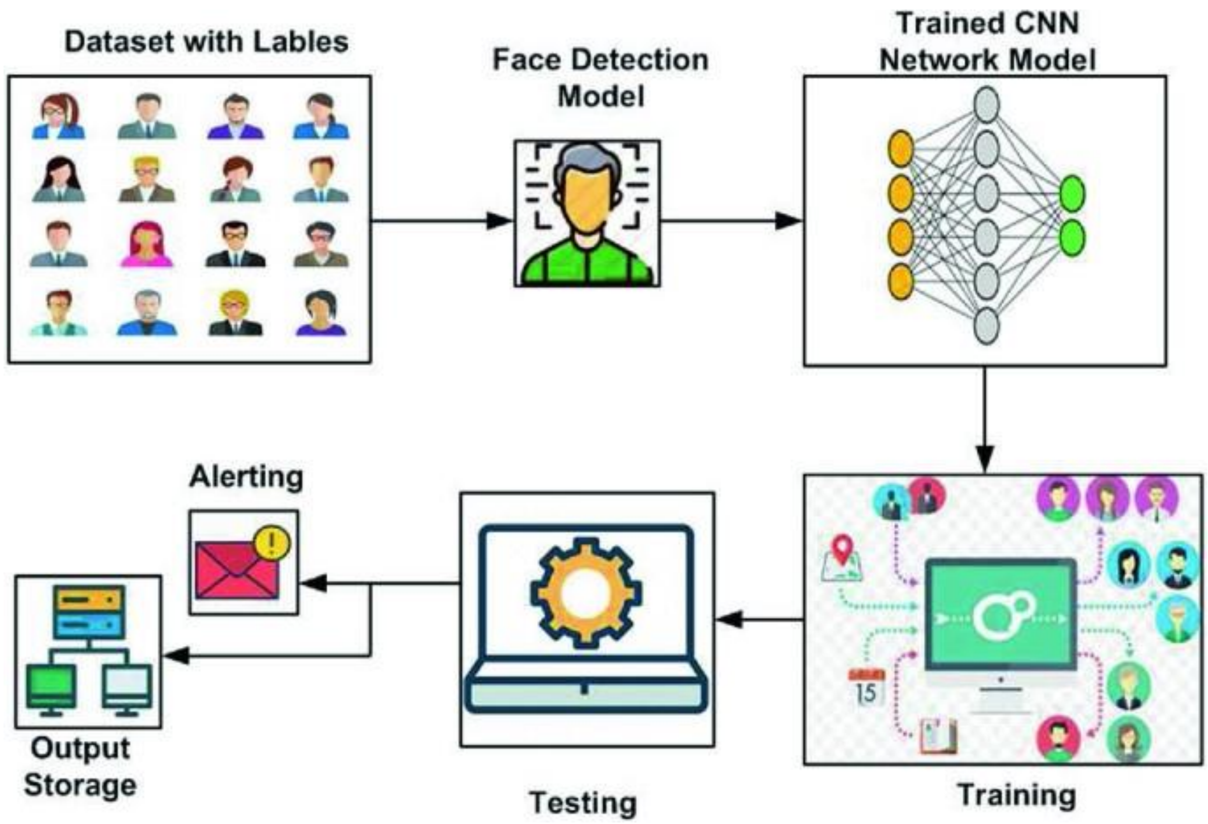


Figure 2. 9 Face recognition system using CNN (Springer, 2020)

### 2.2.3 Performance Comparison between Fingerprint and Face Recognition

- **Accuracy:** Fingerprint recognition systems typically offer higher accuracy rates compared to face recognition systems. This is because fingerprints exhibit greater uniqueness and stability over time, leading to more reliable authentication outcomes.
- **Speed:** Fingerprint systems are generally faster than face recognition systems in terms of user authentication. Fingerprint recognition algorithms can process rapidly, enabling quicker access to the vehicle.
- **Robustness:** Fingerprint recognition systems are more robust against environmental factors such as lighting conditions, dirt, and moisture. In contrast, face recognition systems may encounter challenges in low-light environments or when individuals wear accessories such as hats or sunglasses.

- **Spoofing Resistance:** Fingerprint recognition systems are susceptible to spoofing attacks using fake fingerprints or molds. In comparison, face recognition systems may be vulnerable to spoofing using photographs or masks, although advanced techniques such as liveness detection can mitigate this risk.
- **User Acceptance:** Face recognition systems are often perceived as more user-friendly and non-intrusive compared to fingerprint recognition systems, as they do not require physical contact with sensors. However, individual preferences may vary based on cultural and personal factors.

Table 2. 1 Comparison between different biometric modalities (ResearchGate, 2019)

| Modalities | Accuracy | Ease to Use | User Acceptance | Speed | FAR (%) | FRR (%) |
|---|---|---|---|---|---|---|
| Facial | Medium | High | High | Medium | 1% | 20% |
| Iris | High | Medium | Medium | Medium | 2% | 2% |
| Fingerprint | High | High | High | High | 0.94% | 0.99% |
| Voice | Medium | High | medium | High | 2% | 10% |
| Signature | Medium | Medium | Medium | High | - | - |
| Hand scan | Medium | High | Medium | High | 2% | 2% |

In summary, both fingerprint and face recognition technologies offer unique advantages and challenges in the context of biometric vehicle security systems, as presented in table 2. 1. While fingerprint recognition excels in accuracy, faster authentication and robustness, face recognition offers greater user acceptance. The choice between these modalities depends on factors such as security requirements, environmental conditions, and user preferences.

### 2.3 Selecting the Best Biometric Modality for Vehicle Security Systems

Selecting the most suitable biometric modality for vehicle security systems is a crucial decision that impacts the effectiveness, usability, and overall performance of the system. This section explores the factors to consider when choosing between fingerprint and face recognition modalities from the perspective of vehicle security applications.

- **Accuracy and reliability:** are paramount considerations when selecting a biometric modality for vehicle security systems. Fingerprint recognition systems typically offer higher accuracy rates compared to face recognition systems. Fingerprint patterns are highly unique and stable over time, resulting in reliable authentication outcomes (Al-Assam et al., 2011). In contrast, face recognition systems may exhibit variability in accuracy due to factors such as changes in facial appearance (e.g., aging, hairstyles) and environmental conditions (e.g., lighting, angle of view) (Sardar et al., 2024). However, advancements in facial recognition algorithms and sensor technologies have improved the accuracy and reliability of face recognition systems in recent years.

- **Environmental factors:** play a significant role in the performance of biometric modalities in vehicle security applications. Fingerprint recognition systems are generally more robust against environmental conditions such as lighting variations, dirt, and moisture. Capacitive fingerprint sensors, for example, are less susceptible to environmental interference and offer reliable performance in various conditions (Arora & Bhatia, 2022). In contrast, face recognition systems may encounter challenges in low-light environments or when individuals wear accessories such as hats or sunglasses. However, advances in sensor technology, such as infrared and depth-sensing cameras, have enhanced the robustness of face recognition systems in challenging environments.

- **User acceptance and convenience:** are essential factors in the adoption and usability of biometric vehicle security systems. Face recognition systems are often perceived as more user-friendly and non-intrusive compared to fingerprint recognition systems. Facial recognition does not require physical contact with sensors, making it more hygienic and comfortable for users. Additionally, face recognition allows for seamless and passive authentication, where users can be identified without explicit interaction with the system (Al-Assam et al., 2011). In contrast, fingerprint recognition requires users to place their fingers on sensors, which may be perceived as less convenient, especially in adverse weather conditions or when wearing gloves.

- **Spoofing and security vulnerabilities:** are critical considerations in the selection of biometric modalities for vehicle security systems. Fingerprint recognition systems are susceptible to spoofing attacks using fake fingerprints or molds. However, advancements in fingerprint sensor technology, such as capacitive sensors with live finger detection capabilities, have improved resistance to spoofing attacks (Dhir et al., 2010). Face recognition systems may be vulnerable to spoofing using photographs or masks, although advanced techniques such as liveness detection can mitigate this risk. Additionally, multi-factor authentication methods combining biometric modalities (e.g., fingerprint and face recognition) can enhance security and resilience against spoofing attacks.

- **Cost and implementation complexity:** are practical considerations that influence the selection of biometric modalities for vehicle security systems. Face recognition systems involve higher initial costs due to the camera sensor technology and need for capable image processing algorithms and controllers (Khairnar & Khairnar, 2018). Advancements in sensor manufacturing and economies of scale have contributed to reducing the cost of fingerprint sensors over time. Face recognition systems require additional hardware components such as high-resolution cameras and processing units, increasing implementation costs (Pawar & Rizvi, 2018). However, the availability of off-the-shelf face recognition software and libraries (Tippannavar et al., 2023) has simplified integration and reduced development costs for face recognition applications.

In summary, selecting the best biometric modality for vehicle security systems requires careful consideration of factors such as accuracy, environmental robustness, user acceptance, security, cost, and implementation complexity. While fingerprint recognition offers higher accuracy and robustness, face recognition provides greater user acceptance and convenience. Ultimately, the choice between these modalities depends on the specific requirements, constraints, and priorities of the vehicle security application.

### 2.4 Face recognition algorithm

Convolutional neural network (CNN) has several applications, including facial recognition, object detection, and categorization. It finds applications in speech recognition, natural language processing, image processing, restoration, and bioinformatics. CNN efficiently analyzes objects and requires minimal pre-processing for detection and classification (Alzubaidi et al., 2021). As a result, it is best suited for face recognition purpose. CNN consists convolutional, pooling, activation function, and completely connected layers to make up the primary four layers correlated in figure 2. 5.

- **Convolutional Layer:** The convolution layer is the inspiration for CNN. It extracts a feature map from the input image through a matrix operation. By gradually moving a filter across the image, multiplying corresponding values and adding them up, a smaller new matrix is generated from the input picture.

- **Pooling Layer:** The pooling layer follows the convolutional layer. It reduces feature map dimensionality, introduces translation invariance, and decreases learnable parameters. After the convolution process, a feature map is obtained. The pooling layer scales down this feature map, typically using a 2x2 filter.

- **Activation Function:** In deep learning, tasks like image classification, object recognition, and detection rely on non-linear activation functions within CNN architecture. These functions determine operability by calculating weighted sums and applying bias. Different types of activation functions exist, and selecting the optimal one enhances the learning process (Traore et al., 2021).

    - **Softmax:** is frequently used for decision-making tasks, similar to sigmoid activation function tasks. The input variable is given a number based on their weight, and their sum equals one.
    - **ReLU:** is with a number range of 0 to infinity that is currently most commonly used.
    - **Sigmoid:** It has long been a very well-liked activation mechanism. The function changes between 0 and 1 depending on the input. Similar to this, an input value greater than 1 changed to 1, and an input value less than 0 changed to 0.

- **Fully Connected Layer (Dense layer):** is a crucial element of CNN that effectively recognizes and categorizes an image using computer vision. The input image is fed into the CNN algorithm, which breaks down the image into a feature and analyzes it separately after passing through the conv. and pool strata. In order to classify a picture, the yield of the pooling level is flattened by the dense layer.

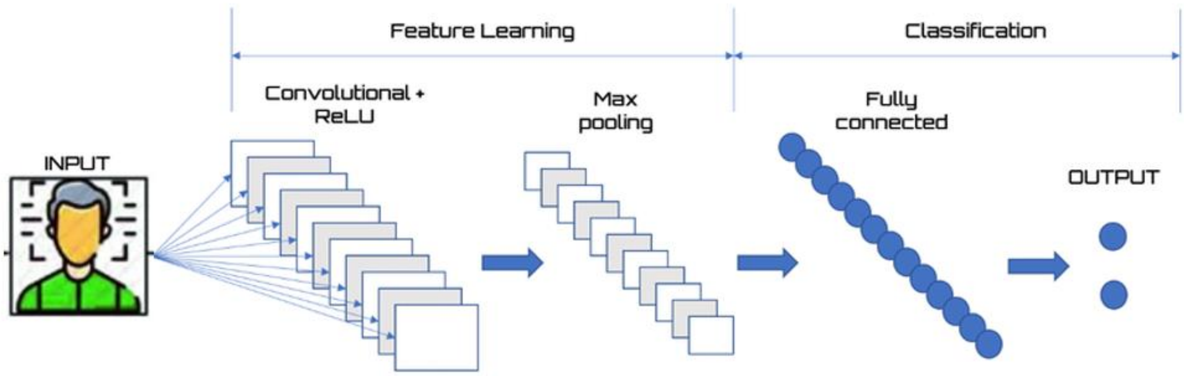


Figure 2. 10 CNN architecture (ResearchGate, 2020)

### 2.5 Use of IoT for Vehicle Security and Theft Deterrence

In recent years, the integration of (IoT) technologies has revolutionized vehicle security systems, enhancing their capabilities for theft deterrence and location tracking. This section explores the use of IoT, specifically GSM and mobile applications, in biometric vehicle security systems.

#### 2.5.1 Overview of IoT in Vehicle Security

IoT technology enables the connectivity of physical devices and systems over the internet, allowing them to collect, exchange, and analyze data in real-time (Obaidat et al., 2018). In the context of vehicle security, IoT facilitates seamless communication between vehicles, owners, and external monitoring systems, enabling proactive security measures and rapid response to security breaches (Pawar & Rizvi, 2018).

#### 2.5.2 GSM Integration for Remote Monitoring and Control

GSM technology enables cellular communication between vehicles and remote monitoring centers or mobile devices (Chandran et al., 2023). By integrating GSM modules into vehicle security systems, owners can remotely monitor and control various security features (Ramesh et al., 2019), including:

- **Remote Locking and Unlocking:** Owners can lock or unlock their vehicles remotely using a mobile app or SMS commands. This feature provides added convenience and flexibility for vehicle access control, especially in emergency situations.

- **GPS Tracking:** enabled vehicle can provide real-time location tracking and geo-fencing capabilities. Owners can monitor the location of their vehicles and receive alerts if they deviate from predefined boundaries, enabling quick recovery in the event of theft.

- **Alarm Activation:** In the event of unauthorized access or security breaches, GSM-enabled systems can trigger alarms and send alerts to owners or monitoring centers. This immediate notification facilitates prompt action to deter intruders and prevent further damage or theft.

- **Immobilization:** Some advanced vehicle security systems incorporate remote immobilization functionality, allowing owners or authorized personnel to remotely disable the vehicle's engine or fuel supply. This feature is particularly effective in thwarting theft attempts and recovering stolen vehicles.

### 2.5.3 Mobile App for Enhanced Security Features

Mobile applications play a central role in enhancing the functionality and usability of biometric vehicle security systems. By developing dedicated mobile apps, manufacturers can provide users with intuitive interfaces for managing security settings, accessing vehicle status, and receiving real-time alerts (Pawar & Rizvi, 2018)(Kumar et al., 2022). Key features of mobile apps for vehicle security include:

- **Secure Authentication:** Mobile apps enable users to authenticate themselves securely using biometric authentication methods such as fingerprint or face recognition. This ensures that only authorized individuals can access the app and control vehicle security settings.

- **Remote Monitoring:** Users can remotely monitor the status of their vehicles, including door lock status, engine ignition, and alarm activation. Real-time updates and notifications provide peace of mind and timely intervention in case of security incidents.

- **Event Logging and Reporting:** Mobile apps can log security events, including attempted break-ins, GPS tracking data, and system alerts. Users can review historical data and generate reports for insurance claims or law enforcement purposes.

- **Two-Way Communication:** Mobile apps facilitate two-way communication between users and their vehicles, allowing for remote interaction and control. Users can send commands to their vehicles, such as locking doors or activating alarms, and receive confirmation of successful execution.

### 2.5.4 Advantages of IoT Integration in Vehicle Security

The integration of IoT, GSM, and mobile app technologies offers several advantages (Malhotra et al., 2022) for biometric vehicle security systems:

- **Remote Accessibility:** Owners can access and control their vehicles from anywhere, using their smartphones or other connected devices. This remote accessibility enhances convenience and enables proactive security measures.

- **Real-Time Monitoring:** IoT-enabled systems provide real-time monitoring of vehicle status, allowing owners to stay informed about security events and take immediate action when necessary.

- **Enhanced Security Features:** GSM integration enables advanced security features such as remote locking, GPS tracking, and alarm activation, which enhance theft deterrence and facilitate vehicle recovery.

- **User-Friendly Interfaces:** Mobile apps offer intuitive and user-friendly interfaces for managing vehicle security settings, making it easier for users to interact with their vehicles and monitor security status.

In conclusion, the integration of IoT, GSM, and mobile app technologies enhances the functionality, accessibility, and security of biometric vehicle security systems. By enabling remote monitoring, control, and communication, these technologies provide owners with greater peace of mind and enable proactive measures to deter theft and protect valuable assets.

## 2.6 Prior Literature on Biometric and IoT Based Vehicle Security Systems

In recent years' significant advancements in biometric vehicle security systems and the integration of GSM, mobile app IoT security technologies were witnessed. This section presents a detailed review of prior literature, focusing on key developments, challenges, and future directions in the field.

The study by (Kiruthiga et al., 2015) presented protection to the vehicle against unwanted entry by utilizing a cost-effective fingerprint recognition technology. The car security system used GSM communication technology to notify the authoritative person (owner) of the vehicle's state. Access to vehicles is permitted only if the individual fingerprint is authenticated.

The system developed by (Bhargav et al., 2022) examines the driver's license using a facial recognition system that includes an Eigen-face algorithm. The camera records the driver's image and compares it to an existing database. If the results match, the system will proceed with fingerprint verification. The fingerprint module functions as the ignition key for the vehicle. If the fingerprint matches the previously enrolled dataset, the car's ignition is turned on. The experimental findings revealed that at threshold values of $3.2 \times 10^3$ and $3.5 \times 10^3$, the designed auto safety device achieves 98.3% accuracy in various illumination circumstances.

The system established by (Zamin et al., 2022) consisted of a facial identification system, a GPS, and an Android administration platform. The technology takes photos of the driver and compares them to a registry to figure out if he is an approved driver. The authors used Raspberry Pi circuitry to manage all of the events and build a face detection module using a sophisticated local binary pattern (LBPH) algorithm.

The suggested solution by (Elngar & Kayed, 2020), when it sensed someone who is not authorized inside the car, it will inform and communicate his image to the vehicle's owner and/or a police workstation via the Internet, as well as its position in the event that the vehicle in question goes missing or damaged. They achieved an accuracy of 98.2% on the ORL dataset and 99.6% when applied to their own dataset. It took the system 0.152 seconds for authentication under varied lighting circumstances when the threshold value was $3\times10^3$ and $3.50\times10^3$.

The embedded system developed by (Uma Maheswari et al., 2023) recognized fingerprints, OTP, and RFID. The microcontroller was equipped with a GSM. The mobile app displayed the progress of each activity, and the system sends each operation it performs to the IoT cloud. A magnetic key can be actuated when registered finger is detected, and any illegal access triggers an alert and sends the appropriate message notifications.

According to (Malhotra et al., 2022), if the fingerprints and RFID presented were legit, the control module initiates the ECM power circuit. Else if anyone tries to access the car in any other way, obtrusive warning messages with the car's position are sent to the owner's smartphone application via the cloud.

The system by (Sundararajan, 2022) relied of an Arduino Nano, an EM18 RFID, and an R305 fingerprint sensor. The RFID module validates the RFID tagging information before proceeding and the fingerprint sensor verifies the legitimacy of the fingerprint and initiates ignition.

The security system presented in (Muhammad Syarif Hartawan, 2022) shows the flow of operation is first to start, then to undergo detection, after which there are two choices: if yes, the car will turn on, it communicates a message to the owner of the vehicle, and the mechanism recognizes the precise whereabouts of the vehicle, after which the system ends, the automobile will recognize the owner straight away.

The motorcycle security system by (Hamidi et al., 2023) employed identification of fingerprints and Telegram notification. The reading duration is from 0.27 to 1 second depending on the cleanliness of the fingerprint sensor. If there is fingerprint grease before it, the reading will be sluggish.

According to (Konatham et al., 2023), if an individual desire to gain entry to the car, their fingerprint must match the one in the record. Otherwise, the individual might submit an OTP query to the proprietor. Drivers are constantly put in risk when driving alone in scenarios that might involve an emergency. If an emergency occurs while a car and driver are on the road, specific contacts can be signaled with the press of a button.

The suggested system by (Akshay et al., 2018) had three attributes: indication of the intruder, control of the vehicle, and the ability to recognize known users or distribute taken images of unknown people (intruders) via SMS and MMS. The suggested method notified the owner of the unlawful entrance via SMS. The Owner may prevent the car from starting via an SMS.

The tools used by (Khairnar & Khairnar, 2018) offered protection by sending an alarm message if something has been taken or relocated without the owner's knowledge. The system also provided frequent location updates to the authorized user via the IoT. GPS provides this option for tracking stolen vehicles. GSM technology is utilized to deliver warning notifications.

The security option offered by (Al-Assam et al., 2011) attempted to assess the efficacy of a two-factor biometric system under various presumptions regarding the safety of the non-biometric component. Three biometric traits—fingerprint, iris, and face—were assessed in three different situations. Biometric alone authentication, two-factor authorization with a biometric plus an encrypted key, and two-factor identification with a breached (stolen) user-based key.

A work by (Sadhukhan et al., 2017) employed fingerprint and RFID to verify the owner, and the control unit activates the ECM's powering channel; otherwise, if the thief tries to power up the car in any other means, the controller sends intervention alarm messages with the car's position to the owner's cellphone application via cloud.

The system presented by (Vikhankar, A D, 2016) indicated a Raspberry Pi based control. If an unauthorized individual attempted to take the car, the alarm will go off and the main control system will blackout immediately. In addition, a picture of the ill-fated individual will be captured, and the date, time, and anonymous face will be saved into an online database.

The work by (Dasani, 2022) addressed vehicle protection by developing a system comprising a microcontroller, and a fingerprint sensor. When an accredited fingerprint is detected, a user is able to assume command of the vehicle, and the engine's ignition mechanism commences. If it is an invader, the engine is never going to start.

To safeguard automobiles from burglary, (Taywade & Bhiwani, 2022) created a three-level security system. Finger print authentication, face recognition and alcohol detection system. Thus, including these elements advances the car's security and prevents theft.

A fingerprint-based motor vehicle safety system was developed by (Saritha & Arun, 2018) integrating the R307 fingerprint module with an Arduino UNO. An individual could power up the vehicle only after fingerprint authentication. When a fingerprint is identified, the valve in the fuel tank's outlet slips open permitting gasoline flow to the engine.

According to (Arabelli & Revuri, 2019), a user may run the car by tapping the thumb on a fingerprint reader, linked to the Raspberry Pi. The processor permits those who are authorized to operate the car. When an illegitimate person tries to start the car, a safety alarm will be triggered using the signals provided and the vehicle can be tracked via GPS.

The study by (Bukola, 2020) described an efficient vehicle protection system which incorporates GPS, GSM, and fingerprints for user recognition and verification. SMS requests will be used to immobilize the vehicle via relay, safeguarding them from robbery and illicit use.

Face recognition was used by (Anjana et al., 2022) to authenticate the user's identity. A camera installed inside the car captured the user's view and compare it to previously collected data. It searches for a match by comparing the information to a database.

A smart theft detection system by (Chandran et al., 2023) was presented that made use of GSM, GPS, Arduino, and fingerprint verification. The GPS module implies the vehicle's position in real time, while the GSM module urges the owner via text message or email if a probable robbery is identified. Furthermore, the fingerprint authentication method is employed to confirm the driver.

The Open CV FDS, which uses GPS and GSM module in conjunction with Arduino, is a low-cost safety device for autos. This system by (Akila et al., 2021) made it simple to recognize the thief and keep track the precise location of the car, which was quicker and more affordable than the prior approach.

The built-in system by (Pawar & Rizvi, 2018) employed biometric verification to access the car. A camera that captures one's picture before permitting or rejecting entry. In the event that vehicle entry is refused, the camera will collect pictures and communicate to its proprietor.

The suggested system by (Ramesh et al., 2019) complements fingerprint authentication to turn on the engine. To get entry to the car, the owner must use both fingerprint and the key. Regardless of whether only one of the two inputs is accessible, the car will not start. When a stranger attempt to start the car, the proprietor receives a warning SMS with the position coordinates.

The circuit's hardware prototype by (Yusuf et al., 2022) demonstrated that the sensitivity, specificity, and accuracy were 96%, 97%, and 97% respectively. This means that a could grant access to 96% of registered users while accurately denying 97% of unregistered users, but is unlikely to accept 4% of permitted users and grant access to 3% of unregistered users.

The approach suggested by (Srinivasan et al., 2021) allows access to the automobiles using a dactylogram scanner. If fingerprint authentication fails, the car is not turned on. The GSM module uses SMS to transmit the unauthorized entry attempt to the vehicle's owner. The average time for authorization before starting the car was 3.81 seconds.

The concept by (Tamilselvan et al., 2018) proposed a fingerprint based electronic engine ignition. Test findings revealed that the developed system identified the proper individual and authorized them to operate the motorcycle.

The prior literatures highlighted several advancements in biometric vehicle security systems, with a focus on improving authentication accuracy, enhancing user experience, and addressing security vulnerabilities. The studies have explored different biometric modalities, face recognition and fingerprint, for vehicle access control, demonstrating promising results in terms of accuracy and robustness. Additionally, research efforts have been directed towards multi-modal biometric systems that combine multiple biometric modalities, such as fingerprint and face recognition, to enhance security and mitigate spoofing attacks.

Furthermore, the studies have investigated the use of machine learning and artificial intelligence techniques for biometric template protection and secure authentication. For example, a deep learning-based approach for biometric template protection, leveraging transfer learning techniques (Kute et al., 2021). These advancements contribute to the development of more secure and privacy-preserving biometric vehicle security systems.

The integration of GSM and mobile app IoT security technologies has emerged as a critical area of research in enhancing the functionality and security of biometric vehicle security systems. The studies have focused on addressing security challenges associated with remote access, data transmission, and authentication in IoT-enabled vehicle security systems. Researchers also investigated the security vulnerabilities of GSM-enabled vehicle security systems, highlighting potential risks such as SIM card cloning, network interception, and remote hacking. Their study proposed encryption and authentication mechanisms to mitigate these risks and enhance the security of communication between vehicles and remote monitoring centers.

Moreover, the prior literatures have addressed security concerns related to mobile app-based remote control and monitoring of vehicle security systems. Studies explored security best practices for mobile app development, including secure authentication mechanisms, data encryption, and secure coding practices. Additionally, research efforts have focused on user-centric security measures, such as biometric authentication and two-factor authentication, to enhance the security of mobile app-based interactions with vehicle security systems.

The literatures reflected significant advancements and ongoing research efforts in biometric vehicle security systems, GSM, GPS, and mobile app IoT security. These advancements hold promise for enhancing the security, functionality, and user experience of vehicle security systems. Yet, each literature had their limitations presented in the summary table below. Despite significant advancements, several challenges remain in the development and deployment of biometric vehicle security systems GSM, GPS, and mobile app IoT technologies. Challenges are summarized in table 2. 2.

Table 2. 2 Literature summary

| No. | Author | Title | Methodology | Findings | Limitations or Gap |
|---|---|---|---|---|---|
| **1** | (Bhargav et al., 2022) | Real Time Vehicle Security System Using Face Recognition and Finger Print | Raspberry Pi, camera, face detection, RFID, fingerprint sensor | e-mail alert, alarm, 98.3% accuracy | No intruder clue, intruder can enter cabin unopposed, no location tracking, RFID tag can be lost |
| **2** | (Zamin et al., 2022) | Vehicle Anti-Theft Face Recognition System Based on IoT using Raspberry Pi4 | Raspberry Pi, camera, face detection, GPS, mobile app | Engine immobilization, intruder image clue | No night time function, no fingerprint, intruder can enter cabin unopposed, mobile app shows log in data only |
| **3** | (Elngar & Kayed, 2020) | Vehicle Security Systems using Face Recognition based on Internet of Things | Raspberry Pi, camera, face detection, GPS, PIR sensor, car lock mobile app | e-mail notification, engine immobilization, intruder image clue sent, 99.6% accuracy, 0.152 s response time | No night time function, no fingerprint, no alarm, mobile app only used for remote lock/unlock |
| **4** | (Saritha & Arun, 2018) | Fingerprint based security system for vehicles | Arduino UNO, R307 fingerprint module, fuel | Engine immobilization by disabling flow from the fuel | No alarm, No real-time alert, no location tracking, no |

| | | | | | |
|---|---|---|---|---|---|
| | | | tank valve lock | tank | intruder clue, intruder can enter cabin unopposed |
| **5** | (Anjana et al., 2022) | Smart Security System For Vehicle Anti-Theft | Arduino UNO, fingerprint module, camera | Fingerprint for door unlocking and face ID for engine starting | No alarm, no intruder clue, intruder can enter cabin unopposed, no location tracking, no alert to the owner during theft attempt, no nighttime functionality |
| **6** | (Chandran et al., 2023) | Smart theft detection of vehicles by GSM and GPS with fingerprint verification | Arduino UNO, fingerprint sensor, GSM, GPS, relay | SMS and e-mail alert | No alarm, no intruder clue, intruder can enter cabin unopposed |
| **7** | (Yusuf et al., 2022) | Simulation and Construction of Fingerprint Vehicle Starter System Using Microcontroller | Arduino UNO, R305 fingerprint module, buzzer | Engine control, alarm, 97% accuracy | No real-time alert, no location tracking , no intruder clue, intruder can enter cabin unopposed |
| **8** | (Srinivasan et al., 2021) | Development of keyless biometric authenticated vehicles ignition System | ATmega 162 controller, fingerprint module, GPS, GSM | SMS alert to owner, average authentication time 3.18 s, keyless access | No location tracking , no intruder clue, intruder can enter cabin unopposed |
| **9** | (Tamilselvan et al., 2018) | Design and Implementation of Biometric Based Smart Antitheft Bike Protection System | Arduino UNO, finger print scanner, OLED display, battery, relay, voltage regulator | Ignition control, 98% accuracy | No alarm, no location tracking, no intruder clue, intruder can enter cabin unopposed |

## 2.7 Research Gap

The current gap analysis lays the foundation for a critical exploration into the design of a biometric vehicle security system with a focus on theft deterrence and intruder identity communication. Through the extensive review of relevant literatures, numerous approaches were implemented to address theft. Nonetheless, some limitations in the vehicle security implementation have been identified. These challenges encompass a range of issues, including the lack of intruder identity clues for law enforcement after detecting intrusion, lack real-time location tracking capabilities, the face recognition based systems did not have nighttime functionality, and the mobile applications used had limited features such as displaying access data only or offering remote lock/unlock options without real-time alerts, location tracking and intruder clue information. Furthermore, the analysis highlights instances where the system's operation is hindered by dependencies on external factors such as power source, the availability of sufficient lighting conditions and cleanliness of finger tips. Besides, the presented systems focused on protecting the vehicle but nowadays forced theft with armed coercion is becoming a common thing threatening the driver’s life.

Expanding upon these identified challenges, it becomes evident that the presented vehicle security systems can be improved to provide comprehensive protection against theft and unauthorized access. The lack of effective intruder detection and communication mechanisms not only compromises the safety of vehicles but also hampers law enforcement's ability to respond swiftly to incidents of theft. Moreover, the absence of feature packed android app for intruder identification, real-time vehicle monitoring, location tracking and access control deprives vehicle owners of crucial tools needed to take timely action and recover stolen assets.

To address these shortcomings and bridge the identified research gap, this thesis aims to design a biometric vehicle security system that not only deters vehicle theft but also aids the driver’s safety in panic armed robbery situations by enabling real-time communication of intruder identities to relevant stakeholders. By means of leveraging advanced fingerprint and night mode capable face recognition biometric technologies for accurate identification and incorporating seamless communication protocols for instant alerts, the envisioned system seeks to enhance the landscape of vehicle security. Through the integration of intelligent biometric sensors, and feature packed android app, the proposed system aims to empower both authorities and vehicle owners in combating vehicle theft and enhancing overall safety.

In a nutshell, the research gap identified underscores the pressing need for strengthening solution options in vehicle security that prioritize real-time communication of intrusion and leverage integrated biometric authentication for enhanced protection. By addressing these challenges and designing a comprehensive security system, this thesis endeavors to contribute significantly to the advancement of vehicle security technologies and the reduction of theft-related crimes.

# CHAPTER THREE

# MATERIALS AND METHODS

This section discusses the tools utilized, and the research execution method used for designing the biometric security system.

## 3.1 Research method/process

To meet the thesis objectives, a series of activities are needed. Since the start of this thesis work the extent and depth of the existing vehicle theft problem, the existing solution and the unaddressed limitations of the prior works is identified. Then, the biometric modalities available are compared and contrasted in terms of suitability, ease of use, accuracy, user convenience, speed of response cost and availability for possible integration in to vehicle security. As per the literatures reviewed, fingerprint authentication and face recognition-based modalities are the best biometric modalities for vehicular use. For the fingerprint bloc, different types of modules are compared for vehicle security. The selected module is initiated to enroll the user's fingerprints and verification is made to ensure everything is on track. For the face recognition bloc, various algorithms are available. The convolutional neural network algorithm selected for vehicle use is trained using the facial image dataset of the user. Then, the fingerprint module with the enrolled fingerprint data and the trained face recognition algorithm are integrated to design the biometric vehicle security system. After that, the designed system is programmed to respond to various operational conditions like user authentication, vehicle control, security breach sensing, alarm and real-time communication. IoT based methods are used for enabling real-time communication. Then, the performance of the fingerprint module and the face recognition for vehicular security worth is evaluated. The outcome of this evaluation is metered. If the accuracy obtained exceeds 95% hardware implementation follows. Otherwise, go back to square one and refine. Figure 3. 1 shows the research flow in detail.

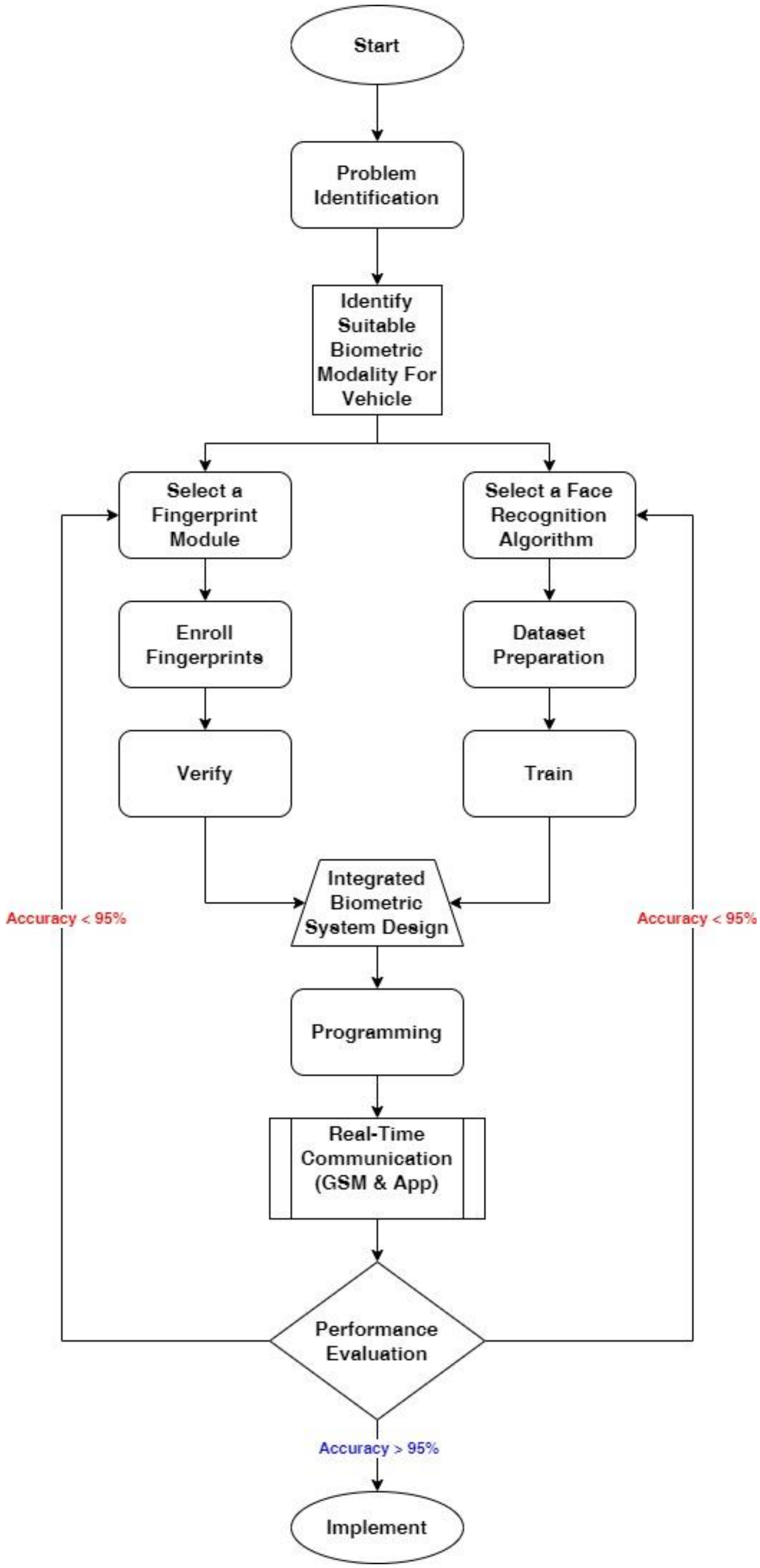


Figure 3. 1 Methodology flowchart

## 3.2 Materials

### 3.2.1 Software Tools

In order to effectively govern the biometric system, the various assortments of software tools listed below are employed.

- **Teachable Machine:** is a web-based tool for quickly and easily developing machine learning models. The original version went live in 2017. Using a Teachable Keras-based face recognition model can be developed and exported for further use (Carney & Webster, 2020; Godavari, 2022). Keras and Tensor Flow are the finest deep learning platforms (Bakr et al., 2022).

- **Google Colab:** is a free cloud-based platform provided by Google that allows users to write and execute Python code in a browser-based environment. It offers a Jupyter Notebook-like interface where users can write and execute Python code interactively, similar to how one would work with Jupyter Notebooks locally (Google Colab, 2020).

- **Raspberry Pi OS:** is required for Raspberry Pi to work. Previously Raspbian, was the officially supported operating system. The Raspberry Pi operating system is loaded on a micro SD card. (Ltd, 2024).

- **Arduino IDE:** The Arduino IDE is a cross-platform application that integrates a C++ code editor, the GNU C++ compiler, and a program upload utility. It's possible to work in real-time with the Arduino IDE, and the code can be moved to the Cloud for easy access (Arduino, 2024).

- **Mobile app development:** for the android app development the following tools were used:
    - Flutter mobile framework: for UI development
    - BLoC state management: helps separate the presentation layer from business logic, ensuring that the UI reacts to state changes rather than dictating or managing the state.

- Web socket: for real-time communication
- Express: for the backend

- **SFG Demo V2.0:** is a windows based software designed to enroll fingerprints and extract the digital fingerprint template signature in .bmp image format. See appendix A2 for more details.

- **VS Code:** is a scratch-cipher corrector Microsoft powers this software. The capabilities include code rewriting, snippets, syntax highlighting, intelligent code completion, and debugging aid. (Vol, 2016).

### 3.2.2 Hardware Tools

For commendable integration of the biometric system onto a vehicle, the hardware tools listed below are needed.

- **Camera**
  - The face data was collected using a 64 MP camera.

- **Computer System Specification**
  - Device brand: HP
  - Processor: Intel(R) Core(TM) i5-8350U CPU @ 1.70GHz 1.90 GHz
  - Installed RAM: 16.0 GB (15.8 GB usable)
  - System type: 64-bit operating system, ×64-based processor

- **Raspberry Pi 4 Model B**
  - For the realization of the facial recognition system, a separate board was needed, which was provided by the powerful Raspberry Pi 4 Model B (8 GB RAM version). (Pi, 2020).

- **Arduino board**
    - For the implementation of the fingerprint security and theft deterrence system Arduino UNO and MEGA boards are used.

- **A6 GSM/GPRS module**
    - In order to effectively relay the security status of the vehicle, a GSM module can give a quick call or text message to the owner instantly when unauthorized entries happen.

- **HC-SR04 ultrasonic sensor**
    - Is used for motion sensing purpose in the cabin of the vehicle. Once the vehicle has been locked and secured the ultrasound waves generated by the sensor can detect the presence of an individual in the cabin by measuring a change in obstacle distance echoing in the cabin.

- **Fingerprint module selection**
    - **R307 fingerprint module:** is a fingerprint sensor that can be connected directly to a microcontroller UART or a PC. It has a TTL UART interface and can store fingerprint data. The R307S fingerprint module has a storage capacity of 1000, a security level of 5, and a false rejection ratio of less than 0.1%. It also has a false acceptance ratio of less than 0.001% (Conti, 2017). The fingerprint module is widely used in security systems and access control systems. It has a UART interface that allows it to integrate with microcontrollers like Arduino and Raspberry Pi (Hangzhou Grow Technology Co., 2012).

    - **R307S fingerprint module:** is a newer version of the R307 module. Structurally similar, shown in figure 3. 2, except it is interfaced by using a more capable RS232 processing and a USB 2.0.

    - **FPM10A-DY50 fingerprint module:** is also an optical type sensor, shown in figure 3. 2, has the specs listed in table 3. 1 (Last & Edt, 2014):

Figure 3. 2 R307 (left), R307S (middle) and FPM10A-DY50 (right) fingerprint modules

Table 3. 1 Comparison between the three fingerprint modules

| | R307 | R307S | FPM10A-DY50 |
|---|---|---|---|
| **Sensor Technology** | Optical | Optical | Optical |
| **FAR (%)** | 0.001 | 0.001 | 0.001 |
| **FRR (%)** | 0.1 | 0.1 | 1 |
| **Processing Speed (Sec)** | 0.5 | 0.3 | 1 |
| **Power Consumption (mA)** | 50 mA | 50 mA | 120 mA |
| **Form Factor** | Slightly compact | Compact | Very compact |
| **Cost (USD)** | 22 | 24 | 18 |
| **Storage Capacity** | 250 | 1,000 | 162 |
| **Security Level** | 5 | 5 | 3 |
| **Compliance Certification** | Certified | Certified | Certified |

The comparison in table 3. 1, shows the difference in the three modules. Before selecting one module, a performance evaluation is conducted as detailed in section 3.3.5.

- **5V Relay module**
    - For effective vehicle immobilization, a relay module controls the engine by immobilizing ignition or fuel system when unauthorized entries happen.

- **IR LED**
    - For seamless nighttime face recognition and to capture clear intruder images in the dark, an infrared LED is used.

- **Vibration / Shock sensor**

- Is required to detect any forced entry attempts in to the vehicle and towing tilt.

### 3.3 Procedure

The following procedures are put in to action in order to realize the vehicular biometric system.

#### 3.3.1 Enrolling the vehicle user's fingerprint

The owner or driver authorized to operate the vehicle, must clean the module scanning area frequently from smudges and also need to keep his fingertips clean from dirt or sweat oil buildup before enrolling or authenticating with any finger. After deciding which fingers to use for authentication, run the Adafruit enroll code given in appendix A1, select ID number for each fingers and register the fingerprint following the given prompt. A total of 4 fingerprints, two index and two thumb prints from the left and right hand are enrolled in the process.

#### 3.3.2 Dataset preparation for face recognition

To verify the vehicle owner or driver using facial recognition, the face images necessary for the dataset were collected by capturing the owner in different outfits and lighting conditions, seen in figure 3. 3, as well as shots of other persons' face was taken for control purposes. A total of 8,000 images after augmentation is prepared for the face recognition use. The images were then equally divided into two classes of 4,000 images for each named Class 0: Authorized Driver and Class 1: Unauthorized Driver. Dataset pre-processing is the stage that occurs before training a face recognition model. This step is essential to transform a raw picture to the desired data format for training.

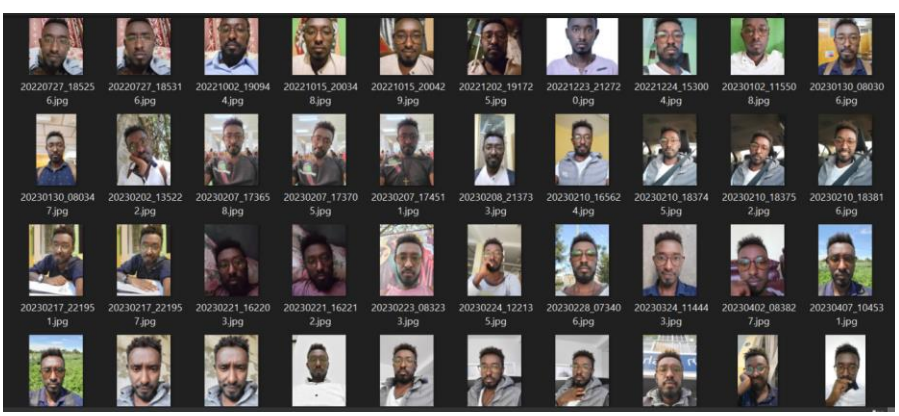

Figure 3. 3 Face images in different conditions for training the face recognition model

### 3.3.3 Face recognition model selection

Using the various hyper-parameters listed below, a deep learning convolutional neural network model for the available dataset number was adopted from the author's previous work (Marie & Huluka, 2023) to address the binary face recognition challenge.

```
[ ]  model = Sequential()
     model.add(Conv2D(32, (3, 3), activation='relu', input_shape=(150, 150, 3)))
     model.add(MaxPooling2D((2, 2)))
     model.add(Conv2D(64, (3, 3), activation='relu'))
     model.add(MaxPooling2D((2, 2)))
     model.add(Conv2D(128, (3, 3), activation='relu'))
     model.add(MaxPooling2D((2, 2)))
     model.add(Conv2D(128, (3, 3), activation='relu'))
     model.add(MaxPooling2D((2, 2)))
     model.add(Flatten())
     model.add(Dense(512, activation='relu'))
     model.add(Dense(1, activation='sigmoid'))
```

This deep learning CNN model has 11 layers, including:

1. Input level - The first coat in the model, defined by the **input_shape** argument of the first **Conv2D** cover, which is **(150, 150, 3)**. This means the input to the model is a 3-channel (RGB) image of size 150x150 pixels.
2. Convolutional layer - The first **Conv2D** sheet has 32 sifters of size 3x3, and applies the Rectified Linear Unit (ReLU) AF.
3. Pooling layer - A **MaxPooling2D** with a pool dimension of 2x2.
4. Convolutional level - The next **Conv2D** level has 64 sifters of size 3x3, and also smears the ReLU AF.
5. Pooling level - Additional **MaxPooling2D** sheet with a pool extent of 2x2.
6. Convolutional layer - The third **Conv2D** coat has 128 sifters of size 3x3, and also smears the ReLU AF.
7. Pooling layer - One more **MaxPooling2D** coat with a pool scope of 2x2.
8. Flatten layer - This sheet translates the yield of the prior coat into a 1-dimensional vector, which can be handed as involvement to the FC layers.
9. Fully connected layer - A **Dense** coat with 512 units and the ReLU AF.
10. Output layer - A **Dense** coat per a sole unit and the sigmoid AF. This coat spawns the

model's final output, a binary classification (0 or 1) signifying authorized face or not. Therefore, the overall amount of trainable parameter is about 3.5 million.

### 3.3.4 Face recognition model optimization

Due to the availability of three fingerprint modules and various hyper-parameters listed above, testing the efficiency of each module and tuning the available hyper-parameters is necessary to determine the best fingerprint module for vehicle use and the optimal hyper-parameters for best face recognizer model. Hyper-parameter optimization, sometimes called hyper-parameter tuning, is the challenge of choosing the optimal set of parameters for a learning system. The value of a hyper-parameter parameter is used to control the learning process. While other parameter values are learned, in contrast (Claesen & De Moor, 2015). The optimization algorithm, learning rate, loss function, number of iterations, and batch size are the hyper-parameters of the model. After doing numerous experiments, the value of each was set. There is no set method for configuring a model's hyper-parameters. Instead, alternative configurations can be utilized depending on the computing challenge. Because there is no universal formula for choosing excellent hyper-parameters, hyper-parameter tweaking is a time consuming process (Zhang et al., 2018). As a result, different hyper-parameter values are set in chapter four to train the face recognition model.

### 3.3.5 Biometric System Performance Evaluation

The reliability of using the selected biometric modalities for vehicle security needs to be quantified before deployment. As a result, we need to gauge the system performance using the following evaluation techniques.

- **Fingerprint module performance evaluation:** The performance evaluation determines the functioning of the fingerprint authentication device. This is done to ensure that the fingerprint module is reliable enough for integration in to vehicle security system. By enrolling user’s fingerprint and recording the True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) for each trials, the module accuracy can be quantified (Yusuf et al., 2022).

- **Face recognition model performance evaluation:** It's critical to evaluate a model's efficiency and efficacy. This is termed model evaluation. Assessment metrics such as recall, accuracy, and F1-score are used to decide which class an instance belongs to in computational issues such as classification and detection. Using categorization metrics to compute such measurements. The classification metrics reflect the model's performance in each class (Juba & Le, 2019). The True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) measures are all calculated using the confusion matrix. A result in which the model correctly predicted the positive class is assigned to a TP. A TN, like a TP, is an outcome in which the model accurately predicts the negative class. A FP occurs when the model incorrectly predicts the positive class. A FN occurs when the model incorrectly projects the negative class. All assessment metrics are summarized in to confusion matrix shown in table 3. 2.

Table 3. 2 Confusion matrix

| | **Positive** | **Negative** |
|---|---|---|
| **Positive** | TP | FP |
| **Negative** | FN | TN |

### 3.3.6 Operational decision flow of the system

The biometric system is an integration of a microcontroller based authorized authentication, access control, attempted theft detection, deterrence, real-time communication and android based control. As a result, a set of operational decision flow is needed for controlling the biometric security system. As shown in the figure 3. 4 below, there are three operation modes namely automatic, android and panic mode. The automatic mode will function by itself based on inputs from the sensors and the programming algorithm on the controller. The android mode will be controlled by the vehicle owner for access control and also during emergency situations to track lost vehicle and immobilize the engine. The panic mode is to be activated by the driver when he faces in-vehicle emergencies like accident or forced theft to contact family or police.

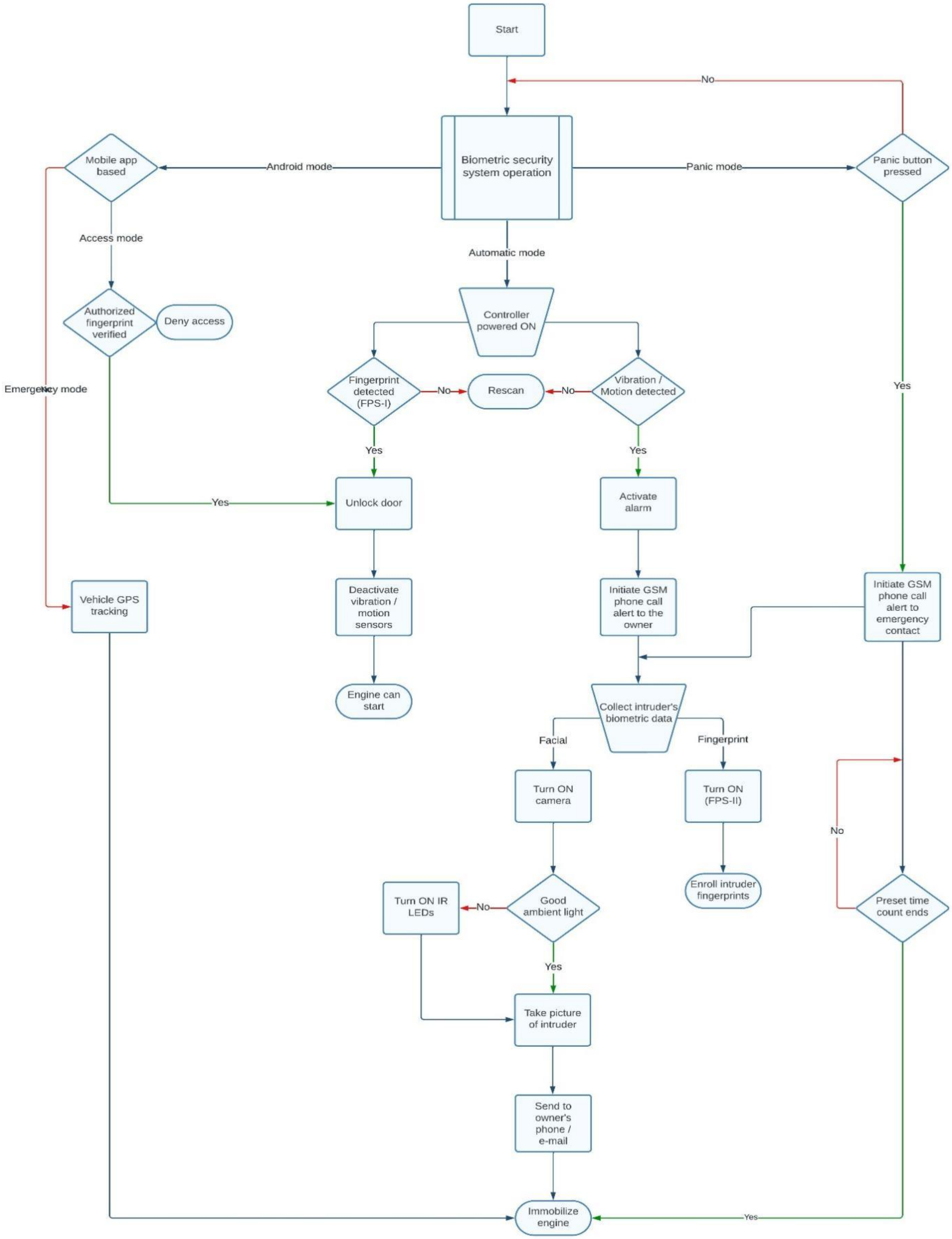


Figure 3. 4 Overall system operation/control flow

### 3.3.7 Programming

Following the system operation flow, C++ code is developed for controlling the fingerprint, alarm and GSM sub-systems using Arduino board. While the python code is used for the face recognition subsystem. The sample codes used are presented from A1- A3 in the appendix.

### 3.3.8 Control circuits

Based on the operation modes described in figure 3. 4, control circuitries are presented below. Figure 3. 5 shows the setup for connecting the fingerprint sensor to the microcontroller, the actuator relay for access control and engine starting.

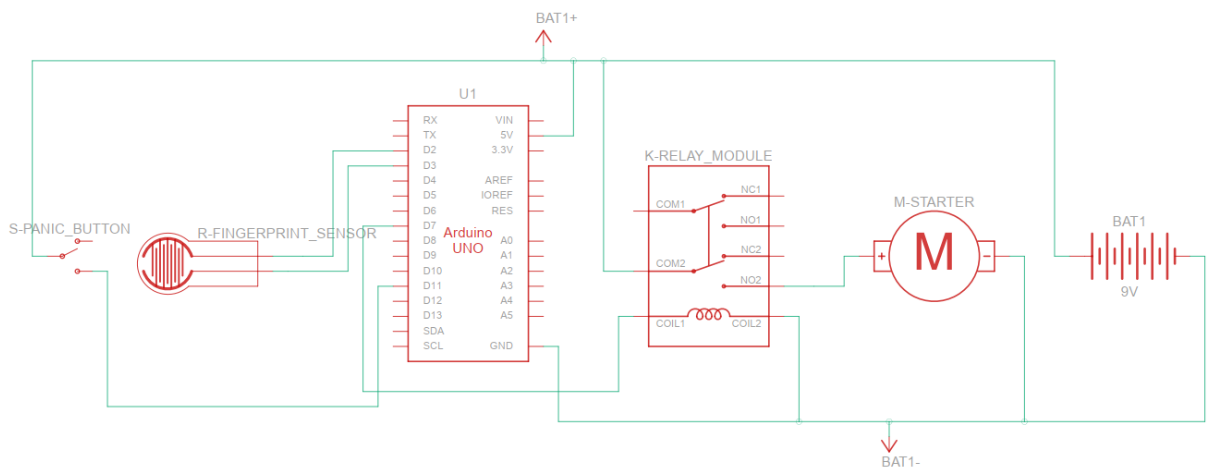


Figure 3. 5 Circuit diagram for fingerprint authentication and access control

The next figure 3. 6, shows the circuit for controlling the theft deterrence subsystem. As shown below, the ultrasonic motion sensor and the vibration/shock sensor detect unauthorized intruder action. As a result, the microcontroller initiates alarm and the GSM will make a quick alert phone call to the owner of the vehicle.

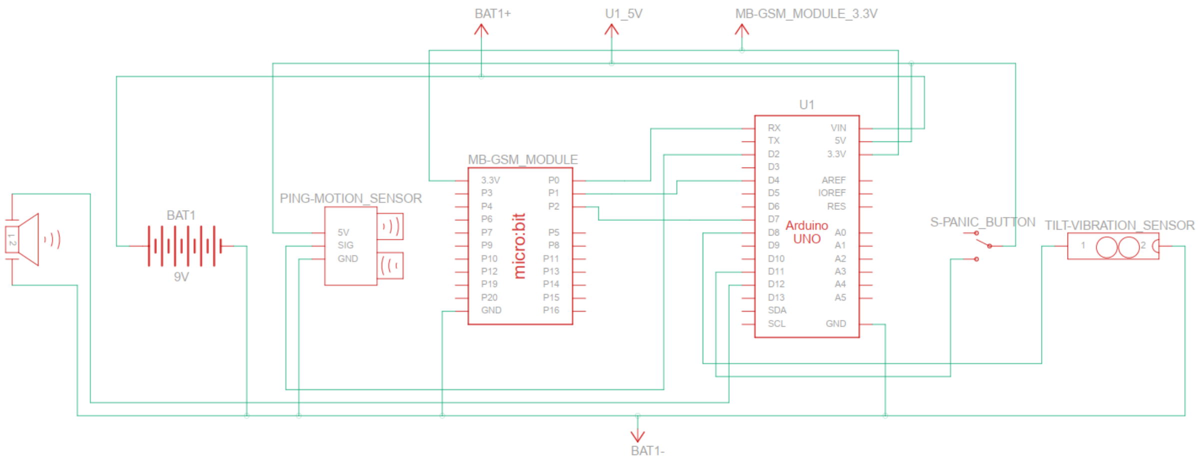


Figure 3. 6 Circuit diagram for theft deterrence and GSM control

The next figure 3. 7, shows the circuit diagram to illuminate the infrared LEDs. The light intensity sensor, presented as R, detect the ambient light. When light intensity falls below the camera working threshold, the transistor switch will turn ON the array of IR LEDs to enable the camera capture intruder images in low light conditions.

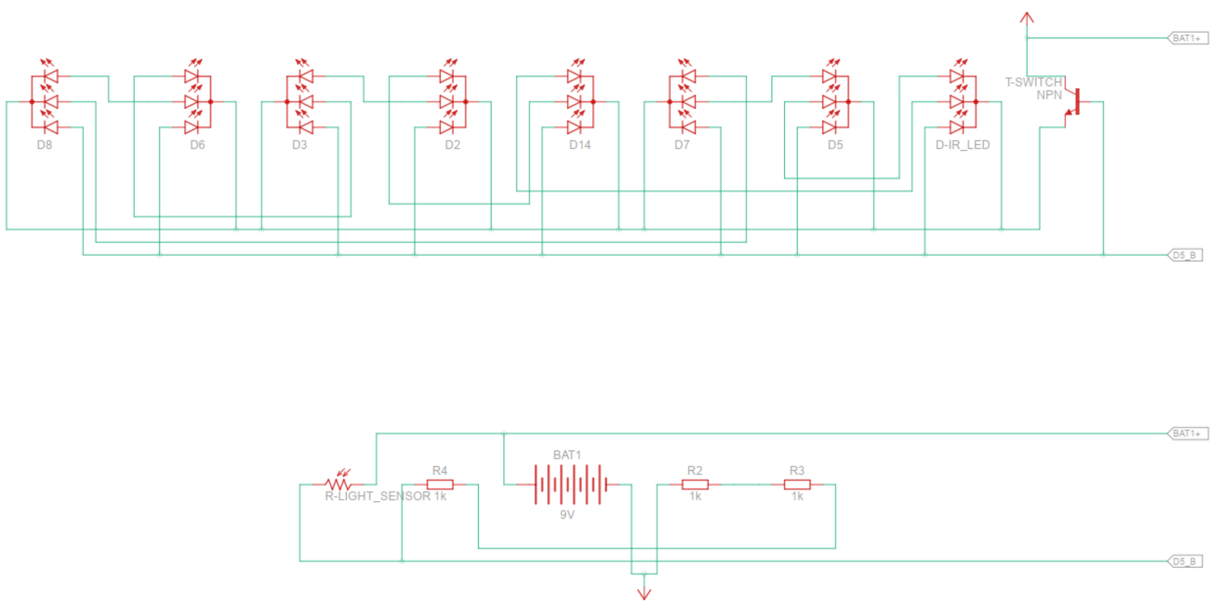


Figure 3. 7 Control circuit diagram for the nighttime IR LEDs

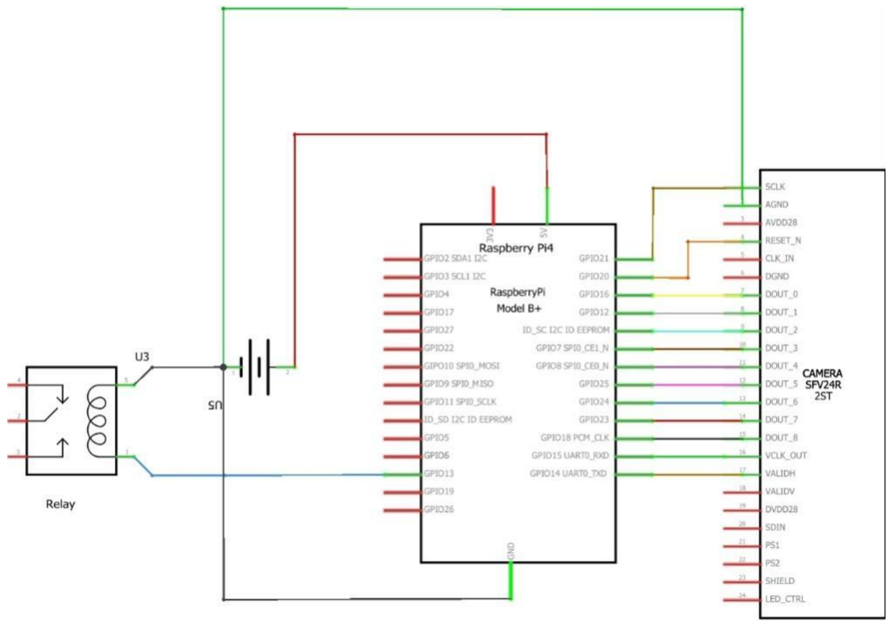


Figure 3. 8 Raspberry Pi control circuit for face recognition

Unlike the fingerprint authentication and theft deterrence subsystems, the face recognition needs high computation power control unit. Raspberry Pi 4B meets the needed requirement to process the face recognition algorithm. For enabling such function, the circuit diagram in the figure 3. 8 is used to control the face recognition based authentication. Furthermore, the same circuit is used to capture and communicate the intruder's image to the vehicle owner via the android app during theft attempts.

### 3.4 System Architecture

The nexus of sensors and actuators shown in the figure below are the building blocks of the biometric vehicle security system. The blueprints for the biometric vehicle security system schematics is presented in figure 3. 9.

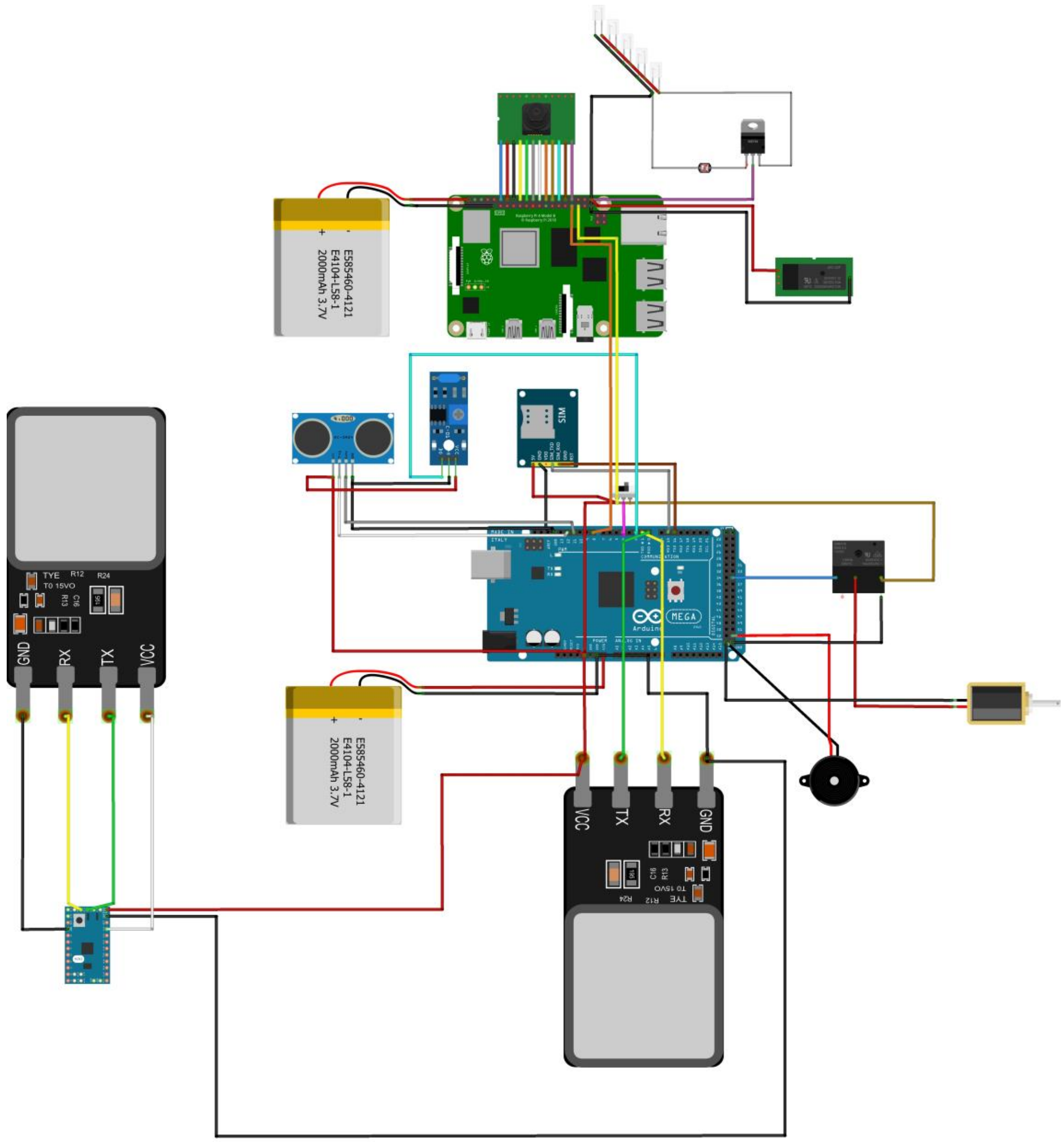


Figure 3. 9 The biometric security system control schematics and flow diagram

### 3.5 Biometric system optimization

#### 3.5.1 Fingerprint performance optimization

The performance optimization test determines which of the three R307, R307S and FPM10A-DY50 fingerprint modules is the best functioning fingerprint module. This is done to ensure that the selected fingerprint module works reliably for authentication purposes under different situations. To run the performance evaluation, ten (10) fingers from each hand are picked (four (4) enrolled fingerprints and six (6) unenrolled fingerprints). A total of 310 trials are conducted in five stages, with 10, 20, 40, 80 and 160 incremental trials per stage, as shown in table 3. 3. The true positive, false negative, true negative, and false positive for each module is recorded.

- **True Positive (TP)** = The number of valid users the system appropriately accepted.
- **False Negative (FN)** = The number of valid users the system inappropriately denied.
- **True Negative (TN)** = The number of invalid users that the system appropriately denied.
- **False Positive (FP)** = The number of invalid users inappropriately accepted by the system.

In order to quantify the fingerprint modules performance, the parameters Specificity(Sp), Sensitivity(Se) and Accuracy(Acc) are computed with the ratios given below (Yusuf et al., 2022).

$$Sp = \frac{TN}{TN + FP} \dots (1)$$

$$Se = \frac{TP}{TP + FN} \dots (2)$$

$$Acc = \frac{TP + TN}{TP + FN + TN + FP} \dots (3)$$

Table 3. 3 Performance test record

| **Stages** | **No. of trials** | **R307** | | | | **R307S** | | | | **FPM10A-DY50** | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | TP | FN | TN | FP | TP | FN | TN | FP | TP | FN | TN | FP |
| **1** | 10 | 10 | 0 | 10 | 0 | 10 | 0 | 10 | 0 | 10 | 0 | 10 | 0 |
| **2** | 20 | 20 | 0 | 20 | 0 | 19 | 1 | 20 | 0 | 20 | 0 | 20 | 0 |
| **3** | 40 | 40 | 0 | 40 | 0 | 40 | 0 | 40 | 0 | 39 | 1 | 40 | 0 |
| **4** | 80 | 79 | 1 | 80 | 0 | 80 | 0 | 80 | 0 | 79 | 1 | 80 | 0 |
| **5** | 160 | 158 | 2 | 160 | 0 | 160 | 0 | 160 | 0 | 158 | 2 | 160 | 0 |
| **Total** | **310** | **307** | **3** | **310** | **0** | **309** | **1** | **310** | **0** | **306** | **4** | **310** | **0** |

In addition to the above metrics, equal error rate ERR graph is plotted based on the false acceptance FAR and false rejection rates FRR for the best performing fingerprint module given by the manufacturer (Hangzhou Grow Technology Co., 2012), on python matplotlib using the code in A4 of the appendix.

### 3.5.2 Face recognition model optimization

In order to optimize the face recognition model, the hyper-parameters for training the face recognition model are tuned in three stages as shown in table 3. 4. Then, the model is trained using the tuned hyper-parameters and the one with the optimal performance is used for the face recognition task.

Table 3. 4 Hyper-parameter tuning

| Hyper-parameters | Stage - 1 | Stage - 2 | Stage - 3 |
|---|---|---|---|
| **Training image** | 10,000 | 8,000 | 4,000 |
| **Validation image** | 2,000 | 1,600 | 800 |
| **Learning rate** | 0.1 | 0.001 | 0.0001 |
| **Optimizer** | Adam | Adam | Adam |
| **Epoch** | 40 | 15 | 10 |
| **Steps per epoch** | 362 | 125 | 100 |
| **Validation step** | 50 | 30 | 15 |

### 3.5.3 Face recognition performance evaluation

After training the face recognition model, the performance of the model selected from the optimum training output in 3.5.2 is evaluated using the evaluation metrics precision, recall, f1-score and confusion matrix. Unlike the fingerprint sensor, the evaluation can be handled using Colab as shown in the figure 3. 10. The face recognition evaluation is conducted on 229 test images.

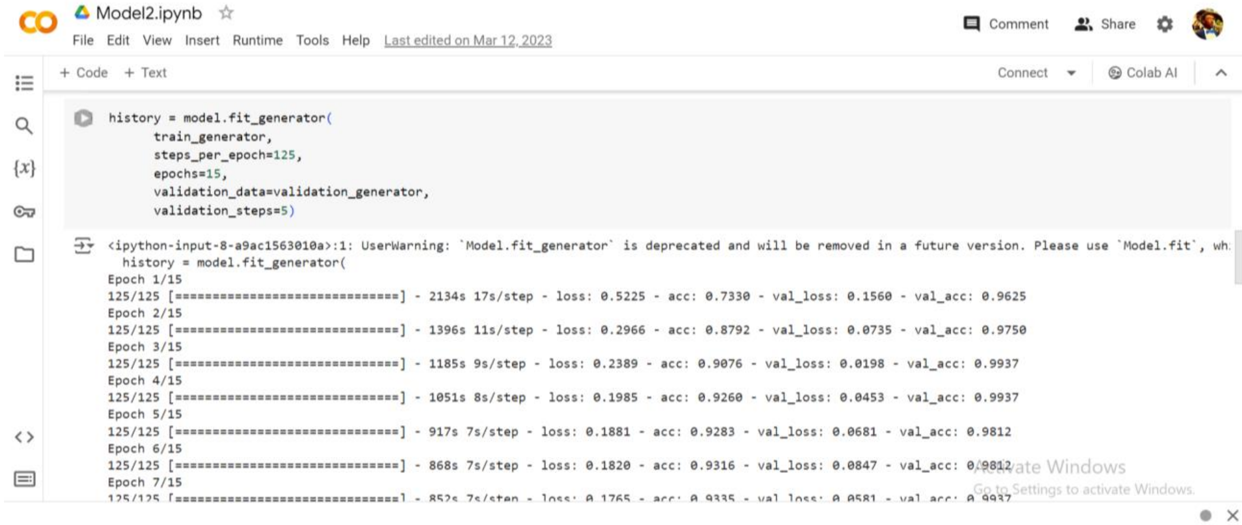


Figure 3. 10 Performance evaluation of the face recognition model in Google Colab

## 3.6 Biometric authentication

### 3.6.1 Fingerprint based authentication

The fingerprint module selected in section 3.5.1 is used for vehicle based authentication. The owner's fingerprint enrolled will be kept in the module's memory. Multiple fingerprints can be stored. After enrollment, the module can be used for authentication purpose by using the circuit in figure 3. 11. When enrolled fingerprint is detected by the module, a relay is activated to actuate the door unlock solenoid and also turn the vehicle ignition on.

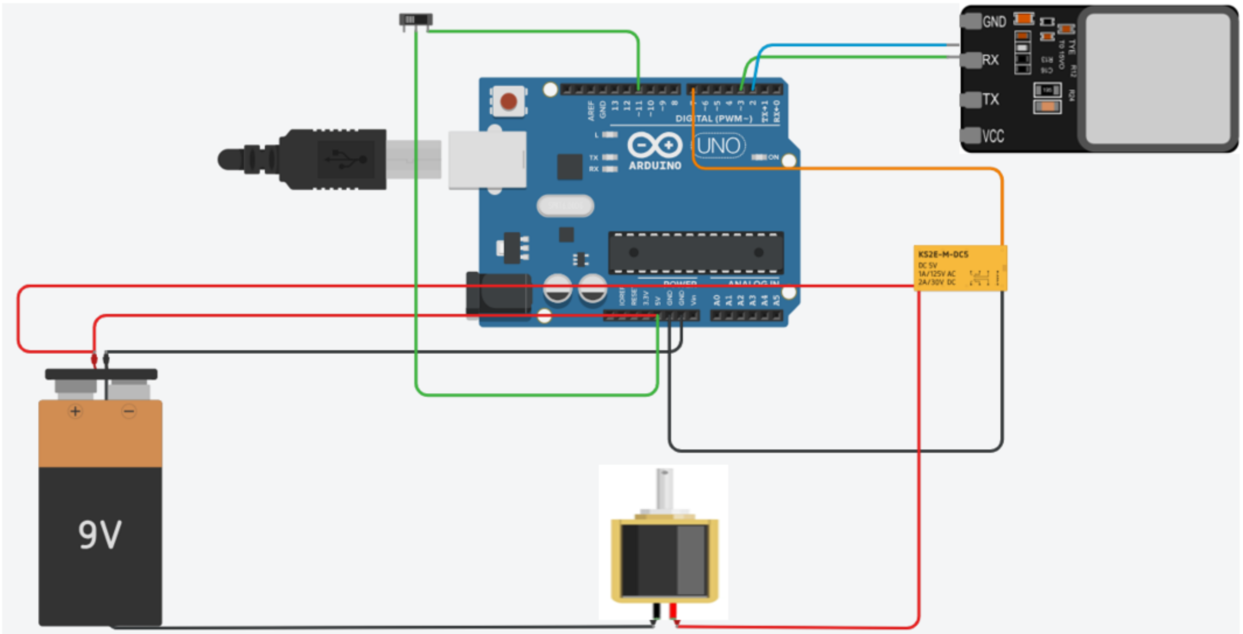


Figure 3. 11 Interfacing the fingerprint module with Arduino

### 3.6.2 Face recognition based authentication

The open source Google Colab and Teachable Machine are free platforms for training and testing machine learning models. After training the face recognition model, results can be previewed using a webcam or tested by importing images as shown in figure below 3. 12. The final model can be exported in different file formats for further practical use in a Raspberry Pi controller.

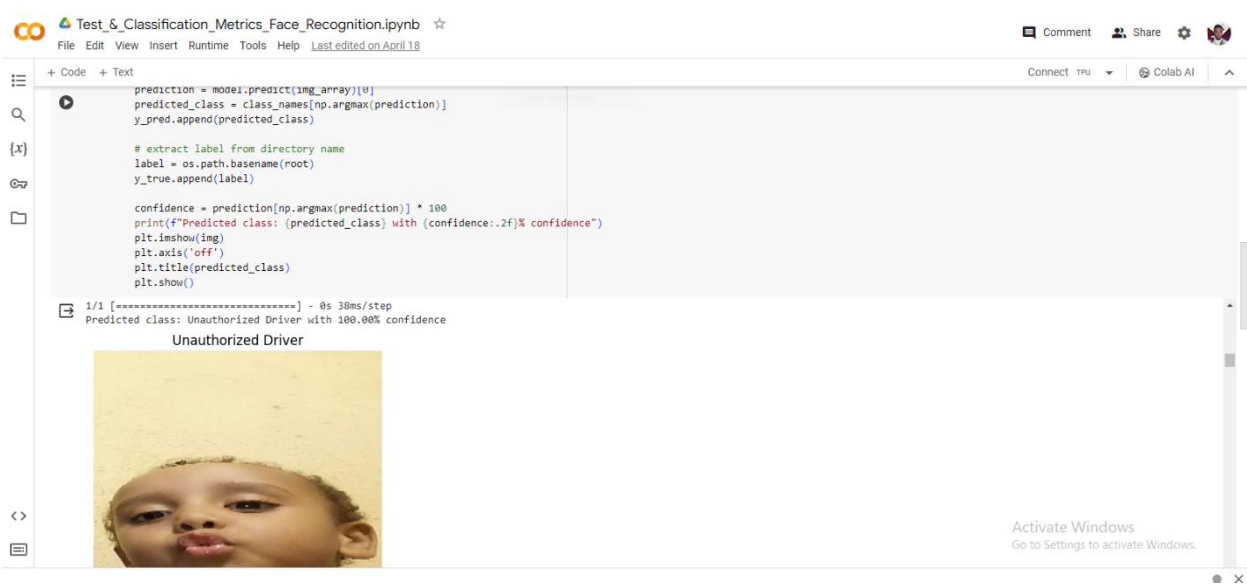


Figure 3. 12 Face recognition model training on Colab

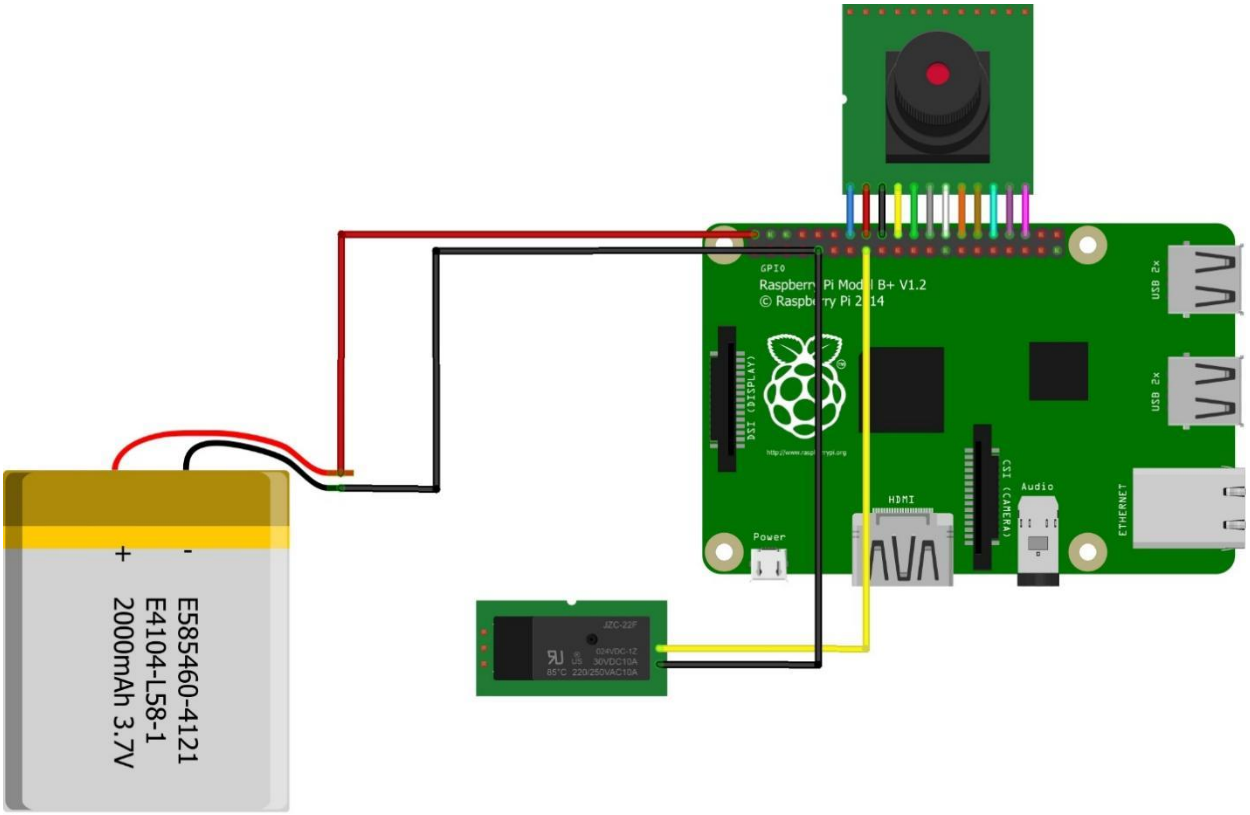


Figure 3. 13 Raspberry Pi circuit with camera and relay for the face recognition system

Following the face recognition model training, a Raspberry Pi 4B controller is used to set up the face recognition based biometric vehicular security using the circuit shown in figure 3. 13. The same circuit is activated to capture intruder images during theft detection.

### 3.7 Theft deterrence subsystem

By using the ultrasonic motion sensor, vibration/shock sensor and A6 GSM/GPRS module shown in figure 3. 14 below, unauthorized entry or theft attempt can be detected. Then the controller will tip the GSM module to notify the vehicle owner about the incident via a phone call and a buzzer siren will be initiated to deter the intruder.

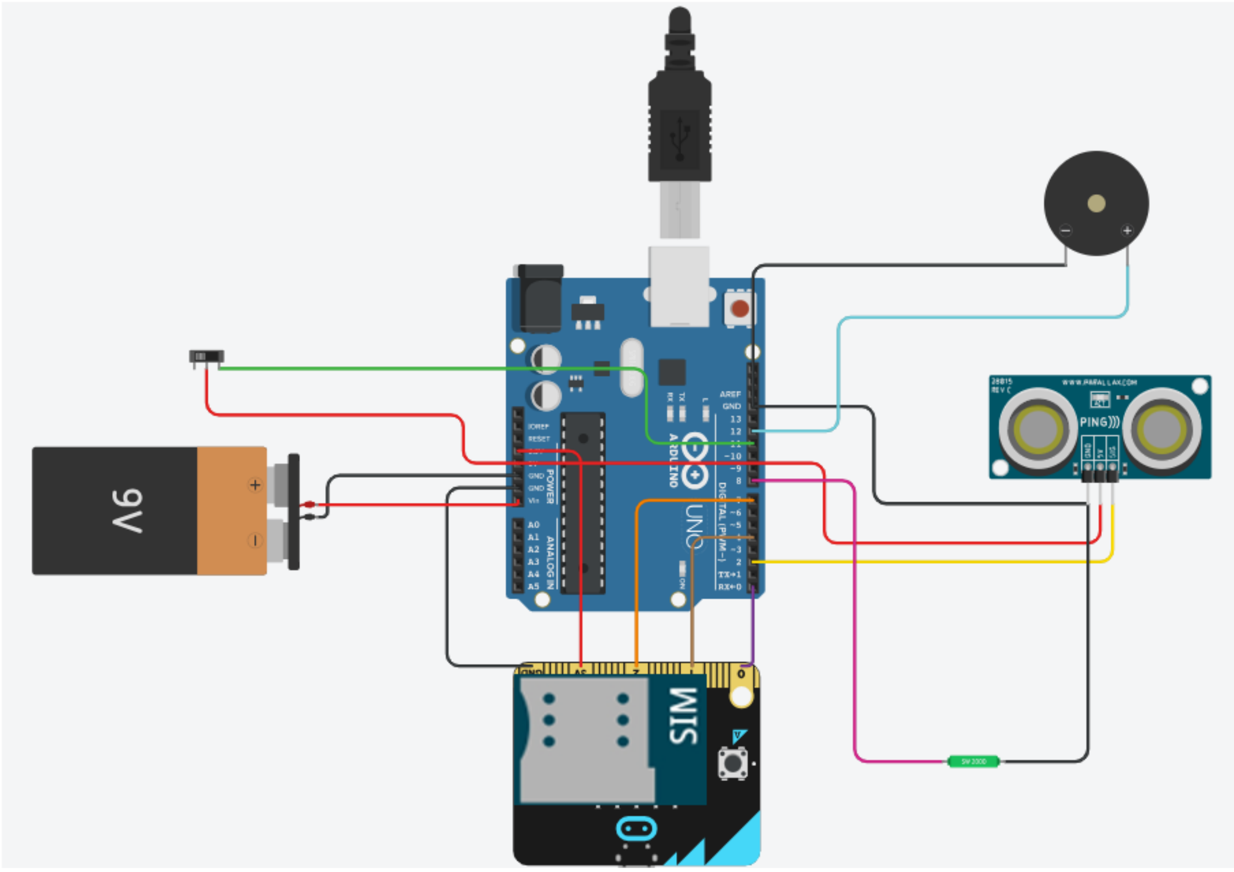


Figure 3. 14 Theft deterrence with ultrasonic sensor and GSM module

### 3.8 Intruder identity communication

The vehicle monitoring android app shown in the figure 3. 15 below, is developed for added control ease and convenience of the vehicle owner. The app allows two-way real-time communication between the owner and his vehicle. During theft incidents, the intruder image, vehicle location, incident date and time will be communicated to the owner via the app and e-mail back up. As a result, the vehicle owner can lock or disable his vehicle from anywhere in the world with a single tap as a safety feature to protect his vehicle via the app. The app also allows the driver to grant access from the app to individuals who have not registered their fingerprint or face data but want to get authorized access to the owner's vehicle. For security reason, the app has access to android biometric authentication to confirm a genuine user has logged in. In addition to the app, every intruder related images and incidents are sent to the owner's e-mail, and can be accessed incase the owner's phone is lost.

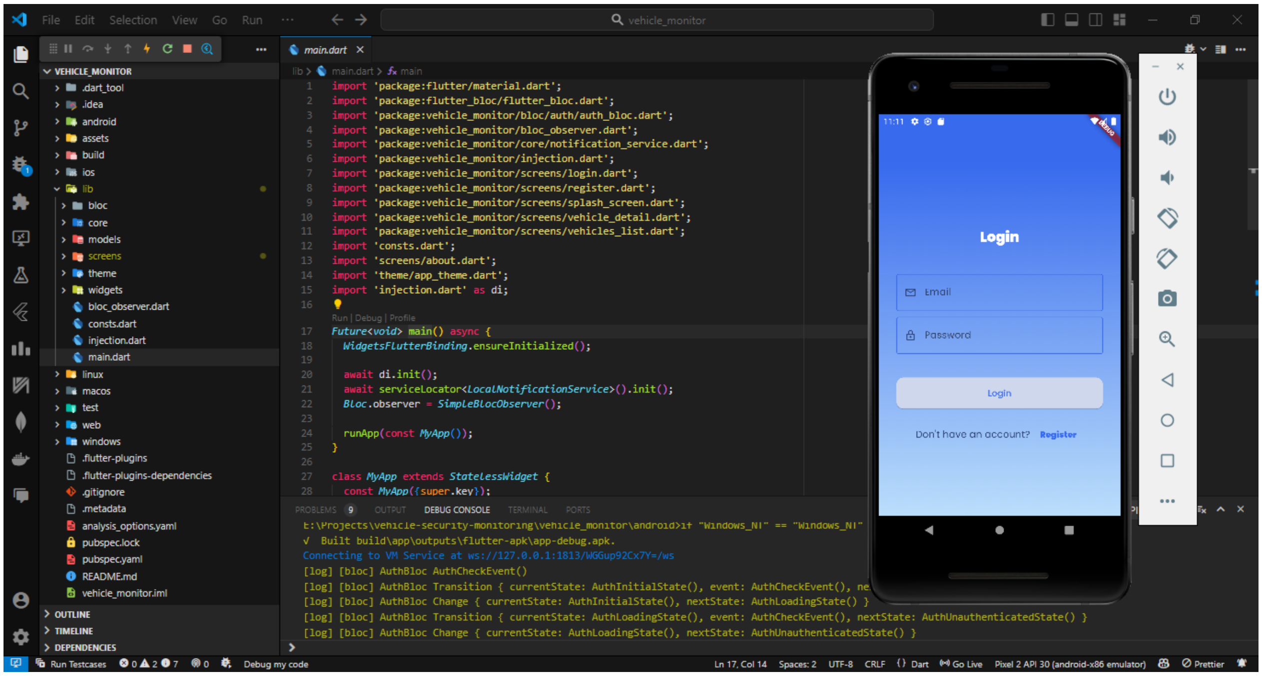


Figure 3. 15 Screenshot of the android app development

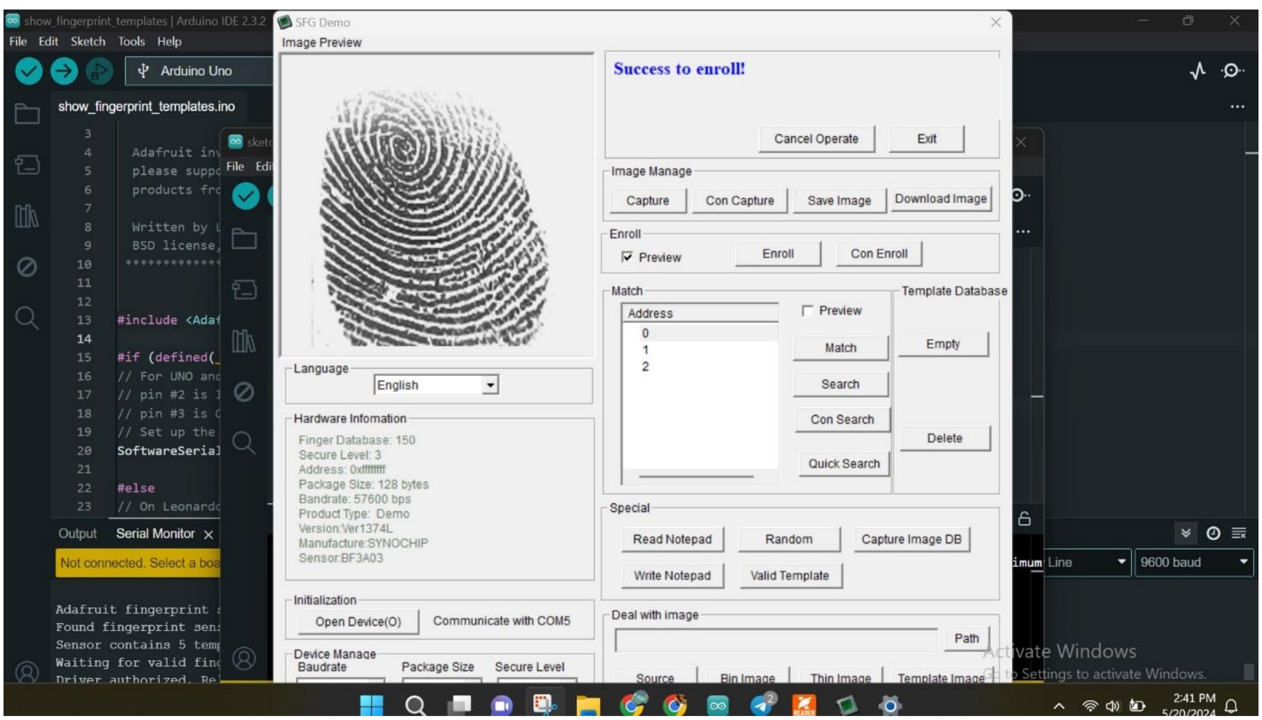


Figure 3. 16 Screenshot of intruder fingerprint captured

In addition to the intruder facial image, a fingerprint sensor placed on engine start button stores the intruder's fingerprint data that can be extracted for law enforcement as evident in figure 3. 16.

### 3.9 IR blaster for taking clear nighttime images

As long as the ambient light is bright enough, the camera can capture clear pictures. But as it gets darker the IR LEDs in figure 3. 17 will kick in to illuminate the camera with infrared light invisible to the naked eye.

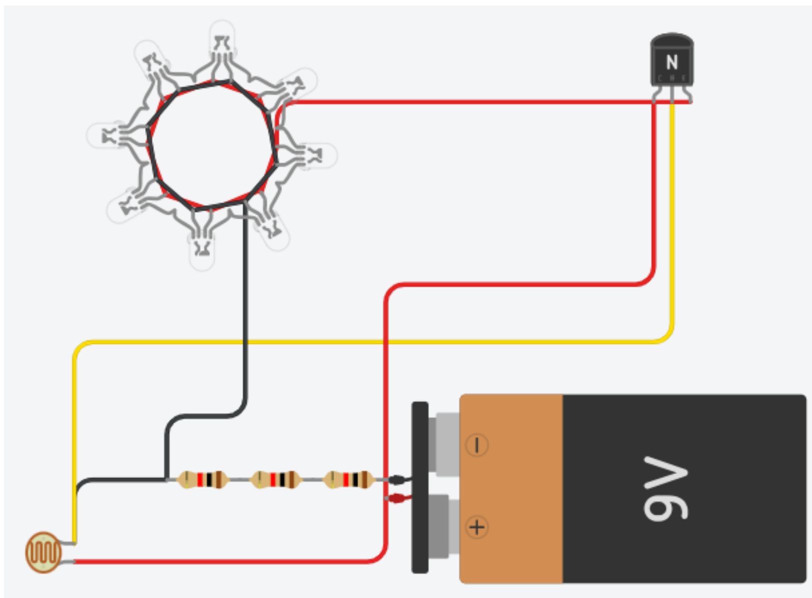


Figure 3. 17 IR LEDs for night mode

# CHAPTER FOUR

# RESULTS AND DISCUSSIONS

As per the biometric vehicle security system architecture developed in chapter 4, the results of the biometric system optimization, performance evaluation, biometric based authentication, hardware implementation of the theft deterrence and intruder identity communication systems is presented in this chapter.

## 4.1 Results

### 4.1.1 Biometric system optimization result

As per the performance evaluation table and the equations presented in section 4.2, the specificity, sensitivity and accuracy of each R307, R307S and FPM10A-DY50 fingerprint module is calculated as follows:

- **R307 module**

$$Sp = \frac{TN}{TN + FP} = \frac{310}{310 + 0} = 100\%$$

$$Se = \frac{TP}{TP + FN} = \frac{307}{307 + 3} = 99\%$$

$$Acc = \frac{TP + TN}{TP + FN + TN + FP} = \frac{307 + 310}{307 + 3 + 310 + 0} = 99.5\%$$

- **R307S module**

$$Sp = \frac{TN}{TN + FP} = \frac{310}{310 + 0} = 100\%$$

$$Se = \frac{TP}{TP + FN} = \frac{309}{309 + 1} = 99.68\%$$

$$Acc = \frac{TP + TN}{TP + FN + TN + FP} = \frac{309 + 310}{309 + 1 + 310 + 0} = 99.84\%$$

- **FPM10A-DY50 module**

$$Sp = \frac{TN}{TN + FP} = \frac{310}{310 + 0} = 100\%$$

$$Se = \frac{TP}{TP + FN} = \frac{306}{306 + 4} = 98.71\%$$

$$Acc = \frac{TP + TN}{TP + FN + TN + FP} = \frac{306 + 310}{306 + 4 + 310 + 0} = 99.36\%$$

- **Specificity** ($\boldsymbol{Sp}$) indicates the percentage at which the system correctly denied all unauthorized users.
- **Sensitivity** ($\boldsymbol{Se}$) indicates the percentage of all authorized users at which the system gave access.
- **Accuracy** ($\boldsymbol{Acc}$) indicates the arithmetic mean of specificity and sensitivity.

The evaluation result shows the R307S is the most reliable of the three with a specificity of 100%, sensitivity of 99.68% and an accuracy of 99.84%. As a result, the **R307S fingerprint module is selected** for the fingerprint authentication system.

Following the evaluation result, the ERR vs threshold graph for the R307S fingerprint module, seen in figure 4. 1, is plotted to further understand the performance of the fingerprint sensor, allowing system designers to make informed decisions about threshold settings to optimize both security and user experience.

In the context of a fingerprint sensor, an ERR (Equal Error Rate) vs threshold graph illustrates the trade-off between the False Rejection Rate (FRR) and the False Acceptance Rate (FAR) at different decision thresholds. For the graph presented in figure 4. 1, the following interpretations are made:

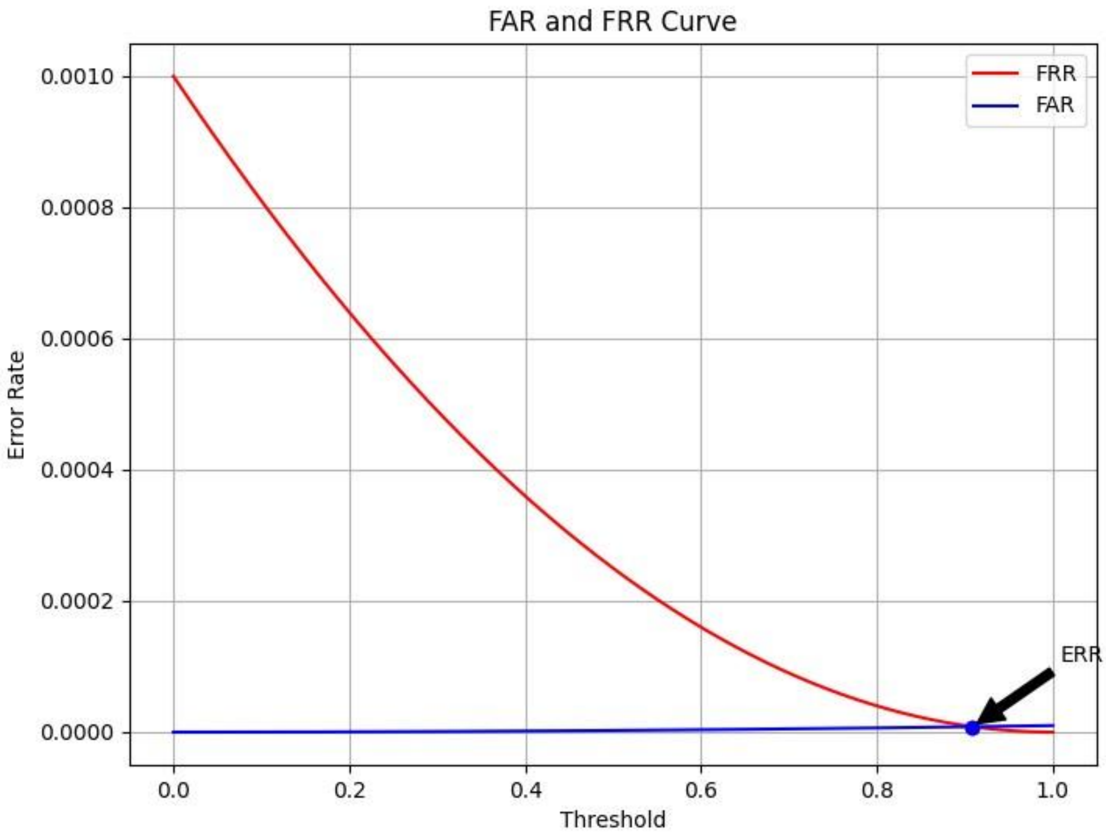


Figure 4. 1 FAR and FRR plot in python for R307S fingerprint module

- **Interpretation of the Graph:**
    - The graph illustrates the relationship between the decision threshold and the ERR, with the ERR occurring at a threshold value of approximately 0.9.
    - At this threshold, the system achieves a balance between minimizing false rejections and false acceptances.
    - Lowering the threshold would decrease the FRR but increase the FAR, while raising the threshold would decrease the FAR but increase the FRR.
    - The specific threshold value chosen depends on the desired balance between security and convenience for the application.

- **ERR of Almost 0 and Threshold of 0.9:**
    - The ERR represents the point at which the FRR and FAR intersect, indicating the

threshold value at which the system achieves an equal balance between false rejections and false acceptances.
    - An ERR of almost 0 suggests that the system is highly accurate in distinguishing between genuine users and impostors.
    - A threshold of 0.9 means that the system's decision boundary is set relatively high, requiring a high level of similarity between the presented fingerprint and the stored template to be accepted.

- **False Rejection Rate (FRR) of 0.1%:**
    - FRR represents the percentage of genuine users whose fingerprints are incorrectly rejected by the system.
    - A FRR of 0.1% indicates that 0.001 or 1 out of 1,000 of legitimate attempts to access the system are falsely rejected, indicating acceptable performance.

- **False Acceptance Rate (FAR) of 0.001%:**
    - FAR represents the percentage of impostors whose fingerprints are incorrectly accepted by the system.
    - A FAR of 0.001% indicates that 0.00001 or 1 out of 100,000 of unauthorized attempts to access the system are falsely accepted, indicating a low level of false acceptance.

As a result, the plot confirmed the R307S fingerprint module is a reliable sensor that can enhance vehicle security with low FAR and FRR.

### 4.1.2 Result of the face recognition model optimization

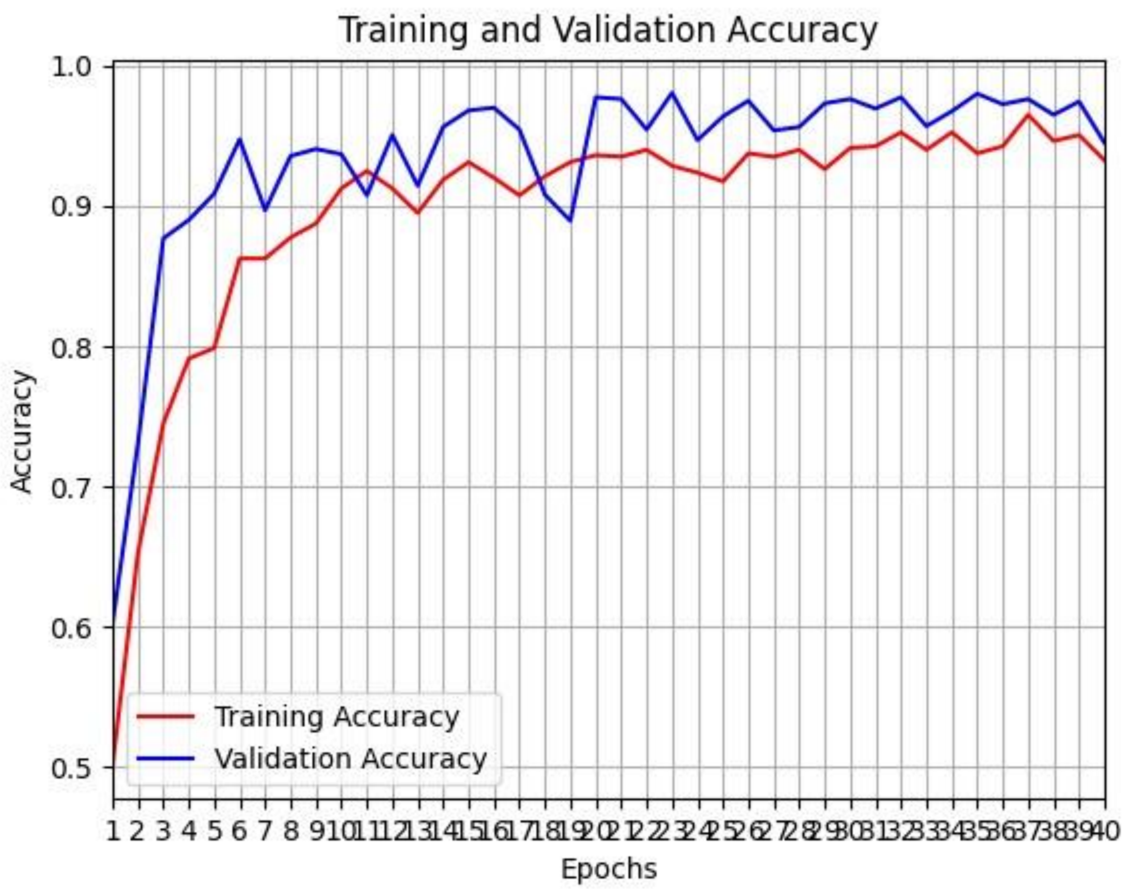


Figure 4. 2 Training and validation accuracy for stage – 1

The stage -1 training results indicate both training and validation accuracies of the model generally increased as the number of epoch increased. Except for the epoch's 16 to 19 where validation accuracy dipped as shown in figure 4. 2. Since the validation accuracy pattern indicates a value of 0.95 compared to the training accuracy of 0.93, the model is properly learnt the face recognition pattern.

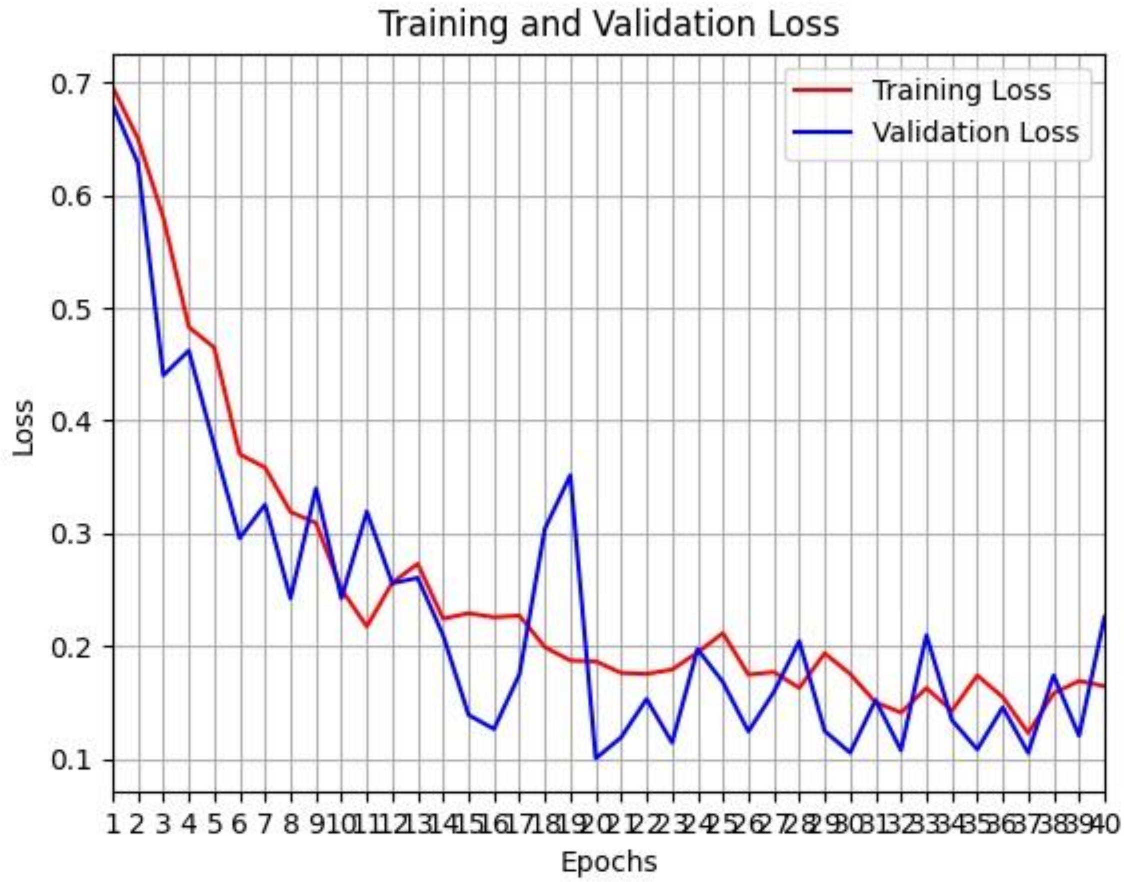


Figure 4. 3 Training and validation loss for stage – 1

However, the most important plot to understand the model generalization pattern is the loss graph seen in figure 4. 3. The training and validation loss for stage - 1 indicates the model is not generalizing well since the validation loss is intermittently zig zagging, which points toward overfitting. Overfitting is a condition in machine learning where the model is learning patterns not essential to the output needed. In our case it means the model is not good enough in extracting the proper facial pattern needed to recognize the authorized driver.

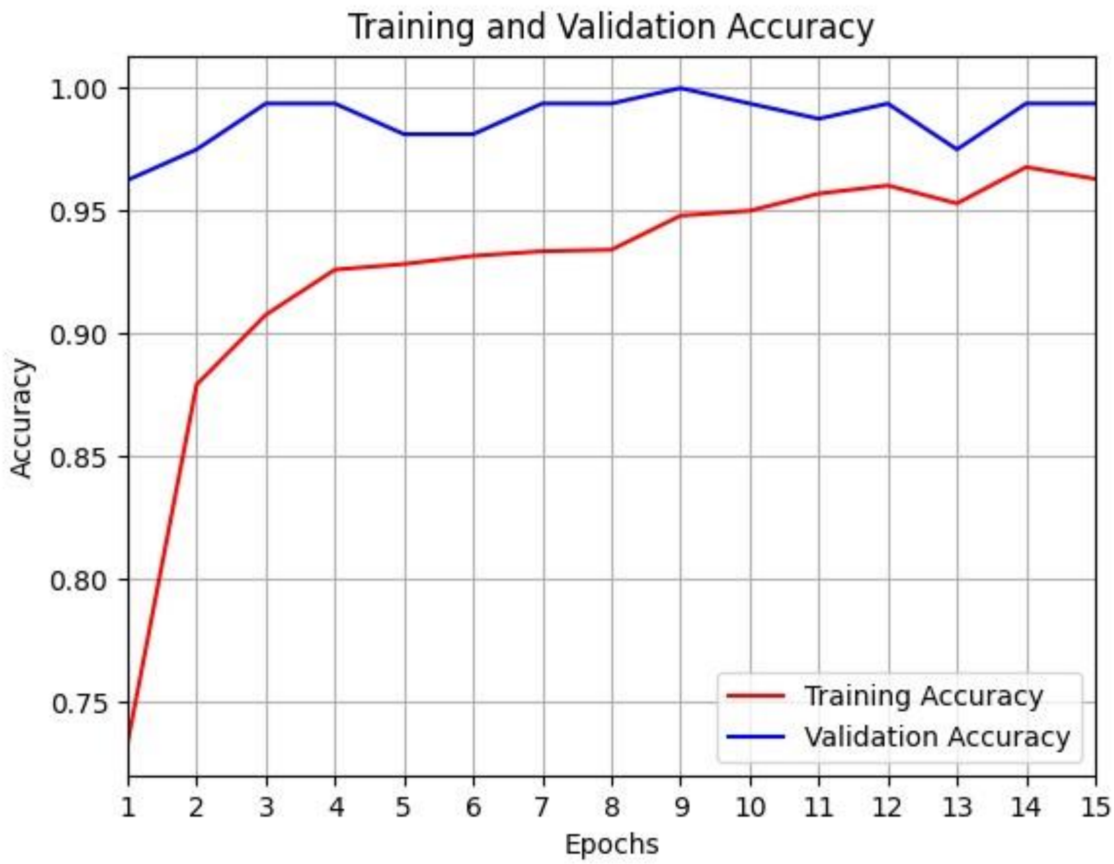


Figure 4. 4 Training and validation accuracy for stage – 2

The stage - 2 training results indicate both training and validation accuracies of the model increased as the number of epoch increased as shown in figure 4. 4. Since the validation accuracy pattern indicates a value of 0.99 compared to the training accuracy of 0.96, the model has accurately learnt the face recognition pattern.

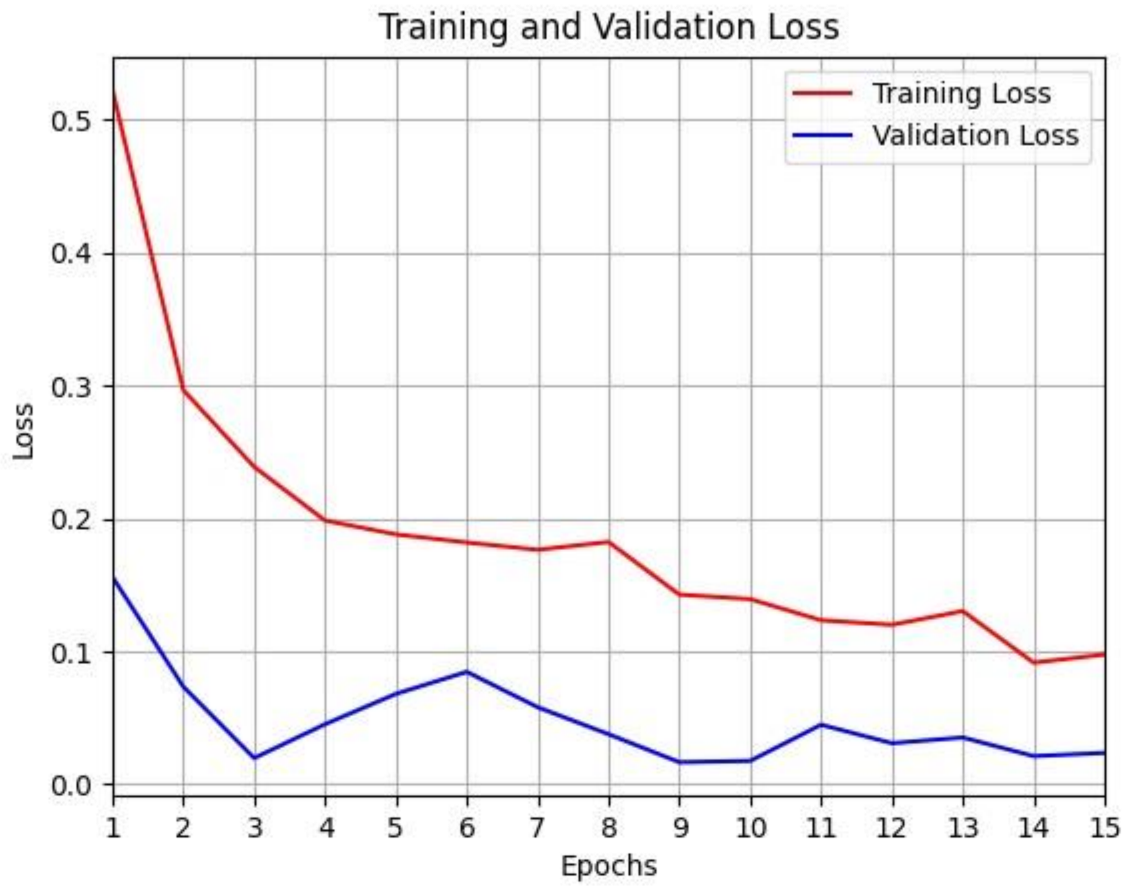


Figure 4. 5 Training and validation loss for stage – 2

Regarding the most important plot to understand the model generalization pattern, the loss graph seen in figure 4. 5, the training and validation loss for stage - 2 indicate the model demonstrated significant perfection over 15 epochs, achieving high accuracy and low loss on both training and validation sets, suggesting successful training and good generalization. In our case, it means the model is capable enough to recognize the proper facial pattern needed to recognize the authorized driver.

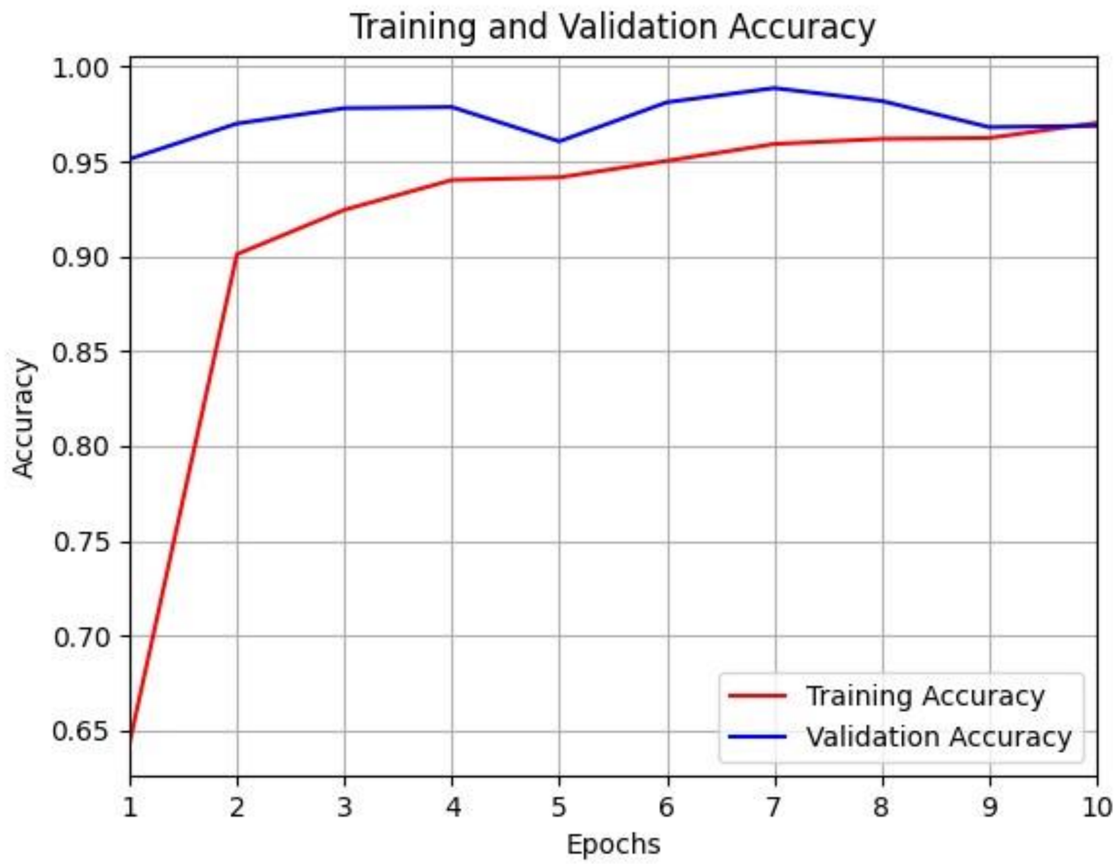


Figure 4. 6 Training and validation accuracy for stage – 3

The stage - 3 training results indicate both training and validation accuracies of the model increased as the number of epoch increased. Except for the epoch's 4 to 6 where validation accuracy dipped as shown in figure 4. 6. The accuracy pattern indicates a converging value of 0.96 for training and validation at the end of the training, the model seems to have learnt the face pattern.

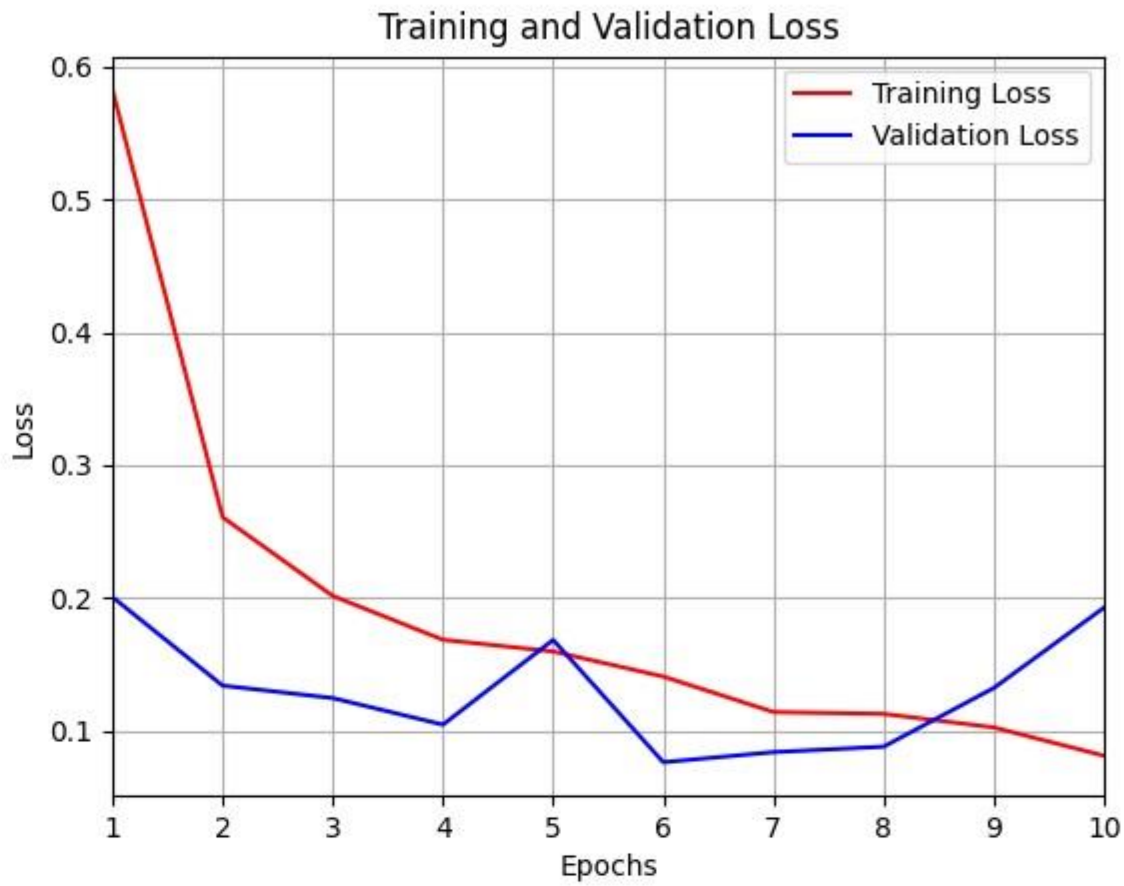


Figure 4. 7 Training and validation loss for stage - 3

On the other hand, to understand the model generalization pattern, the loss graph seen in figure 4. 7 indicates a validation loss increment after the sixth epoch. Hence, the model is overfitting to the giver dataset. In our case, it means the model did not extract the proper facial pattern needed to recognize the authorized driver.

Following the training results, the **model trained in stage – 2 is selected** from the three stages for facial recognition based biometric authentication intended for vehicle use. To confirm the selected model's vehicle worthiness, its performance is assessed in Colab using the metrics shown below.

```
                      precision    recall  f1-score   support

   Authorized Driver       1.00      0.98      0.99       126
 Unauthorized Driver       0.97      1.00      0.99       103

            accuracy                           0.99       229
           macro avg       0.99      0.99      0.99       229
        weighted avg       0.99      0.99      0.99       229

[[123   3]
 [  0 103]]
```

Figure 4. 8 Google Colab evaluation result of the selected face recognition model

The provided face recognition model evaluation metrics in figure 4. 8 are precision, recall, F1-score, confusion matrix and support. Here's an interpretation of each metrics:

- **Precision (0.99):**
    - Precision measures the accuracy of the positive predictions made by the model.
    - A precision score of 0.99 indicates that 99% of the instances predicted as positive by the model are indeed positive (i.e., correctly recognized faces).
    - In other words, the model has a very low rate of false positives, making it highly reliable in identifying authorized faces.

- **Recall (0.99):**
    - Recall, also known as sensitivity or true positive rate, measures the ability of the model to correctly identify all positive instances in the dataset.
    - A recall score of 0.99 indicates that the model correctly identifies 99% of all actual positive instances (i.e., faces) in the dataset.
    - This suggests that the model has a very low rate of false negatives, meaning it rarely misses recognizing authorized faces.

- **F1-score (0.99):**
    - The F1-score is the harmonic mean of precision and recall and provides a balance between the two metrics.
    - A high F1-score (0.99 in this case) indicates that the model has both high precision

and high recall, achieving a balance between minimizing false positives and false negatives.

  - It is particularly useful when classes are imbalanced, as it considers both false positives and false negatives.

- **Support (229):**
  - Support represents the number of actual occurrences of each class in the test dataset.
  - In this case, a support of 229 suggests that the evaluation was performed on a dataset containing 229 instances (e.g., images) of faces.
  - It provides context for interpreting the precision, recall, and F1-score metrics and helps understand the scale of the dataset.

Overall, the evaluation metrics indicate that the face recognition model performs exceptionally well, with high precision, recall, and F1-score. It correctly identifies faces with very few false positives and false negatives, making it highly reliable for face recognition tasks. The support value provides additional context about the size of the dataset used for evaluation.

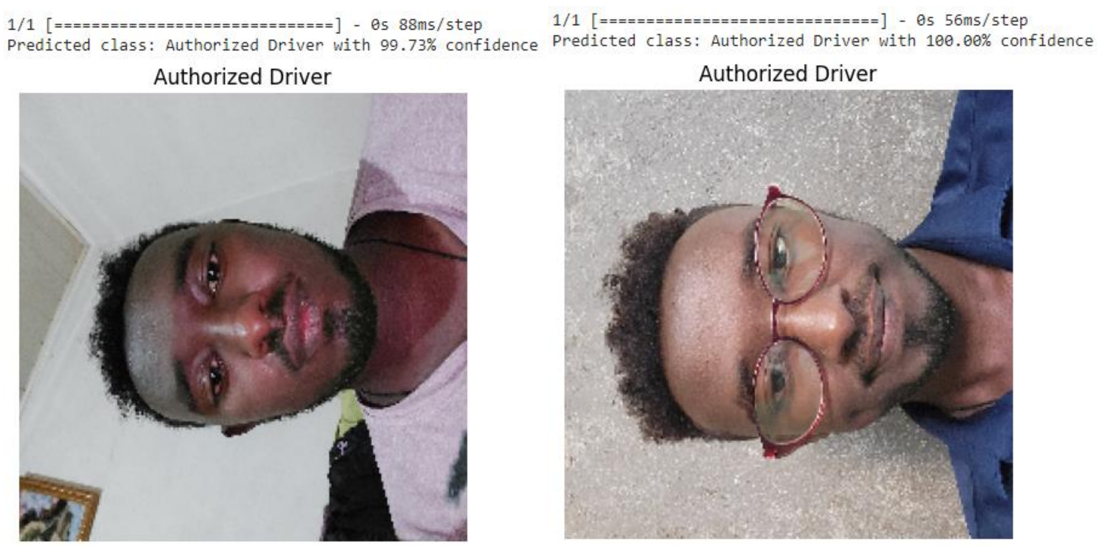


Figure 4. 9 Test results labeled as authorized driver with confidence percentages

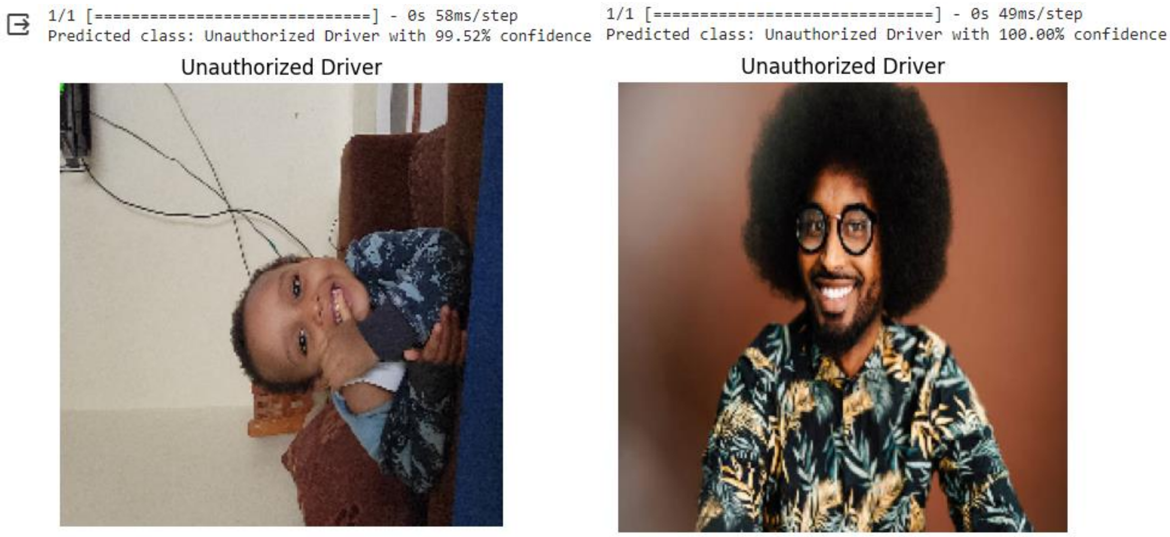


Figure 4. 10 Test results labeled as unauthorized driver with confidence percentages

The figures 4. 9 and 4. 10, show the predicted class labeling with confidence percentage for each images tested.

### 4.1.3 Fingerprint authentication hardware implementation

As per the control circuit given in the previous chapter, the R307S module was connected to the controller and the fingerprint based authentication for vehicle control was initiated as shown in the figure 4. 11.

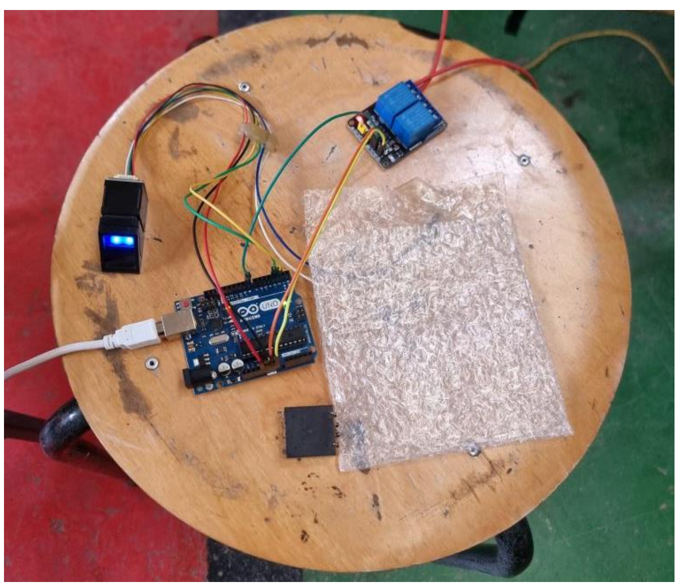

Figure 4. 11 Fingerprint authentication test

Figure 4. 12 Fingerprint authentication based engine starting on Nissan diesel TD27

After successfully enrolling the fingerprint of the owner, a relay was connected to the controller for actuating the engine fuel cut-off solenoid of the injection pump, seen in figure 4. 12, fuel could reach the engine only if it detects the owner's enrolled fingerprint. As a result, the engine couldn't be started unless a registered fingerprint is used for authentication. In such manner, the designed biometric system is functional in immobilizing the engine.

### 4.1.4 Face recognition simulation and hardware implementation

The trained face recognition model was able to identify the authorized driver's face from other faces. As shown in figure 4. 13, and figure 4. 14.

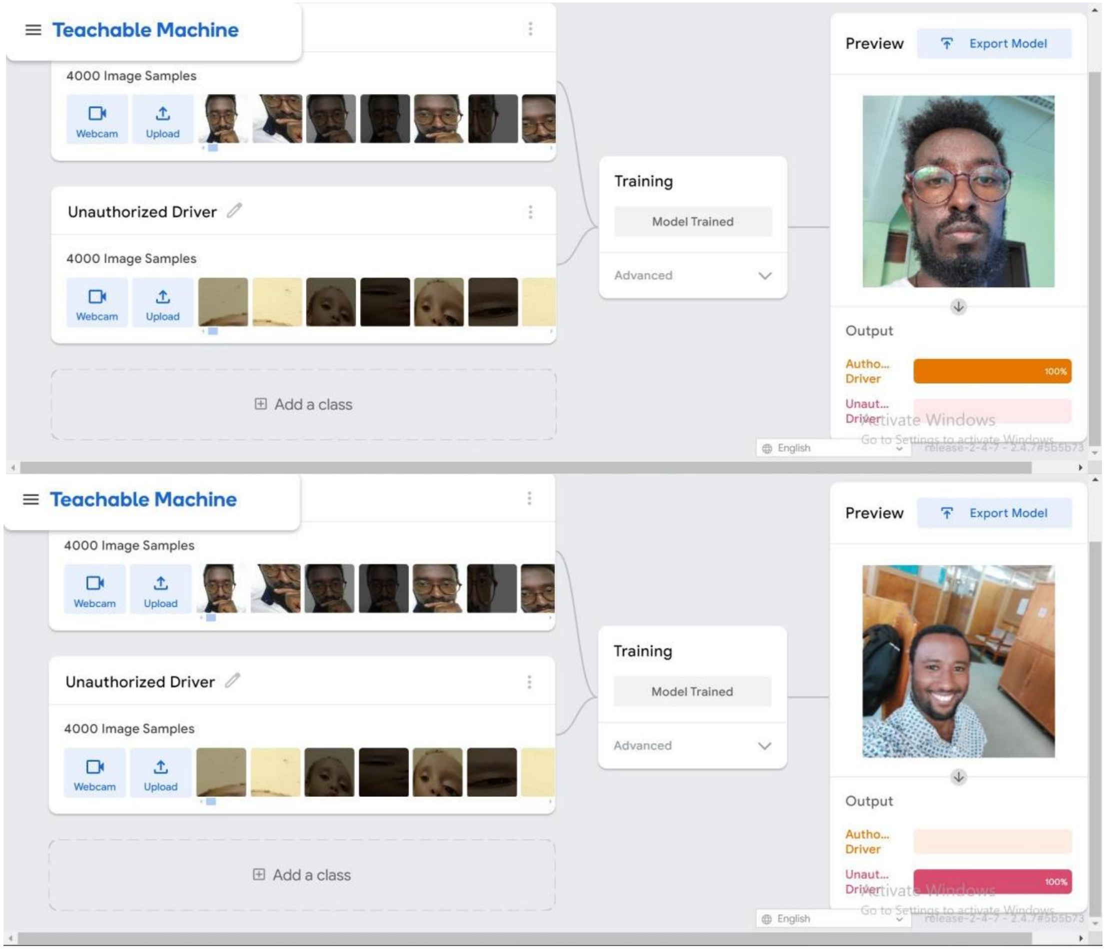


Figure 4. 13 Testing on Teachable Machine after training

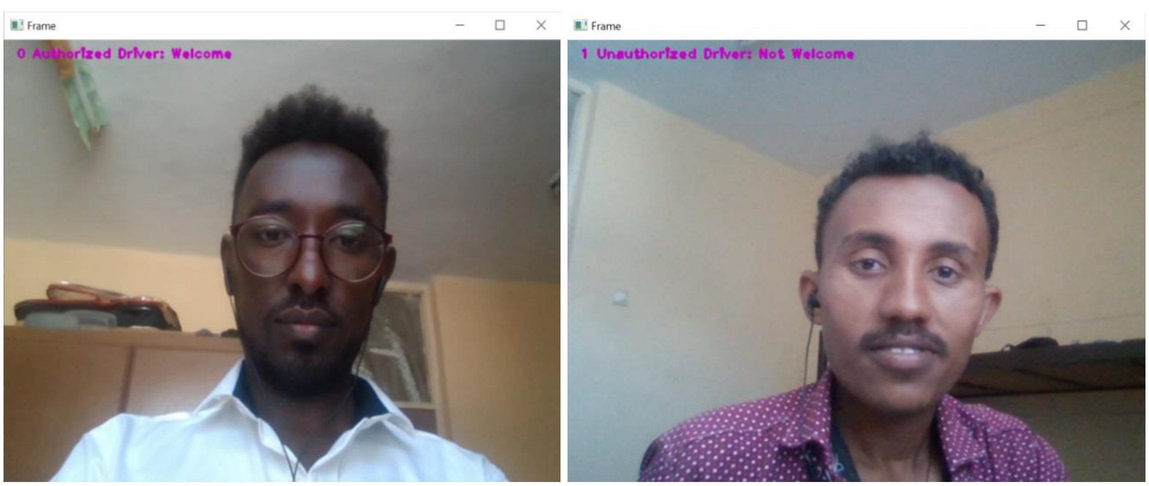


Figure 4. 14 Face recognition test on python using the trained model

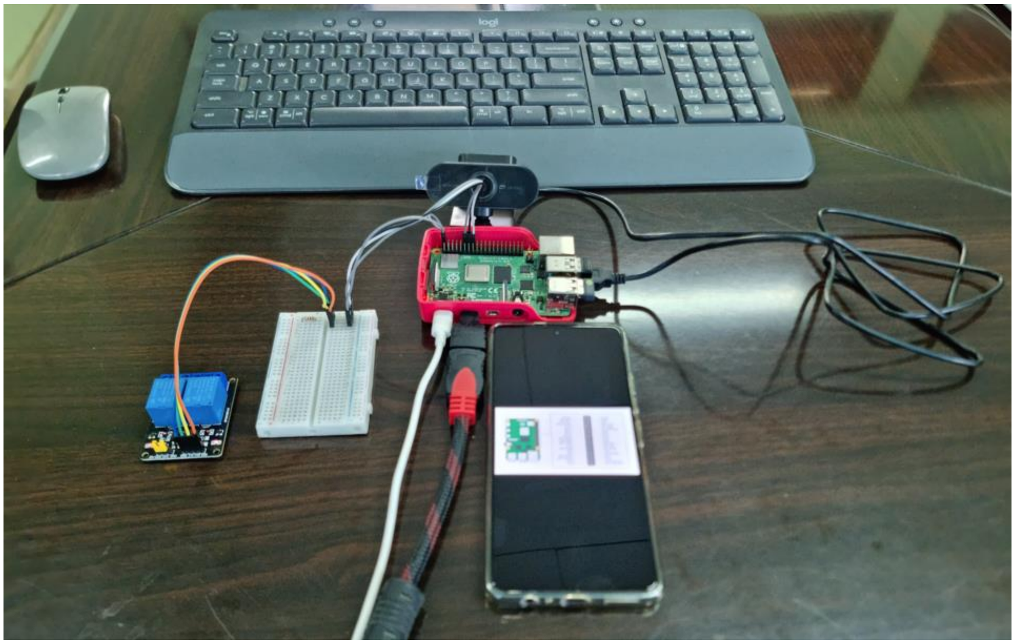

Figure 4. 15 Face recognition test using Raspberry Pi 4B

By means of the Raspberry Pi setup displayed in figure 4. 15, when the camera identifies the face of the authorized driver, as shown in figure 4. 16, the relay is actuated to enable engine starting.

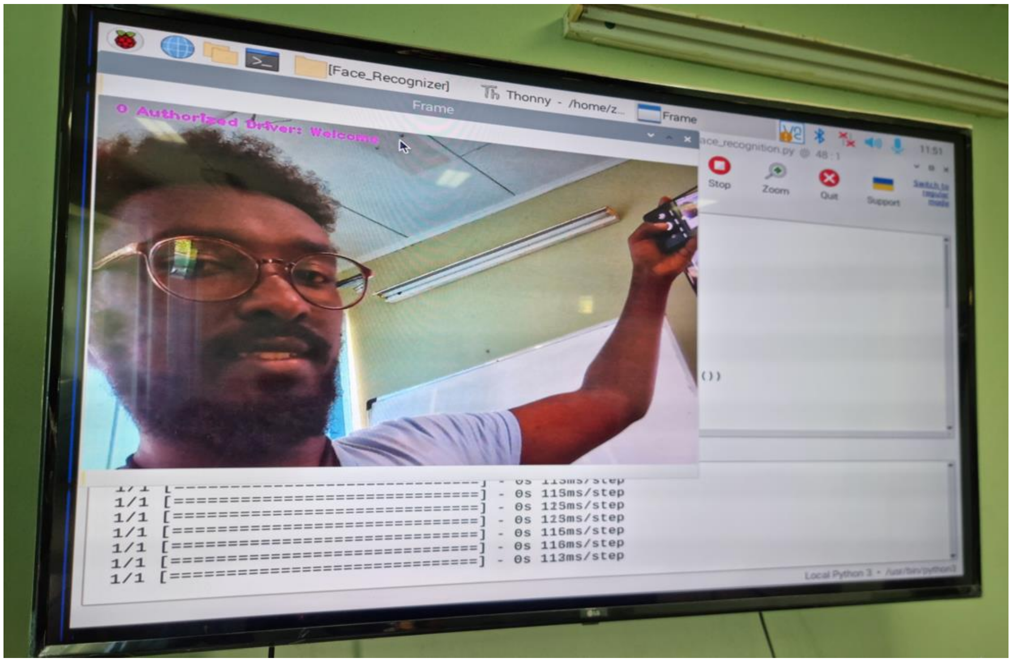


Figure 4. 16 Face recognition test result using Raspberry Pi 4B

### 4.1.5 Theft deterrence hardware implementation

As presented in the control circuit, the motion sensor, shock/vibration sensor and the GSM module are connected to the controller. When unauthorized motion is detected, the vehicle triggers a siren and alerts the vehicle owner via a phone call. The figure 4. 17 below shows the components used for theft deterrence.

Figure 4. 17 Theft deterrence system set up

Following the theft deterrence system set up, it was deployed on a Jos-Hansen dashboard CAN model resembling a real vehicle cabin environment, as shown in figure 4. 18.


Figure 4. 18 Implementation of the theft deterrence system

### 4.1.6 Real-time intruder identity communication implementation on the android app

As shown in the figure 4. 19, each theft incidents are recorded in the app with intruder image, GPS location, date, and time. The GSM used in figure 4. 17 is an added security feature in the sense that if the driver is offline or does not notice the app or e-mail incident notification, an appropriate call can alert him to take action and follow up the situation from his smartphone app.

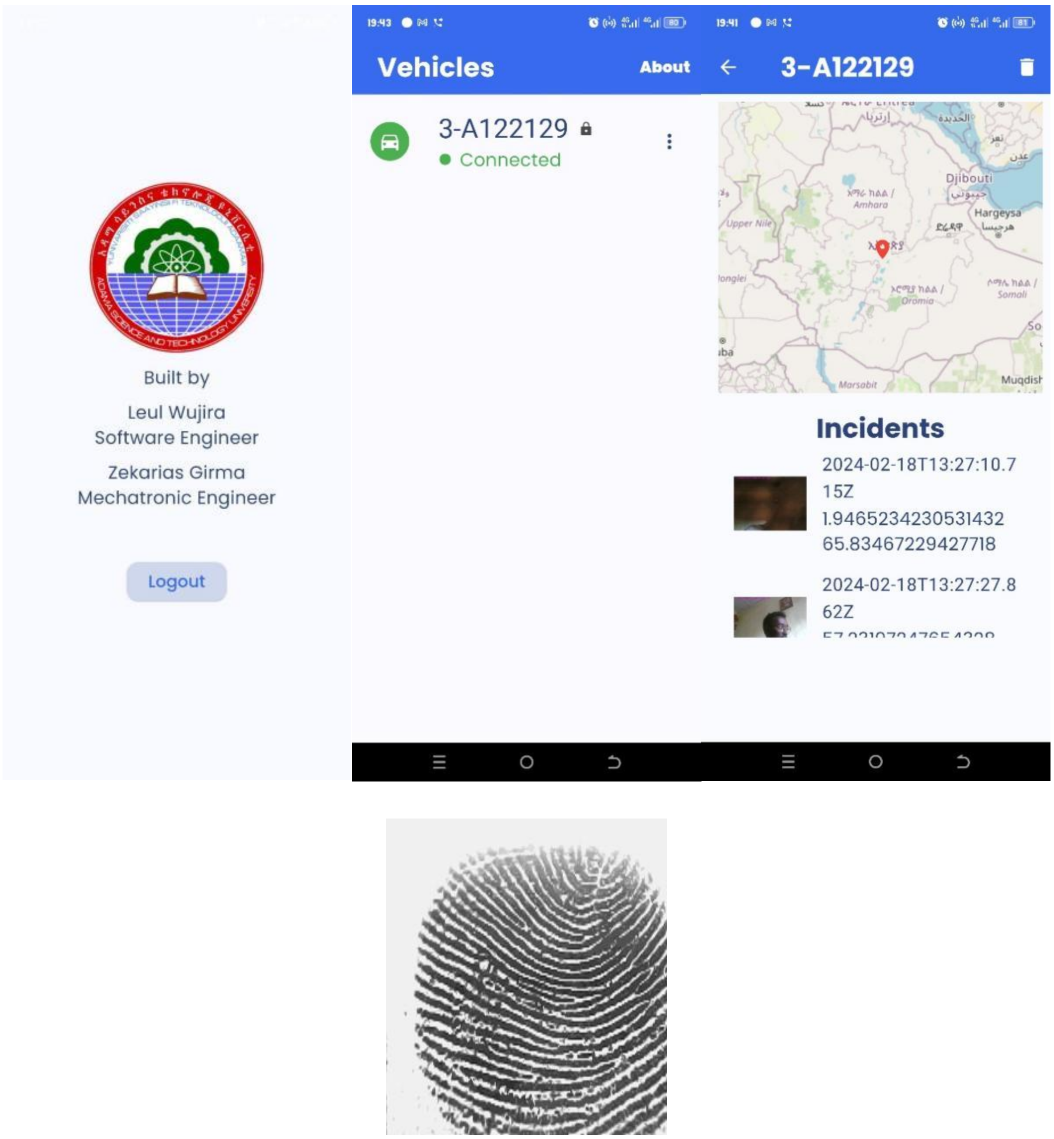


Figure 4. 19 Vehicle monitoring app showing intruder images and SFG showing a fingerprint

The versatility of the system in capturing intruder information is not limited to images. The system is also capable of storing the intruder's digital fingerprint signature as shown above.

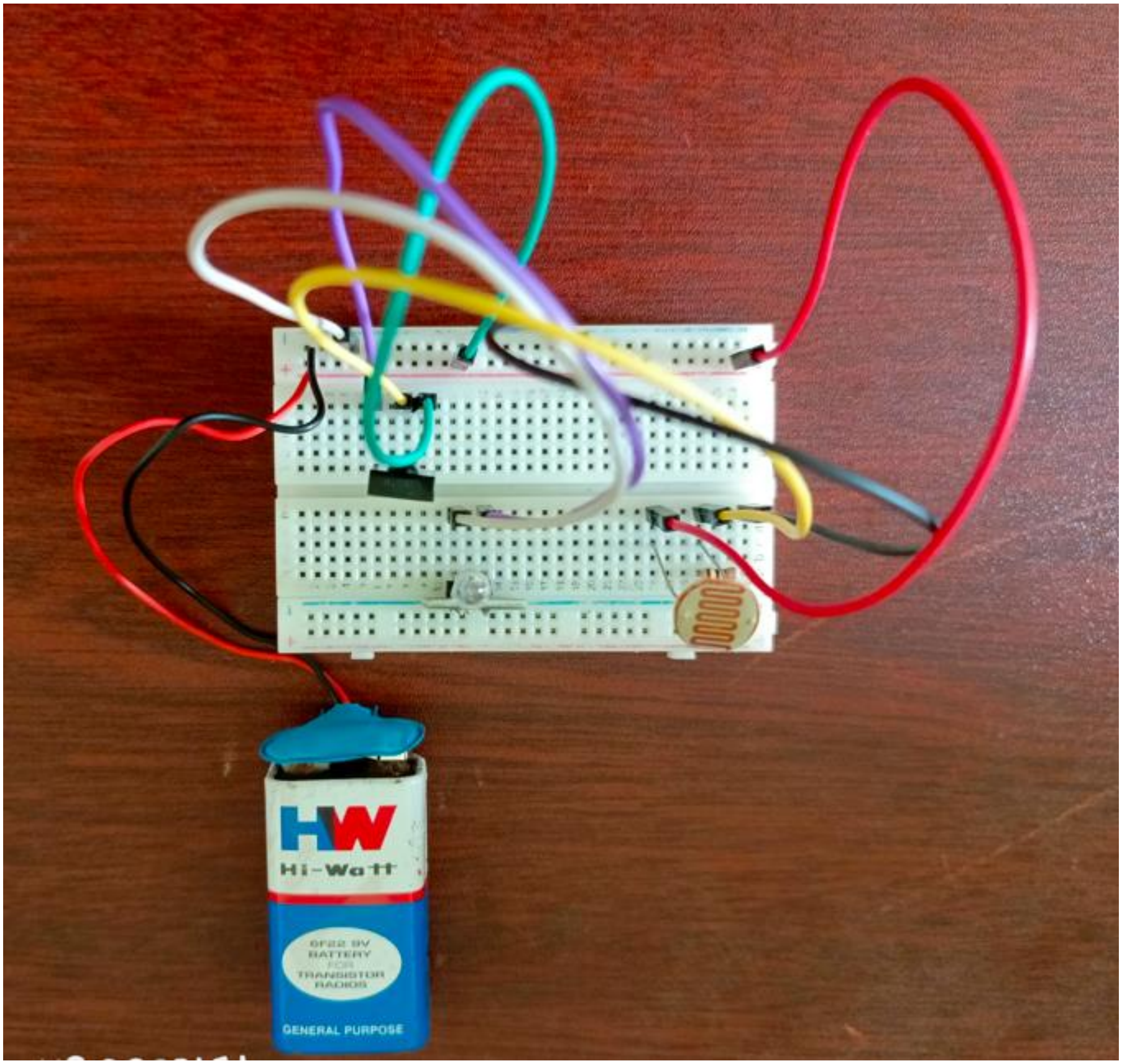

Figure 4. 20 IR LED testing

Following the control circuit diagram in chapter 3, an IR LED is connected with the light dependent resistor, as shown in figure 4.20, to monitor the ambient light and when darkness falls, the signal from the light sensor triggers the transistor base to light up the infrared LED. In the same manner, by connecting an array of IR LEDs in the vicinity of the camera, nighttime functionality can be enabled.

## 4.2 Discussion

In order to validate the results obtained, comparing the biometric system, the intruder identity communication and the hardware execution with prior literatures is crucial to understand the distinctive contribution of this work.

### 4.2.1 Integrated biometric system

The designed vehicle security system integrated fingerprint and facial based biometric modalities. As evident in the works of (Kute et al., 2021), (Bhargav et al., 2022), (Stanwood, 2023) and (Anjana et al., 2022), combining the two modalities makes the system versatile giving the user convenience and enhance the safety factor of the system.

### 4.2.2 Optimization

The fingerprint evaluation result of a specificity, sensitivity and accuracy of 100%, 99.68% and 99.84% respectively, improved up on the result obtained by (Yusuf et al., 2022) with a specificity, sensitivity and accuracy of 96%, 97% and 97% and edged up the 99% accuracy obtained by (Rafay et al., 2019). When comparing the face recognition result of 99% with the accuracy of 98.3% and 99.6% obtained by (Bhargav et al., 2022) and (Elngar & Kayed, 2020) respectively, it indicates the developed model is performing well with a room for more improvement. The 0.30s average processing time of the fingerprint system when compared with the 0.27s and 3.81s obtained by (Hamidi et al., 2023) and (Srinivasan et al., 2021) respectively, indicates a decent processing speed that can be further clocked up. The 0.13s time for face recognition when compared to 0.152s obtained by (Elngar & Kayed, 2020) indicates excellent processing speed.

### 4.2.3 Real-time intruder identity communication

The real-time intruder identity communication took the bench mark from the likes of SMS, MMS and e-mail based work by (Akshay et al., 2018), (Pawar & Rizvi, 2018), (Zamin et al., 2022) and stepped it up towards a feature packed mobile app based communication capable of not only communicating intruder image but also includes vehicle tracking, remote locking/unlocking and biometric authentication from the phone and on top of that, the intruder’s fingerprint image can also be extracted for legal purposes.

### 4.2.4 Hardware implementation

The extensive hardware implementation for the proposed biometric vehicle security system indicated promising insights. The implementation of the biometric (face recognition and fingerprint) authentication on a Raspberry Pi 4 board and Nissan TD27 diesel engine indicated the designed system's practicality. The effective communication of intrusion incidents through phone call and android platform showcases added expediency for the vehicle owner. Addition of the IR LED lights for nighttime function fills the drawback of the prior face recognition based works by (Zamin et al., 2022), (Muhammad Syarif Hartawan, 2022) and (Akila et al., 2021).

# CHAPTER FIVE

# CONCLUSIONS AND RECOMMENDATIONS

## 5.1 Conclusion

In conclusion, the design and implementation of the proposed biometric vehicle security system represent a significant adoption in vehicle security technology. The persistent threat of vehicle theft necessitates embracing a robust security measures capable of deterring theft attempts and aiding in the identification of perpetrators. This thesis offered a comprehensive solution to address these challenges by leveraging biometric technology and real-time communication capabilities.

By considering factors such as accuracy, cost, availability, and adaptability, fingerprint and face recognition emerged as the most effective biometric modalities for integration into the proposed security system. Integrating the two not only enhances system performance but also ensures its applicability across a wide range of operating conditions, vehicle types, and models. Through a rigorous optimization and performance evaluation in various stages, the R307S fingerprint module and the deep learning CNN model exhibited 99.84% and 99% accuracy.

Central to the proposed system is its real-time communication capability, enabling immediate identification and notification of unauthorized access attempts. Upon detection of motion and shock events, the system activates an alarm, initiates a phone call, and captures images of the intruder, promptly transmitting them to the vehicle owner via a dedicated mobile application. Moreover, through the app, the owner can lock engine access and monitor the GPS coordinates of their vehicle with a single tap, further enhancing overall security.

The hardware implementation of the system, based on the Arduino and Raspberry Pi platform, underwent thorough testing on the Nissan Diesel TD27 four-cylinder engine and the CAN dashboard training model. This evaluation provided valuable insights into the system's functionality under real-world conditions.

The integration of this biometric security system into existing vehicle systems holds the potential to significantly enhance both the safety and recoverability of valuable assets. By facilitating prompt identification and apprehension of perpetrators, the system serves as a deterrent to theft and supports law enforcement efforts in combating vehicle-related crimes.

## 5.2 Recommendation

Based on the findings and observations from the development and evaluation of the biometric vehicle security system, the following recommendations are proposed for future research and development.

- **Enhancement of Biometric Modalities:** Future studies should explore the use of more accurate capacitive or ultrasonic fingerprint sensors, thermal and 3D camera to further enhance security and user experience.

- **Commercial Deployment and Pilot Testing:** Conduct pilot testing in real-world scenarios to evaluate the system's performance under various environmental conditions and usage patterns. Collaborate with automotive manufacturers and security companies to facilitate commercial deployment.

- **Integration with Existing Security Systems:** Develop interfaces and protocols for seamless integration with existing vehicle security systems and IoT platforms. This would enhance the system's versatility and allow for broader adoption across different vehicle models and makes.

- **User Experience Optimization:** Continuous improvement in the user interface and experience of the dedicated android application is essential to ensure ease of use, accessibility, and effectiveness in vehicle security management.

- **Collaboration with Law Enforcement Agencies:** Develop partnerships with law enforcement agencies to facilitate the use of the system in vehicle recovery operations. Share data and insights to aid in the development of more effective vehicle theft prevention strategies.

By addressing these recommendations, future research and development endeavors can further advance the field of biometric vehicle security systems, offering enhanced protection and peace of mind for vehicle owners while contributing to the overall reduction of vehicular theft and related crimes.

# REFERENCES


Adafruit. (2024). *Optical fingerprint scanner*. https://www.engineersgarage.com/arduino-adafruit-r30x-r307-fingerprint-scanner/

Akila, V., Sriharshini, K., Sravani, P., Sravanthi, D., Gopi, R., & Sheela, T. (2021). Intelligent Car Anti-Theft Face Recognition System. *International Journal of Online and Biomedical Engineering*, *17*(1), 120–128. https://doi.org/10.3991/ijoe.v17i01.18583

Akshay, P., Mrudangee, H., Jignesh, P., & Hiren, M. (2018). Intruder Insinuation and Identification for Vehicle Security. *2018 3rd International Conference for Convergence in Technology, I2CT 2018*, 1–6. https://doi.org/10.1109/I2CT.2018.8529499

Al-Assam, H., Sellahewa, H., & Jassim, S. (2011). Accuracy and Security Evaluation of Multi-Factor Biometric Authentication. *International Journal for Information Security Research*, *1*(1), 11–19. https://doi.org/10.20533/ijisr.2042.4639.2011.0002

Alzubaidi, L., Zhang, J., Humaidi, A. J., Al-Dujaili, A., Duan, Y., Al-Shamma, O., Santamaría, J., Fadhel, M. A., Al-Amidie, M., & Farhan, L. (2021). Review of deep learning: concepts, CNN architectures, challenges, applications, future directions. In *Journal of Big Data* (Vol. 8, Issue 1). Springer International Publishing. https://doi.org/10.1186/s40537-021-00444-8

Anjana, R., Preethi, P. R., Sujitha, J., & Karthika, S. (2022). Smart Security System for Vehicle Anti-Theft. *International Journal of Research and Analytical Reviews*, *9*(2), 209–214. www.ijrar.org

Arabelli, R. R., & Revuri, K. (2019). Fingerprint and Raspberri Pi based vehicle authentication and secured tracking system. In *International Journal of Innovative Technology and Exploring Engineering* (Vol. 8, Issue 5). https://www.researchgate.net/publication/344015936

Arduino. (2024). *Arduino IDE*. https://www.arduino.cc/en/software

Arora, S., & Bhatia, M. P. S. (2022). Challenges and opportunities in biometric security: A survey. *Information Security Journal*, *31*(1), 28–48. https://doi.org/10.1080/19393555.2021.1873464

Bakr, M., Abdel-Gaber, S., Nasr, M., & Hazman, M. (2022). Tomato Disease Detection Model Based on Densenet and Transfer Learning. *Applied Computer Science*, *18*(2), 56–70. https://doi.org/10.35784/acs-2022-13

Bayometric. (2024). *Fingerprint Technology*. https://www.bayometric.com/fingerprint-reader-technology-comparison/

Bhargav, B., Krishna, D., & Abudhagir, U. (2022). *Real Time Vehicle Security System Using Face Recognition and Finger Print*. *71*(3), 1731–1744.

Bisogni, C., Cascone, L., Nappi, M., & Pero, C. (2024). IoT-enabled Biometric Security: Enhancing Smart Car Safety with Depth-based Head Pose Estimation. *ACM Transactions on Multimedia Computing, Communications, and Applications*, *20*(6), 1–24. https://doi.org/10.1145/3639367

Bukola, A. (2020). Development of an Anti-Theft Vehicle Security System using GPS and GSM Technology with Biometric Authentication. In *International Journal of Innovative Science and Research Technology* (Vol. 5, Issue 2). www.ijisrt.com

Carney, M., & Webster, B. (2020). *Teachable Machine : Approachable Web-Based Tool for Exploring Machine Learning Classification*.

Chandran, P., Pragadeeshwaran, Ranjith, Mani Sivaraja Pandi, & Kumaresan. (2023). Smart theft detection of vehicles by GSM and GPS with fingerprint verification. *International Research Journal of Engineering and Technology (IRJET)*, *10*(4). www.irjet.net

Claesen, M., & De Moor, B. (2015). *Hyperparameter Search in Machine Learning*.

Conti, V. (2017). Biometric Authentication Overview: a Fingerprint Recognition Sensor Description. *International Journal of Biosensors & Bioelectronics*, *2*(1), 26–31. https://doi.org/10.15406/ijbsbe.2017.02.00011

Dasani, A. R. (2022). Biometric Ignition and Vehicle Safety System-A Novel Approach to Reduce Vehicle Theft. *International Journal of Scientific Research and Engineering Development*, *5*(4), 4–10. www.ijsred.com

Dhir, V., Kumar, R., & Singh, G. (2010). BIOMETRIC RECOGNITION: A MODERN ERA FOR SECURITY. In *International Journal of Engineering Science and Technology* (Vol. 2, Issue 8).

Elngar, A. A., & Kayed, M. (2020). Vehicle Security Systems using Face Recognition based on Internet of Things. *Open Computer Science*, *10*(1), 17–29. https://doi.org/10.1515/comp-2020-0003

Europol. (2020). *Vehicle Crime*. https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/vehicle-crime

F. Adebayo, A., M. Iyabode, A., N. Nureni, Y., & A. Kikelomo, A. (2015). Electronic Theft

Deterrent Biometric Module: An Automated Immobilizer and Access Control System for Millennium Vehicles. *International Journal of Electronics and Communication Engineering*, *2*(12), 1–6. https://doi.org/10.14445/23488549/ijece-v2i12p101

Francesco Turroni. (2012). Fingerprint Recognition : Enhancement , Feature Extraction and Automatic Evaluation of Algorithms. *Alma Mater Studiorum Università Di Bologna. Dottorato Di Ricerca in Informatica, 24 Ciclo*. http://amsdottorato.unibo.it/id/eprint/4378

Godavari, W. (2022). *Implementation of Machine Learning Based Google Teachable Machine in Early Childhood Education Implementation of Machine Learning Based Google Teachable Machine in Early Childhood Education Computer Science Engineering Department*. *May*.

Google Colab. (2020). *Google Colab*. Getting Started - Introduction. https://research.google.com/colaboratory/intl/es/faq.html

Hamidi, E. A. Z., Effendi, M. R., Mulyana, E., & Mardiati, R. (2023). Implementation security system using motorcycle fingerprint identification and notification Telegram. *Telkomnika (Telecommunication Computing Electronics and Control)*, *21*(1), 88–96. https://doi.org/10.12928/TELKOMNIKA.v21i1.24250

Hangzhou Grow Technology Co., L. (2012). R307S fingerprint module user manual. In *Data Base* (Vol. 3304, Issue January).

Hans, R. T. (2015). Using a biometric system to control access and exit of vehicles at shopping malls in South Africa. *2014 4th International Conference on Engineering Technology and Technopreneuship, ICE2T 2014*, *2014-Augus*(I4ct), 148–151. https://doi.org/10.1109/ICE2T.2014.7006236

Hyundai. (2018). *Hyundai Reveals World's First Smart Fingerprint Technology to Vehicle*. https://www.hyundai.news/eu/articles/press-releases/hyundai-reveals-worlds-first-smart-fingerprint-technology-to-vehicles.html#:~:text=Hyundai Motor Company announced the,the first quarter of 2019.

Institute of Electrical and Electronics Engineers., IEEE ITSS., & Institute of Electrical and Electronics Engineers. Bombay Section. (2009). *ICVES 2009 : 2009 IEEE International Conference on Vehicular Electronics and Safety : November 11-12, 2009, Pune, India*. IEEE.

Juba, B., & Le, H. S. (2019). Precision-Recall versus accuracy and the role of large data sets. *33rd AAAI Conference on Artificial Intelligence, AAAI 2019, 31st Innovative Applications of Artificial Intelligence Conference, IAAI 2019 and the 9th AAAI Symposium on Educational*

*Advances in Artificial Intelligence, EAAI 2019*, 4039–4048. https://doi.org/10.1609/aaai.v33i01.33014039

Khairnar, N. S., & Khairnar, R. S. (2018). *IOT based Electricity Theft Detection*. *1*(8), 75–78.

Khan, M. B., Khan, M. K., Jiashu, Z., & Zhang, D. Y. (2005). Implementing biometric security in intelligent transportation systems (ITS). *2005 Pakistan Section Multitopic Conference, INMIC*. https://doi.org/10.1109/INMIC.2005.334388

Kiruthiga, N., Latha, L., & Thangasamy, S. (2015). Real time biometrics based vehicle security system with GPS and GSM technology. *Procedia Computer Science*, *47*(C), 471–479. https://doi.org/10.1016/j.procs.2015.03.231

Konatham, H. R., Sunchu, P., Reddy Bojja, A., Reddy, K. H., Pranay, S., Reddy, B. A., & Phani Vidyadhar, R. (2023). *Intelligent Automotive Safety and Security System For Vehicles*. https://doi.org/10.22541/au.167308279.91194622/v1

Kumar, V., Mohammed Ali Al-Tameemi, A., Kumari, A., Ahmad, M., Falah, M. W., & Abd El-Latif, A. A. (2022). PSEBVC: Provably Secure ECC and Biometric Based Authentication Framework Using Smartphone for Vehicular Cloud Environment. *IEEE Access*, *10*(August), 84776–84789. https://doi.org/10.1109/ACCESS.2022.3195807

Kute, R., Vyas, V., & Anuse, A. (2021). Transfer learning for face recognition using fingerprint biometrics. *Journal of King Saud University - Engineering Sciences*. https://doi.org/10.1016/j.jksues.2021.07.011

Landgeist. (2024). *Car theft rate in Europe*. https://landgeist.com/2024/01/19/car-theft-rate-in-europe/

Last, L., & Edt, A. M. (2014). *Adafruit Optical Fingerprint Sensor*.

Lozoya-Santos, J. de J., Sepúlveda-Arróniz, V., Tudon-Martinez, J. C., & Ramirez-Mendoza, R. A. (2019). Survey on biometry for cognitive automotive systems. *Cognitive Systems Research*, *55*, 175–191. https://doi.org/10.1016/j.cogsys.2019.01.007

Ltd, R. P. (2024). *Getting started with your Raspberry Pi*. https://www.raspberrypi.com/documentation/computers/getting-started.html

Malhotra, D., Bhatia, M. K., Shahi, A., & Narula, J. (2022). *Vehicle Theft Control System using Fingerprint Sensor and IOT Devices*. *9*(11), 20090–20097.

Marie, Z. G., & Huluka, A. W. (2023). *Design of a Camera-Based Driver Monitoring System With Deep Learning Convolutional Neural Network To Prevent Onboard Catha Edulis Leaf*

*Chewing*.

MDPI. (2018). *Capacitive Fingerprint Sensor*. https://www.mdpi.com/1424-8220/18/7/2200

Muhammad Syarif Hartawan. (2022). Design and Build a Facial Recognition Based Motor Vehicle Security System. *International Journal of Science, Technology & Management*, *3*(1), 209–214. https://doi.org/10.46729/ijstm.v3i1.414

National Highway Traffic Safety Administration (NHTSA). (2022). *Vehicle Theft Prevention.* https://www.nhtsa.gov/road-safety/vehicle-theft-prevention

National Insurance Crime Bureau (NICB). (2021). *Hot Wheels Report: A Comprehensive Analysis of Vehicle Theft in the United States.* https://www.nicb.org/news/news-releases/2020-hot-wheels-report-a-comprehensive-analysis-of-vehicle-theft-in-the-united-states.

New Bussiness Ethiopia. (2022). *Cars stolen in Addis Ababa*. https://newbusinessethiopia.com/crime/211-cars-stolen-in-addis-ababa/

Obaidat, M. S., Rana, S. P., Maitra, T., Giri, D., & Dutta, S. (2018). Biometric security and internet of things (IOT). In *Biometric-Based Physical and Cybersecurity Systems*. https://doi.org/10.1007/978-3-319-98734-7_19

Office for National Statistics (ONS). (2021). *Crime in England and Wales: Year Ending March 2021*. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2021.

Pawar, M. R., & Rizvi, I. (2018). IoT Based Embedded System for Vehicle Security and Driver Surveillance. *Proceedings of the International Conference on Inventive Communication and Computational Technologies, ICICCT 2018, Icicct*, 466–470. https://doi.org/10.1109/ICICCT.2018.8472984

Pi, R. (2020). Raspberry Pi 4 Computer Model B. *Raspberrypi.Org*, *May*, 1–6. https://www.researchgate.net/figure/Raspberry-pi-4-Model-B-processor_fig1_345261155

Police, H. (2023). *Vehicle theft image*. https://www.haltonpolice.ca/en/staying-safe/resources/b---vehicle-theft---GettyImages-526745055.jpg

Rafay, A., Hasan, Y., & Iqbal, A. (2019). Recognition of fingerprint biometric system access control for car memory settings through artificial neural networks. In *Advances in Intelligent Systems and Computing* (Vol. 887). Springer International Publishing. https://doi.org/10.1007/978-3-030-03405-4_26

Ramesh, M., Akruthi, S., Nandhini, K., Meena, S., Joseph Gladwin, S., & Rajavel, R. (2019). Implementation of Vehicle Security System using GPS,GSM and Biometric. *Proceedings - 2019 Women Institute of Technology Conference on Electrical and Computer Engineering, WITCON ECE 2019*, 71–75. https://doi.org/10.1109/WITCONECE48374.2019.9092918

ResearchGate. (2015). *Ultrasonic Fingerprint Scanner*. https://www.google.com/imgres?q=ultrasonic fingerprint sensor working principle&imgurl=https%3A%2F%2Fwww.researchgate.net%2Fpublication%2F285770473%2Ffigure%2Ffig5%2FAS%3A614398913683465%401523495524613%2F6-Ultrasonic-fingerprint-sensor-based-on-micromach

ResearchGate. (2019). *Biometric modality comparison*. https://www.researchgate.net/figure/Biometric-modality-comparison_tbl3_332737027

ResearchGate. (2020). *Convolutional Neural Networks*. https://www.researchgate.net/figure/Example-of-architecture-of-a-convolutional-neural-network-for-binary-classification_fig1_343699218

Sadhukhan, S., Acharyya, A., & Prasad, R. (2017). Car Security System using Fingerprint scanner and IOT. *Indian Journal of Science and Technology*, *10*(40), 1–4. https://doi.org/10.17485/ijst/2017/v10i40/109854

Sardar, A., Umer, S., Rout, R. K., Sahoo, K. S., & Gandomi, A. H. (2024). Enhanced Biometric Template Protection Schemes for Securing Face Recognition in IoT Environment. *IEEE Internet of Things Journal*, *PP*(8), 1. https://doi.org/10.1109/JIOT.2024.3374229

Saritha, N., & Arun, P. (2018). Fingerprint based security system for vehicles. In *International Journal of Advance Research*. www.IJARIIT.com

Springer. (2020). *Face Recognition Using CNN*. https://media.springernature.com/lw685/springer-static/image/chp%3A10.1007%2F978-981-15-7106-0_31/MediaObjects/500709_1_En_31_Fig3_HTML.png

Srinivasan, P., Anthoniraj, S., Anguraj, K., Kumarganesh, S., & Thiyaneswaran, B. (2021). Development of keyless biometric authenticated vehicles ignition system. *Materials Today: Proceedings*, *81*(2), 464–469. https://doi.org/10.1016/j.matpr.2021.03.632

Stanwood, R. H. (2023). Design and implementation of an integrated information system. *Journal of Spacecraft and Rockets*, *5*(3), 361–362. https://doi.org/10.2514/3.59586

Sundararajan, S. N. (2022). BIOMETRIC AND RFID BASED VEHICLE SECURITY SYSTEM.

In *International Journal of Engineering Applied Sciences and Technology* (Vol. 6). http://www.ijeast.com

Tamilselvan, K. S., Murugesan, G., & Sasikumar, S. (2018). Design and implementation of biometric based smart antitheft bike protection system. *Proceedings of IEEE International Conference on Intelligent Computing and Communication for Smart World, I2C2SW 2018*, 136–138. https://doi.org/10.1109/I2C2SW45816.2018.8997118

Taywade, S. R., & Bhiwani, R. J. (2022). *Car security system using biometrics*. https://d1wqtxts1xzle7.cloudfront.net/52558564/16December10.pdf?1491752285=&response-content-disposition=inline%3B+filename%3DCAR_SECURITY_SYSTEM_USING_BIOMETRICS.pdf&Expires=1602695466&Signature=ZHHy2C~gH2478k50Cn2AmtgPufknaFYFz0S0tE2s5VVy7hxi2X3Vq01J-ub

The Reporter. (2022). *Stolen car report in Addis*. https://www.thereporterethiopia.com/22174/

Tippannavar, S. S., D, Y. S., & Madappa, E. A. (2023). Two Factor Authentication using RFID and Biometric sensor – A Progressive Review. *International Journal of Advanced Research in Computer and Communication Engineering ISO*, *12*(6). https://doi.org/10.17148/IJARCCE.2023.12647

Traore, A., Ata-Ul-karim, S. T., Duan, A., Soothar, M. K., Traore, S., & Zhao, B. (2021). Predicting equivalent water thickness in wheat using UAV mounted multispectral sensor through deep learning techniques. *Remote Sensing*, *13*(21). https://doi.org/10.3390/rs13214476

Uma Maheswari, K., Balasubramanian, K., Ishwarya Niranjana, M., Dhanu Aravinth, K., Karthik, V., & Padmanaban, V. K. (2023). Smart Multi Verification Based Security System. *El-Cezeri Journal of Science and Engineering*, *10*(2), 193–207. https://doi.org/10.31202/ecjse.1099817

Vikhankar, A D, P. R. . C. (2016). *Advanced Vehicle Security System with Theft*. *5*(7,July 2016), 12881–12894.

Villa, M., Gofman, M., & Mitra, S. (2018). Survey of Biometric Techniques for Automotive Applications. *Advances in Intelligent Systems and Computing*, *738*, 475–481. https://doi.org/10.1007/978-3-319-77028-4_62

Vol, T. (2016). *Visual Studio Code*. *1*(March), 1–26.

Wirtz, B. (2004). Biometric System Security. *Securing Electronic Business Processes*, 108–119.

https://doi.org/10.1007/978-3-322-84982-3_12

Yusuf, S. D., Dalhatu, A., Umar, I., & Loko, A. Z. (2022). Simulation and Construction of Fingerprint Vehicle Starter System Using Microcontroller. *International Journal of Research and Scientific Innovation*, *09*(09), 135–144. https://doi.org/10.51244/ijrsi.2022.9912

Zamin, A. K., Sajida, K., & Darakhshan, S. (2022). Vehicle Anti-Theft Face Recognition System Based on IoT using Raspberry Pi4. *Journal of Information & Communication Technology*, *16*(2).

Zhang, K., Wu, Q., Liu, A., & Meng, X. (2018). Can deep learning identify tomato leaf disease? *Advances in Multimedia*, *2018*. https://doi.org/10.1155/2018/6710865

# APPENDIX

### A1. Fingerprint enrollment code by Adafruit

```
#include <Adafruit_Fingerprint.h>
SoftwareSerial mySerial(3, 2);
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
uint8_t id;

void setup()
{
Serial.begin(9600);
while (!Serial); // For Yun/Leo/Micro/Zero/...
delay(100);
Serial.println("\n\nAdafruit Fingerprint sensor enrollment");

// set the data rate for the sensor serial port
finger.begin(57600);

if (finger.verifyPassword()) {
Serial.println("Found fingerprint sensor!");
} else {
Serial.println("Did not find fingerprint sensor :(");
while (1) { delay(1); }
}
}

uint8_t readnumber(void) {
uint8_t num = 0;

while (num == 0) {
while (! Serial.available());
```

```
num = Serial.parseInt();
}
return num;
}

void loop() // run over and over again
{
Serial.println("Ready to enroll a fingerprint!");
Serial.println("Please type in the ID # (from 1 to 127) you want to
save this finger as...");
id = readnumber();
if (id == 0) {// ID #0 not allowed, try again!
return;
}
Serial.print("Enrolling ID #");
Serial.println(id);

while (! getFingerprintEnroll() );
}

uint8_t getFingerprintEnroll() {

int p = -1;
Serial.print("Waiting for valid finger to enroll as #");
Serial.println(id);
while (p != FINGERPRINT_OK) {
p = finger.getImage();
switch (p) {
case FINGERPRINT_OK:
Serial.println("Image taken");
break;
```

```
case FINGERPRINT_NOFINGER:
Serial.println(".");
break;
case FINGERPRINT_PACKETRECIEVEERR:
Serial.println("Communication error");
break;
case FINGERPRINT_IMAGEFAIL:
Serial.println("Imaging error");
break;
default:
Serial.println("Unknown error");
break;
}
}

// OK success!

p = finger.image2Tz(1);
switch (p) {
case FINGERPRINT_OK:
Serial.println("Image converted");
break;
case FINGERPRINT_IMAGEMESS:
Serial.println("Image too messy");
return p;
case FINGERPRINT_PACKETRECIEVEERR:
Serial.println("Communication error");
return p;
case FINGERPRINT_FEATUREFAIL:
Serial.println("Could not find fingerprint features");
return p;
```

```
case FINGERPRINT_INVALIDIMAGE:
Serial.println("Could not find fingerprint features");
return p;
default:
Serial.println("Unknown error");
return p;
}

Serial.println("Remove finger");
delay(2000);
p = 0;
while (p != FINGERPRINT_NOFINGER) {
p = finger.getImage();
}
Serial.print("ID "); Serial.println(id);
p = -1;
Serial.println("Place same finger again");
while (p != FINGERPRINT_OK) {
p = finger.getImage();
switch (p) {
case FINGERPRINT_OK:
Serial.println("Image taken");
break;
case FINGERPRINT_NOFINGER:
Serial.print(".");
break;
case FINGERPRINT_PACKETRECIEVEERR:
Serial.println("Communication error");
break;
case FINGERPRINT_IMAGEFAIL:
Serial.println("Imaging error");
```

```
break;
default:
Serial.println("Unknown error");
break;
}
}

// OK success!

p = finger.image2Tz(2);
switch (p) {
case FINGERPRINT_OK:
Serial.println("Image converted");
break;
case FINGERPRINT_IMAGEMESS:
Serial.println("Image too messy");
return p;
case FINGERPRINT_PACKETRECIEVEERR:
Serial.println("Communication error");
return p;
case FINGERPRINT_FEATUREFAIL:
Serial.println("Could not find fingerprint features");
return p;
case FINGERPRINT_INVALIDIMAGE:
Serial.println("Could not find fingerprint features");
return p;
default:
Serial.println("Unknown error");
return p;
}
```

```
// OK converted!
Serial.print("Creating model for #"); Serial.println(id);

p = finger.createModel();
if (p == FINGERPRINT_OK) {
Serial.println("Prints matched!");
} else if (p == FINGERPRINT_PACKETRECIEVEERR) {
Serial.println("Communication error");
return p;
} else if (p == FINGERPRINT_ENROLLMISMATCH) {
Serial.println("Fingerprints did not match");
return p;
} else {
Serial.println("Unknown error");
return p;
}

Serial.print("ID "); Serial.println(id);
p = finger.storeModel(id);
if (p == FINGERPRINT_OK) {
Serial.println("Stored!");
} else if (p == FINGERPRINT_PACKETRECIEVEERR) {
Serial.println("Communication error");
return p;
} else if (p == FINGERPRINT_BADLOCATION) {
Serial.println("Could not store in that location");
return p;
} else if (p == FINGERPRINT_FLASHERR) {
Serial.println("Error writing to flash");
return p;
} else {
```

```
Serial.println("Unknown error");
return p;
}
}
```

**A2. Enrolled fingerprints template digital signature and image**

```
Found fingerprint sensor!
------------------------------------
Attempting to load #1
Template 1 loaded
Attempting to get #1
Template 1 transferring:
495 bytes read.
Decoding packet...
03015A188E00F8FEF0068006000200020002000200000000000000000000280028006C0
0EF07EFFFE00000000000000000000000000005C2D078B525519D0F22BACAC7A25BFEF
01FFFFFFFF0200822D09E3B337AAAB3B511BE772332C55F83934169235340010000000
0000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000916EF01
FFFFFFFF020082030161138F00FFFEFFFEFFFEF01E800600060006000200020002000 2
000200020006800EE03EF9000000000000401B92FE0823033E52A6125E63A751DE3EAF
EA1E47BD6B3E4E9367570D9F1B1F1B9F80BF5DA0273F2A38003F2B206ABC2EA356BC1C
AE813C312A6AFD2AAC153A32B3D752222D2C5B2799EF01FFFFFFFF0800822DB380D200
0000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000002BCFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
done.
------------------------------------
```

------------------------------------

Attempting to load #2

Template 2 loaded

Attempting to get #2

Template 2 transferring:

495 bytes read.

Decoding packet...

030157168E00FFFEFFFEF0FEC03EC00E8006800600020002000200020002800680
06E00EF01E00000000000000000000000000009313A21E72243497F350B056D12871EF
01FFFFFFFF02008243AC80144B2C969255AE29AC5712D5500000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000070CEF01
FFFFFFFF0200820301463187000000000000000000000000000000000000000000000
00000000000000000000000000000000002DAF029E2EA85BFF3CB1987E3734415E4535
97BE3E0EE33F5613CB7F4C3A561F488DCB7E450DE5BF6C9CA4FE64B6A83E6B3F133F12
39C4DF561B133D50B794DA5D9C8E5A4AB86B5A20B0EF01FFFFFFFF0800825917E0FB5B
9EE4D6263286B64E140A365095A170169B1ECE2B9A9E8F1DBB876F610C208E568CCAAE
2B9A9E8F2E3F182F2FB7026E6016E22F1A07608F64848ECF0AA31C2E3014E04C489461
AA3641CA0A103F1B0A3014622675AED1063684A4861804618727BFC1652D391D253FC2
53C5514294025DB5E9832DA69C020000000030FEFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

done.

------------------------------------

```
------------------------------------
Attempting to load #3
Template 3 loaded
Attempting to get #3
Template 3 transferring:
495 bytes read.
Decoding packet...
030163258A00F80EF00280000000000000000000000000000000000000000000000000
000000F80E00000000000000000000000000001E6D3D023E0C3F845E619BD4FF1FD9EF
01FFFFFFFF020082732814DF27AA82FF6232ACFF7433EBD72FBEC35F4308163C3C086C
7C4810D61C5413159C509DEC5C600D93FA420DEB9A52102ABA619068FA3F112C9A54A3
EC9A462E81FA5420EC384BAD8099000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000220DEF01
FFFFFFFF020082030166279A0000000000000000000000000000000000000000000000
00000000000000000000000000000000004694EB7E2B96015E0717423E1918991E4DB8
C27E3041041E1B9DC25F48A1175F05A3035F56A42CFF283382BF3B20C0FE411E801E5D
1555DE659A54FE68A56CFF63AE41BF6DAE403F1EA2EF01FFFFFFFF080082498355DE78
A5155E0F9242CE4030020E4545462E0F3C844F4030020E4291AC2E548E55AE641154CE
73B36C8F4A0EEC2E771ECE6E3107C02E1E9A834655A540863AA042865E95D5C665B300
876830D766690292050000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000002080FFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
done.
------------------------------------
```

```
------------------------------------
Attempting to load #4
Template 4 loaded
Attempting to get #4
Template 4 transferring:
495 bytes read.
Decoding packet...
030163158D00FFFEFF06FF06E000C00000000000000000000000000000000000000000
00000280060000000000000000000000000000001F243DD53F473FD31F2022983C2483EF
01FFFFFFFF0200826430E8D470AB13DD6A2ED252000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000069BEF01
FFFFFFFF0200820301631B940000000000000000000000000000000000000000000000
0000000000000000000000000000000000598C507E4B0F113E3413D47E6315661E2016
AB5E2819555E5B19D0DE1C9E565E2A9F29DE2F26945E5DB1CFFE3E33D2BE0C346CBE67
A20FFF0BA3ECBF33AE53FF58B510DF7313D05E1FFEEF01FFFFFFFF0800823A1F932E15
AD966E2D3FD42E3C08928E3A1F932E75184E0E721C650D2CAA006831AA150900000000
0000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000B76FFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
done.
------------------------------------
```

**A3. Face recognition test code**

```
import cv2
# import requests
import numpy as np

from tensorflow.keras.models import load_model

# Initialize model
model = load_model('model/keras_model.h5')

# Load class
with open('model/labels.txt') as f:
    classes = tuple(label.strip() for label in f.readlines())
url = 'http://192.168.1.3:8080/shot.jpg'
camera = cv2.VideoCapture(0)

while True:
    ret, frame = camera.read()

# img_resp = requests.get(url)
    # img_arr = np.array(bytearray(img_resp.content), dtype=np.uint8)
    # frame = cv2.imdecode(img_arr, -1)

# Resize the raw image into (224-height,224-width) pixels.
   image = cv2.resize(frame, (224, 224), interpolation=cv2.INTER_AREA)
   image = np.asarray(image, dtype=np.float32).reshape(1, 224, 224, 3)

# Normalize the image array
    image = (image / 127.5) - 1
    prediction = model.predict(image)
    label = classes[prediction.argmax()]
```

```
    cv2.putText(frame, label, (15, 20),
                cv2.FONT_HERSHEY_PLAIN, 1, (200, 0, 200), 2)
    cv2.imshow('Frame', frame)
    if cv2.waitKey(1) == 27:  # click ESC to close window
        break
camera.release()
cv2.destroyAllWindows()
```

**A4. Theft deterrence test code**

```
#include <NewPing.h>
#include <SoftwareSerial.h>

#define TRIGGER_PIN          9   // Arduino pin tied to trigger pin on
the ultrasonic sensor.
#define ECHO_PIN             10  // Arduino pin tied to echo pin on
the ultrasonic sensor.
#define SHOCK_SENSOR_PIN     2   // Digital pin for the shock sensor.
#define RELAY_PIN           11  // Arduino pin connected to the relay.
#define BUZZER_PIN           12  // Arduino pin connected to the
buzzer.
#define GSM_TX               3   // A6 Tx connected to Arduino pin 3
#define GSM_RX               4   // A6 Rx connected to Arduino pin 4
#define MAX_DISTANCE         200  // Maximum distance we want to ping
for (in centimeters).
#define SHOCK_THRESHOLD      HIGH // Adjust based on your sensor's
characteristics.

NewPing sonar(TRIGGER_PIN, ECHO_PIN, MAX_DISTANCE); // NewPing setup
of pins and maximum distance.
SoftwareSerial gsmSerial(GSM_TX, GSM_RX); // Create a SoftwareSerial
object for GSM communication.
void setup() {
  pinMode(RELAY_PIN, OUTPUT);
  pinMode(BUZZER_PIN, OUTPUT);
  Serial.begin(9600);
  gsmSerial.begin(9600);
  // Initialize GSM module
  gsmInit();
}
```

```
void loop() {
  // Measure the current distance.
  unsigned int currentDistance = sonar.ping_cm();
  // Read the shock sensor value.
  int shockValue = digitalRead(SHOCK_SENSOR_PIN);
  // Print the current distance and shock sensor value to the Serial
Monitor.
  Serial.print("Distance: ");
  Serial.print(currentDistance);
  Serial.print(" cm | Shock Sensor: ");
  Serial.println(shockValue == HIGH ? "HIGH" : "LOW");
  // Check for significant shock or presence.
  if (shockValue == SHOCK_THRESHOLD || currentDistance < MAX_DISTANCE)
{
    // Trigger the alarm, activate the relay, and make a call.
    activateAlarm();
    activateRelay();
    makeCall();
  }
else
{
    // Reset the alarm, deactivate the relay, and allow normal
operation.
    deactivateAlarm();
    deactivateRelay();
  }
  // Wait for some time before taking the next measurement.
  delay(1000);
}
void activateAlarm() {
```

```
  // Turn on the buzzer to activate the alarm.
  digitalWrite(BUZZER_PIN, HIGH);
}
void deactivateAlarm() {
  // Turn off the buzzer to deactivate the alarm.
  digitalWrite(BUZZER_PIN, LOW);
}
void activateRelay() {
  // Activate the relay to take action based on your specific
application.
  digitalWrite(RELAY_PIN, HIGH);
}
void deactivateRelay() {
  // Deactivate the relay to return to normal operation.
  digitalWrite(RELAY_PIN, LOW);
}
void gsmInit() {
  gsmSerial.println("AT");
  delay(1000);
  updateGsmSerial();
  gsmSerial.println("AT+CMGF=1"); // Set SMS mode to text
  delay(1000);
  updateGsmSerial();
}
void makeCall() {
  gsmSerial.println("ATD+251*********;"); // Replace with the
recipient's phone number
  delay(1000);
  updateGsmSerial();
}
void updateGsmSerial() {
```

```
  delay(500);
  while (Serial.available()) {
    gsmSerial.write(Serial.read());
  }
  while (gsmSerial.available()) {
    Serial.write(gsmSerial.read());
  }
}
```

**A5. ERR plot code**

```
import numpy as np
import matplotlib.pyplot as plt

# False Rejection Ratio (FRR) in percentage
frr = 0.1 / 100

# False Acceptance Ratio (FAR) in percentage
far = 0.001 / 100

# Generate a range of decision thresholds (0% to 100%)
thresholds = np.linspace(0, 1, 1000)

# Calculate FAR and FRR for each threshold
frr_values = frr * (1 - thresholds)**2
far_values = far * thresholds**2

# Plot FAR and FRR
plt.figure(figsize=(8, 6))
plt.plot(far_values, frr_values, color='blue')

# Mark the intersection point
intersection_point = np.argmin(np.abs(frr_values - far_values))
plt.plot(far_values[intersection_point],
frr_values[intersection_point], 'ro')  # Mark intersection

# Annotate intersection point
plt.annotate('ERR',
             xy=(far_values[intersection_point],
frr_values[intersection_point]),
```

```
             xytext=(far_values[intersection_point] + 0.00002,
frr_values[intersection_point] + 0.0002),
             arrowprops=dict(facecolor='black', shrink=0.05))

plt.xlabel('FAR')
plt.ylabel('FRR')
plt.title('FAR vs FRR Curve')
plt.grid(True)
plt.show()
```