International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 03 | March - 2024 SJIF Rating: 8.176 ISSN: 2582-3930

Fingerprint Based Driving License Management System

1st Snehal Chavan, 2nd Sushant Tupurwadkar, 3rd Pranali Jagtap, 4th Siddhi Pore
Electronics Telecommunication Engineering Department, Vishwakarma Institute of Information Techonology Pune, Maharashtra, India.

snehal.22120146@viit.ac.in , sushant.22120182@viit.ac.in,
pranali.22120204@viit.ac.in, siddhi.22120275@viit.ac.in

Abstract- ***The "Fingerprint-Based Driving License Detector" is an innovative system designed to enhance the security and authenticity of driving licenses through the integration of biometric technology. This system leverages fingerprint recognition as a robust method to verify the identity of drivers, aiming to reduce instances of license fraud and unauthorized use. The proposed system consists of a comprehensive framework that involves capturing and storing the fingerprint data of individuals during the driving license issuance process. This biometric data is then securely linked to the respective driving license records in a centralized database. During routine traffic stops or license verification processes, law enforcement authorities can use fingerprint scanners to quickly and accurately verify the identity of the license holder. The implementation of this system offers several advantages, including heightened security, reduced instances of identity theft, and a more streamlined and efficient license verification process. Additionally, the integration of fingerprint-based authentication enhances the overall trustworthiness of the driving license system, fostering a safer and more reliable environment on the roads.***

Keywords: *Fingerprint Recognition, Driving License Authentication, Biometric Technology, Identity Verification.*

I. INTRODUCTION

The "Fingerprint-Based Driving License Detector" project represents a pioneering initiative aimed at revolutionizing the conventional methods of driving license authentication and verification. In an era where identity fraud and unauthorized use of licenses pose significant challenges, integrating advanced biometric technology, specifically fingerprint recognition, emerges as a robust solution to enhance the security and reliability of driving licenses. The traditional reliance on visual inspection and document-based verification has proven susceptible to manipulation and fraudulent activities. To address these concerns, our project proposes a sophisticated system that captures and stores the unique fingerprint data of individuals during the driving license issuance process. This biometric information is then securely linked to the corresponding driving license records within a centralized database. The primary objective of this project is to establish a more foolproof method for verifying the identity of license holders. Fingerprint-based authentication offers a high level of accuracy and security, significantly reducing the risk of identity theft and unauthorized use of driving licenses. By seamlessly integrating this technology into the existing driving license system, our project aims to create a more reliable and tamper-resistant framework. The implications of this innovation extend beyond individual identity verification. Law enforcement authorities conducting routine traffic stops or license checks can benefit from a swift and accurate means of confirming the authenticity of a driver's license. Moreover, the centralized database ensures that the fingerprint data remains securely stored, contributing to a more efficient and secure management of driving license records.

II. LITERATURE SURVEY

1) Paper Name: A Fingerprint Based Driving Licensing Authentication System Using FPGA Implementation. Author: M. Ramkumar Abstract: This project introduces an innovative approach to driving license authentication by combining fingerprint recognition

technology with Field-Programmable Gate Array (FPGA) implementation. The "Fingerprint-Based Driving Licensing Authentication System" aims to enhance the security and efficiency of license verification processes, offering a reliable solution to combat identity fraud and unauthorized license use. The system involves capturing and processing fingerprint data during the driving license issuance phase, where unique biometric information is securely linked to individual license records in a centralized database. What sets this project apart is the utilization of FPGA technology for real-time processing and authentication, ensuring rapid and efficient verification during on-the-spot checks. The FPGA implementation allows for the acceleration of complex fingerprint matching algorithms, contributing to swift and accurate identification of license holders. The system's robustness lies in its ability to handle large datasets of fingerprint information with minimal latency, making it suitable for practical, real-world scenarios.

2) Paper Name: A Review: Fingerprint Based Wireless Terminal for Driving License Verification. Author: Prof. Priya Hankare, Rhythm Billore, Nikhil Deorukhakar , Pushkar Deshpande, Kunal Gandhi Abstract: With the increasing need for secure and efficient methods of identity verification, this paper proposes a Fingerprint-Based Wireless Terminal for Driving License Verification. The system leverages fingerprint biometrics to enhance the security and reliability of driving license authentication processes. A portable wireless terminal equipped with fingerprint scanning technology is employed for on-the-spot verification of a driver's identity. The system integrates advanced fingerprint recognition algorithms to ensure accurate and rapid identification. A secure wireless communication protocol facilitates real-time data transmission between the terminal and a centralized database containing authorized driver information. The proposed solution not only enhances security but also streamlines the verification process, contributing to improved traffic management and law enforcement efficiency.

3) Paper Name: Smart License-Based Vehicle Safety And Security System. Author: S.Gayathri1, P.Kaveen2, P.Kaviya3 , Dr.E.S.Shamila4PRECIADO Abstract: The Smart License-Based Vehicle Safety and Security System is an innovative and advanced technology designed to enhance the safety and security of vehicles. This system leverages smart license technology to integrate various features and capabilities aimed at ensuring a comprehensive and effective approach to vehicle safety. Key components of this system include real-time monitoring, intelligent sensors, and communication modules embedded within the vehicle. The smart license serves as a central identifier and authentication tool, allowing for seamless integration with the vehicle's safety and security systems. The system utilizes advanced sensors to constantly monitor various aspects of the vehicle, such as driver behavior, environmental conditions, and vehicle performance. In the event of any anomaly or potential threat, the system can trigger immediate alerts and responses. This includes notifying the driver, relevant authorities, or implementing predefined safety protocols to mitigate risks.

III. METHODOLOGY

1) Data Collection: Gather a diverse dataset of fingerprint images and corresponding driving licenses. Ensure the dataset represents a variety of fingerprints and license formats.

2) Preprocessing: Clean and preprocess the fingerprint images to enhance their quality. This may involve normalization, noise reduction, and standardization. Extract relevant features from the fingerprints, such as minutiae points.

3) Fingerprint Matching: Use a fingerprint matching algorithm to compare the extracted features from a captured fingerprint with those stored in the database. Common algorithms include:

Minutiae-Based Matching: Compares the location and orientation of minutiae points.

Pattern-Based Matching: Analyzes overall ridge patterns.

Correlation-Based Matching: Measures the correlation between two fingerprint images.

4) License Verification: Extract information from the detected license using Optical Character Recognition (OCR) for text recognition. Verify the license details against a database of valid licenses.

5)Biometric Fusion: Combine the results from fingerprint matching and license verification to enhance overall accuracy. Fusion techniques include decision-level fusion, feature-level fusion, and score-level fusion.

IV. HARDWARE AND SOFTWARE USED

1) FINGERPRINT SENSOR R307: Fingerprint Module consists of optical fingerprint sensor, high-speed Digital signal processor, high-performance fingerprint alignment algorithm, high-capacity FLASH chips and other hardware and software composition, stable performance, simple structure, with fingerprint entry, image processing, fingerprint matching, search and template storage and other functions.

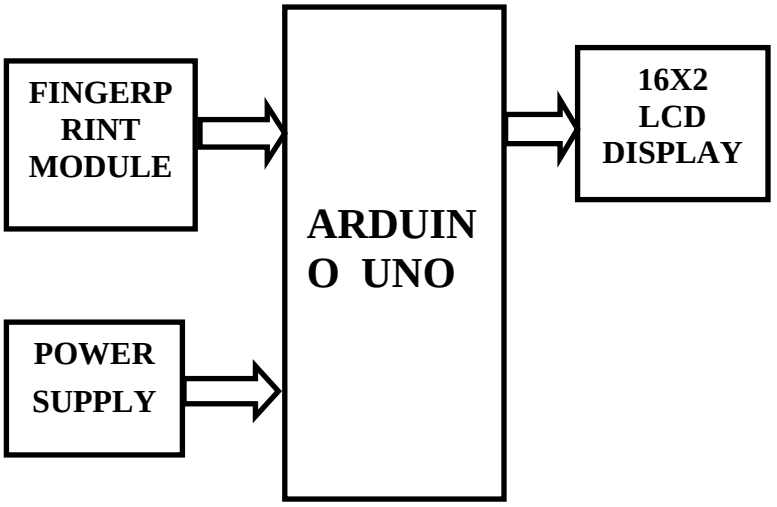
2) Arduino UNO: Arduino Uno board is a micro-contoller based on the ATmega328P. It is programmable with the Arduino IDE through a type B USB cable. Arduino Software (IDE) consists of a serial screen which permits easy textual information to be dispatched to and from the board.

3) 16 * 2 LCD (Liquid Crystal Display): A type of flat panel that uses liquid crystal as its main function. LCDs have a large and varied use case for consumers and businesses, as they are commonly seen in smartphones, televisions, laptop video displays, and dashboards. LCD characters are suitable for displaying text, numbers and special characters. LCDs contain a small accessory circuit (case) mounted on the back of the LCD module. In this project, we used lcd to display messages like enrolling, and matching.

4) Arduino IDE: To interface fingerprint module with Arduino we have used Adafruit Fingerprint Sensor Library in Arduino IDE which is platform to code Arduino. The Arduino Integrated Development Environment (IDE) is a software to write a code and upload it on arduino, IDE contains a text box, a text field, a text editor, a buttoned toolbar, and various instructions for writing code. The editor has cut/paste and search/replace functions for text. Native messages provide feedback while saving and exporting, and also indicate errors. The console displays the output of the including all error messages and other information. The bottom corner of the window shows the card configuration and serial port. Toolbar buttons allow checking and loading programs, creating, opening and saving sketches, and opening the serial viewer.

V. MODELING AND ANALYSIS

5.1 Working:

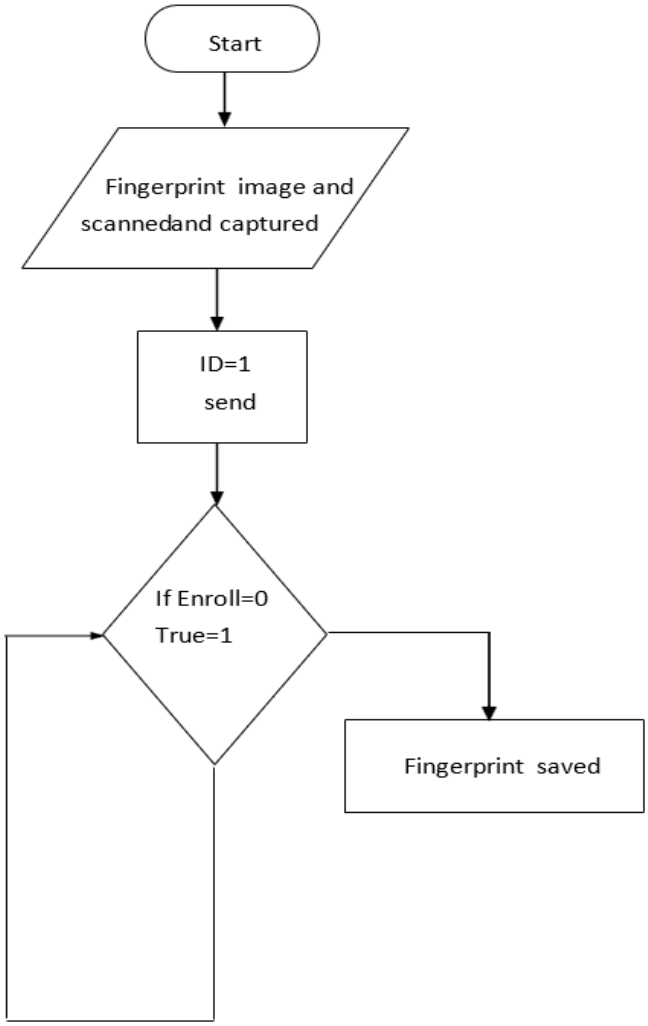


Firstly discussing about Biometrics we are concentrating on Fingerprint scanning. For this we are using R305 module as a scanner. This module has in-built ROM, DSP and RAM. In this we can store up to 256 user's fingerprints. This module can operate in 2 modes they are Master mode and User mode. We will be using Master mode to register the fingerprints which will be stored in the ROM present on the scanner with a unique id. When this module is interfaced to the Arduino, we will be using it in user mode. In this mode we will be verifying the scanned images with the stored images. When coming to our application the images of the citizens will be stored in the module with a unique id. Citizens have to scan their image on demand by police, which is then verified with the image present in

fingerprint module and their record will be updated. This scanner is interfaced to Arduino through controller enabling serial communication. By using this Arduino we will be controlling the scanning process. After the scanning has been completed the result is stored in the Arduino. By simply pressing a switch we can get the details of the polling. This project uses regulated 5V, 500mA power supply. 7805 three terminal voltage regulator is used for voltage regulation.

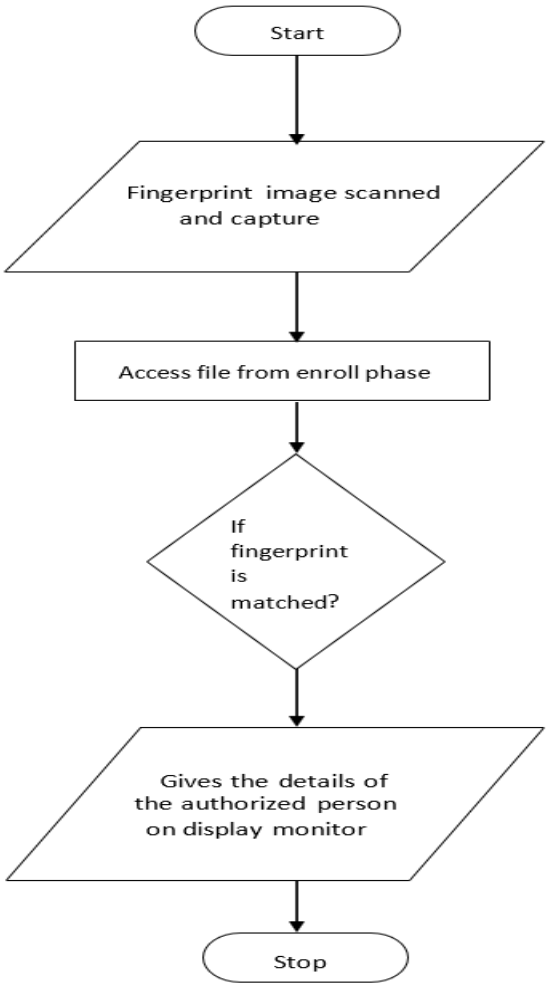
5.2 Flowchart:

Flow chart of Enroll phase: The Enrollment starts here. Image of the finger print is scanned from the finger print sensor and stored in the database. The sensor will correctly saves the fingerprint image. Flowchart to execute Enroll code.



The above flowchart gives the details of enrolling the fingerprint using sensor. During this phase the sensor scans the users fingerprint from the fingerprint sensor and converts it into a digital image, and it is stored in the database along with their uniquely generated ID. Initialization is done by randomly choosing any one of the uniquely generated ID from the serial monitor and it should be sent. The fingerprint is saved in the database. If the fingerprint is not properly placed then it needs to be rescanned and it is saved.

Flow chart of Access Code: Start the access code. Place the finger on fingerprint sensor and it captures the fingerprint image and stored as a template. The stored fingerprint image from the database of enroll phase is accessed. If the fingerprint is matched with the template the details of the individual is displayed in the serial monitor.



VI. CONCLUSION

The Fingerprint-Based Driving License Detector represents a significant advancement in enhancing security and accuracy in the issuance and verification of driving licenses. By leveraging fingerprint technology, this system ensures a more reliable and tamper-resistant method for confirming the identity of drivers. The integration of fingerprints adds an extra layer of authentication, reducing the likelihood of fraudulent activities and contributing to overall road safety. Additionally, the system streamlines the verification process, making it more efficient and convenient for both authorities and license holders. Ultimately, this technology marks a crucial step forward in modernizing and securing the process of managing driving licenses.

VII. REFERENCES

1) A.K. Jain, P. Flynn, and A.A.Ross, eds, Handbook of Biometrics, Springer, 2007.
2) H.C.Lee and R.E.Gaensslen eds, advances in Fingerprinting Technology,2nd CRC press 2001.
3) Feng,"Combining Minutiae Descriptors for Fingerprint Matching," Pattern Recognition.
4) https://www.irjet.net/archives/V8/i10/ICRTST-2021/IRJET-V8I1031.pdf
5) https://ieeexplore.ieee.org/document/6508343
6) "https://r.search.yahoo.com/_ylt=AwrKAIVfimhlEX4UMAi7HAx.;_ylu=Y29sbwNzZzMEcG9zAzEEdnRpZAMEc2VjA3Ny/RV=2/RE=1701378783/RO=10/RU=https%3a%2f%2fwww.academia.edu%2f6993811%2fFingerprint_Based_Driving_Licensing_Authentication_System_Using_FPGA_Implementation/RK=2/RS=qq3tJR9Ba5OAO3J0QBqehXPGAmE-
7) "https://r.search.yahoo.com/_ylt=AwrKAIVfimhlEX4UMgi7HAx.;_ylu=Y29sbwNzZzMEcG9zAzIEdnRpZAMEc2VjA3Ny/RV=2/RE=1701378783/RO=10/RU=https%3a%2f%2fwww.erpublication.org%2fpublished_paper%2fIJETR023001.pdf/RK=2/RS=Yx1jpeotzFr8Lb0HEmTa2uZNl4U-
8) "https://r.search.yahoo.com/_ylt=AwrKAIVfimhlEX4UOQi7HAx.;_ylu=Y29sbwNzZzMEcG9zAzMEdnRpZAMEc2VjA3Ny/RV=2/RE=1701378783/RO=10/RU=https%3a%2f%2fwww.researchgate.net%2fpublication%2f327672181_Fingerprint_Based_Driver%2527s_Identification_System/RK=2/RS=kb64kPVTuDhxRoRC1.a03q3o1wM-
9) "https://r.search.yahoo.com/_ylt=AwrKAIVfimhlEX4UOgi7HAx.;_ylu=Y29sbwNzZzMEcG9zAzQEdnRpZAMEc2VjA3Ny/RV=2/RE=1701378783/RO=10/RU=https%3a%2f%2fjit.ac.in%2fpdf%2fissues2021%2fpaper10.pdf/RK=2/RS=Xelnx4BTtnS9SffV4N.0huWoajM-