E-Driving License Management System

[1]SWETA MORE, [2]PRAJAKTA NAVATAKE, [3]NEERAJ RAJE, [4] PROF. V.B. RASKAR

[123]Student, [4]Assistant Professor
Dept. of Electronics & Telecommunication Engineering
JSPM's Imperial College of Engineering & Research
Wagholi, Maharashtra, India.

***Abstract*- The proposed project involves developing and implementing an "E-Driving License Management system" that aims to replace manual authentication methods for driver's licenses with digital authentication. The system will utilize a bio-metric-based approach to monitor and control access, with fingerprint identification being the chosen method of human identification due to its high reliability and uniqueness. The project involves designing and assembling a bio-metric access control system that will incorporate fingerprint scanning and recognition technology to authenticate users. This will involve the development of software algorithms for processing and matching fingerprint data, as well as selecting and integrating appropriate hardware components such as fingerprint scanners and microcontrollers.**

***Index Terms*- Bio-metric, Fingerprint, Identification.**

1. INTRODUCTION

The automated process of identifying a person based on their physiological or behavioral traits is known as bio-metrics. This technology consists of facial recognition, voice recognition, fingerprint recognition, voice analysis, hand geometry, iris analysis, vein analysis, finger geometry, and fingerprint recognition. The person being identified must be physically present for bio-metric systems to work. In many office and service sector operations, fingerprint recognition is a popular bio-metric technique for security access control and identity systems. Fingerprint identification and authentication are the main components of the majority of fingerprint systems used in biometric solutions. Fingerprints are photographed and kept in a database as part of the fingerprint recognition identification procedure. To match and confirm the individual's identification, this database is used. In order to confirm the user's identity and that they are in possession of it.

2. LITERATURE SURVEY

The simple procedure of fingerprint system authentication entails comparing a live template to an already-existing template to confirm a claimed identity. Usually, a smart card is used for this authentication. The adoption of ID-card based fingerprint systems for public sector applications has significantly increased. Digital parking meters, phones, vending machines, ATM cards, digital fingerprint security system identities, personal identification verification numbers, and other devices can all use these cards.

- A.K. Jain, P. Flynn, and A. A. Ross, 'Handbook of Biometrics, Springer, 2007': For automatic fingerprint recognition systems, friction ridge patterns are the perfect biometric identifier because they are unique and permanent to each individual. The patterns are created when a fete is developing and are impacted by both genetic and environmental factors. The dermal papillae that are developing push on the epidermis and cause ridges on the skin's surface. These ridges are grouped in an intricate design of loops, arches, and whorls. Automatic fingerprint identification systems photograph the fingerprint and check it against a database of recognized fingerprints to see if there is a match. Since it has been used by authorities to great effect for more than a century, the technology is now being used for a wide range of other purposes, including access control and identity management.
- Sangita K Chaudahri: Numerous studies have been done on the subject, and it is still a widely used method to represent fingerprints using minute patterns. This method, however, is vulnerable to problems caused by poor impression quality, such as distortion, which changes the geometric position and orientation of the fingerprint. Because of this, it might be difficult to match up several prints made with the same fingertip.

Additionally, there is still ongoing research into accurately detecting all minutiae and rejecting false minutiae. Our approach combines a variety of techniques that were found through a thorough evaluation of research papers to tackle these issues. Notably, we offer unique approaches including segmentation using morphological operations, enhanced thinning, incorrect minutiae removal techniques, minutia marking with particular focus.

- K. Sujatha and R. S. Ponmagal and K. Senthil Kumar and Rajneesh Rani and Golda Dilip, 'IoT Based e- License System using Fingerprint Sensor': The development of a driving license system is a challenging task for the government because it requires the recording of all citizen data. In this project, when a citizen ignores traffic laws, a police officer scans their fingerprint with a fingerprint scanner and then extracts the citizen's license information from the system's database. The citizen can then use a server to access their account, which is connected to their license, and use it to pay the fine. Additionally, citizens can use their user ID and password to access the account information associated with their license number. This technology ensures efficient monitoring of traffic infractions and permits prompt retrieval of citizen information, supporting the effective imposition of penalties.

3. SYSTEM ARCHITECTURE

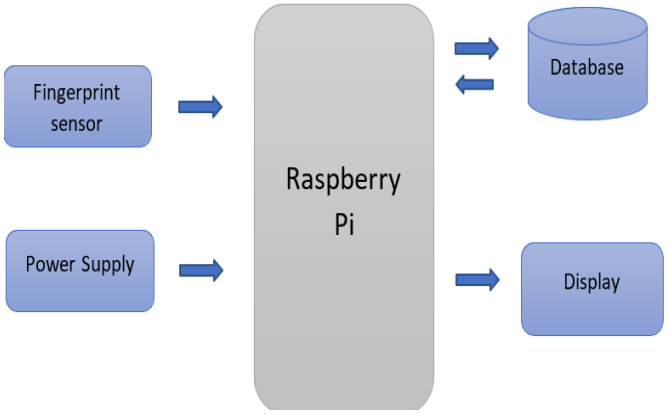

Fig. 1 System Architecture.

4. METHODOLOGY

The R307 module is used for fingerprint scanning in the biometrics industry. The user's fingerprints are recorded by the sensor and turned into digital photographs. this process is called as enrolment. Then these fingerprints are then entered into a database and given individual identity (ID) numbers. To make the process of scanning possible, serial communication is created between a Raspberry Pi controller and the fingerprint sensor. The technology allows users to scan their fingerprints for verification compared to the recorded fingerprints and maintains photographs of them along with their unique IDs in a module. The Raspberry Pi controller controls the scanning process and evaluates whether the person is authorized or not by comparing the scanned fingerprint image with those already stored in the database. This procedure involves comparing the scant fingerprint's minute patterns. In this process, the minute patterns of the scanned fingerprint are compared to those in the database to determine a match score, which represents how similar the two patterns are. The system then decides whether to grant the user access or not depending on this score.

5. FLOWCHART

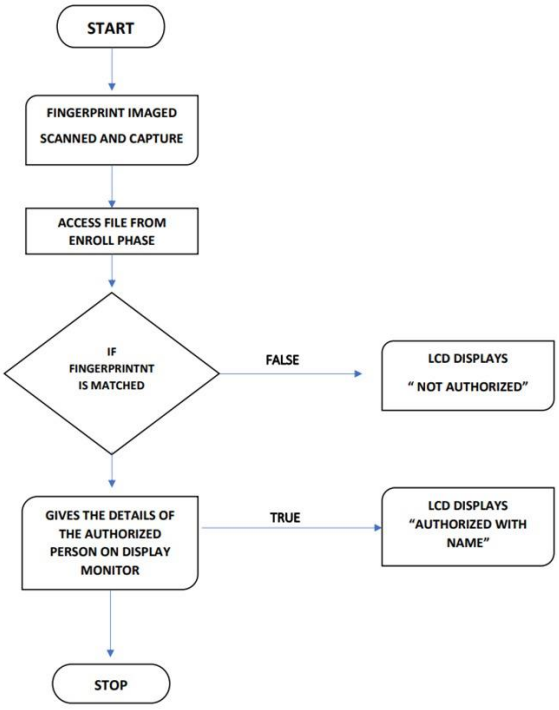

Fig. 2 Flowchart

6. ALGORITHM

1. Initialize the Raspberry Pi and connect the fingerprint sensor.
2. Create a database to store the driving license information, including personal details and fingerprint data.
3. Set up a user interface on the Raspberry Pi to interact with the system.
4. Prompt the user to either register a new driving license or verify an existing one.
5. If the user chooses to register a new driving license:

- Collect the necessary personal information (name, address, date of birth, etc.) using the user interface.
- Prompt the user to scan their fingerprint using the fingerprint sensor.

- Store the personal information and fingerprint data in the database.

6. If the user chooses to verify an existing driving license:
- Prompt the user to scan their fingerprint using the fingerprint sensor.
- Retrieve the fingerprint data from the database.
- Compare the scanned fingerprint with the stored fingerprint data to verify the user's identity.

7. If the fingerprint verification is successful:
- Display the driving license information (personal details) on the user interface.
- Provide additional functionalities such as updating personal information or revoking the license.

8. If the fingerprint verification fails:
- Display an error message on the user interface indicating that the fingerprint does not match any registered license.

9. Repeat steps 4 to 8 based on the user's input.
10. Implement necessary security measures to protect the database and ensure data privacy.

7. EXPERIMENT AND RESULTS

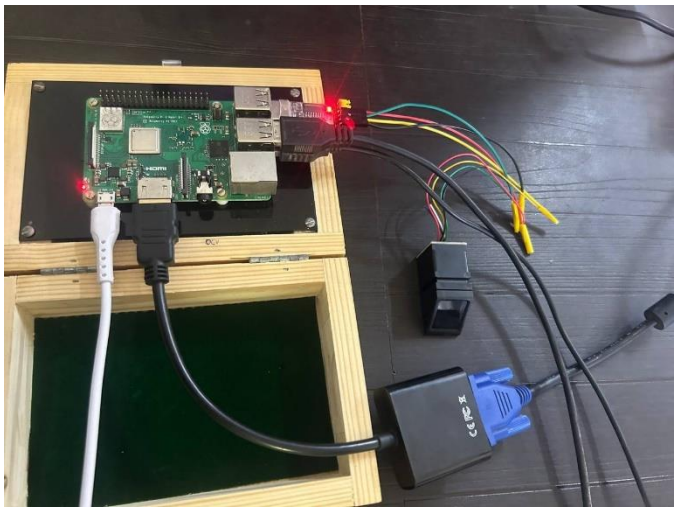

Fig. 3 Hardware Setup.

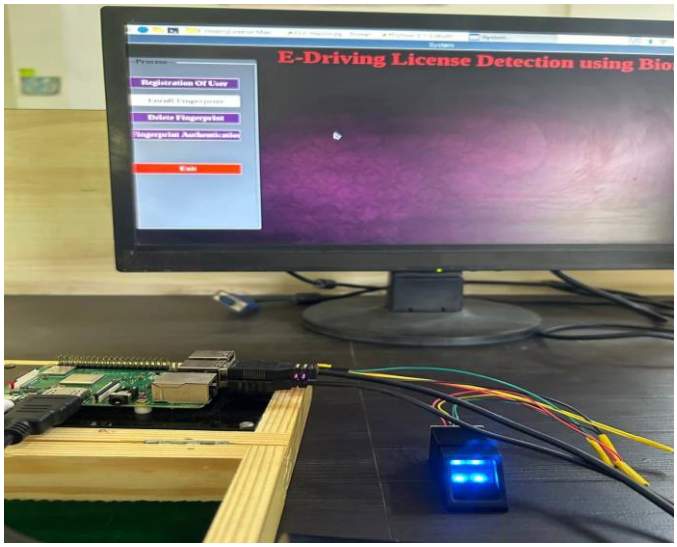

Fig. 4 GUI Screen.

- Next, after the hardware is set, the system starts to follow an algorithm stepwise as shown in the above figure. The GUI of the system is displayed.

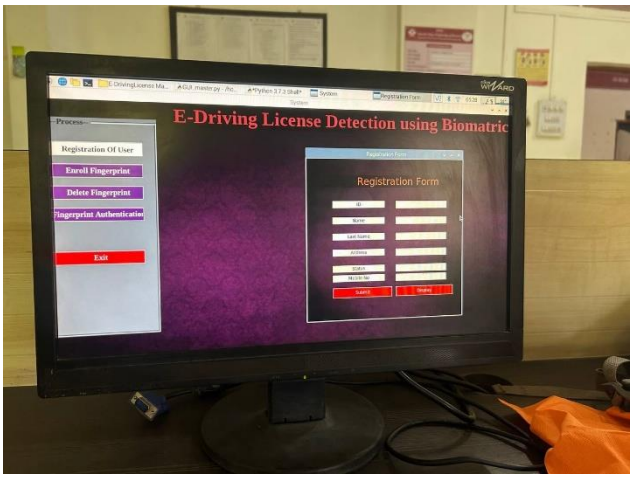

Fig. 5 Registration Form.

- The GUI screen has multiple labels for the process to follow. At first, registration is done by getting user details.

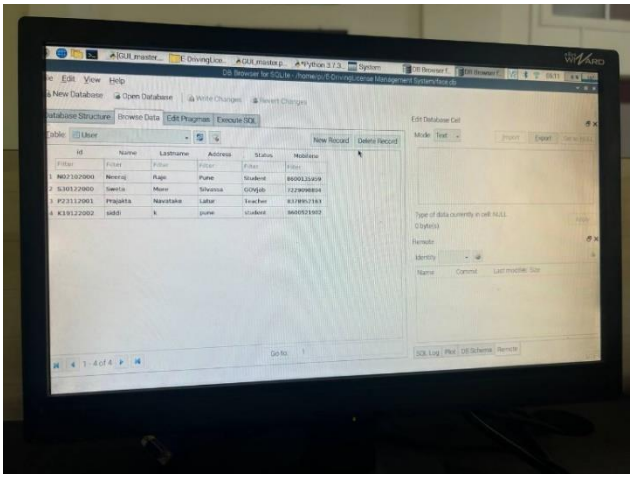

Fig. 6 Database.

- Now the system uses a Raspberry Pi, which has its own database, SQLite, in which registered data will be stored.
- In Figure 6, a set of five data entries is shown, but it has the capacity to store 256 data entries in a database.

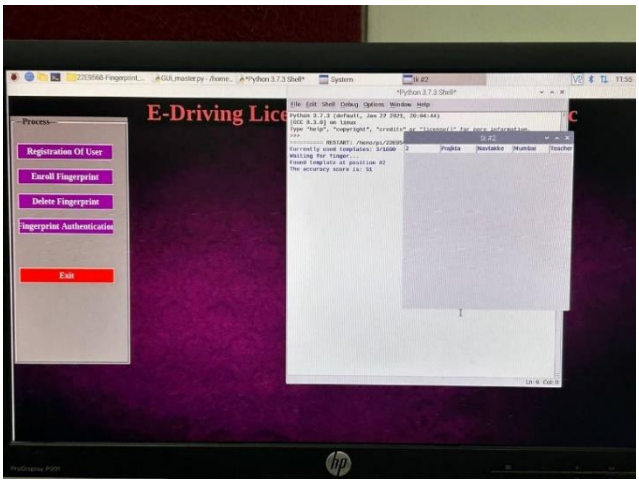

Fig. 7 Final Result.

- At first, registration is done by getting user details. In the figure, we can see that the proposed system is working successfully with the use of the SHA algorithm to authenticate a particular user, with the advanced feature of showing the accuracy percentage of the image taken by the biometric sensor at the time of registration.

8. CONCLUSION

The suggested approach provides a method for manually verifying driver's licenses using fingerprint recognition technology. The technology attempts to improve vehicle security and restrict access to those who have been given permission. By creating a highly accurate technique for simple storing and retrieval of driver's licenses, the project's goal is to increase the efficiency, effectiveness, and competency of the license issuance process. In order to ensure that only authorized people are given access to automobiles, the proposed system will use advanced algorithms to collect and analyze biometric data from people. To attain great accuracy and reliability, the system will rely on cutting-edge deep learning and machine learning algorithms. Overall, this initiative represents a significant step towards automating and expediting the issuance of driver's licenses while boosting security and effectiveness. An innovative idea that has the potential to completely alter how we maintain centralized national databases is the creation of an E-License system. It is a more practical and effective choice since it replaces the requirement for people to carry physical licenses with their fingerprints, which serves as the citizen's license. This system has the added benefit of minimizing corruption in the licensing process by ensuring that licenses are granted on the basis of merit rather than through dubious means or other illegal means. With this system in place, the licensing process will be fair and transparent for all applicants, and authorities will be better able to control and manage it. Overall, the E-License system is an important development because it provides several advantages to both residents and the government.

REFERENCES:

1. A. K. Jain, P. J. Flynn, and A. A. Ross, "Handbook of biometrics," 2007.
2. S. K. Chaudahri, "An algorithm for fingerprint enhancement & matching," 2012.
3. K. Sujatha, R. S. Ponmagal, K. S. Kumar, R. Rani, and G. Dilip, "IoT-based multimodal biometric identification for automation railway engine pilot security system," 2018.
4. M. Regeena and D. Khosla, "Fingerprint identification in biometric security systems" International Journal of Computer and Electrical Engineering, pp. 852–855, Jan. 2010. DOI: 10.7763/IJCEE. 2010.V2.239.
5. M. Ali, H. M. Awad, and I. K. Abdalgader, "Authenticated access control for vehicle ignition system by driver's license and fingerprint technology," 2020. International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE), pp. 1–6, 2021.
6. Deepak and D. Kumar, "License and fingerprint detection for security purpose in automobiles," 2020.
7. S. DineshKumarD, "Human authentication using face, voice and fingerprint biometrics," International Journal for Research in Applied Science and Engineering Technology, 2021.
8. K. A. P. S. Parameswaran, M. A. Majid, H. Ajra, and M. S. Islam, "Fingerprint authentication-based traffic offence control and enforcement system on smart mobile devices for smart city," 2022 International Conference on Intelligent Technology, System and Service for Internet of Everything (ITSS-IoE), pp. 1–6, 2022.
9. N. Hegde, R. S. Rashmi, A. Azeez, J. P. Mohamed, and J. Surendiran, "IoT based biometric supported vehicle user identification system," 2022 IEEE International Conference on Data Science and Information System (ICDSIS), pp. 1–6, 2022.
10. "Smart driving license verification system," Journal of Science and Technology, 2020.