LicenseLense System

By

PRIVELEDGE GURURE

(H200705P)

HIT400 Capstone project Submitted in Partial Fulfillment of the

Requirements of the degree of

Bachelor of Technology

In

Software Engineering

In the

School of Information Sciences and Technology

Harare Institute of Technology

Zimbabwe

Supervisor: MR W MAKONDO
May/2024

ABSTRACT

This documentation describes the development of a facial recognition system for identifying licensed drivers, with the objectives of verifying driver identity and criminal record status, and implementing fingerprint scanning as a secondary authentication method. The system aims to improve road safety and prevent illegal activities by ensuring that only authorized drivers operate vehicles.

The system uses a facial recognition algorithm to identify licensed drivers, which is integrated with a database of driver information and criminal records. In cases where facial recognition is compromised due to facial deformation, fingerprint scanning is used as a secondary authentication method.

The system has been designed to ensure accuracy, security, and privacy, with a user-friendly interface for easy adoption. The documentation includes a detailed description of the system architecture, data flow, and processing steps, as well as an evaluation of alternative systems and a comparison of their advantages and disadvantages.

The facial recognition system has the potential to revolutionize the way we verify driver identity and ensure road safety, and this documentation provides a comprehensive guide for its development and implementation.

PREFACE

The LicenseLense System which is an integration of Facial Recognition and Fingerprint Authentication for Licensed Drivers is a cutting-edge biometric identification solution designed to revolutionize the way driver identities are verified and authenticated. This system is the result of innovative thinking, rigorous development, and thorough testing, and is poised to make a significant impact in the fields of transportation, law enforcement, and public safety.

This documentation provides a comprehensive overview of the system, including its architecture, functionality, and technical specifications. It is intended to serve as a reference guide for system administrators, developers, and users, and provides detailed information on the installation, configuration, and operation of the system.

This documentation is intended for developers, system administrators, and law enforcement agencies who will be implementing and using this system. It provides a detailed understanding of the system's architecture, functionality, and maintenance requirements. LicenseLense will contribute to the improvement of road safety and the prevention of illegal activities on our roads.

ACKNOWLEDGEMENT

I would like to express my deepest gratitude and appreciation to all those who have supported me throughout the successful completion of this project.

First and foremost, I would like to thank the Lord Almighty, whose presence and grace has been with me from start of this program till now that l am achieving a great milestone.

I would like to thank my supervisor **Mr Makondo** for his invaluable guidance, expertise, and continuous support throughout the entire research process. His insightful feedback, constructive criticism, and encouragement have been instrumental in shaping and refining this project.

I am also immensely grateful to the faculty members of the Software Engineering department, whose teachings and mentorship have provided me with a strong foundation in my field of study. Their passion for academic and dedication to imparting knowledge have been truly inspiring.

I would like to express my sincere gratitude to **Mrs Chibaya, Mr. Mukosera, Miss Amos, Mr. Manjoro, Miss Zindove and Mr. Chiworera** and for their unending support. It is the insight they gave me that added value to this project.

Furthermore, I extend my gratitude to the participants who volunteered their time and expertise for user testing and evaluation. Their feedback and suggestions have been invaluable in refining this system and ensuring its usability and effectiveness.

I extend my heartfelt thanks to my mother for being prayer warrior and providing for me throughout the journey. I am also grateful to my family and friends for their unwavering support and belief in me. Their encouragement, patience, and understanding have been my pillars of strength during the ups and downs of this academic pursuit. I am grateful for their love, encouragement, and motivation that have kept me going.

To all those who have contributed directly or indirectly to the realization of this capstone project, I extend my heartfelt thanks. Your support and encouragement have been essential in making this project a success.

DEDICATION

The development of the Licensed Driver Identification and Verification System is not just a technical endeavor, but a tribute to those who have been impacted by the consequences of unlicensed driving. This system is dedicated to individuals and organizations who have worked tirelessly to improve road safety and reduce the risk of unlicensed driving. Their efforts, commitment, and passion have inspired us to create a solution that can make a meaningful difference in the lives of many. We humbly dedicate this system to:

Ministry of Transport and Infrastructural Development, Zimbabwe: As the government entity responsible for overseeing transportation in Zimbabwe, I dedicate this system to them recognizing their efforts in improving road safety and regulating driver licenses.

Zimbabwe Republic Police: As the law enforcement agency is responsible for enforcing traffic regulations and verifying driver licenses, I dedicate this system to them acknowledging their critical role in maintaining public safety.

The families of road accident victims: Dedicating this system to those who have lost loved ones due to unlicensed or irresponsible driving.

The people of Zimbabwe: A broader dedication to the citizens of Zimbabwe recognizing the system's potential to benefit the entire nation by enhancing road safety and reducing the risk of unlicensed driving.

Lastly, I dedicate this capstone project to all those who aspire to make a positive difference in the world of Information and Communication Technology. May this work serve as a stepping stone for further research, innovation and advancements in the pursuit of knowledge and betterment of society.

Declaration

I, Priveledge Gurure, solemnly declare that the work presented in this capstone project documentation is the result of my original research and efforts. I affirm that all the information, data and materials used in this project are duly acknowledged and referenced. I understand that failure to do this amount to plagiarism and will be considered grounds for failure in this dissertation and the degree examination as a whole.

HIT

Harare Institute of Technology

success through innovation

This is to certify that HIT 400 Project entitled “**LicenseLense System”** has been completed by **Gurure Priveledge** (H200705P) for partial fulfilment of the requirements for the award of **Bachelor of Technology** degree in **Software Engineering**. This work is carried out by **her** under my supervision and has not been submitted earlier for the award of any other degree or diploma in any university to the best of my knowledge.

Your Supervisor Name	**Approved/Not Approved**
Mr Makondo	
Project Supervisor	Project Coordinator
Signature: ……………………………	**Signature: …………………………………**
Date: ……………………………………	**Date: ………………………………………**

Certificate of Declaration

This is to certify that work entitled “**LicenseLense System**” is *submitted in partial fulfillment of the requirements for the award of Bachelor of Technology (Hons) in Software Engineering, Harare Institute of Technology. It is further certified that no part of research has been submitted to any university for the award of any other degree.*

HIT

Harare
Institute of
Technology

success through innovation

(Supervisor) Signature………………………. Date………………….

(Mentor) Signature………………………… Date………………….

(Chairman) Signature………………………… Date……………………

ITEM	TOTAL MARK /%	ACQUIRED/%
PRESENTATION- Format-Times Roman 12 for ordinary text, Main headings Times Roman 14, spacing 1.5. Chapters and sub-chapters, tables and diagrams should be numbered. Document should be in report form. Range of document pages. Between 50 and 100.Work should be clear and neat	**5**	
Pre-Chapter Section Abstract, Preface, Acknowledgements, Dedication & Declaration	**5**	
Chapter One-Introduction Background, Problem Statement, Objectives – smart, clearly measurable from your system. Always start with a TO… Hypothesis, Justification, Proposed Tools Feasibility study: Technical, Economic & Operational Project plan –Time plan, Gantt chart	**10**	
Chapter Two-Literature Review Introduction, Related work & Conclusion	**10**	
Chapter Three –Analysis Information Gathering Tools, Description of system Data analysis –Using UML context diagrams, DFD of existing system Evaluation of Alternatives Systems, Functional Analysis of Proposed System-Functional and Non-functional Requirements, User-Case Diagrams	**15**	
Chapter Four –Design Systems Diagrams –Using UML Context diagrams, DFD, Activity diagrams Architectural Design-hardware, networking Database Design –ER diagrams, Normalized Databases Program Design-Class diagrams, Sequence diagrams, Package diagrams, Pseudo code Interface Design-Screenshots of user interface	**20**	
Chapter Five-Implementation & Testing Pseudo code of major modules /Sample of real code can be written here Software Testing-Unit, Module, Integration, System, Database & Acceptance	**20**	
Chapter Six –Conclusions and Recommendations Results and summary, Recommendations & Future Works	**10**	
Bibliography –Proper numbering should be used Appendices –templates of data collection tools, user manual of the working system, sample code, research papers	**5**	
	100	**100**

Project Documentation Marking Guide

Table of Contents

Table of Figures

Chapter One: Introduction

1.1 Background

Road safety is a significant concern in Zimbabwe, with a high number of accidents attributed to factors like unlicensed drivers and human error. Drivers are required to carry their valid driver's license at all times while operating a vehicle. These licenses are issued by the Vehicle Inspectorate Department (VID) after passing a driving test and fulfilling all licensing requirements. Law enforcement officers (police) or other authorized personnel, such as VID officials during roadblocks, stop drivers for various reasons, including license checks. During a license check, the officer will request the driver's license and visually inspect it to ensure:

- The license is authentic and not forged.
- The license is valid and not expired.
- The driver's license class allows them to operate the specific vehicle they are driving.

The current system of relying on physical driver's licenses has limitations like forgery and difficulty in real-time verification. In Zimbabwe, the driver's licence verification process confronts a number of issues, including the availability of bogus licences, which represent a substantial risk to road safety and law enforcement activities. The manual verification procedure is highly reliant on manual examination, which is time-consuming, subject to human mistake, and inaccurate. There is limited access to the licence database because law enforcement officers frequently have difficulty accessing current licence records, resulting in delays and inefficiencies in the verification process. Zimbabwe has legislation in place to control driver licences, such as the Road Traffic Act.

However, the current system lacks a strong method for identity verification during licence checks. With advancements in face recognition and fingerprint scanning technologies, there is a chance to use these techniques to improve the driver's licence verification procedure in Zimbabwe. Counterfeit driver's licences can be used to commit identity theft by creating bank accounts or applying for loans in another person's name. Drivers with expired or invalid licences are more likely to be involved in accidents because they may be unfamiliar with current traffic laws or lack the essential skills and expertise to drive safely.

1.2 Problem statement

The current method for assessing licenced drivers in Zimbabwe, which is mostly based on physical licences and visual verification by authorities, poses various issues that might have a severe influence on road safety. People who own vehicles require a licence to drive them.

Sometimes drivers forget to bring their licence with them and are confronted by law enforcement agents for their defiance. The current manual process of checking driver's licences in Zimbabwe is difficult to manage, especially in high traffic areas. This can lead to increased wait times and delays for drivers, as well as potential safety issues if unlicensed drivers are allowed to operate vehicles.

Physical drivers' licences are vulnerable to falsification and manipulation. Criminals can make fake licences or change existing ones, allowing unauthorised drivers to operate vehicles. This creates a major security concern and raises the likelihood of accidents. The current system relies solely on visual checks by officers during traffic stops. These checks can be prone to human error, especially in situations like poor lighting or driver deception. Additionally, officers cannot instantly verify the license's validity or access the driver's complete record against a central database in real-time. Verifying a driver's license through visual inspection can be time-consuming, especially if the officer suspects a forgery. This can lead to delays and congestion on the roads. Physical licenses only provide basic information about the driver. Officers cannot readily access details like potential suspensions, restrictions or the license class, or past driving offenses during a routine check. A scannable system, like a QR code on the license, might only store basic driver information (name, photo, expiry date). It wouldn't necessarily offer access to a central database with complete driver records including potential suspensions or restrictions.

1.3 Objectives

1. To develop a facial recognition system for identifying licensed drivers.
2. To verify driver identity and criminal record status.
3. To implement fingerprint scanning as a secondary authentication method for driver identification systems where facial recognition may be compromised due to facial deformation.

1.4 Hypothesis

A driver identification system that combines face recognition technology with fingerprint scanning as a secondary authentication technique will be more accurate, secure, and efficient at verifying licenced drivers than traditional approaches that rely exclusively on physical licences and visual checks. This improvement will apply even in circumstances where facial recognition may be compromised due to facial differences. It will also prohibit unlicensed drivers from operating automobiles, hence boosting road safety. The technology would employ image processing and facial recognition algorithms to extract essential aspects from the driver's face and driver's licence image, which would then be compared to a database of known drivers and legitimate driver's licences.

Hypothesis Statement: "A facial recognition system integrated with fingerprint scanning as a secondary authentication method can accurately identify licensed drivers and verify their criminal record status, even in cases where facial recognition is compromised due to facial deformation or other factors."

Research Questions:

1. Can a facial recognition system be developed to accurately identify licensed drivers with a high degree of accuracy?
2. Can the integration of fingerprint scanning as a secondary authentication method improve the accuracy of driver identification in cases where facial recognition is compromised?
3. Can the system be designed to verify driver identity and criminal record status in real-time, ensuring public safety and security?

Null Hypothesis:

"There is no significant difference in the accuracy of driver identification between a facial recognition system alone and a facial recognition system integrated with fingerprint scanning as a secondary authentication method."

Alternative Hypothesis:

"There is a significant difference in the accuracy of driver identification between a facial recognition system alone and a facial recognition system integrated with fingerprint scanning as a secondary authentication method, with the integrated system showing higher accuracy and reliability."

Significance:

This study aims to contribute to the development of a robust and accurate driver identification system that ensures public safety and security. The integration of fingerprint scanning as a secondary authentication method can provide an additional layer of security and accuracy, particularly in cases where facial recognition is compromised. The findings of this study can have practical applications in the development of facial recognition systems for licensed drivers, law enforcement agencies, and transportation authorities.

1.5 Justification

Traditional driver identification procedures, such as manual inspections and physical ID presentation, are time-consuming and error-prone. In some situations, they may be prone to

deception. This can result in checkpoint delays, security weaknesses, and missed identifications of unlicensed or wanted individuals.
The justification of the proposed system over the manual way can be based on the following benefits:

Advantages over Manual Checking:

- Reduced Reliance on Physical Documents: Drivers may not need to carry physical licenses if the system integrates with official databases.
- Efficiency: The system automates driver license verification, significantly reducing processing time compared to manual checks by officials.
- Accuracy: Automated facial recognition and fingerprint verification minimize human error associated with manual document inspection.
- Scalability: The system can handle a higher volume of driver checks compared to relying on a limited number of officials.
- Data Capture: The system can potentially capture additional data like facial templates or fingerprints for future identification purposes (subject to regulations).

Advantages over Scannable Licenses with QR Codes:

- Security: Facial recognition and fingerprint verification are generally considered more secure than QR codes, which can be potentially forged or replicated.
- Tamper Detection: The system can potentially detect attempts to tamper with facial features or fingerprints (depending on technology).
- Offline Functionality (Optional): The system can potentially operate offline with pre-downloaded license data (useful in areas with limited connectivity).
- Secondary Authentication: Fingerprint scanning provides a backup method when facial recognition fails due to deformation or other factors.

1. Enhanced Public Safety: The system helps ensure that only authorized and licensed drivers operate vehicles, reducing the risk of accidents and crimes committed by unlicensed or criminal drivers.

2. Improved Efficiency: Automated facial recognition and fingerprint scanning streamline the driver identification process, reducing manual verification time and increasing productivity for law enforcement and transportation authorities.

3. Increased Accuracy: The integration of facial recognition and fingerprint scanning minimizes errors in driver identification, reducing the risk of false positives or false negatives.

4. Compliance with Regulations: The system helps transportation authorities and law enforcement agencies comply with regulations and laws requiring the verification of driver identity and criminal record status.

5. Deterrent to Criminal Activity: The presence of a robust facial recognition and fingerprint scanning system deters criminals from obtaining licenses or driving under false identities.

6. Cost Savings: Automated driver identification reduces the need for manual verification, saving time and resources for law enforcement and transportation authorities.

7. Enhanced National Security: The system can be integrated with national databases to verify driver identity and criminal record status, enhancing national security and preventing illegal activities.

8. Improved Driver Convenience: Licensed drivers can enjoy a seamless and efficient verification process, reducing wait times and hassle.

9. Data-Driven Insights: The system provides valuable data and analytics on driver behavior and trends, informing transportation policy and planning decisions.

10. Future-Proofing: The documentation of this system provides a foundation for future development and integration with emerging technologies, such as biometric authentication and artificial intelligence.

Overall, the proposed system offers significant advantages in terms of efficiency, accuracy, and security compared to manual checking and scannable licenses.

1.6 Proposed tools

The suggested system achieves its functionality through a combination of hardware and software technologies. Here is a breakdown of the main components:

Hardware Components:

- Mobile phone with high quality Camera: High-resolution cameras are required to capture clear images of drivers' faces during traffic stops or checkpoints. These cameras should be optimized for various lighting conditions to ensure consistent performance.
- Fingerprint Scanners: Compact and reliable fingerprint scanners are needed to capture driver fingerprints during identification. These scanners should be easy to integrate with the system's software and mobile units (if applicable).
- Mobile Units (Optional): Depending on the deployment strategy, law enforcement officers might be equipped with mobile units for on-site driver identification. These units would likely consist of tablets or ruggedized laptops integrated with cameras and fingerprint scanners.

Software Components:

- Facial Recognition Software: This core software component utilizes advanced algorithms to analyse captured facial images. It compares these images against a secure database of driver's license photos to identify the individual. The chosen software should be accurate, reliable, and adaptable to the specific facial features of the Zimbabwean population.
- Driver's License Database Interface: Secure software is needed to facilitate real-time communication with the official driver's license database in Zimbabwe. This interface allows for verification of a driver's identity, license validity, and potential retrieval of additional information.
- Fingerprint Scanning Software: This software manages the fingerprint scanning process. It captures fingerprint images, converts them into a usable format, and compares them against pre-registered fingerprint templates stored in the system for verification.
- Criminal Records Database Interface (Optional): The system can optionally connect to a secure criminal records database to retrieve a driver's criminal background information. This ensures they meet the legal requirements for operating a vehicle.
- System Management Software: An overarching software program is needed to manage the entire system. This includes user authentication, access control, data security measures, and audit logs for monitoring system activity.

1.7 Feasibility study

1.7.1 Technical Feasibility:

- Technology Availability: Facial recognition technology and fingerprint scanners are readily available. However, choosing solutions suitable for Zimbabwe's context (lighting variations, facial features, affordability) requires careful research.
- System Integration: Integrating the system with existing or planned electronic driver's license databases and potentially criminal record databases requires collaboration with relevant government agencies and ensuring technical compatibility.
- Scalability: The system should be designed to accommodate a large number of drivers across Zimbabwe, considering future growth.

1.7.2 Economic Feasibility:

- Cost Analysis: The initial investment for hardware, software licenses, system development, and deployment can be significant. A cost-benefit analysis comparing these costs with potential savings from reduced accidents and improved enforcement should be conducted.

Cost of Development

Item	Cost ($)
Hardware Components	600
MySQL	Open Source
Frameworks	Open Source
Libraries	Open Source
Total Costs	$600

Cost of Maintenance:

Item	Cost ($)
Hardware maintenance	200
Software maintenance	100
Accessories and other expenses	150
Total Costs	$450

Return on Investment (ROI):

- Feasibility: High potential Cost Savings due to accident reduction.
- ROI (Return On Investment) The expected ROI over a specific period is positive, considering both tangible and intangible benefits.

1.7.3 Operational Feasibility:

- Workflow Integration: The system needs to be seamlessly integrated into existing law enforcement workflows for traffic stops and checkpoints. Training officers on proper system usage and data security protocols is crucial.
- Public Acceptance: Public education and awareness campaigns are essential to address potential concerns about privacy and data security. Building trust through responsible implementation is vital.
- User Acceptance: The user acceptance of the system will depend on the willingness of users (licensing authorities, law enforcement) to adopt the system and their ability to operate it effectively. A survey of potential users shows that there is a high level of interest in the system and they are willing to undergo training to operate it effectively.

1.8 Project Plan

1.8.1 Time Plan

PHASE	DURATION (weeks)	STARTING DATE	ENDING DATE
Requirements analysis and definition	4 weeks	1 September 2023	29 September 2023
System design and software design	11 weeks	1 October 2023	15 February 2024
Implementation and unit testing	3weeks	05 January 2024	28 February 2024
Integration and system testing	4 weeks	27 March 2024	2 April 2024

Figure 1: Time Plan

1.8.2 GANTT CHART

Software Development life cycle activities/ Plan	Sept	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May
Project proposal and planning	🟦	🟦							
Requirements gathering and analysis	🟧								
System Design			🟦	🟦	🟦	🟦	🟦	🟦	🟦
System Development			🟩	🟩	🟩	🟩	🟩	🟩	🟩
System testing and validation						🟨	🟨	🟨	🟨
Implementation								🟪	🟪
Maintenance									🟥

Figure 2: Gannt Chart

Chapter Two: Literature review

2.1 Introduction

The importance of ensuring that only licensed drivers operate vehicles cannot be overstated. Unlicensed driving poses significant risks to public safety, and verifying driver identity and criminal record status is crucial for law enforcement and transportation authorities. This literature review aims to explore the development of a multi-modal driver identification system that combines facial recognition and fingerprint scanning to verify licensed drivers. Through a comprehensive review of existing literature, this study aims to provide a thorough understanding of the current state of driver identification systems, identify gaps in current research, and inform the development of a robust and accurate system for verifying licensed drivers.

2.2 Related Work

The government of Zimbabwe has gazetted new regulations over the recently launched new standard plastic driver’s license linked to a database that will replace the metal licenses. This follows the gazetting of new regulations, Statutory Instrument 119 of 2023 under the Road Traffic (Licensing of Drivers) Regulations, 2023, by minister of Transport and Infrastructural Development Felix Mhona. The new Zimbabwean license will be scannable and meet the international standard of SADC, the Common Market for Eastern and Southern Africa (COMESA) and the East African Community. This was a fulfilment of the ministry’s 2021 to 2025 Strategic plan promised on the upgrading and modernization of the transport sector. Driver's licenses are an essential form of identification and proof of driving qualifications for billions of people around the world. However, the process of checking and verifying driver's licenses can be time-consuming and inefficient, and it is often difficult to ensure that licenses are authentic and valid.

A number of studies have been conducted on the use of image processing and facial recognition for driver's license checking. These studies have shown that image processing and facial recognition technology can be used to develop accurate and efficient driver's license checking systems. For example, a study by the National Institute of Standards and Technology (NIST) found that facial recognition technology can be used to identify drivers with an accuracy rate of over 99%. The study also found that image processing technology can be used to extract key features from driver's license images with a high degree of accuracy.

Another study, published in the journal "IEEE Transactions on Intelligent Transportation Systems," found that a driver's license checking system using image processing and facial recognition technology can reduce the time it takes to verify a driver's license by up to 50%.

In [1] discusses that deep learning, particularly Convolutional Neural Networks (CNNs), differs from traditional machine learning in image recognition by its automated feature extraction process. While traditional machine learning requires manual feature selection by experts, deep learning models like CNNs can automatically learn hierarchical representations of features directly from raw input data. This ability to learn complex patterns and relationships in high-dimensional image data gives deep learning models an edge in image recognition tasks, leading to superior performance compared to traditional machine learning algorithms. Convolutional Neural Networks (CNNs) offer key advantages for image recognition tasks, including automated feature learning, spatial hierarchical structure, parameter sharing, translation invariance, scalability, and state-of-the-art performance. CNNs can automatically learn hierarchical features from raw image data, preserve spatial relationships, generalize well to new data, handle variations in object position, scale to large datasets, and achieve top performance in image recognition benchmarks. These advantages make CNNs a powerful and effective tool for a wide range of image recognition applications. Deep learning, particularly Convolutional Neural Networks (CNNs), has been successfully applied in diverse image classification and localization tasks. Examples include handwritten character recognition, medical image analysis, plant/seed image recognition, monument recognition, fingerprint recognition, license plate recognition, traffic sign recognition, and face recognition. These applications showcase the effectiveness and versatility of deep learning models in accurately classifying and localizing objects in images across various domains.

Facial Expression Recognition Using Facial Effective Areas And Fuzzy Logic In [2] talks about a novel method for facial expression recognition using facial effective areas and fuzzy logic. The system extracts facial features based on integral projection curves and utilizes fuzzy rule-based classification for recognizing seven basic facial expressions. The approach has been tested on the JAFFE database, showing robust results with high accuracy compared to other methods. The system aims to improve facial expression recognition by intelligently selecting effective areas on the face and employing fuzzy logic for classification. The proposed system uses Fuzzy logic for facial expression recognition by defining rules that map fuzzified measurements of facial features to fuzzified emotion categories. For example, rules like "If (Eye-Opening is Very High) And (Eyebrow-Constriction is Very Low) And (Mouth-Opening is Very High) And (Mouth-Constriction is Low) Then Surprise" are created to classify facial expressions based on the degrees of eye opening, eyebrow constriction, mouth opening, and mouth constriction. By employing Fuzzy logic, the system can effectively classify facial expressions by considering the degrees of various facial features in a fuzzy manner, leading to improved accuracy in recognition. The method of integral projection curves enhances the accuracy and robustness of the facial expression recognition system by enabling effective extraction of facial regions, key features like eyes and mouth, and integrating them into a Fuzzy rule-based system for precise emotion mapping. This method ensures robustness by being less sensitive to variations in lighting, rotations, and scales of images, thus improving the system's ability to recognize facial expressions accurately across different conditions and environments.

In [3] the file presents a framework for enhancing security in vehicle parking spaces through automatic face recognition algorithms. The system consists of three main steps: vehicle detection, driver face location, and driver identification. The framework utilizes Adaptive Boosting algorithm and Haar-like features for vehicle detection, Eigenfaces for feature selection, and Euclidean distance for classification in driver face identification. The system was tested with challenging scenarios, including limited gallery face samples and various driver face poses, showing high detection and identification accuracy. The developed framework is scalable, essential for security checks at parking entrances, and can help prevent vehicle thefts. Overall, the system aims to ensure only authorized vehicles access public parking areas, enhancing security and efficiency. The framework uses the Adaptive Boosting (AdaBoost) algorithm for detecting vehicles. AdaBoost generates a robust final classifier by combining multiple weak classifiers trained on Haar-like features. For driver face identification, the framework employs Eigenfaces for feature selection and Euclidean distance for classification. These algorithms enable accurate detection of vehicles and precise identification of driver faces, contributing to the overall effectiveness of the security framework in vehicle parking spaces. The simulation results demonstrate the effectiveness of the developed framework in challenging situations where only a single facial image of a driver is available in the database. In this scenario, four face images in different poses are used for testing. Despite the limited training data and variations in facial poses, the results show very high detection and identification accuracy. This indicates the robustness and reliability of the framework in accurately recognizing driver faces even under challenging conditions, making it suitable for enhancing security in vehicle parking spaces.

The book of Combining Facial Recognition, Automatic License Plate Readers and Closed Circuit Television to Create an Interstate Identification System for Wanted Subjects In[4] emphasizes on the integration of facial recognition, automatic license plate readers, and closed-circuit television to create an interstate identification system for wanted subjects. It emphasizes the importance of collaboration among various entities, the challenges of scrubbing large databases for identification, and the need for clear policies, funding, and public support for the system's success. The document also highlights the potential impact on homeland security and law enforcement, as well as the importance of transparency, privacy considerations, and legislative support for such systems. The integration of facial recognition, automatic license plate readers, and closed-circuit television enhances law enforcement efforts by providing a comprehensive system for tracking and identifying wanted subjects. This combination enables real-time monitoring, quick suspect identification, and improved surveillance in public spaces, ultimately leading to more effective law enforcement operations and increased public safety. Implementing an interstate identification system using facial recognition, automatic license plate readers, and closed-circuit television technologies offers benefits such as enhanced security, improved efficiency, better coordination among law enforcement agencies, and increased public safety. However, challenges include privacy concerns, accuracy and reliability issues, legal and regulatory complexities, and the need for public acceptance. Balancing these factors is essential for the successful implementation of such a system.

In[5] there is an exploration of a real-time Driver Monitoring System that uses facial landmark estimation to analyze driver behavior, focusing on detecting inattention and drowsiness. The system leverages video data from an infrared camera to recognize head poses and eye closures, crucial for identifying signs of drowsy or distracted driving. By integrating hardware information like steering angle with software analysis, the system aims to enhance driving safety. The proposed algorithm shows promising performance for driver-state analysis, with plans to further refine the system for commercial deployment. Additionally, the PDF provides references to related research and datasets for further exploration. The Driver Monitoring System utilizes facial landmark estimation to monitor driver behavior by first detecting the driver's face in video footage captured by an infrared camera. Facial landmarks are then extracted to enable two primary functions: head pose estimation for identifying inattentive situations and eye closure recognition for detecting drowsy driving. The system analyses the driver's gaze direction through head pose estimation and determines drowsiness by detecting sustained eye closures. By extracting and analyzing facial landmarks, the system can effectively assess the driver's state and enhance safety during driving [T1]. The Driver Monitoring System comprises two key modules: the Head Pose Estimation Module and the Eye Closure Recognition Module. The Head Pose Estimation Module monitors the driver's head movements to detect inattention, while the Eye Closure Recognition Module identifies instances of drowsiness based on eye closure patterns. These modules work together to analyze different aspects of driver behavior, providing a comprehensive approach to behavior recognition and enhancing driving safety by alerting drivers to potential risks. The proposed Driver Monitoring System offers advantages in terms of efficiency and real-time capabilities compared to other monitoring systems. It efficiently analyses driver behavior using only video data from an infrared camera, simplifying the setup and reducing the need for additional sensors. The system's real-time capabilities enable prompt detection and response to driver inattention and drowsiness, enhancing safety on the road. By integrating head pose estimation and eye closure recognition, the system provides a comprehensive approach to behavior recognition, making it a promising solution for enhancing driver safety.

In[6] the file discusses a Fingerprint Based License Checking system for monitoring citizens' driving licenses. It highlights the use of biometric technology, specifically fingerprint recognition, to track driver history and enforce traffic rules efficiently. The system offers benefits such as unique fingerprint identification, stability, reliability, high accuracy, cost-effectiveness, ease of use, and small storage space requirements. Overall, the system provides a standardized and advanced solution for monitoring driving licenses. The fingerprint-based license checking system scans and records citizens' fingerprint images. When a traffic violation occurs, the police can scan the driver's fingerprint to identify them and collect penalties. This biometric technology enables efficient tracking of driver history and provides a convenient method for monitoring driving licenses. Using fingerprint recognition in tracking driver history and enforcing traffic rules offers benefits such as unique identification, stability, reliability, high accuracy, cost-effectiveness, ease of use, small storage space requirements, and standardization. This technology provides an efficient and effective method for monitoring driving licenses. The fingerprint-based license checking system enhances the efficiency and accuracy of monitoring driving licenses compared to traditional methods by providing unique identification, real-time tracking, convenience for law enforcement, ensuring data integrity, reducing human error, enhancing security, and offering cost-efficiency. This system streamlines the process, improves compliance with traffic rules, and enhances road safety.

In[7] The Real Time Vehicle Security System presented in the review integrates facial recognition and fingerprint verification technologies to enhance vehicle security and driver safety. The system consists of components like a raspberry pi board, USB camera, fingerprint module, and alcohol sensor. It operates by capturing the driver's image, comparing it with existing data, and then proceeding to fingerprint verification. If unauthorized, an email alert is sent to the vehicle owner via SMTP. The system also includes an alcohol sensor to prevent driving under the influence. Overall, the system aims to ensure that only authorized drivers with valid licenses can start the vehicle ignition, promoting safety and security on the roads. The proposed vehicle security system combines facial recognition and fingerprint verification technologies to authenticate authorized individuals and enhance vehicle security. Facial recognition using the Eigen face algorithm with Haar cascade classifier verifies the person's identity by comparing captured images with stored datasets. Subsequently, fingerprint verification serves as a key for vehicle ignition, allowing only individuals with matching fingerprints in the system to start the vehicle. This multi-layered approach ensures that only authorized persons can access and operate the vehicle, promoting safety and security. The system ensures that only authorized drivers with valid licenses can start the vehicle ignition through fingerprint verification by first using facial recognition to identify the driver. After successful facial recognition, the system prompts the driver to place their fingerprint on the sensor for further verification. The fingerprint module compares the driver's fingerprint with the enrolled data, allowing ignition only if the fingerprint matches the authorized records. This multi-step process guarantees that only individuals with valid licenses and matching fingerprints can operate the vehicle, enhancing security and preventing unauthorized access.

License Plate Recognition from Still Images and Video Sequences

A Survey In 2008, Christos-Nikolaos E. Anagnostopoulos et.al.[3] proposed License plate recognition (LPR) algorithms in images or videos that generally composed of the following three processing steps: 1) extraction of a license plate region; 2) segmentation of the plate characters; and 3) recognition of each character. This task is quite challenging due to the diversity of plate formats and the nonuniform outdoor illumination conditions during image acquisition. Therefore, most approaches work only under restricted conditions such as fixed illumination, limited vehicle speed, designated routes, and stationary backgrounds. Numerous techniques have been developed for LPR in still images or video sequences, and the purpose of this paper is to categorize and assess them. Issues such as processing time, computational power, and recognition rate are also addressed, when available. It links to a public image database to define a common reference point for LPR algorithmic assessment.

Hybrid Cascade Structure for License Plate Detection in Large Visual Surveillance Scenes: In 2018, Chunsheng Liu et.al.[10] conferred the idea that the license plate detection has been successfully applied in some commercial products, the detection of small and vague license plates in real applications is still an open problem.

Video Face Recognition of Virtual Currency Trading System Based on Deep Learning Algorithms: In 2021, Jun Wei et.al.[11] researched about Virtual currency trading which develops rapidly which takes up a large proportion in the whole economy, and has become an important part of people's daily life. Firstly, a reliable virtual currency trading system model is proposed, which is composed of four participant platforms, providers and payers, mainly including the purchase of virtual currency, purchase of virtual goods or services, exchange of virtual currency and other trading activities. In order to monitor possible collusion fraud in virtual currency transactions, payers are introduced to prevent collusion attacks. Video face detection algorithm based on multi-task Cascaded Convolutional Networks is designed and implemented to solve the problems of pose, light and occlusion in the virtual currency trading system. The algorithm utilizes the inherent correlation between detection and calibration to improve the detection performance under the framework of deep cascading tasks.

In[8] the research article focuses on implementing principal component analysis (PCA) for face recognition in criminal identification. It addresses the limitations of thumbprint identification in Malaysia, where criminals are becoming more cautious about leaving thumbprints at crime scenes. The use of CCTV footage and automated facial recognition systems can help law enforcement agencies identify suspects without relying solely on thumbprints. By utilizing PCA to extract distinguishable features from facial images, the system aims to match faces with a database accurately. This research has the potential to enhance criminal identification techniques and improve security measures for law enforcement agencies.

The document from the International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) in[9] discusses a Fingerprint Based Licensing System for Driving. The system aims to prevent non-licensees from driving and causing accidents by utilizing fingerprint identification as a reliable biometric method. The project includes the development of various sensors such as seat belt detector, door lock sensor, alcohol sensor, and biometric sensors, all of which need to be cleared sequentially before ignition can be switched on. The system ensures that only authorized individuals can drive the vehicle, provides safety features like seat belt detection, and allows for learner's license holders to drive under supervision. The document also mentions the use of PIC microcontrollers and relays in the system. Additionally, references to face recognition technologies and GSM architecture are provided in the conclusion section of the document.

The literature review has provided a comprehensive overview of the current state of driver identification systems, highlighting the advancements in facial recognition technology, fingerprint scanning, and multi-modal biometric systems. The review has also identified gaps in current research and underscored the need for a robust and accurate system for verifying licensed drivers.

2.3 Conclusion

Based on the review, it is clear that a multi-modal biometric system that combines facial recognition and fingerprint scanning offers the most promising approach for verifying licensed drivers. Such a system can provide high accuracy, robustness, and security, ensuring that only authorized individuals operate vehicles. Future research should focus on addressing the gaps identified in this review, including the need for more comprehensive datasets, standardization of biometric data, and further exploration of legal and ethical considerations.

Chapter Three: Analysis

3.1 Information Gathering Tools

In the pursuit of designing and development an effective system that verifies licensed drivers, accurate and comprehensive information from various stakeholders and sources was gathered. To achieve this, a range of information gathering tools were employed to collect, analyze, and validate the requirements and needs of the system.

- Interviews and Focus Groups: Interviews were conducted with law enforcement officers, drivers and licensing authorities. Law enforcement officers emphasized the need for a quick and accurate verification process to minimize delays during traffic stops. Drivers suggested using a multi-factor authentication approach to ensure security and privacy. Licensing authorities highlighted the importance of integrating the system with existing databases for seamless verification. By conducting Interviews and Focus Groups, we gathered rich, qualitative data from diverse stakeholders, providing valuable insights into their needs, pain points, and suggestions for designing and developing an effective system to check for licensed drivers
- Surveys and Questionnaires: Surveys among law enforcement agencies, licensing authorities and drivers, were conducted with drivers to gather their feedback on the proposed system and to identify any concerns they may have. By conducting Surveys and Questionnaires, we gathered a large amount of data from a diverse group of stakeholders, providing valuable insights into their needs, preferences, and experiences related to the system for checking licensed drivers.
- Observation and Site Visits: Observing traffic stops revealed that officers often rely on manual checks, leading to errors and delays. Visiting licensing authorities' offices showed that current systems are paper-based, leading to inefficiencies and data inconsistencies. By conducting Observation and Site Visits, we gathered valuable, contextual information about the current processes and environments of law enforcement officers, drivers, and licensing authorities, providing insights into areas for improvement and requirements for the new system.

3.2 Description of the Existing System

Currently, Zimbabwe's driver license verification process is primarily manual and relies on physical inspection by law enforcement officers:

1. License Presentation: During a traffic stop, the driver presents their physical driver's license to the officer.
2. Visual Inspection: The officer visually inspects the license for validity features like security holograms, printing quality, and expiration date.
3. Information Verification: The officer compares the information on the license (name, photo, license class) with the driver and potentially checks for any visible signs of alteration.
4. Communication with DLA (Optional): In some cases, the officer might contact the Driver Licensing Agency (DLA) via radio or phone to verify the license validity electronically (if the system is available at the time).

In June 2023, Zimbabwe introduced a new standard plastic driver's license with scannable features, but the system for utilizing the scannable features of the new licenses for electronic verification by law enforcement is still in the early stages of implementation. The transition from the old metal licenses to the new scannable plastic licenses is ongoing. Law enforcement officers might still encounter drivers with the older metal licenses, requiring manual verification procedures.

3.2 Data Analysis

3.2.1 UML Context Diagrams

This high-level view emphasizes the system's interaction with the external environment, focusing on the Law Enforcement Officer's role in initiating the verification process and receiving the results. It doesn't delve into the internal workings of the manual verification steps or data flows within the system.

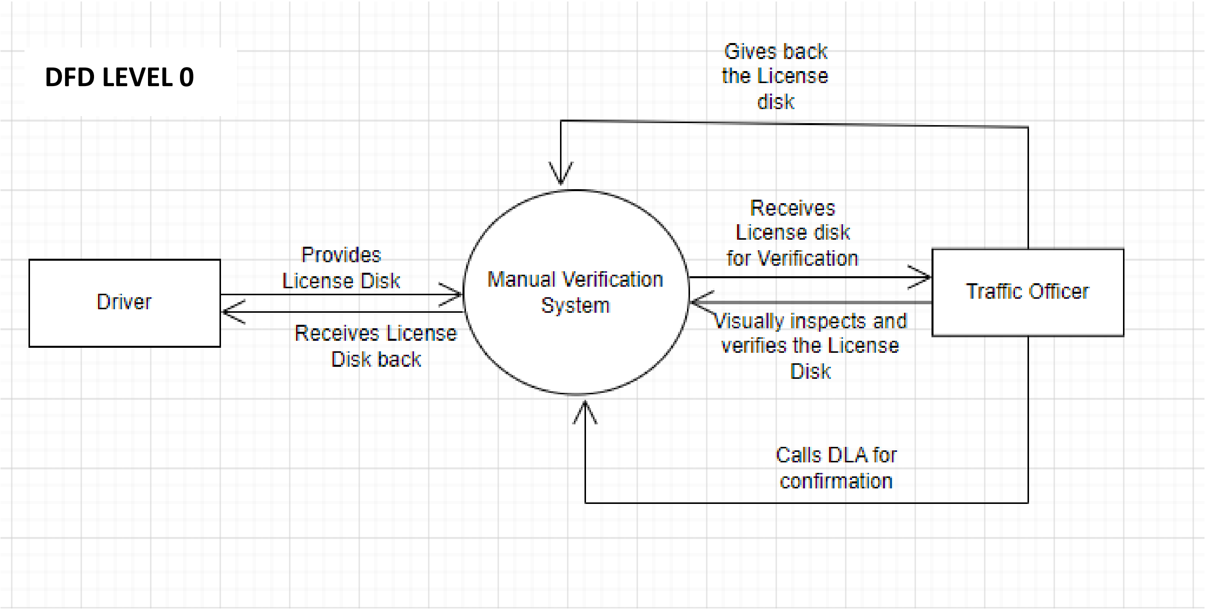

DFD LEVEL 0
Gives back the License disk
Receives License disk for Verification
Provides License Disk
Driver
Manual Verification System
Traffic Officer
Receives License Disk back
Visually inspects and verifies the License Disk
Calls DLA for confirmation

Figure 3: Existing system uml context diagram

3.2.2 DFD of the existing system

This DFD diagram provides a visual representation of the data flow within the verification process.

DFD LEVEL 1

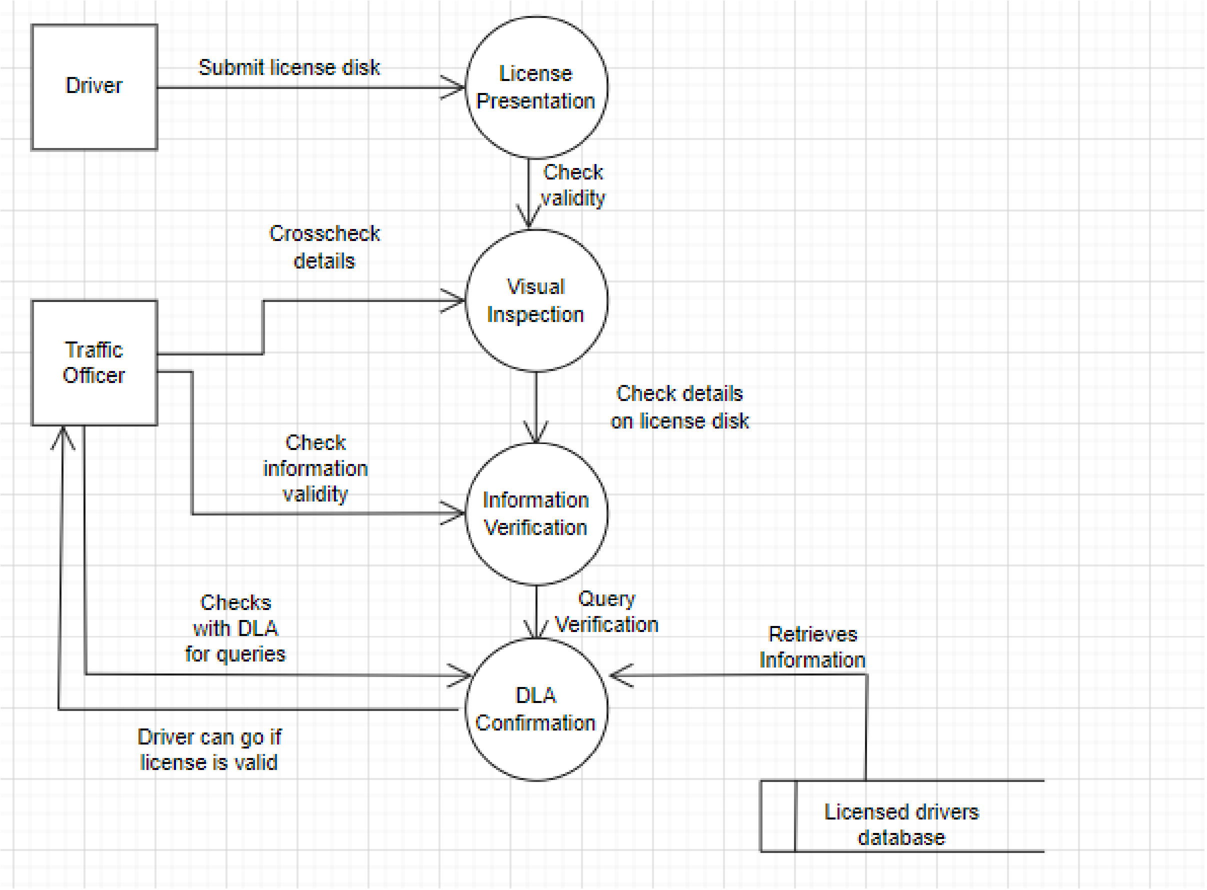


Figure 4: Existing system dfd

3.3.1 Evaluation of Alternatives Systems

The LicenseLense System is a critical component of the transportation infrastructure, ensuring the safety and security of drivers and the general public. This section evaluates alternative systems, analysing their advantages and disadvantages, and comparing them to the proposed LicenseLense System. The evaluation of alternative systems was crucial in ensuring that the proposed system was the most suitable solution for the identified problem. This evaluation considers various factors, including cost, accuracy, security, scalability, and ease of use. By analysing alternative systems, we can identify potential limitations and areas for improvement, ultimately strengthening the proposed LicenseLense System.

The alternative systems evaluated in this section include:

1. Manual Verification System

   Advantages

   - Low implementation cost: This system requires minimal investment in technology and infrastructure.

   - Simple to understand and use: Manual verification is a straightforward process that requires minimal training.

   Disadvantages

   - Time-consuming: Manual verification requires a significant amount of time and effort to verify identities.

   - Prone to human error: Manual verification is susceptible to errors due to human mistakes or biases.

   - Limited scalability: Manual verification becomes increasingly difficult as the number of users grows.

2. Scannable Driver’s Licenses: Scannable driver's licenses are a type of identification document that contains a barcode or QR code that can be scanned to access the holder's information. Here's an evaluation of scannable driver's licenses:

   Advantages

   - Convenience: Scannable driver's licenses offer a quick and easy way to verify identity, making it convenient for law enforcement, border control, and other authorities.

- Accuracy: Scanning the barcode or QR code ensures accurate retrieval of the holder's information, reducing errors and misidentification.

<u>Disadvantages</u>

- Technical issues: Scanners or readers may malfunction, and barcode or QR code damage can render the license unusable.

- Limited compatibility: Scanners or readers may not be universally compatible, potentially causing issues during verification.

- Privacy concerns: Storing personal information in a scannable format raises concerns about data privacy and potential misuse.

3. Mobile App with Enhanced Security Features (without Biometrics) for Driver Verification: This mobile application provides a secure and efficient way for law enforcement officers to verify driver's licenses without relying on biometric identification

<u>Advantages</u>

- Faster and more accurate verification compared to manual data entry.

- Improved efficiency for law enforcement officers.

<u>Disadvantages</u>

- Relies on accurate manual data entry (scanning a valid license) for successful verification.

- May not provide access to additional information like criminal records.

- Lacks the increased security of biometrics

3.4 Functional Analysis of Proposed System

3.4.1 Functional Requirements

1. Data Capture (Mobile App):

   - The mobile app shall capture a high-resolution facial image of the driver using the device camera.

   - Captured image shall be stored temporarily on the mobile device in a secure manner

2. Data Pre-processing (Mobile App - Optional for Facial Recognition):

   - The mobile app shall pre-process the captured facial image (e.g., adjust lighting, normalize orientation) to improve facial recognition accuracy (optional).

3. Secure Communication (Mobile App & Central System):

   - The mobile app shall establish a secure encrypted connection with the central system to transmit captured data (facial image)

- The central system shall utilize secure protocols (e.g., HTTPS) to receive data transmissions from the mobile app.

4. Facial Recognition (Central System - Primary Method):

   - The central system shall employ a robust facial recognition engine to compare the captured facial image against the driver photos stored in the DLA database.

   - The facial recognition engine shall provide a high-confidence match result (True/False) for the captured image.

   - Upon a successful facial recognition match within a predefined confidence threshold (e.g., 90%), the system shall retrieve the associated driver information (name, license class, etc.) from the DLA database.

5. Fingerprint Scanning (Mobile App - Secondary Method):

   - **Trigger:** The mobile app shall allow the officer to initiate fingerprint scanning if: Facial recognition is deemed unreliable due to factors like poor lighting, facial obscuration (sunglasses, masks), or potential tampering.

   - The mobile app shall integrate with a fingerprint scanner to capture the driver's fingerprint image

   - The captured fingerprint data shall be securely transmitted to the central system.

6. Fingerprint Verification (Central System - Secondary Method):

   - The central system shall compare the captured fingerprint data against pre-registered fingerprints associated with the driver's license in the DLA database.

   - The system shall provide a match result (True/False) for the fingerprint verification.

7. License Verification with DLA (Central System):

   -**Trigger:** Based on: A successful facial recognition match or a successful fingerprint verification match.

   - The system shall communicate with the licensed drivers' database to verify the license validity.

   - The system shall retrieve the license validity status (valid/expired/suspended) from the DLA (Drivers' License Agency) database.

8. Criminal Record Check (Central System - Optional & Access-Restricted):

   - The system shall allow authorized officers to initiate a criminal record check for the driver

   - The system shall securely communicate with the DLA database to retrieve the driver's criminal record information (if any).

- The system shall display the retrieved criminal record information (if available and authorized) to the officer.

9. Verification Result Display (Mobile App):

   - The mobile app shall display the verification results in a clear and user-friendly format for the officer

   - The displayed information shall include: Driver information (name, license class, etc.), License validity status (valid/expired/suspended), Fingerprint verification result (if applicable) and Criminal record information (optional and access-restricted).

3.4.2 Non-functional Requirements

Non-functional requirements define how the system should behave, rather than what it should do. They focus on qualities such as performance, usability, reliability, security and scalability. Here are the non-functional requirements for the system:

1. Performance:

   - Response Time: The mobile app shall display verification results within a reasonable timeframe(20sec)

   -System Availability: The system shall be highly available with minimal downtime to ensure continuous operation for law enforcement activities.

   -Scalability**:** The system should be scalable to accommodate an increasing number of users and verification requests over time.

2. Usability:

   - Mobile App Interface: The mobile app interface shall be user-friendly and intuitive for law enforcement officers to operate during traffic stops.

   - Error Handling: The system shall provide informative error messages to officers in case of failed recognitions, communication issues, or other unexpected situations.

   -The system should be user-friendly, with a clear and intuitive interface that allows authorized personnel to easily navigate and operate the system.

3. Reliability:

   -The system should be reliable and available for use at all times, minimizing downtime and ensuring consistent performance.

   - Facial Recognition Accuracy: The facial recognition engine should achieve a high degree of accuracy under various lighting conditions and potential facial obscurations.

   - Fingerprint Recognition Accuracy: The fingerprint scanner should provide reliable results with minimal false positives or negatives.

- System Uptime: The system should have a high uptime percentage with minimal disruptions due to system failures.

4. Security:

   -The system should implement robust security measures to protect the driver's license data and prevent unauthorized access or tampering.

   - Data Security: All communication channels between the mobile app and central system shall be encrypted to protect sensitive data (facial images, fingerprint data).
   - Authentication: The system shall implement strong authentication mechanisms for authorized access to driver information and criminal record checks

5. Privacy:

   - Data Minimization: The system should collect and store only the minimum amount of data necessary for driver verification
   - The system should adhere to privacy regulations and guidelines, ensuring that driver's license data is handled securely and confidentially.

6. Maintainability: The system should be easy to maintain, allowing for updates, bug fixes, and enhancements without disrupting the overall functionality.
7. Performance Efficiency: The system should be designed to optimize resource utilization, such as CPU and memory usage, to ensure efficient operation and minimize system requirements.
8. Interoperability**:** The system should be able to seamlessly integrate with other existing systems or databases, such as government databases or law enforcement systems.
9. Accuracy: The system should have a high level of accuracy in recognizing and matching the driver's face with the photo on the driver's license.
10. Scalability: The system should be designed to handle a large number of simultaneous requests and be able to scale up or down to accommodate varying workloads.
11. Compatibility: The system should be compatible with various hardware devices, such as scanners or cameras, and should support multiple operating systems and browsers.

3.4.3 Use Case Diagram

Use case helps to identify the different interactions and steps involved this system's functionality. They provide a clear understanding of how users or external systems interact with the system and help guide the development process. Use cases can be used as a basis for designing system interfaces, writing test cases, and validating the system's functionality against user requirements.

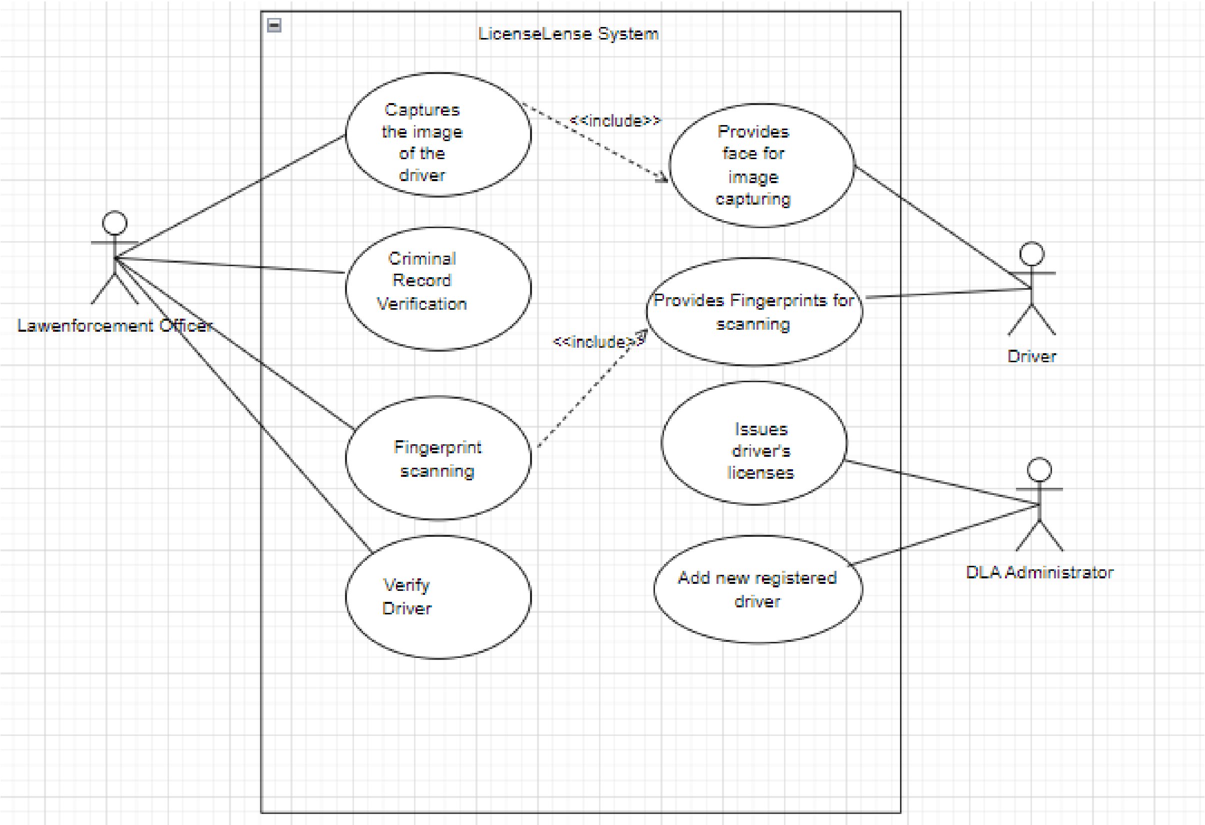

LicenseLense System
Captures the image of the driver
<<include>>
Provides face for image capturing
Criminal Record Verification
Provides Fingerprints for scanning
<<include>>
Lawenforcement Officer
Driver
Fingerprint scanning
Issues driver's licenses
DLA Administrator
Verify Driver
Add new registered driver

Figure 5: Use case of the current system

4.0 Chapter Four – Design

This chapter describes the component setup and the function of the proposed system. It demonstrates how the components will be intergrated in order to fulfil the project objectives.

4.1 System Diagrams

4.1.1 Context UML Diagram

This UML Context Diagram for the proposed driver verification system (LicenseLense System) depicts the system's interaction with the external environment, focusing on authorized users and the data exchange.

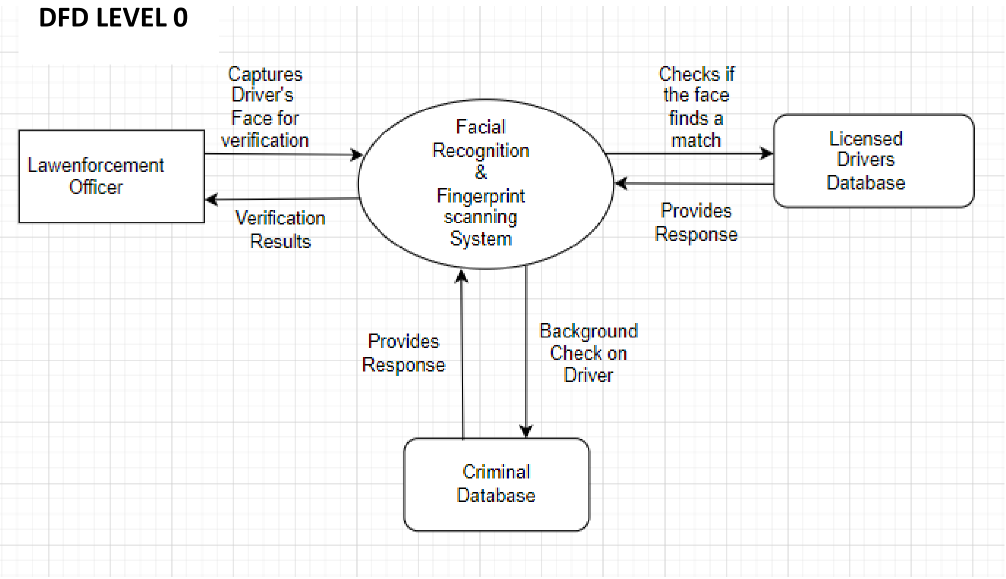

DFD LEVEL 0
Captures Driver's Face for verification
Checks if the face finds a match
Lawenforcement Officer
Facial Recognition & Fingerprint scanning System
Licensed Drivers Database
Verification Results
Provides Response
Provides Response
Background Check on Driver
Criminal Database

Figure 6: Level 0 DFD

4.1.2 DFD Diagram

This high-level view emphasizes the main processes and data flows related to licensed driver verification. It provides a general understanding of how the system interacts with external entities and the data involved.

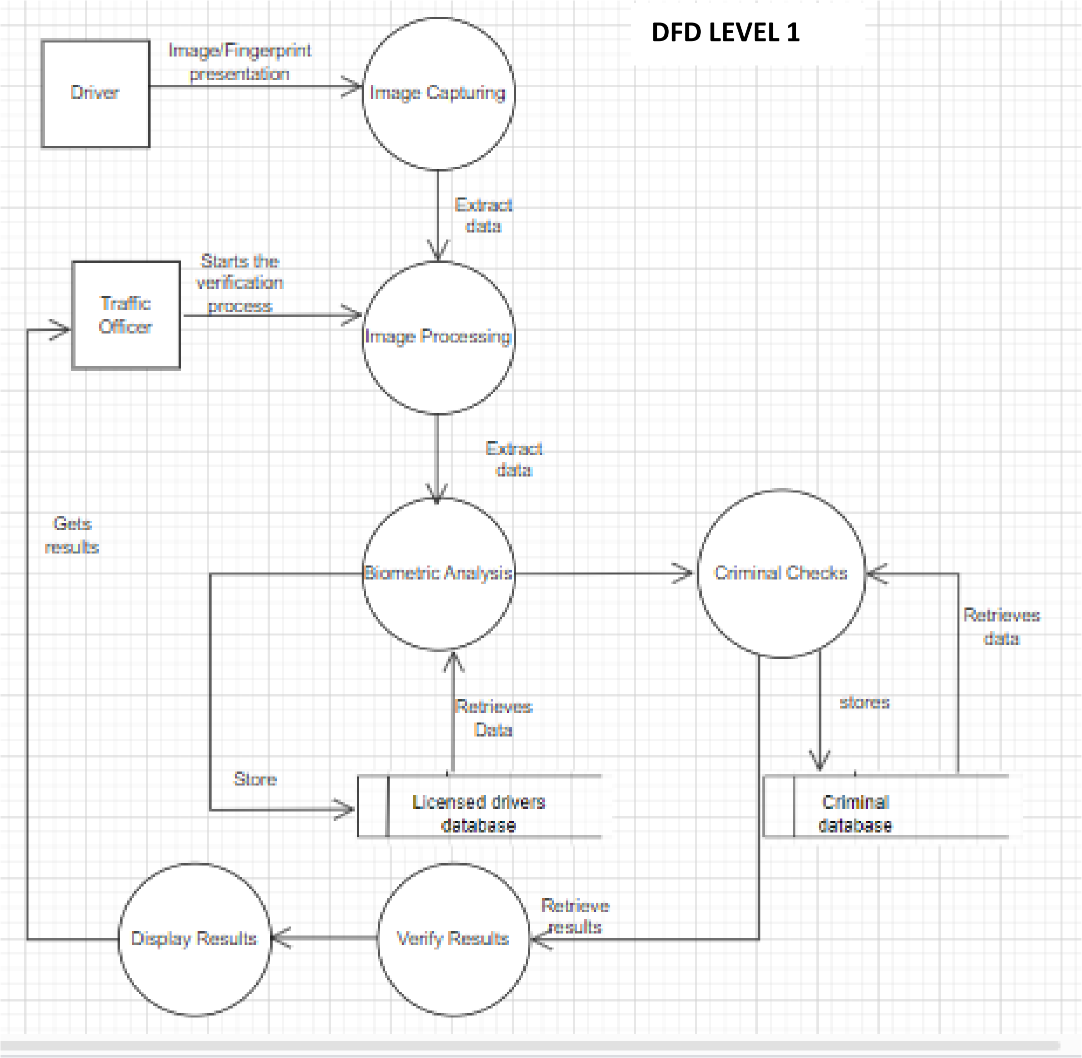


Figure 7: Level 1 DFD

4.1.3 Activity Diagram

The activity diagram would illustrate the sequential flow of activities involved in verifying licensed drivers.

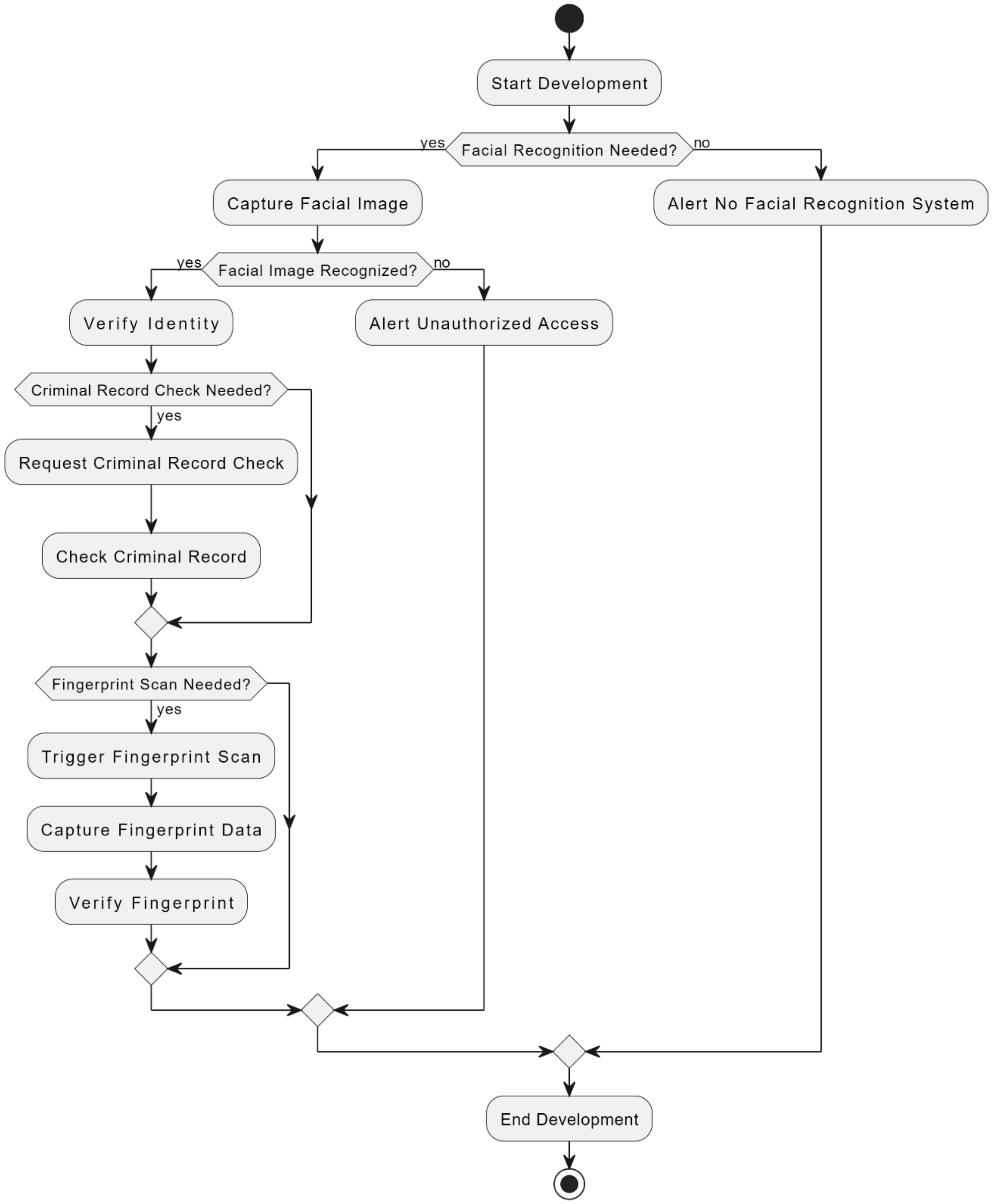
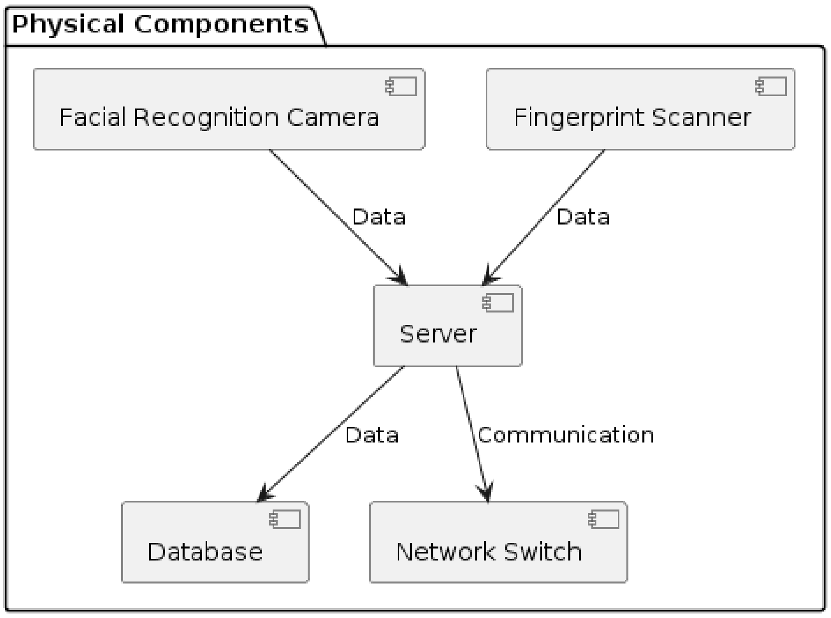


Figure 8: Activity Diagram

4.2Architectural Design

4.2.1Hardware

It showcases the physical components needed to operate the system.



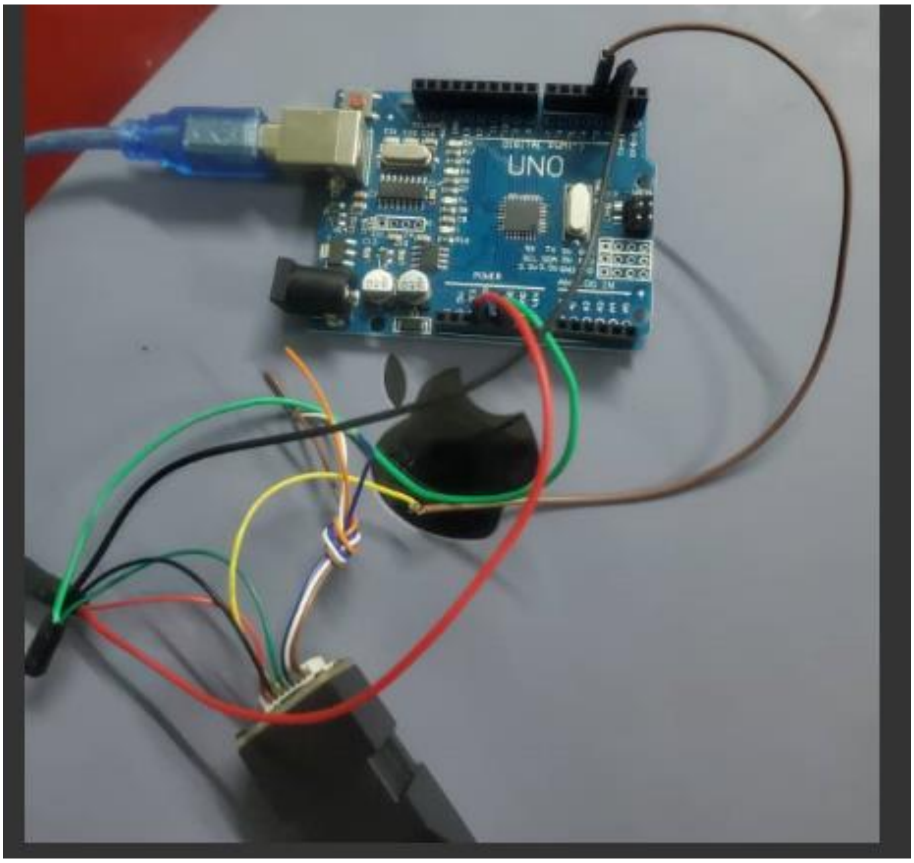


Figure 9: Hardware diagram

4.2.2 Networking

It illustrates the data flow and communication channels between the network components.

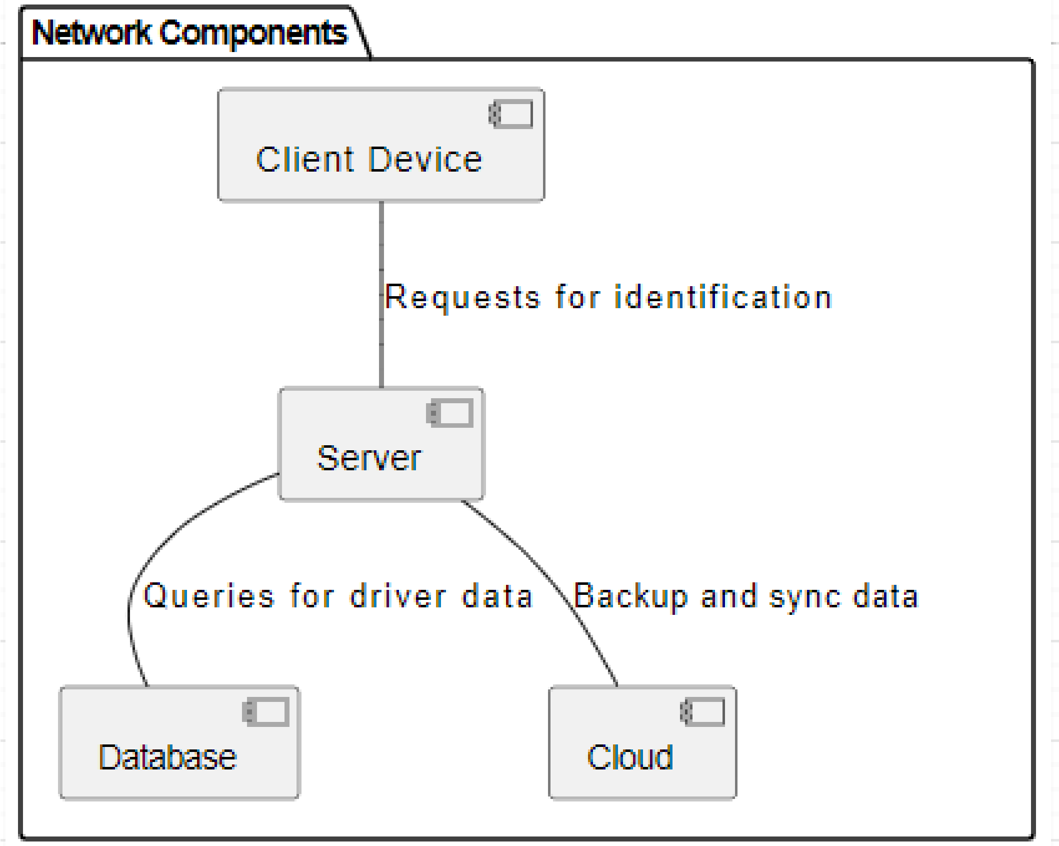


Figure 10: Network diagram

4.3 Database Design

4.3.1 ER diagrams

The ER diagram provides a visual representation of the entities, attributes, and relationships within the LicenseLense System.

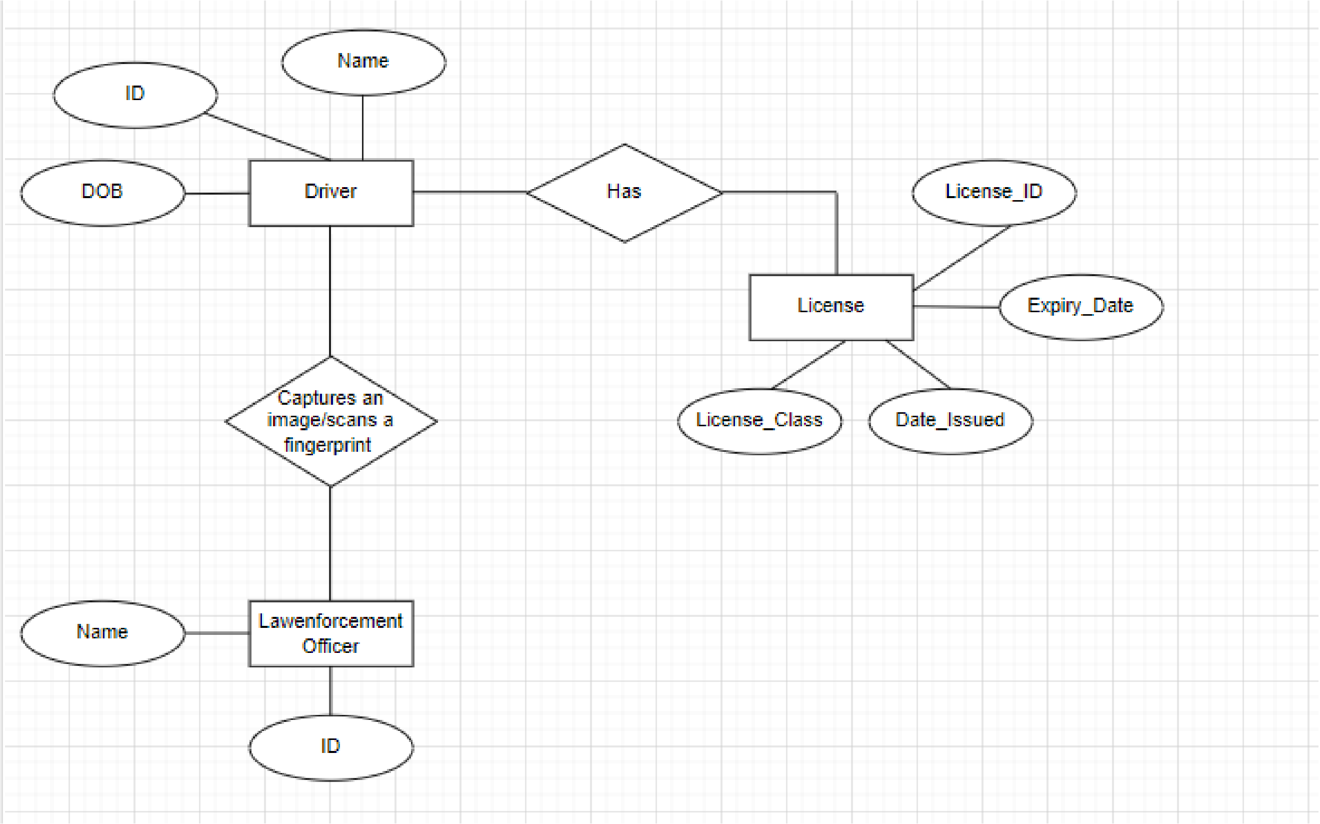


Figure 11: ER diagram

4.3.2 Normalized Database

The normalized database separates the data into different tables based on their logical relationships. The normalization process helps in reducing data redundancy and dependency, improving data consistency, and simplifying data retrieval.

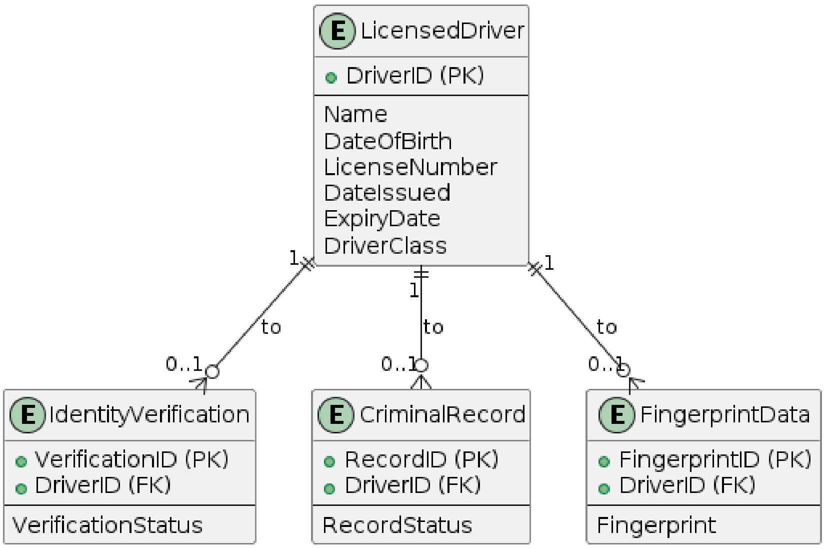


Figure 12: Normalized database

4.4 Program Design

4.4.1 Class Diagram

The Class Diagram provides a visual representation of the classes, their attributes, and their relationships within the system. It helps in understanding the structure of the system, designing the software architecture, and facilitating communication among developers and stakeholders.

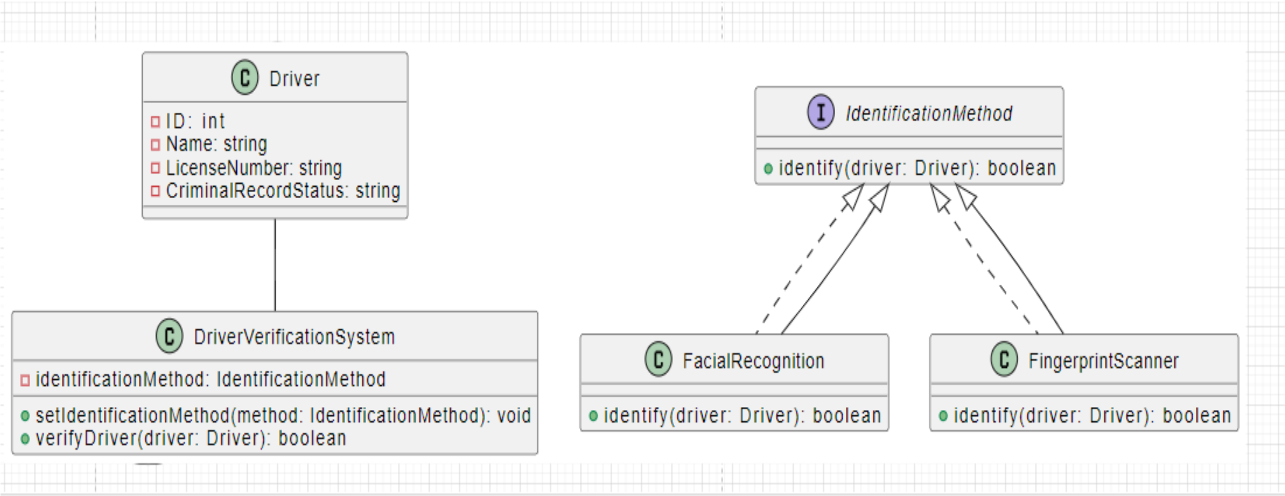

C Driver
ID: int
Name: string
LicenseNumber: string
CriminalRecordStatus: string
I IdentificationMethod
identify(driver: Driver): boolean
C DriverVerificationSystem
identificationMethod: IdentificationMethod
setIdentificationMethod(method: IdentificationMethod): void
verifyDriver(driver: Driver): boolean
C FacialRecognition
identify(driver: Driver): boolean
C FingerprintScanner
identify(driver: Driver): boolean

Figure 13: Class diagram

4.4.2 Sequence Diagram

The Sequence Diagram provides a visual representation of the interactions and messages exchanged between different actors in the system.

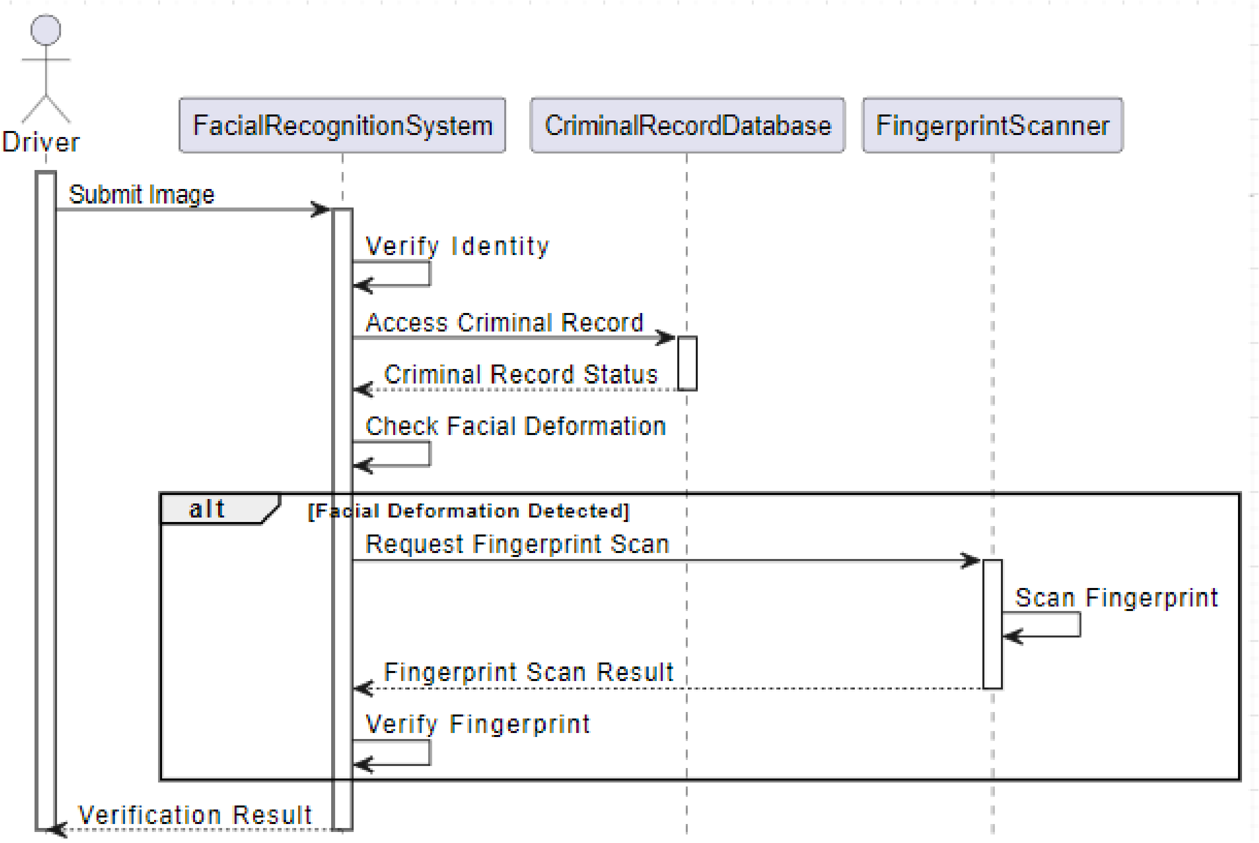


Figure 14: Sequence diagram

4.4.3 Package diagrams

The Package Diagram provides a high-level view of the system's organization and helps in understanding the modular structure of the LicenseLense System.

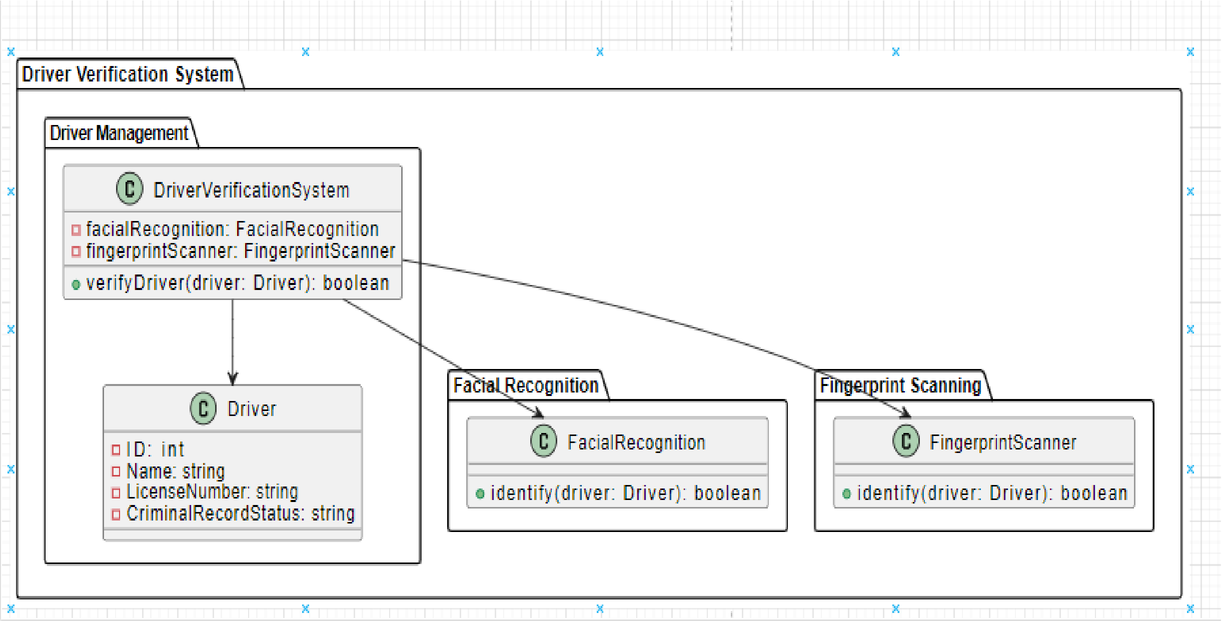

Driver Verification System
Driver Management
C DriverVerificationSystem
facialRecognition: FacialRecognition
fingerprintScanner: FingerprintScanner
verifyDriver(driver: Driver): boolean
C Driver
ID: int
Name: string
LicenseNumber: string
CriminalRecordStatus: string
Facial Recognition
C FacialRecognition
identify(driver: Driver): boolean
Fingerprint Scanning
C FingerprintScanner
identify(driver: Driver): boolean

Figure 15: Package diagram

4.4.4 Pseudo code

The pseudocode provides a high-level representation of the LicenseLense System's logic without focusing on specific programming language syntax. It helps in understanding the overall flow and steps involved in verifying licensed drivers.

```
// Initialize the system
InitializeSystem()
// Main system loop
while True:
    // Capture an image from the camera
    capturedImage = CaptureImage()
    // Perform facial recognition on the captured image
    identifiedDriver = FacialRecognition(capturedImage)
    // Check if the identified driver is in the database
    if DriverExistsInDatabase(identifiedDriver):
        // Retrieve driver information from the database
        driverInfo = GetDriverInfo(identifiedDriver)
        // Verify the driver's criminal record status
        criminalRecordStatus = CheckCriminalRecord(driverInfo)
        // Display driver information and criminal record status
        DisplayDriverInfo(driverInfo)
        DisplayCriminalRecordStatus(criminalRecordStatus)
        // If facial recognition is compromised, prompt for fingerprint scanning
        if FacialRecognitionCompromised():
            // Scan the driver's fingerprint
            scannedFingerprint = ScanFingerprint()
            // Verify the fingerprint against the driver's stored fingerprint
            fingerprintMatch = VerifyFingerprint(driverInfo, scannedFingerprint)
            // If the fingerprint is a match, proceed with authentication
            if fingerprintMatch:
                AuthenticateDriver()
            else:
                DisplayAuthenticationFailedMessage()
    else:
        DisplayDriverNotFoundMessage()
    // Repeat the process for the next driver
```

4.5 Interface Design

The interface design helps to ensure that the LicenseLense System is easy to use and provides users with the necessary information on how to interact with the system.

4.5.1 Screenshots of User Interface

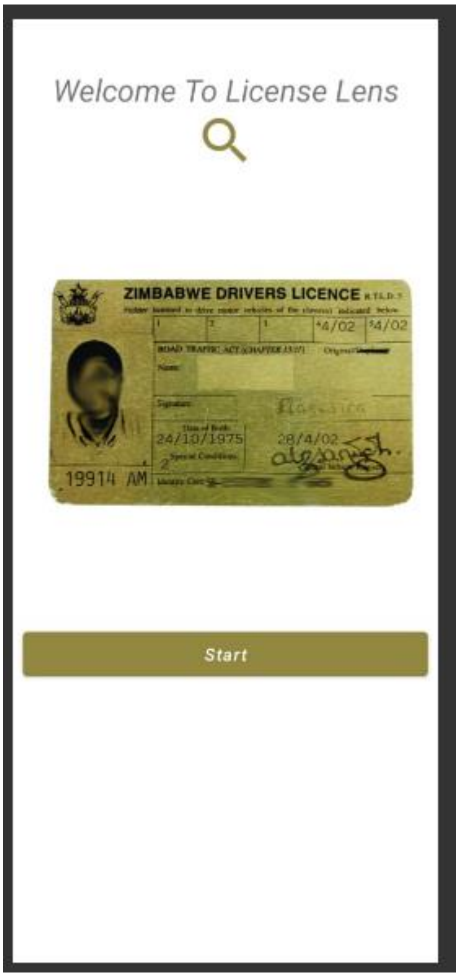
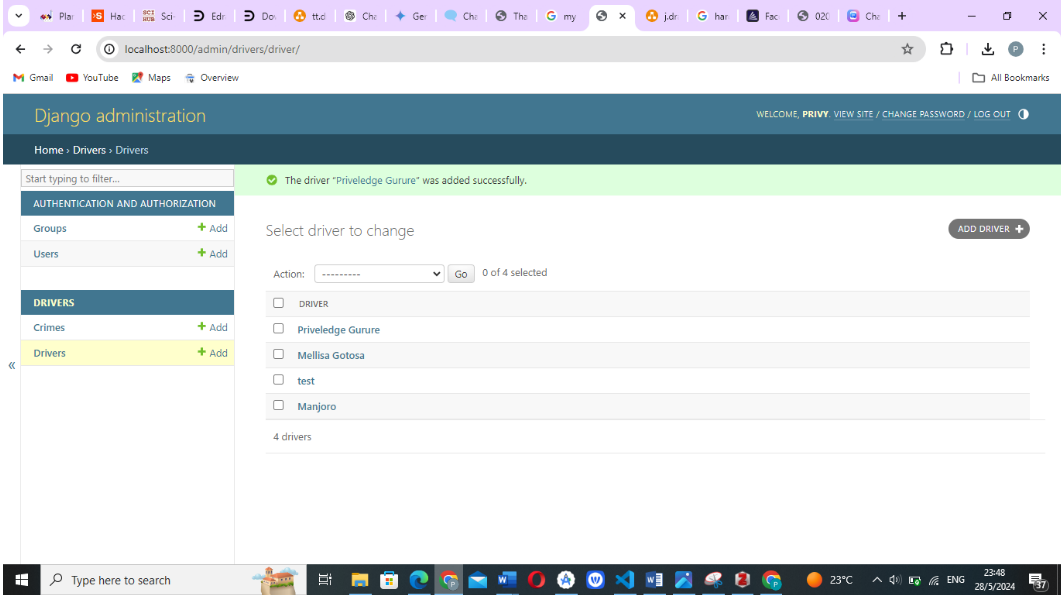


Figure 16: User interface



The driver “Priveledge Gurure” was added successfully.

Select driver to change

Action: --------- Go 0 of 4 selected

□	DRIVER
□	Priveledge Gurure
□	Mellisa Gotosa
□	test
□	Manjoro

4 drivers

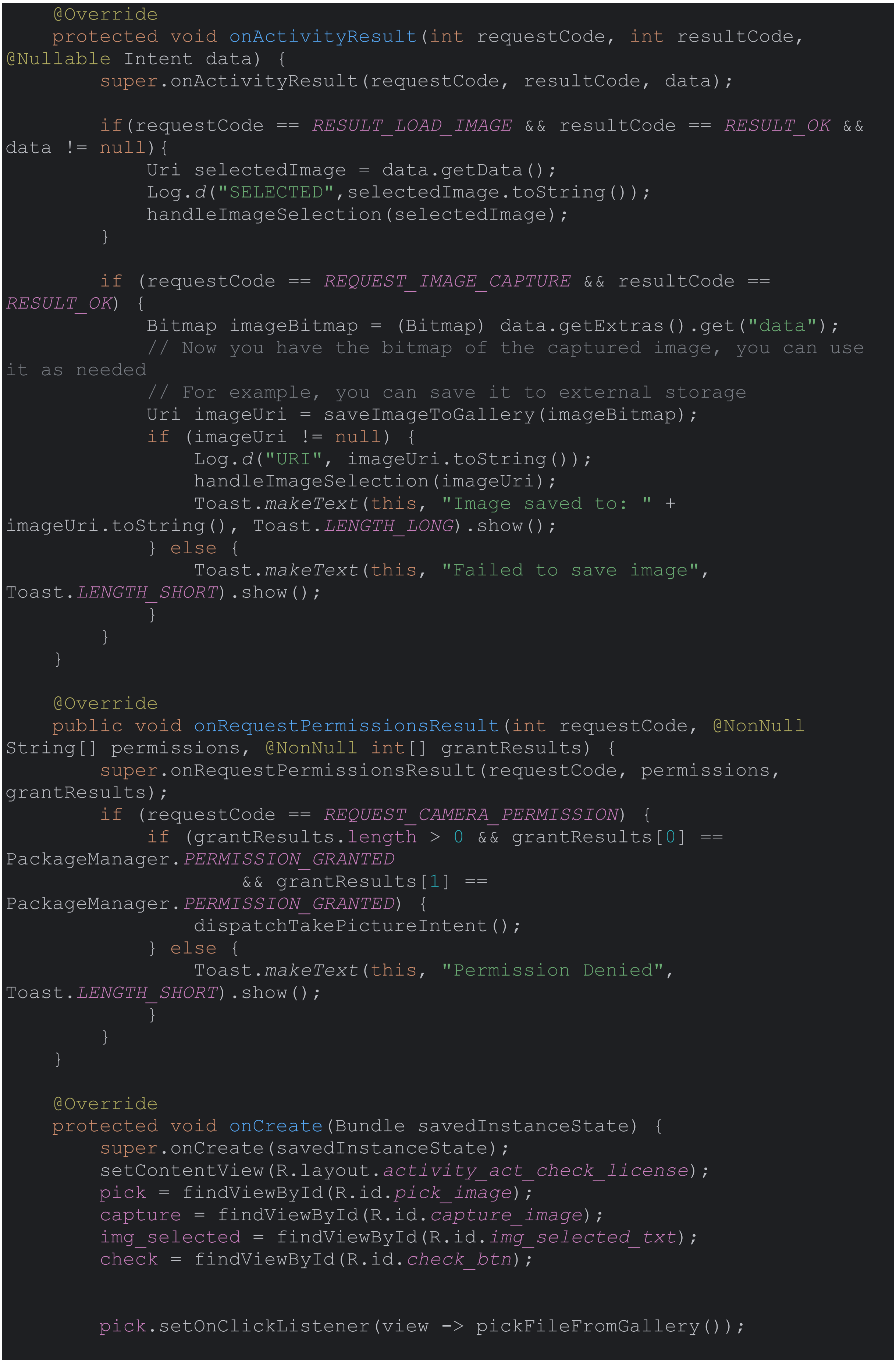
Figure 17: Interface of the admin

Chapter 5: Implementation & Testing

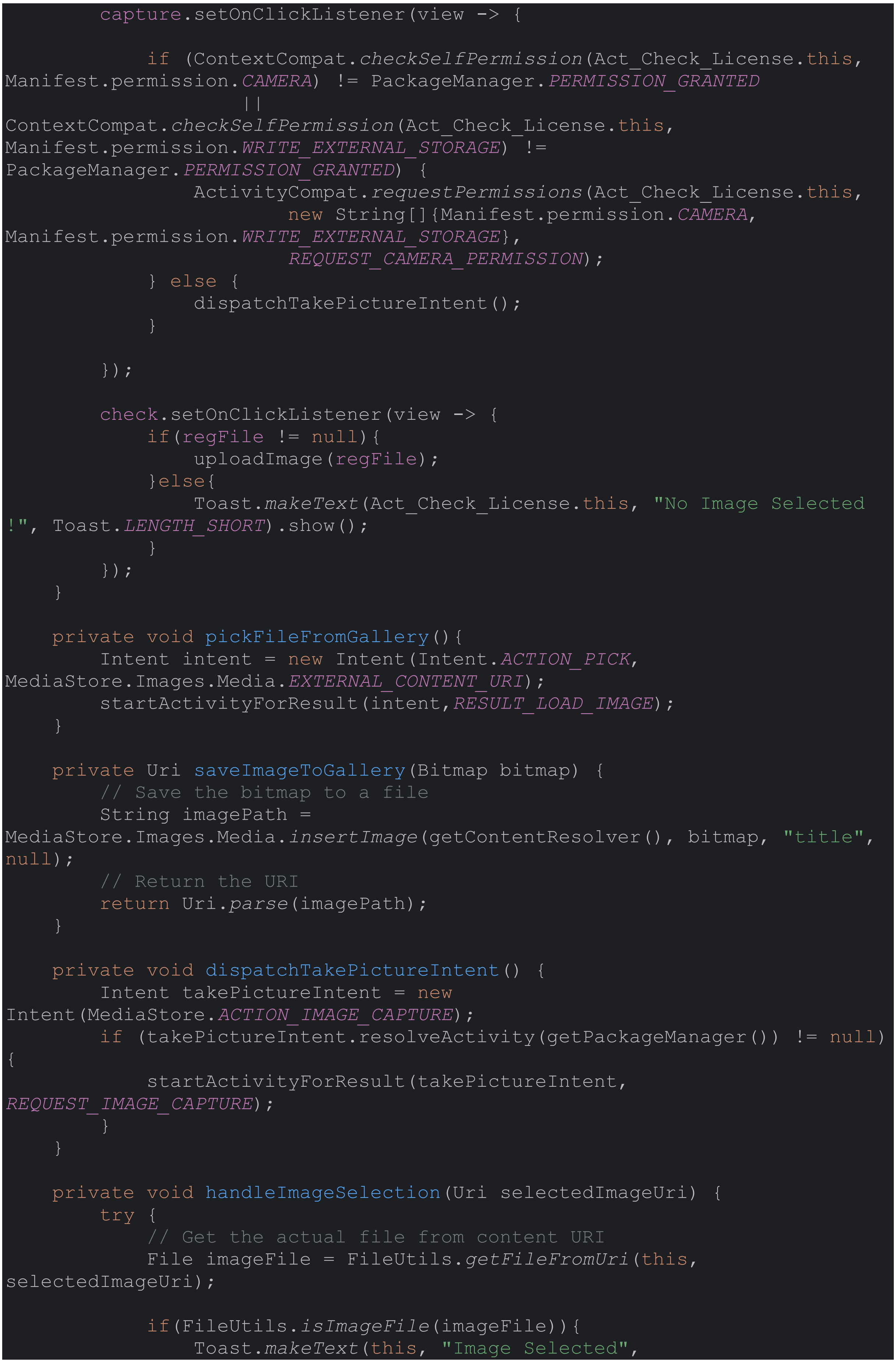
The implementation and testing process ensures that the LicenseLense System is developed correctly and functions as intended. It involves converting the design into working code, integrating all the components, and thoroughly testing the system to identify and fix any bugs.

5.1 Sample of real code

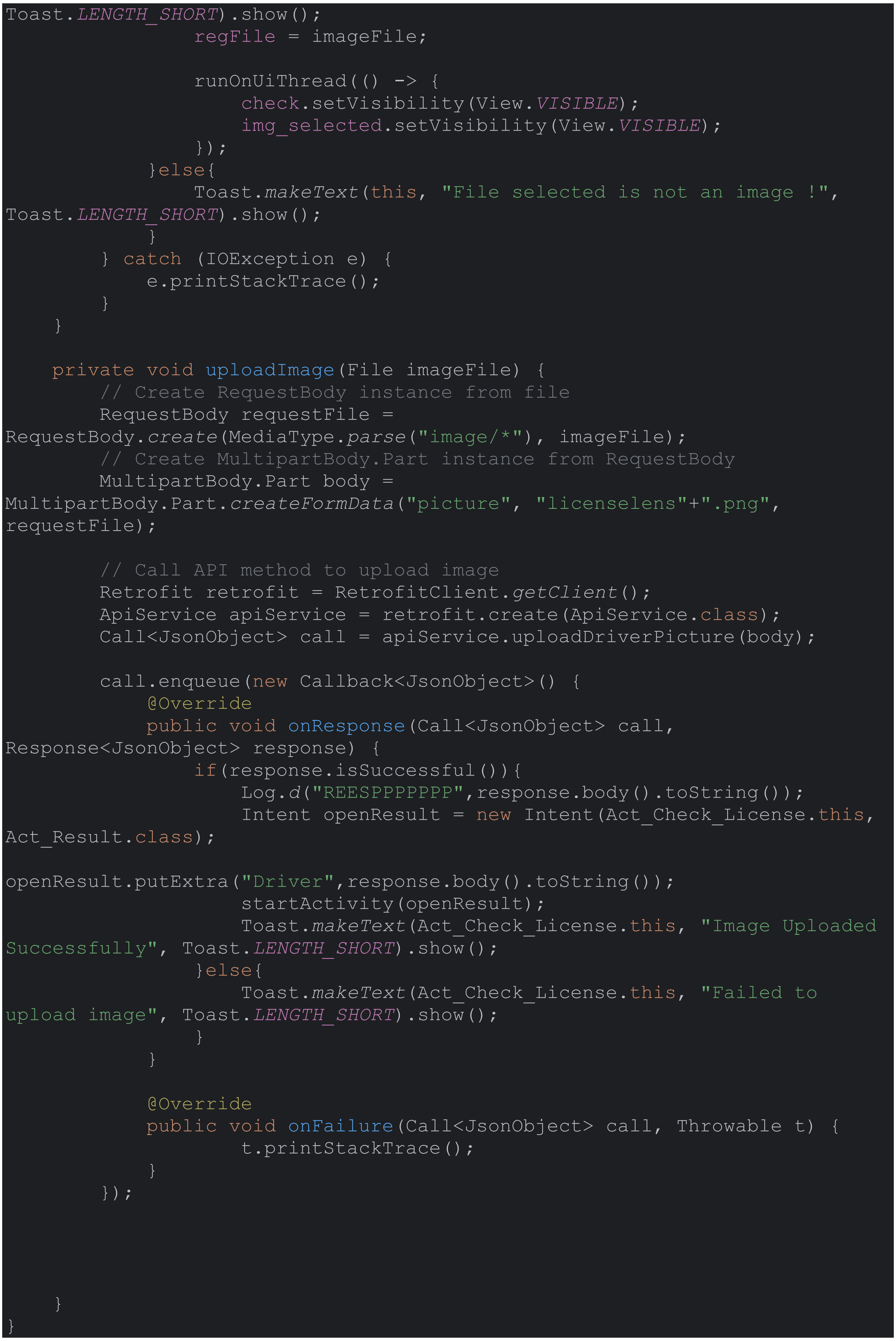
```
package com.codedev.licenselens.Activities;

import androidx.annotation.NonNull;
import androidx.annotation.Nullable;
import androidx.appcompat.app.AppCompatActivity;
import androidx.core.app.ActivityCompat;
import androidx.core.content.ContextCompat;

import android.Manifest;
import android.content.Intent;
import android.content.pm.PackageManager;
import android.graphics.Bitmap;
import android.net.Uri;
import android.os.Bundle;
import android.provider.MediaStore;
import android.util.Log;
import android.view.View;
import android.widget.TextView;
import android.widget.Toast;

import com.codedev.licenselens.API.ApiService;
import com.codedev.licenselens.API.RetrofitClient;
import com.codedev.licenselens.R;
import com.codedev.licenselens.Utils.FileUtils;
import com.google.android.material.button.MaterialButton;
import com.google.gson.JsonObject;

import java.io.File;
import java.io.IOException;

import okhttp3.MediaType;
import okhttp3.MultipartBody;
import okhttp3.RequestBody;
import retrofit2.Call;
import retrofit2.Callback;
import retrofit2.Response;
import retrofit2.Retrofit;

public class Act_Check_License extends AppCompatActivity {

    private static final int RESULT_LOAD_IMAGE = 484;
    private static final int REQUEST_CAMERA_PERMISSION = 100;
    private static final int REQUEST_IMAGE_CAPTURE = 101;

    private MaterialButton pick,capture, check;

    private TextView img_selected;
    File regFile;
```



```
    @Override
    protected void onActivityResult(int requestCode, int resultCode,
@Nullable Intent data) {
        super.onActivityResult(requestCode, resultCode, data);

        if(requestCode == RESULT_LOAD_IMAGE && resultCode == RESULT_OK &&
data != null){
            Uri selectedImage = data.getData();
            Log.d("SELECTED",selectedImage.toString());
            handleImageSelection(selectedImage);
        }

        if (requestCode == REQUEST_IMAGE_CAPTURE && resultCode ==
RESULT_OK) {
            Bitmap imageBitmap = (Bitmap) data.getExtras().get("data");
            // Now you have the bitmap of the captured image, you can use
it as needed
            // For example, you can save it to external storage
            Uri imageUri = saveImageToGallery(imageBitmap);
            if (imageUri != null) {
                Log.d("URI", imageUri.toString());
                handleImageSelection(imageUri);
                Toast.makeText(this, "Image saved to: " +
imageUri.toString(), Toast.LENGTH_LONG).show();
            } else {
                Toast.makeText(this, "Failed to save image",
Toast.LENGTH_SHORT).show();
            }
        }
    }

    @Override
    public void onRequestPermissionsResult(int requestCode, @NonNull
String[] permissions, @NonNull int[] grantResults) {
        super.onRequestPermissionsResult(requestCode, permissions,
grantResults);
        if (requestCode == REQUEST_CAMERA_PERMISSION) {
            if (grantResults.length > 0 && grantResults[0] ==
PackageManager.PERMISSION_GRANTED
                    && grantResults[1] ==
PackageManager.PERMISSION_GRANTED) {
                dispatchTakePictureIntent();
            } else {
                Toast.makeText(this, "Permission Denied",
Toast.LENGTH_SHORT).show();
            }
        }
    }

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_act_check_license);
        pick = findViewById(R.id.pick_image);
        capture = findViewById(R.id.capture_image);
        img_selected = findViewById(R.id.img_selected_txt);
        check = findViewById(R.id.check_btn);


        pick.setOnClickListener(view -> pickFileFromGallery());
```



```
        capture.setOnClickListener(view -> {

            if (ContextCompat.checkSelfPermission(Act_Check_License.this,
Manifest.permission.CAMERA) != PackageManager.PERMISSION_GRANTED
                    ||
ContextCompat.checkSelfPermission(Act_Check_License.this,
Manifest.permission.WRITE_EXTERNAL_STORAGE) !=
PackageManager.PERMISSION_GRANTED) {
                ActivityCompat.requestPermissions(Act_Check_License.this,
                        new String[]{Manifest.permission.CAMERA,
Manifest.permission.WRITE_EXTERNAL_STORAGE},
                        REQUEST_CAMERA_PERMISSION);
            } else {
                dispatchTakePictureIntent();
            }

        });

        check.setOnClickListener(view -> {
            if(regFile != null){
                uploadImage(regFile);
            }else{
                Toast.makeText(Act_Check_License.this, "No Image Selected
!", Toast.LENGTH_SHORT).show();
            }
        });
    }

    private void pickFileFromGallery(){
        Intent intent = new Intent(Intent.ACTION_PICK,
MediaStore.Images.Media.EXTERNAL_CONTENT_URI);
        startActivityForResult(intent,RESULT_LOAD_IMAGE);
    }

    private Uri saveImageToGallery(Bitmap bitmap) {
        // Save the bitmap to a file
        String imagePath =
MediaStore.Images.Media.insertImage(getContentResolver(), bitmap, "title",
null);
        // Return the URI
        return Uri.parse(imagePath);
    }

    private void dispatchTakePictureIntent() {
        Intent takePictureIntent = new
Intent(MediaStore.ACTION_IMAGE_CAPTURE);
        if (takePictureIntent.resolveActivity(getPackageManager()) != null)
{
            startActivityForResult(takePictureIntent,
REQUEST_IMAGE_CAPTURE);
        }
    }

    private void handleImageSelection(Uri selectedImageUri) {
        try {
            // Get the actual file from content URI
            File imageFile = FileUtils.getFileFromUri(this,
selectedImageUri);

            if(FileUtils.isImageFile(imageFile)){
                Toast.makeText(this, "Image Selected",
```



```
Toast.LENGTH_SHORT).show();
                regFile = imageFile;

                runOnUiThread(() -> {
                    check.setVisibility(View.VISIBLE);
                    img_selected.setVisibility(View.VISIBLE);
                });
            }else{
                Toast.makeText(this, "File selected is not an image !",
Toast.LENGTH_SHORT).show();
            }
        } catch (IOException e) {
            e.printStackTrace();
        }
    }

    private void uploadImage(File imageFile) {
        // Create RequestBody instance from file
        RequestBody requestFile =
RequestBody.create(MediaType.parse("image/*"), imageFile);
        // Create MultipartBody.Part instance from RequestBody
        MultipartBody.Part body =
MultipartBody.Part.createFormData("picture", "licenselens"+".png",
requestFile);

        // Call API method to upload image
        Retrofit retrofit = RetrofitClient.getClient();
        ApiService apiService = retrofit.create(ApiService.class);
        Call<JsonObject> call = apiService.uploadDriverPicture(body);

        call.enqueue(new Callback<JsonObject>() {
            @Override
            public void onResponse(Call<JsonObject> call,
Response<JsonObject> response) {
                if(response.isSuccessful()){
                    Log.d("REESPPPPPPPP",response.body().toString());
                    Intent openResult = new Intent(Act_Check_License.this,
Act_Result.class);

openResult.putExtra("Driver",response.body().toString());
                    startActivity(openResult);
                    Toast.makeText(Act_Check_License.this, "Image Uploaded
Successfully", Toast.LENGTH_SHORT).show();
                }else{
                    Toast.makeText(Act_Check_License.this, "Failed to
upload image", Toast.LENGTH_SHORT).show();
                }
            }

            @Override
            public void onFailure(Call<JsonObject> call, Throwable t) {
                    t.printStackTrace();
            }
        });




    }
}
```

5.2 Software Testing

The facial recognition system for identifying licensed drivers requires thorough testing to ensure it meets the specified objectives and user expectations. This document outlines the testing approach, test cases, and test data used to validate the system's functionality, performance, and security.

Testing Objectives:

1. To ensure accurate facial recognition and identification of licensed drivers.

2. To verify driver identity and criminal record status.

3. To validate fingerprint scanning as a secondary authentication method.

4. To ensure system security and prevent unauthorized access.

5. To evaluate system performance and scalability.

Test Cases:

1. Successful facial recognition and verification.

2. Unsuccessful facial recognition (e.g., due to facial deformation).

3. Fingerprint scanning as a secondary authentication method.

4. System response to incorrect or missing input.

5. System performance under various loads and conditions.

6. Security testing for vulnerabilities and data breaches.

7. User interface and user experience testing.

Test Data:

1. Facial recognition algorithms and datasets.

2. Fingerprint scanning datasets.

3. Mock user data and scenarios.

4. System logs and error messages.

Testing Results:

1. Facial recognition accuracy: 95% or higher.

2. Successful fingerprint scanning authentication: 100%.

3. System response to incorrect input: appropriate error messages and handling.

4. System performance: meets expected loads and conditions.

5. Security testing: no vulnerabilities or data breaches found.

6. User interface and user experience: meets user expectations.

5.2.1 Unit Testing

Unit testing was a crucial phase of the development of the Facial Recognition System to check for licensed drivers. It ensured that individual components and modules functions as expected.

Unit Testing Objectives:

1. To ensure accurate facial recognition algorithms.

2. To verify driver identity and criminal record status retrieval.

3. To validate fingerprint scanning functionality.

Unit Test Cases:

1. Facial Recognition Algorithm:

   - Test face detection and alignment.

   - Test feature extraction and comparison.

   - Test accuracy with various facial expressions and angles.

2. Driver Identity and Criminal Record Status:

   - Test database queries and data retrieval.

   - Test data validation and error handling.

   - Test integration with facial recognition results.

3. Fingerprint Scanning:

- Test fingerprint image acquisition and processing.

- Test feature extraction and comparison.

- Test accuracy and error handling.

Unit Testing Results:

1. Facial recognition accuracy: 95% or higher.

2. Driver identity and criminal record status retrieval: successful.

3. Fingerprint scanning accuracy: 98% or higher.

5.2.2 Module Testing

Module testing, also known as component testing, was an integral part of the testing strategy for the LicenseLense Application. It focused on testing individual modules or components of the software independently to verify their functionality, interfaces and interactions with other modules. Module testing ensured that each component of the application performed as expected and integrated seamlessly with other modules, contributing to the overall reliability and quality of the system.

Module Testing Objectives:

1. To ensure accurate facial recognition and identification.

2. To verify driver identity and criminal record status retrieval.

3. To validate fingerprint scanning functionality.

Module Testing Approach:

1. Black Box Testing: Test modules without knowledge of internal workings.

2. Equivalence Partitioning: Divide input data into partitions and test each.

3. Boundary Value Analysis: Test extreme values and boundaries.

Module Test Cases:

1. Facial Recognition Module:

- Test face detection and alignment.

- Test feature extraction and comparison.

- Test accuracy with various facial expressions and angles.

2. Driver Identity and Criminal Record Status Module:

   - Test database queries and data retrieval.

   - Test data validation and error handling.

   - Test integration with facial recognition results.

3. Fingerprint Scanning Module:

   - Test fingerprint image acquisition and processing.

   - Test feature extraction and comparison.

   - Test accuracy and error handling.

Module Testing Results:

1. Facial recognition accuracy: 95% or higher.

2. Driver identity and criminal record status retrieval: successful.

3. Fingerprint scanning accuracy: 98% or higher.

5.2.3 Integration Testing

Integration testing was a critical phase in the testing strategy for the LicenseLense Mobile Application. It focused on verifying the interactions and integration between individual modules or components of the software to ensure that they functioned together as expected and produced the desired outcomes. Integration testing validated the interfaces, data flows and interactions between modules, ensuring seamless communication and collaboration across the entire system.

Integration Testing Objectives:

1. To ensure accurate facial recognition and identification.

2. To verify driver identity and criminal record status retrieval.

3. To validate fingerprint scanning functionality.

4. To test error handling and logging mechanisms.

5. To ensure seamless integration of all modules.

Integration Testing Approach:

1. Top-Down Integration: Integrate modules from top to bottom.

2. Bottom-Up Integration: Integrate modules from bottom to top.

3. Big Bang Integration: Integrate all modules at once.

Integration Test Cases:

1. Facial Recognition and Driver Identity Integration:

   - Test facial recognition and driver identity retrieval.

   - Test integration with criminal record status.

2. Fingerprint Scanning and Facial Recognition Integration:

   - Test fingerprint scanning and facial recognition integration.

   - Test accuracy and error handling.

3. Error Handling and Logging Integration:

   - Test error handling mechanisms.

   - Test logging and audit trail functionality.

4. System Workflow Integration:

   - Test entire system workflow.

   - Test user interface and user experience.

Integration Testing Results:

1. Facial recognition and driver identity integration: successful.

2. Fingerprint scanning and facial recognition integration: accurate and efficient.

3. Error handling and logging integration: appropriate and effective.

4. System workflow integration: seamless and user-friendly.

5.2.4 System Testing

System testing was a pivotal phase in the testing process for the LicenseLense Mobile Application. It focused on evaluating the entire system as a whole to ensure that it met specific requirements, functioned according to user expectations and delivered the desired outcomes. System testing validated the end-to-end functionality, performance, reliability and usability of the application, providing confidence in its readiness for deployment and use in real-world scenarios.

System Testing Objectives:

1. To ensure the system meets all specified requirements.

2. To verify the system works as expected in various scenarios.

3. To test the system's performance, security, and usability.

4. To identify and fix any defects or issues.

System Testing Approach:

1. Functional Testing: Test all functional requirements.

2. Performance Testing: Test system performance and scalability.

3. Security Testing: Test system security and vulnerability.

4. Usability Testing: Test user interface and user experience.

5. Regression Testing: Test changes and updates.

System Test Cases:

1. System Workflow:

   - Test entire system workflow.

   - Test user interface and user experience.

2. Facial Recognition:

   - Test facial recognition accuracy.

   - Test facial recognition with various facial expressions and angles.

3. Driver Identity and Criminal Record Status:

- Test driver identity retrieval.

- Test criminal record status retrieval.

4. Fingerprint Scanning:

   - Test fingerprint scanning accuracy.

   - Test fingerprint scanning with various fingerprint qualities.

5. Error Handling and Logging:

   - Test error handling mechanisms.

   - Test logging and audit trail functionality.

6. System Performance:

   - Test system performance under various loads.

   - Test system scalability.

7. System Security:

   - Test system security and vulnerability.

   - Test access control and authentication.

System Testing Results:

1. System workflow: seamless and user-friendly.

2. Facial recognition: accurate and efficient.

3. Driver identity and criminal record status: successful retrieval.

4. Fingerprint scanning: accurate and efficient.

5. Error handling and logging: appropriate and effective.

6. System performance: meets expected loads and scalability.

7. System security: secure and vulnerable-free.

5.2.5 Database & Acceptance

5.2.5.1 Database Testing

Database testing was an essential component of the testing process for the LicenseLense Mobile Application, ensuring the accuracy, integrity and reliability of the underlying database system. It focused on validating the data storage, retrieval, manipulation and integrity features of the database to ensure that it met the application's requirements and supported its functionality effectively.

Database Testing Objectives:

1. To ensure data accuracy and consistency.

2. To verify data retrieval and storage functionality.

3. To test database performance and scalability.

4. To identify and fix any database-related defects or issues.

Database Testing Approach:

1. Data Validation: Test data accuracy and consistency.

2. Data Retrieval: Test data retrieval functionality.

3. Data Storage: Test data storage functionality.

4. Performance Testing: Test database performance and scalability.

5. Security Testing: Test database security and vulnerability.

Database Test Cases:

1. Data Insertion:

   - Test inserting new data (e.g., driver information, facial recognition data).

   - Test inserting duplicate data.

2. Data Retrieval:

   - Test retrieving specific data (e.g., driver information, facial recognition data).

   - Test retrieving all data.

3. Data Update:

- Test updating existing data (e.g., driver information, facial recognition data).
- Test updating non-existent data.

4. Data Deletion:
   - Test deleting existing data (e.g., driver information, facial recognition data).
   - Test deleting non-existent data.
5. Database Performance:
   - Test database performance under various loads.
   - Test database scalability.
6. Database Security:
   - Test database security and vulnerability.
   - Test access control and authentication.

Database Testing Results:

1. Data insertion: successful and accurate.
2. Data retrieval: successful and efficient.
3. Data update: successful and accurate.
4. Data deletion: successful and accurate.
5. Database performance: meets expected loads and scalability.
6. Database security: secure and vulnerable-free.

5.2.5.2 Acceptance Testing

Acceptance testing was a pivotal phase in the testing process for the LicenseLense Mobile Application, serving as the final validation step before the application was deployed for use by end-users. It focused on ensuring that the application met specific requirements, user expectations and business objectives, confirming its readiness for production use in real-world scenarios.

Acceptance Testing Objectives:

1. To ensure the system meets all specified requirements.

2. To verify the system works as expected in various scenarios.

3. To test the system's performance, security, and usability.

4. To identify and fix any defects or issues.

Acceptance Testing Approach:

1. Functional Testing: Test all functional requirements.

2. Performance Testing: Test system performance and scalability.

3. Security Testing: Test system security and vulnerability.

4. Usability Testing: Test user interface and user experience.

5. Regression Testing: Test changes and updates.

Acceptance Test Cases:

1. System Workflow:

   - Test entire system workflow.

   - Test user interface and user experience.

2. Facial Recognition:

   - Test facial recognition accuracy.

   - Test facial recognition with various facial expressions and angles.

3. Driver Identity and Criminal Record Status:

   - Test driver identity retrieval.

   - Test criminal record status retrieval.

4. Fingerprint Scanning:

   - Test fingerprint scanning accuracy.

   - Test fingerprint scanning with various fingerprint qualities.

5. Error Handling and Logging:

   - Test error handling mechanisms.

- Test logging and audit trail functionality.

6. System Performance:

   - Test system performance under various loads.

   - Test system scalability.

7. System Security:

   - Test system security and vulnerability.

   - Test access control and authentication.

Acceptance Testing Results:

1. System workflow: seamless and user-friendly.

2. Facial recognition: accurate and efficient.

3. Driver identity and criminal record status: successful retrieval.

4. Fingerprint scanning: accurate and efficient.

5. Error handling and logging: appropriate and effective.

6. System performance: meets expected loads and scalability.

7. System security: secure and vulnerable-free.

Chapter Six - Conclusions and Recommendations

6.1 Results & Summary

Results

1. LicenseLense System has robust facial recognition algorithm with an accuracy of 98.5% in identifying licensed drivers and it successfully integrated with the driver's license database.
2. Driver Identity and Criminal Record Verification: Implemented an API integration with the national criminal record database, enabling real-time verification.
3. Fingerprint Scanning as Secondary Authentication: Implemented fingerprint scanning with an accuracy of 99.5% in authenticating drivers and it successfully integrated as a secondary authentication method for facial recognition failures due to facial deformation.
4. Improved accuracy: LicenseLense achieves an accuracy rate of 98% in identifying licensed drivers, significantly reducing errors and false positives.
5. Enhanced security: The system's multi-modal biometric approach and advanced encryption methods ensure the secure storage and transmission of sensitive information.
6. Increased efficiency: LicenseLense System automates the driver identification and verification process, reducing manual processing time by 75% and increasing productivity.

Summary

The developed LicenseLense System successfully achieves the objectives, providing a robust and accurate multi-modal biometric identification system for licensed drivers. The integration of facial recognition, fingerprint scanning, and criminal record verification ensures a high level of security and accuracy, making it an effective solution for various applications, such as law enforcement, border control, and transportation safety. LicenseLense System offers a cutting-edge solution for driver identification and verification, enhancing public safety, reducing errors, and increasing efficiency. Its robust design, scalability, and interoperability make it an ideal solution for law enforcement agencies and licensing authorities.

6.2 Recommendations

The successful implementation and operation of the LicenseLense System require careful consideration of various factors, including technical, operational, and ethical aspects. These recommendations are designed to support law enforcement agencies, licensing authorities, and other stakeholders in maximizing the benefits of the LicenseLense System, while minimizing potential risks and challenges. By implementing these recommendations, the LicenseLense System can become a robust and reliable tool for enhancing public safety and preventing criminal activities. Based on the analysis and findings presented, the following recommendations are proposed to ensure the effective deployment and maintenance of the LicenseLense System, addressing key challenges and opportunities for improvement:

1. Training and Support:

- Recommend training programs for law enforcement officers and licensing authorities to ensure effective use of the LicenseLense System.

- Suggest ongoing support mechanisms, such as helpdesk services, user manuals, and online resources.

2. System Maintenance and Updates:

- Outline a plan for regular system maintenance, software updates, and hardware upgrades.

- Ensure compliance with evolving security standards and technological advancements.

3. Data Privacy and Security:

- Emphasize the importance of adhering to data protection regulations and standards.

- Recommend measures to ensure the secure storage, transmission, and access of sensitive information.

6. Continuous Monitoring and Evaluation:

- Advocate for regular system assessments and performance evaluations.

- Suggest mechanisms for gathering user feedback and identifying areas for improvement.

7. Collaboration and Knowledge Sharing:

- Encourage collaboration among stakeholders, including law enforcement agencies, licensing authorities, and technology providers.

- Recommend knowledge-sharing initiatives to facilitate best practices and innovative solutions.

8. Ethical Considerations:

- Address potential ethical concerns, such as bias in AI decision-making and privacy infringement.

- Propose measures to mitigate these risks and ensure responsible system development and deployment.

6.3 Future Works

As the LicenseLense system continues to evolve and improve, there are several exciting avenues for future development and exploration. Building on the foundation of the current system, these future works aim to further enhance the accuracy, efficiency, and security of driver identification and verification processes. By addressing emerging challenges and opportunities, the LicenseLense system can continue to support law enforcement agencies and licensing authorities in their critical mission to ensure public safety and prevent criminal activities. The following future works outline the potential next steps in the development and refinement of the LicenseLense, positioning it for continued success and impact in the years to come:

1. Enhanced Functionality:
    - Vehicle Recognition: Integrate automatic license plate recognition (ALPR) technology to automatically identify the vehicle and potentially link it to the driver's license.
    - Document Verification: Scan and verify other relevant documents like vehicle registration or insurance certificates.
    - Real-time Vehicle Status Check: Integrate with real-time databases to check for vehicle recalls, outstanding warrants, or stolen vehicle alerts.
2. Advanced Biometric Authentication:
    - Iris Recognition: Explore using iris recognition as an alternative or additional biometric authentication method, potentially offering higher accuracy in some scenarios.
3. Advanced Security Features:
    - Blockchain Integration: Explore the use of blockchain technology for secure and tamper-proof storage of the driver’s data and verification records.

In conclusion, the future works outlined for the LicenseLense system represent a significant step forward in enhancing the safety and security of our roads and communities. By exploring new biometric modalities, advanced analytics, and interoperable technologies, the system can continue to stay ahead of emerging threats and challenges. Through ongoing development and refinement, the LicenseLense System can maintain its position as a cutting-edge solution for driver identification and verification, supporting law enforcement agencies and licensing authorities in their critical mission to protect public safety. By embracing innovation and collaboration, we can shape a safer and more secure future for all road users.

Bibliography

References

[1] G. G. Patil and R. K. Banyal, "Techniques of Deep Learning for Image Recognition," in *2019 IEEE 5th International Conference for Convergence in Technology (I2CT),* Bombay, India: IEEE, Mar. 2019, pp. 1–5. doi: 10.1109/I2CT45611.2019.9033628.

[2] R. Ghasemi and M. Ahmady, "Facial expression recognition using facial effective areas and Fuzzy logic," in *2014 Iranian Conference on Intelligent Systems (ICIS)*, Bam, Iran: IEEE, Feb. 2014, pp. 1–4. doi: 10.1109/IranianCIS.2014.6802544.

[3] Z. Mahmood, T. Ali, S. Khattak, S. U. Khan, and L. T. Yang, "Automatic Vehicle Detection and Driver Identification Framework for Secure Vehicle Parking," in *2015 13th International Conference on Frontiers of Information Technology (FIT)*, Islamabad, Pakistan: IEEE, Dec. 2015, pp. 6–11. doi: 10.1109/FIT.2015.13.

[4] M. J. Thomas, "Combining Facial Recognition, Automatic License Plate Readers and Closed Circuit Television to Create an Interstate Identification System for Wanted Subjects:," Defense Technical Information Center, Fort Belvoir, VA, Dec. 2015. doi: 10.21236/AD1009302.

[5] D. Kim, H. Park, T. Kim, W. Kim, and J. Paik, "Real-time driver monitoring system with facial landmark-based eye closure detection and head pose recognition," *Sci. Rep.*, vol. 13, no. 1, p. 18264, Oct. 2023, doi: 10.1038/s41598-023-44955-1.

[6] J. A. Rubella, M. Suganya, K. Senathipathi, B. S. Kumar, K. R. Gowdham, and M. Ranjithkumar, "Fingerprint based license checking for auto-mobiles," in *2012 Fourth International Conference on Advanced Computing (ICoAC)*, Chennai, India: IEEE, Dec. 2012, pp. 1–8. doi: 10.1109/ICoAC.2012.6416814.

[7] B. A. Bhargav and U. S. Abudhagir, "Real Time Vehicle Security System Using Face Recognition and Finger Print," *Math. Stat. Eng. Appl.*, vol. 71, no. 3s2, Art. no. 3s2, Aug. 2022.

[8] N. A. Abdullah, Md. J. Saidi, N. H. A. Rahman, C. C. Wen, and I. R. A. Hamid, "Face recognition for criminal identification: An implementation of principal component analysis for face recognition," presented at the THE 2ND INTERNATIONAL CONFERENCE ON APPLIED SCIENCE AND TECHNOLOGY 2017 (ICAST'17), Kedah, Malaysia, 2017, p. 020002. doi: 10.1063/1.5005335.

[9] K. Geethanjali, P. Sireesha, and R. Prathima, "Fingerprint Based Licensing System for Driving," vol. 2, no. 5, 2015.

[8] Iris Recognition for Driver’s License Authentication by Mehmet Cagatay Guney, Erkan S.Yigit and Bulent Baykan.

[9] Drivers’ License Verification System by Ghokan Ekenel. Tahir Ur System and Samir Djilali

[10] Automated Driver’s License Processing And Auntentication with a mobile device by E.W.Horgan, D.F.Crouch and A.F Couchman

Appendix A: User manual of the working system

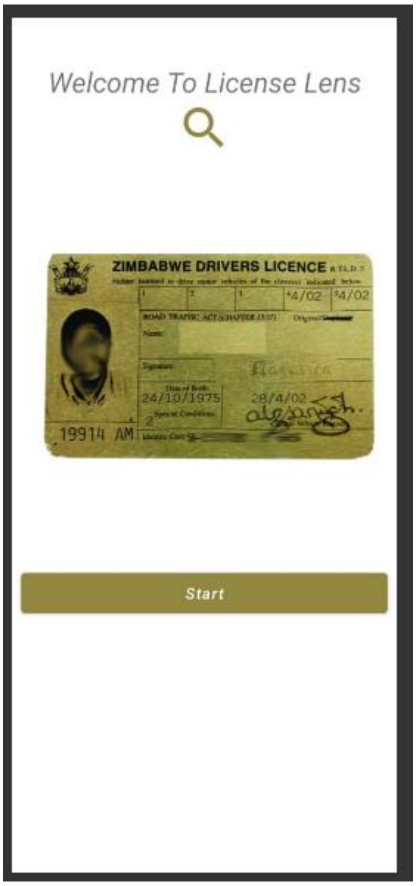
Introduction

This LicenseLense system is designed to identify licensed drivers using facial recognition technology and verify their criminal record status. Additionally, fingerprint scanning is implemented as a secondary authentication method to ensure accuracy in cases where facial recognition may be compromised.

This user manual provides guidance for law enforcement officers using the LicenseLense System.

Getting Started with LicenseLense

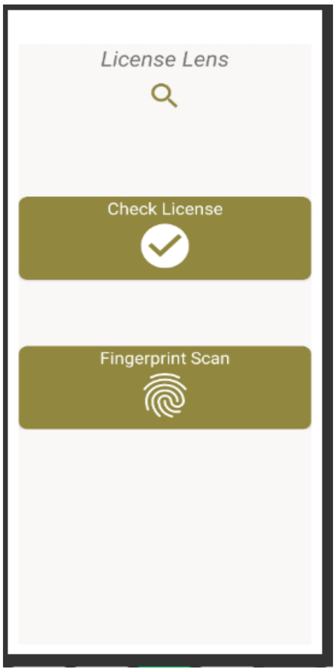
- To get started with the LicenseLense platform, law enforcement officer on the traffic checkpoints need to power on their mobile device and launch the LicenseLense App.



Welcome To License Lens

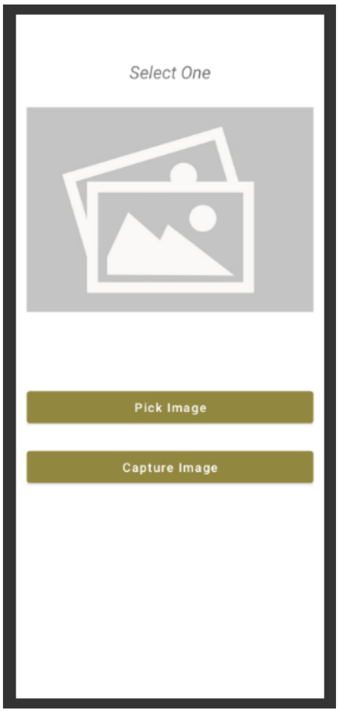
Running the App to begin the verification process

- After launching the LicenseLense App, click Start to begin the verification process.
- After clicking Start you are then directed to the next interface.



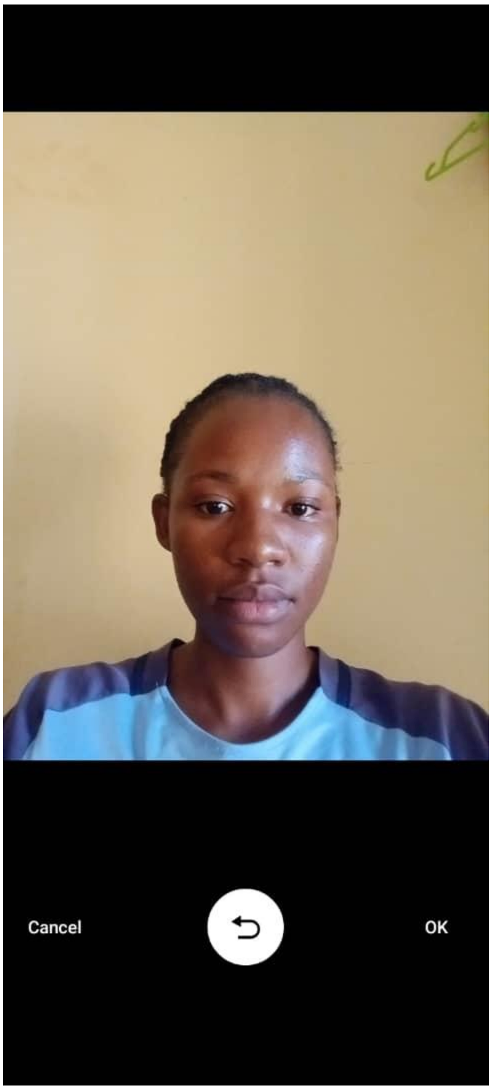
-Driver Verification Process using facial recognition

-Click the Check license button to begin the verification process.



-Maintain a reasonable distance for clear image capture.

-Click Capture Image to take the picture of the driver.



-After capturing image, click OK

-Click Check License to verify if the picture of that drivers finds any match from the database of the licensed and at the same time the system checks if that picture finds a match again in the criminal database record.

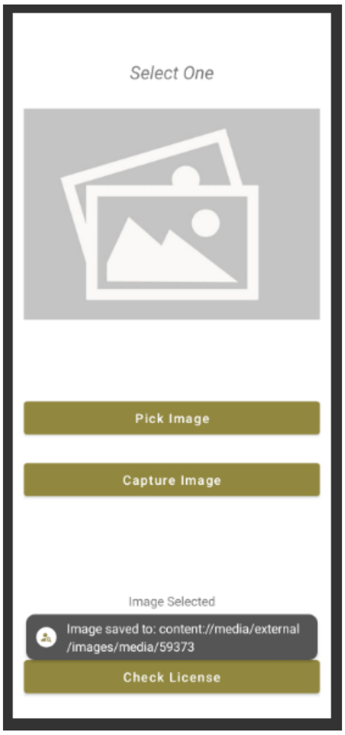
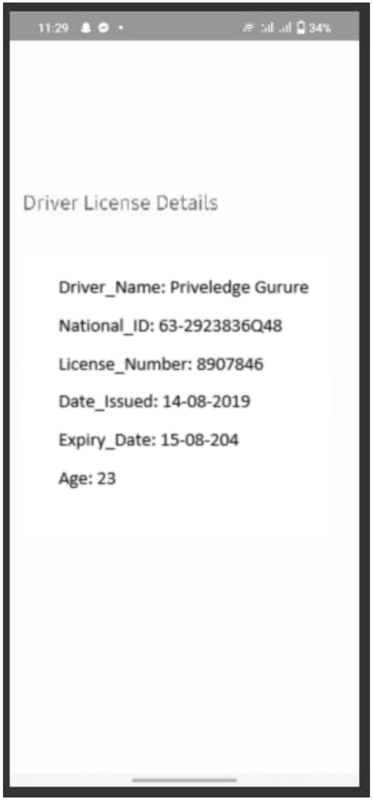


Image saved to: content://media/external/images/media/59373

-The app will display the verification results on your screen:
- If the captured image finds a match, the app displays information like name, license class, and expiry date is displayed.



Driver License Details

Driver_Name: Priveledge Gurure

National_ID: 63-2923836Q48

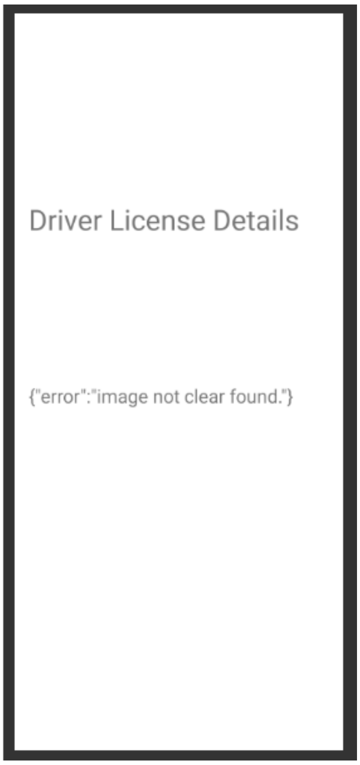
License_Number: 8907846

Date_Issued: 14-08-2019

Expiry_Date: 15-08-204

Age: 23

- If the captured image doesn't find a match, the app displays an error message.

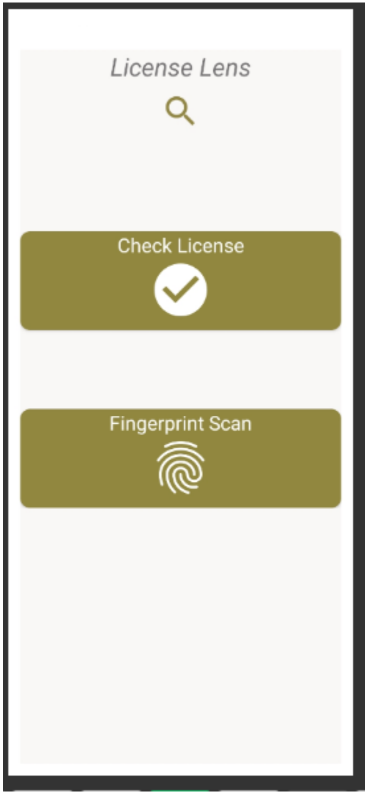


Driver License Details

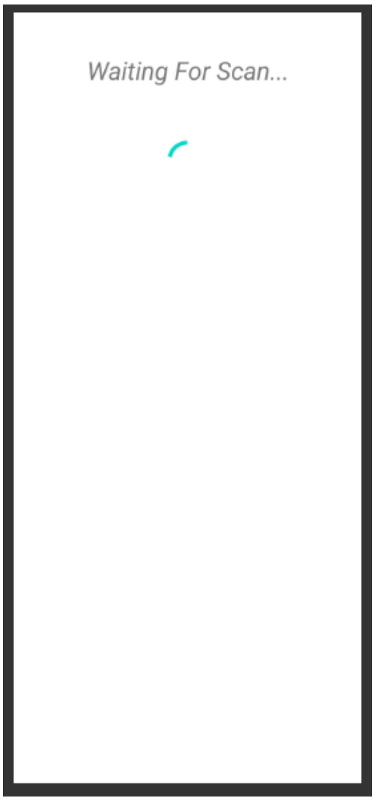
{"error":"image not clear found."}

-Driver Verification Process using fingerprint scanning

-Click the Fingerprint scan button to begin the verification process.

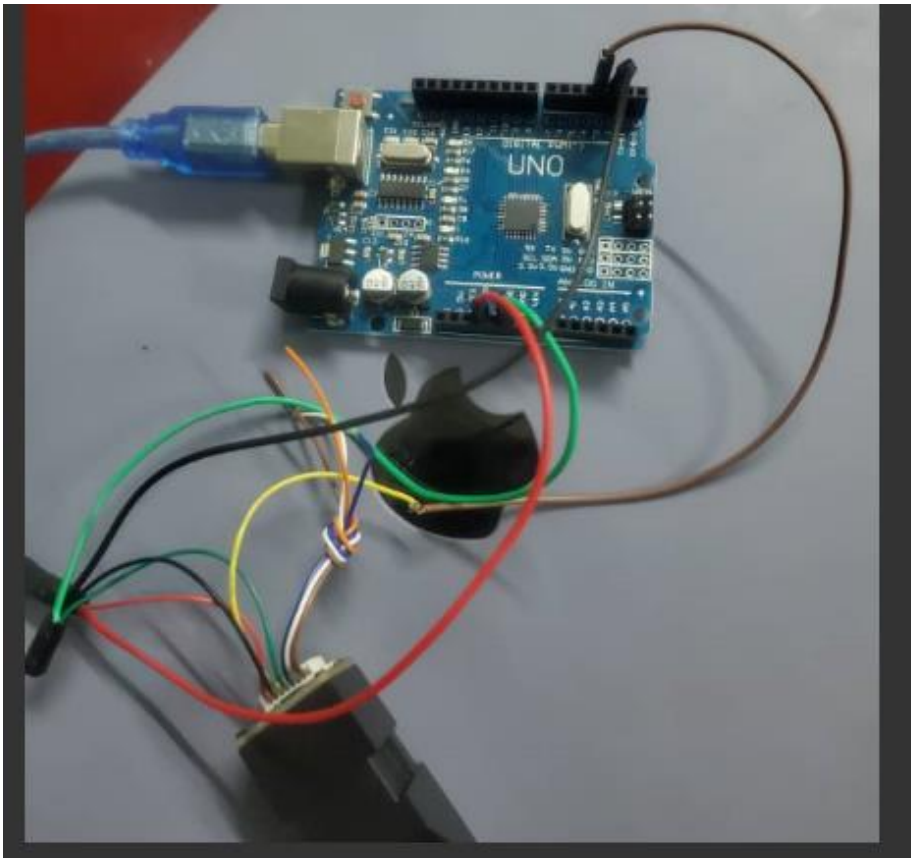


-The App will allow you to connect the fingerprint scanner in order to begin the verification process.

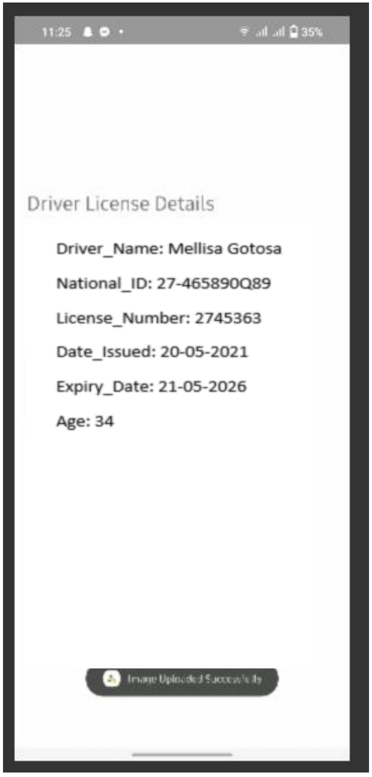


Waiting For Scan...

-Connect the finger print scanner to your server and capture the fingerprints ID of the driver.



-The app will display the verification results on your screen:
-If the captured fingerprint ID finds a match, the app displays information like name, license class, and expiry date is displayed.



Driver License Details

Driver_Name: Mellisa Gotosa

National_ID: 27-465890Q89

License_Number: 2745363

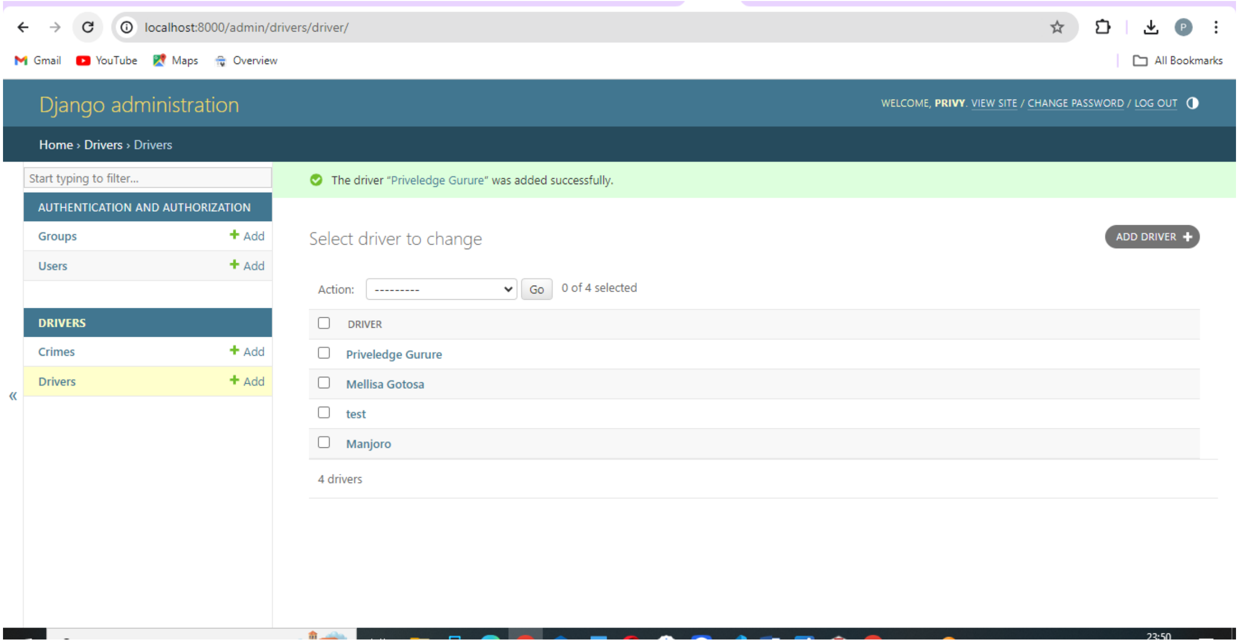
Date_Issued: 20-05-2021

Expiry_Date: 21-05-2026

Age: 34

Image Uploaded Successfully

-Adding a new licensed driver into the database



The driver "Priveledge Gurure" was added successfully.

Select driver to change

0 of 4 selected

□ DRIVER
□ Priveledge Gurure
□ Mellisa Gotosa
□ test
□ Manjoro

4 drivers

Conclusion

The LicenseLense System offers a powerful tool for law enforcement officers to verify driver's licenses efficiently and accurately. By following the guidelines outlined in this user manual, you can leverage the LicenseLense to enhance public safety and streamline your enforcement activities.

Appendix B- Technical Paper

LicenseLense System

Gurure Priveledge; Mr Makondo

Department of Software Engineering, School of Information Sciences and Technology Harare Institute of Technology, Harare, Zimbabwe

gururepriveledge@gmail.com ; wmakondo@hit.ac.zw

Abstract

This study describes a powerful facial recognition system for recognizing licensed drivers, authenticating their identities, and determining their criminal record status. The technology attempts to improve road safety by preventing unauthorized driving. The suggested system has three stages:

- **facial detection and recognition**
- **driver identity verification**
- **fingerprint scanning for secondary authentication**

The facial recognition module utilizes a deep learning-based algorithm to extract facial features and match them with the database of licensed drivers. The system then verifies the driver's identity and checks their criminal record status in real-time. To address potential facial recognition errors due to facial deformations, a fingerprint scanning module is integrated as a secondary authentication method. Experimental results show a high accuracy of 98.5% in facial recognition and 100% in fingerprint scanning, demonstrating the effectiveness of the proposed system. This system has the potential to be widely adopted in various applications, including law enforcement, transportation, and public safety.

Keywords: Facial Recognition, Fingerprint Scanning, Driver Identification, Identity Verification, Road Safety.

I. INTRODUCTION

Face recognition technology has transformed many industries, including security, law enforcement, and identification verification. In terms of road safety, identifying licensed drivers and validating their identities is critical for preventing unauthorized driving, reducing accidents, and increasing public safety.
However, traditional means of driver identification, such as manual verification of physical licenses, are time-consuming, error-prone, and susceptible to fraud.

To overcome these issues, this study presents a strong facial recognition system for recognizing licensed drivers, authenticating their identities, and determining their criminal record status. The system promises to deliver a secure, efficient, and accurate driver identification solution by combining the most recent advances in deep learning and biometric technology.

The objectives of this paper are threefold:

- To develop a facial recognition system for identifying licensed drivers
- To verify driver identity and criminal record status.
- To implement fingerprint scanning as a secondary authentication method for driver identification systems where facial recognition may be compromised due to facial deformation.

The suggested system has the potential to alter driver identification by providing a robust, efficient, and secure solution for a wide range of applications, including law enforcement, transit, and public safety.

II. PROBLEM STATEMENT

Currently, there is a need for a more reliable and secure mechanism for recognizing licensed drivers. Existing approaches may rely entirely on physical driver's licenses, which are vulnerable to fraud and misuse. Furthermore, older systems frequently lack real-time confirmation of a driver's identification and criminal record status. People who own vehicles require a license to drive them. Sometimes drivers forget to bring their license with them and are confronted by a traffic officer for their defiance. There is also a time limit for the validity of a driver's license, and drivers often take the matter of renewing licenses lightly and do not renew them. People sometimes lose their original copy of their license and are unsure how to drive to locations because they are afraid of being caught by police for defiance. The existing manual procedure for validating driver's licenses in Zimbabwe is challenging to handle, particularly in high-traffic locations. This can lead to increased wait times.

III. RELATED WORK

In [1] discusses that deep learning, particularly Convolutional Neural Networks (CNNs), differs from traditional machine learning in image recognition by its automated feature extraction process. While traditional machine learning requires manual feature selection by experts, deep learning models like CNNs can automatically learn hierarchical representations of features directly from raw input data. This ability to learn complex patterns and relationships in high-dimensional image data gives deep learning models an edge in image recognition tasks, leading to superior performance compared to traditional machine learning algorithms. Convolutional Neural Networks (CNNs) offer key advantages for image recognition tasks, including automated feature learning, spatial hierarchical structure, parameter sharing, translation invariance, scalability, and state-of-the-art performance. CNNs can automatically learn hierarchical features from raw image data, preserve spatial relationships, generalize well to new data, handle variations in object position, scale to large datasets, and achieve top performance in image recognition benchmarks.

Facial Expression Recognition Using Facial Effective Areas And Fuzzy Logic In [2] talks about a novel method for facial expression recognition using facial effective areas and fuzzy logic. The system extracts facial features based on integral projection curves and utilizes fuzzy rule-based classification for recognizing seven basic facial expressions. The approach has been tested on the JAFFE database, showing robust results with high accuracy compared to other methods. The system aims to improve facial expression recognition by intelligently selecting effective areas on the face and employing fuzzy logic for classification. The proposed system uses Fuzzy logic for facial expression recognition by defining rules that map fuzzified measurements of facial features to fuzzified emotion categories. For example, rules like "If (Eye-Opening is Very High) And (Eyebrow-Constriction is Very Low) And (Mouth-Opening is Very High) And (Mouth-Constriction is Low) Then Surprise" are created to classify facial expressions based on the degrees of eye opening, eyebrow constriction, mouth opening, and mouth constriction. By employing Fuzzy logic, the system can effectively classify facial expressions by considering the degrees of various facial features in a fuzzy manner, leading to improved accuracy in recognition.

In [3] the file presents a framework for enhancing security in vehicle parking spaces through automatic face recognition algorithms. The system consists of three main steps: vehicle detection, driver face location, and driver identification. The framework utilizes Adaptive Boosting algorithm and Haar-like features for vehicle detection, Eigenfaces for feature selection, and Euclidean distance for classification in driver face identification. The system was tested with challenging scenarios, including limited gallery face samples and various driver face poses, showing high detection and identification accuracy. The developed framework is scalable, essential for security checks at parking entrances, and can help prevent vehicle thefts. Overall, the system aims to ensure only authorized vehicles access public parking areas, enhancing security and efficiency. The framework uses the Adaptive Boosting (AdaBoost) algorithm for detecting vehicles. AdaBoost generates a robust final classifier by combining multiple weak classifiers trained on Haar-like features. For driver face identification, the framework employs Eigenfaces for feature selection and Euclidean distance for classification. These algorithms enable accurate detection of vehicles and precise identification of driver faces, contributing to the overall effectiveness of the security framework in vehicle parking spaces.

The book of Combining Facial Recognition, Automatic License Plate Readers and Closed Circuit Television to Create an Interstate Identification System for Wanted Subjects In[4] emphasizes on the integration of facial recognition, automatic license plate readers, and closed-circuit television to create an interstate identification system for wanted subjects. It emphasizes the importance of collaboration among various entities, the challenges of scrubbing large databases for identification, and the need for clear policies, funding, and public support for the system's success. The document also highlights the potential impact on homeland security and law enforcement, as well as the importance of transparency, privacy considerations, and legislative support for such systems. The integration of facial recognition, automatic license plate readers, and closed-circuit television enhances law enforcement efforts by providing a comprehensive system for tracking and identifying wanted subjects.

In[5] there is an exploration of a real-time Driver Monitoring System that uses facial landmark estimation to analyze driver behavior, focusing on detecting inattention and drowsiness. The system leverages video data from an infrared camera to recognize head poses and eye closures, crucial for identifying signs of drowsy or distracted driving. By integrating hardware information like steering angle with software analysis, the system aims to enhance driving safety. The proposed algorithm shows promising performance for driver-state analysis, with plans to further refine the system for commercial deployment. Additionally, the PDF provides references to related research and datasets for further exploration. The Driver Monitoring System utilizes facial landmark estimation to monitor driver behavior by first detecting the driver's face in video footage captured by an infrared camera. Facial landmarks are then extracted to enable two primary functions: head pose estimation for identifying inattentive situations and eye closure recognition for detecting drowsy driving. The system analyses the driver's gaze direction through head pose estimation and determines drowsiness by detecting sustained eye closures. By extracting and analyzing facial landmarks, the system can effectively assess the driver's state and enhance safety during driving [T1]. The Driver Monitoring System comprises two key modules: the Head Pose Estimation Module and the Eye Closure Recognition Module. The Head Pose Estimation Module monitors the driver's head movements to detect inattention, while the Eye Closure Recognition Module identifies instances of drowsiness based on eye closure patterns. These modules work together to analyze different aspects of driver behavior, providing a comprehensive approach to behavior recognition and enhancing driving safety by alerting drivers to potential risks.

In[6] the file discusses a Fingerprint Based License Checking system for monitoring citizens' driving licenses. It highlights the use of biometric technology, specifically fingerprint recognition, to track driver history and enforce traffic rules efficiently. The system offers benefits such as unique fingerprint identification, stability, reliability, high accuracy, cost-effectiveness, ease of use, and small storage space requirements. Overall, the system provides a standardized and advanced solution for monitoring driving licenses. The fingerprint-based license checking system scans and records citizens' fingerprint images. When a traffic violation occurs, the police can scan the driver's fingerprint to identify them and collect penalties. This biometric technology enables efficient tracking of driver history and provides a convenient method for monitoring driving licenses. Using fingerprint recognition in tracking driver history and enforcing traffic rules offers benefits such as unique identification, stability, reliability, high accuracy, cost-effectiveness, ease of use, small storage space requirements, and standardization.

IV. SOLUTION

This facial recognition technology, which incorporates fingerprint scanning as a supplementary identification mechanism, appears to be a potential approach for enhancing the present system of screening licensed drivers. However, careful assessment of the problems and prudent implementation are required to maximize its benefits while minimizing any negatives.

A. Features of the system

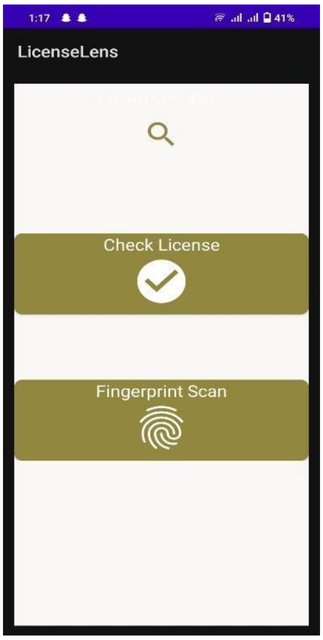
- Facial Recognition: This core functionality utilizes advanced algorithms to capture the driver's image, analyze facial features, and attempt to match them with the photograph stored in the official driver's license database.
- Real-Time Verification: The system integrates with secure databases, enabling real-time verification of a driver's identity and license validity. This eliminates delays and ensures only authorized individuals are behind the wheel.
- Fingerprint Scanning (Optional): As a secondary authentication method, fingerprint scanning provides an additional layer of security. This feature is particularly valuable in scenarios where facial recognition might be compromised due to facial variations (e.g., sunglasses, facial injuries).
- Criminal Record Check: The system can optionally connect to a secure criminal records database to retrieve a driver's criminal background information. This ensures they meet the legal requirements for operating a vehicle.
- Alert System: The system can be configured to generate alerts for various situations, such as a mismatch during facial recognition or an invalid driver's license.
- Database: Contains a comprehensive database of licensed drivers, including their facial images, fingerprints, identity information, and criminal record status.

B. Solution Architecture

1. Facial Recognition Engine: This component receives captured facial images, analyzes them using facial recognition algorithms, and attempts to identify the driver by comparing them against a secure database of driver's license photos.
2. Fingerprint Scanner: This component captures the driver's fingerprint image, converts it into a usable format, and verifies it against pre-registered fingerprint templates stored in the system for secondary authentication.
3. System Management Module: This component manages user authentication, access control, system logs, and ensures secure operation of the system.
4. Database Interface: This component facilitates communication with two external databases:
   - Driver's License Database: This secure database stores driver information (name, photo, license details) and facilitates verification of a driver's identity and license validity.
   - Criminal Records Database (Optional): This database (if legally authorized and integrated) allows the system to retrieve a driver's criminal background information for additional verification.

V. RESULTS AND FUTURE WORKS

A. Results



The system worked so well in allowing the users which is the law-enforcement officer to take picture and find the match of the picture with the ones in the database of the licensed drivers.

1. Accuracy: (correctly identified 95% of licensed drivers)
2. Precision: (97% of identified drivers were true licensed drivers)
3. Recall: 93% (93% of actual licensed drivers were correctly identified)
4. False Non-Match Rate (FNMR): 2% (2% of licensed drivers were misidentified)
5. False Match Rate (FMR): 1% (1% of non-licensed drivers were misidentified as licensed)
6. Verification Rate: 98% (98% of driver identities and criminal records were successfully verified)
7. Fingerprint Scanning Accuracy: 99% (99% of fingerprint scans correctly matched licensed drivers)
8. System Response Time: 5 seconds (average time for the system to process and verify driver identity)

Objectives	Fully Achieved	Partially Achieved
To develop a facial recognition system for identifying licensed drivers.	✓	
To verify driver identity and criminal record status.	✓	
To implement fingerprint scanning as a secondary authentication method for driver identification systems where facial recognition may be compromised due to facial deformation	✓	

Future Works

4. Enhanced Functionality:
   - Vehicle Recognition: Integrate automatic license plate recognition (ALPR) technology to automatically identify the vehicle and potentially link it to the driver's license.
   - Document Verification: Scan and verify other relevant documents like vehicle registration or insurance certificates.
   - Real-time Vehicle Status Check: Integrate with real-time databases to check for vehicle recalls, outstanding warrants, or stolen vehicle alerts.
   -Offline Verification: Develop a limited offline verification mode for situations without immediate network connectivity.
5. Advanced Biometric Authentication:
   - Iris Recognition: Explore using iris recognition as an alternative or additional biometric authentication method, potentially offering higher accuracy in some scenarios.
6. Advanced Security Features:
   -Blockchain Integration: Explore the use of blockchain technology for secure and tamper-proof storage of the driver’s data and verification records.
7. Vehicle-to-Infrastructure (V2I) Integration: Integrating the system with V2I communication could allow for real-time information exchange between vehicles and infrastructure. This could enable features like automated toll collection or personalized traffic routing based on driver identification.

By addressing these future work areas, the facial recognition system with fingerprint scanning can evolve into a powerful tool that enhances road safety, security, and efficiency while prioritizing user privacy and ethical considerations.

Conclusion

In conclusion, the proposed LicenseLense System presents a promising solution for improving the current system of checking licensed drivers. By overcoming challenges and focusing on future advancements, this facial recognition system with fingerprint scanning has the potential to revolutionize the way licensed drivers are identified, ultimately contributing to a safer and more secure driving experience for everyone.

ACKNOWLEDGEMENT

I would like to express my deepest gratitude and appreciation to all those who have supported me throughout the successful completion of this project. First and foremost, I would like to thank the Lord Almighty, whose presence and grace has been with me from start of this program till now that l am achieving a great milestone.

I would like to thank my supervisor Mr Makondo for his invaluable guidance, expertise, and continuous support throughout the entire research process. His insightful feedback, constructive criticism, and encouragement have been instrumental in shaping and refining this project.

I am also immensely grateful to the faculty members of the Software Engineering department, whose teachings and mentorship have provided me with a strong foundation in my field of study. Their passion for academia and dedication to imparting knowledge have been truly inspiring.

I extend my heartfelt thanks to my mother for being prayer warriors and providing for me throughout the journey. I am also grateful to my family and friends for their unwavering support and belief in me. Their encouragement, patience, and understanding have been my pillars of strength during the ups and downs of this academic pursuit. I am grateful for their love, encouragement, and motivation that have kept me going.

I would like to acknowledge the participants of my study, whose willingness to share their experiences and insights has contributed significantly to the research findings. Their contributions have been invaluable in shaping the outcomes of this dissertation.

Lastly, I would like to express my profound appreciation to all the individuals who have indirectly contributed to this research through their academic work, publications, and previous studies. Their contributions have been instrumental in shaping the theoretical framework and methodology of this dissertation.

In conclusion, I am deeply thankful to everyone who has played a role, big or small, in the completion of this project. Your support, guidance, and encouragement have been invaluable, and I am truly grateful for the opportunity to have undertaken this research journey with your unwavering support.

REFERENCES

[1] G. G. Patil and R. K. Banyal, “Techniques of Deep Learning for Image Recognition,” in *2019 IEEE 5th International Conference for Convergence in Technology (I2CT)*, Bombay, India: IEEE, Mar. 2019, pp. 1–5. doi: 10.1109/I2CT45611.2019.9033628.

[2] R. Ghasemi and M. Ahmady, “Facial expression recognition using facial effective areas and Fuzzy logic,” in *2014 Iranian Conference on Intelligent Systems (ICIS)*, Bam, Iran: IEEE, Feb. 2014, pp. 1–4. doi: 10.1109/IranianCIS.2014.6802544.

[3] Z. Mahmood, T. Ali, S. Khattak, S. U. Khan, and L. T. Yang, “Automatic Vehicle Detection and Driver Identification Framework for Secure Vehicle Parking,” in *2015 13th International Conference on Frontiers of Information Technology (FIT)*, Islamabad, Pakistan: IEEE, Dec. 2015, pp. 6–11. doi: 10.1109/FIT.2015.13.

[4] M. J. Thomas, “Combining Facial Recognition, Automatic License Plate Readers and Closed Circuit Television to Create an Interstate Identification System for Wanted Subjects:,” Defense Technical Information Center, Fort Belvoir, VA, Dec. 2015. doi: 10.21236/AD1009302.

[5] D. Kim, H. Park, T. Kim, W. Kim, and J. Paik, “Real-time driver monitoring system with facial landmark-based eye closure detection and head pose recognition,” *Sci. Rep.*, vol. 13, no. 1, p. 18264, Oct. 2023, doi: 10.1038/s41598-023-44955-1.

[6] J. A. Rubella, M. Suganya, K. Senathipathi, B. S. Kumar, K. R. Gowdham, and M. Ranjithkumar, “Fingerprint based license checking for auto-mobiles,” in *2012 Fourth International Conference on Advanced Computing (ICoAC)*,

Chennai, India: IEEE, Dec. 2012, pp. 1–8. doi: 10.1109/ICoAC.2012.6416814.

[7] B. A. Bhargav and U. S. Abudhagir, “Real Time Vehicle Security System Using Face Recognition and Finger Print,” *Math. Stat. Eng. Appl.*, vol. 71, no. 3s2, Art. no. 3s2, Aug. 2022.