

Fingerprint-Based Vehicle Authentication System Using Computer Vision Techniques

¹T. Dansy Sri Abeesh, ²P. Raja Sekhar, ³S. Pravallika, ⁴CH. Swapna Priya

^{1,2,3}Department of Artificial Intelligence, ⁴Department of Computer Science Engineering

Vignan's Institute of Information Technology (A), Visakhapatnam, India

Abstract -- The Fingerprint-Based Vehicle Authentication System is an automated biometric verification system designed to authenticate licenses, challans, and other physical documents required by traffic enforcement agencies. It incorporates an electronic ticketing system (e-Challan) to enhance the efficiency and security of vehicle violation monitoring. The system authenticates users through biometric identification using fingerprint recognition, implemented with OpenCV's Scale-Invariant Feature Transform (SIFT) and the Fast Library for Approximate Nearest Neighbors (FLANN). A web-based interface is developed using Streamlit, while SQLite is employed as a lightweight database for storing system information. Users can authenticate themselves in real time and access their vehicle-related tickets, while administrators can monitor and manage violation records. The experimental results demonstrate that the proposed system performs effectively under different environmental conditions and provides an accessible platform for traffic enforcement agencies. The system further facilitates automated e-Challan management, offering improved security and efficiency in tracking vehicle violations. It provides real-time authentication of vehicle owners, access to challans associated with specific vehicles, and comprehensive management of violation records. The experimental evaluation indicates that the system operates effectively across various conditions and provides a practical platform for supporting traffic enforcement activities.

Keywords: OpenCV, SIFT, FLANN, SQLite, Streamlit, Vehicle Authentication, e-Challan.

I. INTRODUCTION

Traffic enforcement plays a crucial role in maintaining public safety and ensuring compliance with traffic regulations. The rapid growth in the number of vehicles and traffic violations has made effective enforcement increasingly difficult. Existing traffic enforcement practices in both urban and rural regions may involve delays, operational inefficiencies, and risks associated with identity verification. Current e-Challan mechanisms commonly depend on vehicle registration

numbers, CCTV recordings, and physical documentation, which can introduce challenges such as human errors, lengthy verification procedures, and the possibility of impersonation by offenders. To address these limitations, this project proposes a fingerprint-based vehicle authentication system that uses the biometric identity of the vehicle owner for license verification and retrieval of previous challan records [1]. The continuous growth in vehicle ownership and traffic violations presents a significant challenge to enforcement authorities. The proposed system employs a text-independent identification approach by performing fingerprint matching using the Scale-Invariant Feature Transform (SIFT) and the Fast Library for Approximate Nearest Neighbors (FLANN).

An intuitive web-based interface developed using Streamlit provides administrators with facilities for issuing, monitoring, and managing e-Challans. Fingerprint-based authentication enables controlled access to violation records and can improve the reliability of vehicle-owner identification. The availability of authenticated records can also support future analytical and predictive applications related to traffic violations. The biometric authentication framework can be extended with advanced functionalities, including behavioral analysis and mechanisms for resolving identity-related disputes in cases of incorrect attribution. The proposed system is significant because of its potential practical application in public-sector traffic enforcement and its use of biometric verification to reduce problems associated with identity fraud. Furthermore, its modular architecture can be adapted and implemented in different cities and traffic management environments.

The use of biometric verification also provides opportunities for integrating additional capabilities, such as behavior-based analysis and improved identification of individuals associated with traffic violations. The proposed framework focuses on addressing practical inefficiencies in existing traffic enforcement processes through a modular and adaptable architecture. Conventional e-Challan solutions primarily depend on textual identification, vehicle registration numbers, or video surveillance, which may be affected by human errors, incomplete information, or potential manipulation. The

proposed framework incorporates computer vision techniques for fingerprint feature extraction and matching, together with a web-based frontend designed to simplify access and operation. As digital governance continues to expand, secure and tamper-resistant identification mechanisms are becoming increasingly important for protecting public records and improving the reliability of citizen-oriented services.

This paper presents a fingerprint-based vehicle authentication system integrated with an e-Challan management framework to support reliable identification of vehicle owners and effective tracking of traffic violations. The proposed system combines fingerprint matching with computer vision techniques and provides web-based tools to improve usability and administrative efficiency. The framework is designed to support the ongoing digital transformation of traffic governance while enhancing the security and reliability of enforcement data. To address the need for secure and tamper-resistant identification, the system employs SIFT and FLANN for feature-based fingerprint recognition, SQLite for backend data management, and Streamlit for developing the web-based user interface.

II. RELATED WORK

In recent years, biometric technologies have gained significant attention as reliable approaches for identity verification based on an individual's digital and physiological characteristics. Among the different biometric modalities, fingerprint recognition is particularly prominent because fingerprints are generally stable throughout an individual's lifetime and are widely accepted for authentication applications. To address the challenges associated with fingerprint recognition, researchers have increasingly explored feature-based approaches such as the Scale-Invariant Feature Transform (SIFT), which provides robustness to variations in scale, orientation, and illumination. Lowe (2004) introduced and validated SIFT as an effective feature-based technique for matching high-dimensional descriptors [8-12].

For practical implementation, fingerprint authentication systems require both high processing speed and reliable matching accuracy. The Fast Library for Approximate Nearest Neighbors (FLANN), available through the OpenCV library, provides an efficient approach for matching feature descriptors and is suitable for applications requiring near real-time processing. Several research studies have demonstrated that FLANN can significantly reduce feature-matching time in latency-sensitive biometric applications. When SIFT is employed for feature extraction and FLANN is used for descriptor matching, the combined approach provides an effective framework for fingerprint verification and security-oriented identification applications [6].

Streamlit can significantly improve the usability of computer vision applications such as fingerprint identification by providing an interactive visual interface for users and administrators. As a Python-based web application framework, Streamlit simplifies the development and deployment of machine learning and computer vision

prototypes without requiring extensive frontend programming. Conventional fingerprint authentication systems frequently use minutiae-based techniques; however, their performance can be affected by noise, poor-quality images, or incomplete fingerprint impressions. In this context, interactive frameworks such as Streamlit have become useful for developing and demonstrating biometric research systems and proof-of-concept implementations.

Although e-Challan systems have been introduced in several regions to support the digital management of traffic violations, many existing approaches depend primarily on manual data entry, vehicle registration details, or camera-based vehicle identification. Such approaches may create challenges in accurately establishing the identity of the person responsible for a violation and may also introduce risks associated with incorrect or manipulated records. In addition, conventional e-Challan mechanisms may provide limited direct verification of the driver's identity. Incorporating biometric authentication, particularly fingerprint-based verification, can provide an additional mechanism for associating a recorded traffic violation with a verified individual [2-4].

Jain et al. (2004) and Gupta and Sharma (2019) [5] have discussed the application of biometric technologies in law-enforcement-related contexts; however, comparatively limited research has presented an integrated prototype combining biometric authentication, real-time fingerprint matching, web-based interaction, and digital traffic-violation management within a single operational framework. Existing studies have generally addressed these components independently, including fingerprint recognition techniques, real-time matching applications, web-based interfaces, and digital mechanisms for recording traffic violations. The proposed work combines these components into a unified and deployable system intended for practical traffic-enforcement applications.

The objective of this study is to address the identified research gap by developing an integrated biometric authentication and challan management framework through an interactive web-based platform. The proposed approach combines fingerprint-based user verification, real-time feature matching, and digital management of traffic violation records to support secure, efficient, and user-friendly traffic enforcement technologies.

III. PROPOSED METHODOLOGY

The proposed fingerprint-based verification and authentication system, illustrated in Figure 1, is integrated with an e-Challan management framework to provide reliable identity verification, convenient access and retrieval of information, and a user-friendly operational environment. The proposed framework consists of four major modules: the user registration module, fingerprint authentication module, challan management module, and administrator module. During registration, the user provides the required personal details, vehicle information, and fingerprint image. The submitted fingerprint image is registered within the system

and processed accordingly, while the associated user and vehicle metadata are stored in the database for subsequent authentication and retrieval.

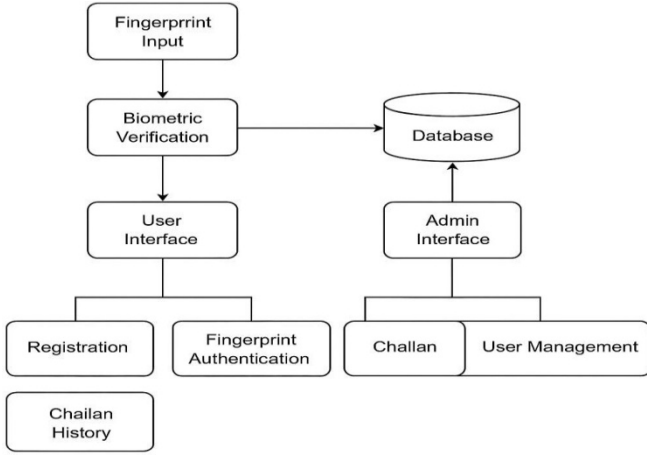


Fig. 1. Proposed System Architecture for Fingerprint-Based Vehicle Authentication System

The fingerprint image is pre-processed using OpenCV, after which distinctive features, including keypoints and descriptors, are extracted using the Scale-Invariant Feature Transform (SIFT) algorithm. The extracted descriptors serve as a digital representation of the corresponding fingerprint image and are stored in the database for subsequent identification and matching operations. When a registered user attempts to log in or undergo authentication, a new fingerprint image is captured or submitted to the system. The input image undergoes the same processing procedure as the registered fingerprint image to maintain consistency during feature extraction. The extracted descriptors are then compared with the stored descriptors using the Fast Library for Approximate Nearest Neighbors (FLANN) matcher. The matching process evaluates the similarity between the presented fingerprint and the stored fingerprint data and generates a matching confidence level to determine whether the submitted fingerprint corresponds to the registered user [13-16].

When the matching process produces a result that exceeds the predefined threshold, the system identifies the user and retrieves the corresponding information from the database. The authenticated user's details and any outstanding challans associated with the vehicle are subsequently presented through the interface. All system modules operate using a lightweight SQLite backend and a Streamlit-based frontend, providing low-overhead data management, modular extensibility, and real-time interaction. The Streamlit interface forms an important part of the user experience by allowing users to register their information, submit fingerprint images, and access their challan details. Administrators can access comprehensive user records, generate new challans, update the payment status of violations, and search for registered users using available identification information such as name or fingerprint data [17-18].

The modular design of the Streamlit interface enables convenient navigation between different system functions while supporting the dynamic presentation of authentication and transaction results. The overall architecture maintains a functional separation between the computer vision processing, authentication mechanism, database layer, and user interface, while allowing these components to operate together as an integrated system. This architecture also facilitates future enhancements, such as replacing the existing fingerprint image input method with a live fingerprint-scanner interface or integrating the application with a centralized government database. Such extensions can improve the system's capabilities and support larger-scale deployment. The high-level system architecture illustrates the major components and demonstrates how input data flows through the processing, authentication, database, and interface layers to complete the required operations [19-20].

IV. RESULTS AND DISCUSSIONS

A. Dataset

A series of experiments was conducted to assess the applicability and performance of the proposed system using a synthetic fingerprint dataset designed to represent realistic usage conditions. The dataset consisted of multiple fingerprint samples belonging to ten users, with each user associated with relevant personal and vehicle information. All fingerprint images were obtained in grayscale format and subsequently resized and pre-processed before being supplied to the fingerprint-matching pipeline. The synthetic dataset was designed to replicate the operational scenario of a fingerprint-based vehicle authentication system and included grayscale fingerprint samples corresponding to ten individual users.

For each user, two or three fingerprint samples were considered and associated with the respective name and vehicle information. The fingerprint images were obtained from publicly accessible fingerprint datasets. The images were organized into folders using individual user identifiers, while each corresponding user record was maintained in the SQLite database. The database contained information such as the user's name, license number, vehicle registration details, and challan history. The same dataset was utilized during both the registration and verification phases of the experiments, enabling the evaluation of fingerprint-matching performance under controlled and predefined conditions.

B. Data Augmentation

To evaluate the robustness of the proposed fingerprint-matching pipeline under different and imperfect acquisition conditions, the original fingerprint dataset was progressively augmented to simulate situations that may occur during real-world fingerprint scanning. Controlled transformations were applied to the fingerprint images to reproduce common imperfections that can affect the quality of captured fingerprint samples. These augmentations were introduced systematically so that the performance of the matching system could be examined under varying image conditions. One of

the initial augmentation techniques applied to the fingerprint images was the addition of Gaussian blur.



The Gaussian blur augmentation was used to simulate the effects of blurred or improperly focused fingerprint images, which can commonly occur because of finger movement during image acquisition or limitations in low-resolution imaging devices. To represent variations in finger placement, the fingerprint images were also rotated within a range of -15° to $+15^\circ$. This transformation simulates inconsistent finger positioning on the scanner surface during practical authentication. To evaluate the sensitivity of the proposed system to incomplete fingerprint information, image cropping was additionally applied. This form of partial image removal represents real-world situations in which fingerprint impressions may be incomplete because of improper scanner alignment or other acquisition-related issues that can result in the loss of ridge structures.

C. Model Evaluation

Fingerprint descriptors were extracted using the Scale-Invariant Feature Transform (SIFT) available in OpenCV. The extracted descriptors were subsequently compared with the descriptors stored in the registered fingerprint dataset using the Fast Library for Approximate Nearest Neighbors (FLANN) matcher. A fingerprint was considered successfully matched when more than 20 good matches were obtained and the resulting matching confidence exceeded 70%. The performance of the proposed system was evaluated using the True Positive Rate (TPR), False Positive Rate (FPR), and Average Matching Time. These metrics were used to assess the authentication reliability, false-matching behavior, and computational efficiency of the fingerprint-matching process.

D. Experimental Setup

The experiments were conducted on a Windows 10 computer equipped with an Intel Core i5 processor and 8 GB of RAM. The software environment consisted of Python 3.10 and

OpenCV 4.7, integrated with Streamlit for developing and operating the web-based interface. SQLite was employed as the local database for storing user, vehicle, fingerprint, and challan-related information. All major operations, including fingerprint image uploads, feature matching, authentication requests, and database queries, were performed through the Streamlit-based platform.

E. Results and Analysis

Figure 3 presents the fingerprint-matching results obtained under different image conditions, including clear, blurred, and cropped fingerprint images. The results illustrate the matching accuracy of the proposed system when fingerprint images are subjected to variations in image quality and partial information loss.

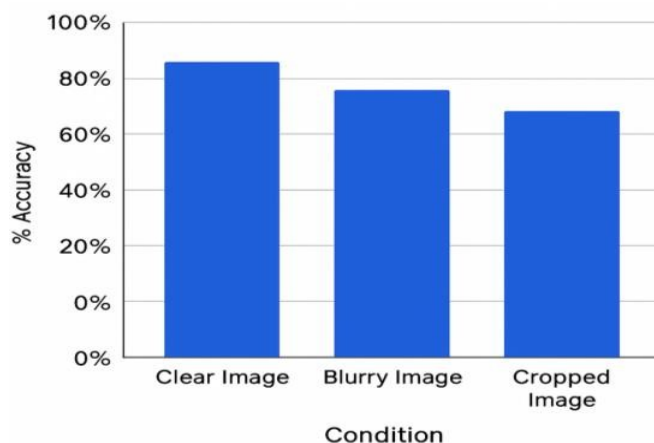


Fig. 3. Fingerprint Matching Accuracy for Clear, Blurred, and Cropped Images

The proposed model achieved high matching accuracy under ideal fingerprint image conditions and produced acceptable results when the images contained noise, blur, or partial cropping. The average processing time remained below 2 seconds, demonstrating the suitability of the system for near real-time authentication. Administrative operations, including challan issuance and record retrieval, were also completed with minimal delay due to the efficient backend database implementation. These results indicate that the integrated system can perform both fingerprint recognition and e-Challan management efficiently within a single platform.

Table 1. Fingerprint Image Condition, Accuracy, and Average Matching Time (s)

Image Condition	Accuracy (%)	Average Match Time (s)
Clear Image	95%	1.4
Blurred Image	87%	1.6
Cropped Image	76%	1.8

F. Fingerprint Matching Results

The combined use of SIFT and FLANN produced accurate fingerprint matches in more than 90% of the test cases when

Fingerprint-Based Vehicle Authentication System Using Computer Vision Techniques

high-quality input images were provided. As the fingerprint images experienced increased levels of blur, cropping, or reduced contrast, the rate of successful automatic matching decreased. Overall, the system demonstrated its highest matching performance for thumb and index-finger impressions when the fingerprint images were captured under appropriate illumination conditions.

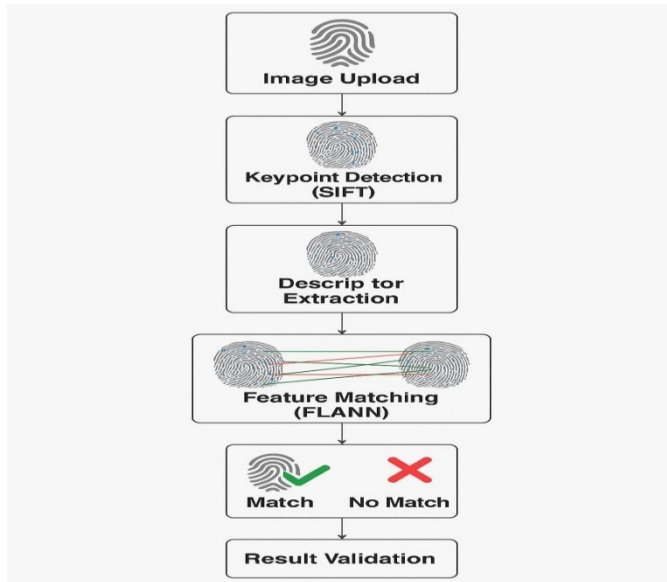


Fig. 4. Fingerprint Matching Process Using SIFT and FLANN

G. Streamlit Interface

The user interface was developed using Streamlit and provides several features, including simple fingerprint image and file uploading, visual preview of the biometric input, immediate feedback on fingerprint-matching accuracy, and access to comprehensive challan history with a detailed breakdown of outstanding and paid amounts. The experimental findings are summarized in Table 1 and visually presented in Figure 4. These results illustrate the influence of different types of fingerprint image distortions on both matching accuracy and the time required to complete the matching process.

V. CONCLUSION AND FUTURE SCOPE

A fingerprint-enabled e-Challan administration system was proposed, developed, and implemented in this study using OpenCV libraries for biometric image processing, the Streamlit framework for the user interface, and SQLite as the backend data storage system. The proposed fingerprint-based framework for e-Challan management is intended to improve conventional traffic-enforcement processes that may depend on paper-based procedures or less secure methods of identity verification.

The experimental evaluation of the fingerprint authentication system demonstrated its ability to identify registered users under various image-quality conditions, including noise, blur, and partial occlusion. SIFT was employed to extract distinctive keypoints and descriptors from fingerprint images,

while FLANN was used for efficient feature matching in time-sensitive authentication operations. The combination of these techniques enabled real-time user identification with the observed matching accuracy reported in the experimental evaluation. The administrative dashboard provided a simple and functional environment for issuing, viewing, and managing traffic challans with minimal processing delay.

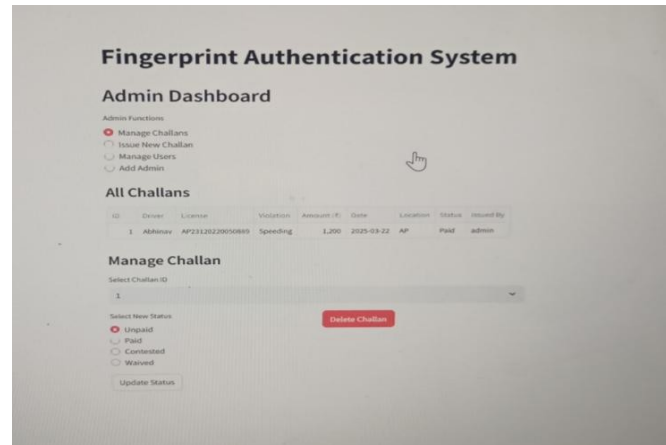


Fig. 5. Admin Dashboard for Challan Management

In conclusion, the study successfully developed and demonstrated a functional prototype that addresses the primary objectives of the research. The application-based fingerprint authentication framework provides a biometric approach for improving the security of user identification and the management of traffic-related records. However, the current implementation has certain limitations, particularly its dependence on image-based fingerprint input rather than a dedicated hardware fingerprint scanner. Integrating a hardware-based scanner in future implementations could provide more direct and reliable fingerprint acquisition and improve the usability, scalability, and practical deployment of the system in larger traffic-enforcement environments.

REFERENCES

- [1] Ali, M., & Khan, S. (2023). "Secure Biometric Authentication in Transportation Systems." *arXiv preprint*.
- [2] IEEE. (2023). "A Deep Learning-Based Real-Time Driver Authentication Using Fingerprints." *IEEE Xplore*.
- [3] IEEE. (2022). "Fingerprint Verification in IoT-Based Smart Transportation Systems." *IEEE Xplore*.
- [4] IEEE. (2022). "Biometric-Driven Vehicle Access Control." *IEEE Xplore*.
- [5] Anil K. Jain, Arun Ross and Salil Prabhakar, An Introduction to Biometric Recognition, IEEE transactions on circuits and systems for video technology, vol. 14, no. 1, january 2004.
- [6] Goyal, P., & Singh, I. (2014). "Security System for Vehicle Using Number Plate Detection and RFID." *International Journal of Computer Applications (IJCA)*, 97(8).
- [7] Barawkar, Shivraj, et al. (2020). "Smart Driving License Verification System." *Journal of Science and Technology*, 5(3).

- [8] Ziegen, Abraham, et al. (2021). "License Verification System with Face Recognition Using IoT." *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, 4(2).
- [9] Jacob, Christy Mary, et al. (2020). "An IoT-Based Smart Monitoring System for Vehicles." *IEEE Conference on Emerging Trends in Information Technology and Engineering (ICOETI)*.
- [10] Chung, C. Kung, et al. (2016). "RFID and License Plate Recognition Systems Integrated in Parking Guidance."
- [11] Sheddi, R., et al. (2017). "E-Verification of Driving License Through Aadhaar Database." *IJeDr*.
- [12] Wisanmongkol, et al. (2008). "Automatic Vehicle Identification with Sensor Integrated RFID." *ECTICON*, 8(1).
- [13] J., J., & O., A. (2016). "Vehicle Tracking Using RFID." *International Journal of Engineering Research and General Science*, 4(2).
- [14] Shelar, S., et al. (2015). "Vehicle Information System." *International Journal of Computer and Information Technology (IJCIT)*, 6(2).
- [15] Guangxian, X. (2006). "Research and Application of RFID in Electronic Toll Systems." Department of Computer Science and Engineering, VIIT, Visakhapatnam.
- [16] Divya, D., & Padmasarath, S. (2013). "Finger Vein-Based Licensing Using GSM." *International Journal of Computer Engineering*.
- [17] Margale, Komal A., et al. (2015). "Driving License Test Automation Using VB." *International Journal of Engineering and Advanced Studies (IJEAS)*, 2(4).
- [18] Wang, W., & Fan, S. (2017). "RFID Application in Container Transportation." Shanghai Maritime Academy.
- [19] Al-Hindawi, Asaad M. J., & Talib, Ibraheem. (2012). "Experimental Evaluation of GPS/GSM Based System Design." *Journal of Electronic Systems*.

Funding Declaration

The authors declare that no funds, grants, or other forms of financial support were received from any organization or institution for the conduct of this research.