ISSN No:-2456-2165

Providing Security to the Vehicle Ignition System Using Fingerprint Technology and Driving License

Bindu B S [1DS20CS404]
Darshini B S [1DS20CS406]
Dhanushree M S[1DS20CS407]
Tarun K P[1DS19CS752]
Prasad A M [Professor]
Dayananda Sagar College of Engineering, Bengaluru, Karnataka

Abstract:- Nowadays vehicles are been used hugely but protection for those vehicles are not been taking care of. In this advanced technology security of the vehicle are most important. Vehicles are been an important part of a human's life at least for this reason security is very important for vehicles. These days vehicle theft can happen anytime and anywhere like vehicle parking and some crowded places. Biometrics is one of the methods which is been used hugely, fingerprint identification is a very common method in human identification. If an owner needs to start thevehicle he is required to keep his finger on the fingerprint sensor. By comparing it to the fingerprint that is already saved in the database, the system will determine if it is authenticated or not, if only the fingerprint matches, the owner is allowed to ride on it; if not, an alarm message is sent to the owner. Additionally, the owner has the abilityto add new users to the database and delete it at any time. In this paper, we are mainly focusing on security purposes that is by using fingerprint recognition to start the vehicle.

Keywords:- *GSM, Fingerprint Sensor, GPRS, Arduino.*

I. INTRODUCTION

High security for many sectors is primarily by biometric systems. The oldest and most popular biometric identification method is based on fingerprints. For over a century, fingerprint identification has been used. The development of fingerprint verification is the main focus of thisproject. The data of the registered fingerprint image and the incoming fingerprint image are compared during verification, followed by the registered fingerprint image and the incoming fingerprint image, and finally, the incoming fingerprint image's data is compared with the registered fingerprint image. It is an advanced and luxurious automobile insurance device. This framework cannot be set up to provide the vehicle with total security and direction, thus a more secure frame uses an inserted frame system that is centered on GSM and GPS technology. Therefore, this developed framework is installed in the vehicle with the intention of giving the user active notification and real-time tracking while assisting in the prevention of potential theft. system security is the primary goal of the vehicle tracking system. Rescue operations are the primary objective of the accident alarm system. The system is therefore very helpful nowadays; it allows one to watch and track his vehicle and learn about its current whereabouts as well as its past activities. This technology is known as vehicle tracking systems, and it has done wonders for the security ofvehicles.

This gear is mounted to the vehicle in such a way that it cannot be seen from either inside or outside the vehicle. Location information from the tracking system can be used to locate the vehicle after it has been stolen and can also be used to alert the authorities for further action. Some car tracking systems can even warn the owner when the vehicle is moved without authorization. For the same reason, this offers it a competitive advantage over other technological workers. The accident alert system in it recognizes an accident, pinpoints where it happened, and transmits GPS coordinates to the designated mobile device, computer, etc. a notice will be sent right away tothe designated recipient if the temperature within the car increases over a predetermined threshold in the fire detector circuit, which is used to detect fire inside the automobile. The connections between the microcontroller and infrared sensor are also used to identify obstacles and mishaps. If one of these things occurs, the intended recipient will receive a warning straight away. The system automatically transmits the return response with the latitude and longitude of the vehicle to the designated mobile when a user sends a request to the number at the modem. On Google Maps, a tool has been developed that may be used to locate an automobile and track it as it moves.

II. METHODOLOGY

Only individuals whose fingerprints have previously been stored in the database are permitted access through fingerprint recognition technology. Fingerprints that have been saved are maintained even if the power goes out completely or the batteries run out. These take the place of the requirement to remember a PIN or combination password as well as keeping track of keys. Since there are no keys, combinations, or locks that may be picked, they can only be opened when an authorized person is present.

Therefore, the fingerprint-based lock offers a fantastic remedy for the problems that are typically experienced. In contrast to the conventional way of employing keys, the focus of this report is on the use of fingerprints to unlock locks. Satellite locations aredetermined using messages that GPS receives from the satellites. For biometric verification,

a fingerprint sensor is also utilized. Technologies used to detect fingerprints include optical, capacitive, thermal, RF, ultrasonic, piezo-resistive, and MEMS. This system makes use of optical sensor technologies. A digital template is created from the finger image that was captured and saved in memory. This device captures the driver's fingerprint before the vehicle even starts. To verify authenticity, a previously enrolled image is compared with a fingerprint using a matching algorithm. Due to its efficiency and accuracy, correlation-based matching is preferred over minutiae-based matching, ridge feature-based matching, and minutiae-based matching. The system will think that something is amiss if the position of the F car is altered without fingerprint verification. The GPS system will then link the location's coordinates and send the vehicle owner's cell phone number an SMS message.

III. LITERATURE SURVEY

- In [1] There is active research in the area of biometrics. The papers' suggestion focuses on the use of biometrics for two-wheelers in particular, motor scooters and bicycles. Many motorbikes are overlooked in daily life because it is challenging to locate them. An efficient way to increase security and prevent unauthorized motorbike use is offered in this paper. This proposal proposes a straightforward and effective electric engine starter based on fingerprints. the starter unit for the engine may be able to guarantee enough security for the automobiles.

- In [2] Autonomous vehicles are becoming more common, but there are still a number of problems that need to be fixed before their use can be increased. One of the many countermeasures that are suggested is the addition of remote control capabilities to AVS in order to reduce the failure of self-driving features. The results show that the protocol achieves good security levels at affordable processing and communications costs. We also rate CT performance and formally validate security in real time. Fuzzy vault, Fuzzy commitment algorithm, and Fuzzy extractor, three widely used biometric encryption real- time from AKA, are combined to create three- factor authentication while protecting user privacy.

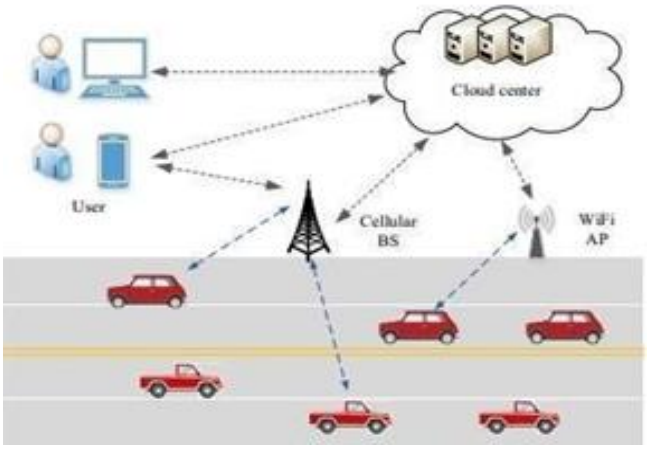

Fig 1 The Model of Cloud-Assisted AV

- In [3] The automotive business, cutting-edge technologies are continually being developed that not only make driving more enjoyable for real- timers but also increase passenger safety. Automobile driver fingerprinting is one security issue that needs to be resolved in cars, among others. At the moment, real-time identification monitoring of the driver's building is possible with identification technologies like fingerprint and iris recognition. We conduct a detailed examination of the driving styles of two distinct cars, the Luxgen U5 SUV an the Buick Regal, in order to construct real-time automotive driver fingerprinting, which is essential to ensuring the safety of people's property and even lives. We use the actual data to create a driver by removing and evaluating the feature data from the Controller Area Network(CAN). Identifying cross-referencing database. Then, using CNN and Support Vector Domain Description, we construct a hybrid model to successfully identify automobile driver fingerprints (SVDD). According to substantial trail data, the proposed driver fingerprinting approach may dynamically match the driver's identification in real-time without interfering with regular driving.

- In [4] The use of driver identification and fingerprints for enhanced driver profiling and vehicle security in linked cars is investigated in this study. We present a new driver identification model based on data received from smartphone sensor and/or the OBD- II protocol using CNN and RNN/LSTM. Unlike previous, studies, weemploy a cross-validation method that, when used on hypothetical realistic data, yields results that can be replicated. We also looked at how resistant the model was to anomalies in sensor data. The results show that our model's accuracy is still sufficient even when the rate of anomalies dramatically rises. After being tested on multipledatasets, the suggested model was implemented in the Automotive Grade Linux Framework as a real-time anti-theft and driver profiling system.

- In [5] The Internet of Automobiles (IOV) will connect mobile devices and vehicles in addition to smart offices, homes, buildings, theatres, retail malls, and cities. The IOV makes it possible for connected vehicles to get the best and most dependable communication services in smart cities. The crucial implementation of V2X infrastructure serves as the foundation for communication betweenlinked vehicles. The amount of spectrum used is determined by the demand from end users, the development of infrastructure with efficient automation methods, and the Internet of Things. This infrastructure allows us to create intelligent settings for spectrum use, which we call SSU. This study presents an integrated system composed of SSU and IoV. IoT security and cyber-attack defense, however, present considerable challenges. In order to provide reliable services and secure applications, this article provides an IoV security architecture that makes use of deep learning. The IoT security systemmight be optimized using deep learning, which combines supervised learning with unsupervised learning. To keep track of

security threats, deep learning is used. Simulation findings indicate that the suggested security systems' monitoring accuracy is better than that of the established system.

- In [6] since biometric technology employs bodily characteristics and properties to identify persons, it is becoming more and more common as a security precaution to prevent instances of fraud and theft. While more modern biometric identification methods make use of voice and hand prints, iris/eye scans, and hand and fingerprints, older ones relied on fingerprints and handwriting. The goal of biometric voice recognition technology is to teach the system to identify each person's distinctive vocal characteristics. The technology is well suited for many different uses and industries, such as mobile phone security access control, ATM manufacturers, and automakers. In this article, we show how to build a security that employs voice recognition as the primary means of access control. MATLAB function blocks are used to develop a verification algorithm that can authenticate a document. Vocal characteristics might be used to recognize someone. Logic "1" will be returned if the voice matches, but logic "0" will be returned if it doesn't.

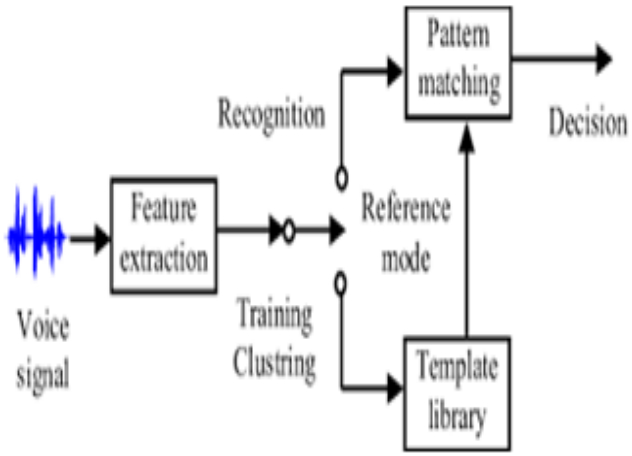

Fig 2 Basic Structure of Automatic Speech Recognition System

- In [7] As the number of urban automobiles rises in accordance with the state of the economy, people are becoming more and more concerned about vehicle theft, which creates new market potential for anti-theft vehicle solutions. Recently, a variety of vehicle antitheft systems have been created, however, the results are still unsatisfactory because each type of vehicle has disadvantages. The results of this study have recommended an upgraded method to guarantee vehicle safety and track the vehicle in the event of theft. This proposed system includes a fingerprint-based identification to start the engine in addition to the key technique. The owner must use both their fingerprint and key to start the car. Even if one of the two inputs is present, the car cannot be started. When an unauthorized person tries to operate the vehicle using a different way, bypassing the fingerprint identification and key, the owner receives an alert SMS with the location coordinates, enabling the owner to track the vehicle using GPS and GSM technology.

- In [8] Customers have a choice of a station service with automobile sharing or a peer-to-peer service. Nevertheless, connectedness to Remote sites and locations with multipath impediments and line-of-sight-sight is particularly problematic (LOS). That is the situation; network uptime is not always guaranteed, especially with untethered wireless networks made up of moving cars and a typical online service. The authentication method is therefore useless. in terms of locking up the automobiles. Moreover, the harmful rerun of the attack would allow attackers to get access to the cars. The term "replay assault" is also used to describe signals. In chronological order, we offer a time-based, one-time password used for offline authentication in order to give a solid authentication approach (TOTP). OTP favors its defense against the notorious replay assault that frequently occurs while using keyless vehicle ignition. It also employed a different security biometric. Factor to boost the driver's security's reliability. Online and offline components make up the newly proposed strategy. Strategies to offer a secure answer. The peculiarity is the fact that it allows authorized drivers to start and operate safely while merely using their mobile devices, during the offline duration.

- In [9] There are more cars on the road nowadays, and crime and accidents are increasing exponentially, making it difficult for governments to control such behavior, especially from seasoned criminals. This essay offers planning and creating drivers' safety and antitheft systems integrated surveillance system with biometric identification to get inside the car. This setup includes cameras that capture and visualize a person attempting to enter a vehicle, then compare it with the photograph of the authorized individual, and then approve or reject access. The camera will take a picture and transmit it to the approver or owner if a car is not allowed to enter or even if there is an accident. This will also help law enforcement catch criminals. Permits monitoring of the driver and the inside of the vehicle.

Recent research on an embedded system proposal is planned in this document. Raspberry Pi is used in systems development and design. A high-resolution camera, a pi, a vibration sensor, and open-source software.

- In [10] Women's safety is a growing concern today. When they are traveling GPS stands for global positioning system added to vehicles for tracking to assure travel safety, however, a complete monitoring system is currently lacking. The situation results in problems like kidnapping the girl snatching young children and demanding money from their cash, etc. Currently, the system relays on hand one of the ways of hiring drivers and cleaners forvehicles that they cause by bad authentication. Very few current systems combine

face detection andvehicle tracking, in addition to where Open CV running on areceives video frames From the camera windows PC.Such a system has an incorrect design flaw. The act of taking a picture when the camera's output image doesn't match the X and Y coordinates. Additionally, these systems make use of necessary using individual componentsleads to a lack of coordination. Among the factor that contributes to weak authentication. All the suggested system to meet these issues addresses these issues. The requirements for flawless trackingand validation of the vehicle and driver together. Utilizing a biometric device inside the car completesthe authentication stage. If it is successful, a facial recognition module will then be engaged to take a picture of the appropriate motorist.

- In [11] VANET, or vehicular Ad-hoc network, assists numerous access to critical information bystakeholders including passengers, the traffic management team, manufacturers, owners, and drivers' mobile network that's extremely dynamic. Restricting unauthorized access is an important difficulty in preventing consumers from free information sharing. In we suggest a dynamic, lightweight biometric based after successful registration, users can access vehicle- to-vehicle communication networks via an authentication mechanism. Immediately access his/her account from any nearby mobile device straight from the authentication servers, services, or data. In our analysis of the system security, we showed that it provides mutual anonymity, location privacy, resistance to spoofing attacks, and authentication to threat attacks such forging alteration and replay.Also, we contrast the efficiency of our plan in comparison to other similar plans and demonstrate that our authentication method is quicker and more secure compared to other available techniques in theliterature.

- In [12] Theft is the primary danger to an automobile or truck the drivers of cars. It is growing worse rightnow. If not, stolen cars are frequently sold again, modified, or even destroyed if the resale price is thought to be too low. Finding and tracking a stolen car becomes challenging, which drastically reduces the likelihood of finding it again. To lessen this, anti-theft car security has been developed. Problem. This device includes a PIC16 F876A. a microcontroller, RFID, GPS,and GSM modules, as well as a tilt detector. Using an RFID reader, fingerprint reader, or password. The appropriate RFID, password, or fingerprint will be required if a stranger tries to open the automobile door. The vehicle's windows, doors, and moments all have tilt sensors that detect any cracking of the notification that would be shown on them. These are applied to the location of the car to the owner's mobile device through a GPS and GSM module. The system also emits a warning. Additionally, the automobile's link to its fuel injector is deactivated to stop the vehicle from being started by someone else anyhow. This antitheft protection technology increases the likelihood of reclaiming the vehicle.

- In [13] Due to the rapid growth in the number of urban automobiles, vehicle theft has become a problem that affects all citizens. Safety and security have always become essential for urban residents. However, the tracking and monitoring features are missing from current anti-theft systems. The internet of things (IOT) has been in control of the electronics era, with cloud services dominating the rapidly expanding market for electronics products. Segment. As a result, an IOT-based solution for protecting vehicles from issues like theft and towing is required. For the protection of passengers and autos. With the use of a cheap Bluetooth module and wireless communication, our system suggest a revolutionary security method. The user can control the engine or ignition and, if necessary, turn it off tanks to this steady presentation of a message-sending model that takes advantage of the GSM. The system also employs a keypad password to regulate the opening of a safety locker door and the seatbelt warning. The IR module or sensor detects any window trespassers if there any intrusion, abstraction, or signal is sent to the microcontroller. The controller is linked to an alarm and Bluetooth module. System. The dashboard, which is nothing more than a cell phone, receives an alert signal from the system and delivers it to the phone used by the user.

- In [14] Electronic keys for remote keyless entry are gradually replacing traditional mechanical keys as the automobile industry expands quickly thanks to advancements in embedded technology [RKE]. When a vehicle's RKE system is activated, entrance to the car is made safer while also allowing for convenience. Additionally, the RKE system introduces numerous dangers including eavesdropping, real and replay attacks, the key fob attack, onboard diagnostic (OBD) port scan attack jamming, examples, or cloning. In this essay, we address the using a keyless car entry method and look for possible security flaws. Discuss a current RKE system and display a new one. Their system employs the idea of proposed unclonable security modules to lessen the OBD port scan attack and other Known dangers. Vehicles are authenticated via the proposed RKE system. By preserving conversant privacy, you can protect key fobs as well. The suggested RKE system is practical and safe in terms of both effectiveness and user comfort, as shown by the security analysis and test results.

- In [15] Theft that uses vehicles as targets includes grown in recent years, particularly for motorcycles. The present maximum protection cannot be provided by a vehicle security System. The process of taking the car radiation patterns technology for identification (RFID) offers an option. Method for enhancing vehicle security that uses RFID wristbands and microcontrollers based on Arduino motorcycles equipped with RFID readers and Arduino use the detecting system as a control to automatically turn on or off the motorcycles. The RFID reader will look for RFID signals continually.The relay is used to operate a bracelet-based car security system.

To switch the car's electrical system on or off. As a result, a real-time motorcycle securitysystem is an option.

- In [16] The entire system is built around an intricate algorithm that an Arduino processor employs. The gasoline line that was put in close proximity to the fuel pump controls the fuel injection used by the car's engine. And only starts working after the vehicle owner enters the correct password to access the module. The module serves as a key lock for the engine as an accessory attached to the ignition key. Along with cost-effective performance, monitoring is possible with the security system. The proximity switch serves as a construction tool for the system motion sensor and displays the current vehicle speedin the show.

- In [17] The contemporary day, there are numerous those without their initial driving license. As a resultof their maintenance of false licenses, the daily accident rate is rising. The purpose of the goal of this project is to use fingerprints to identify phony license IDs. Readers, it can be challenging to find a man with a phony driver's license. The police and RTOs. To prevent issues of this nature the project is designed to verify driving licenses. A system with afingerprint reader and a harm 9 processor. Using with the use of a fingerprint reader, the user's fingerprints will be taken. And their specificinformation, such as their license identification number, photo, and Aadhar card numbers are kept with the driving record. With a harm 9 processor, and licensing database anytime the officers want to verify that drivers have valid licenses, the verification system is utilized to confirm thevehicle's legality.

- In [18] The modern times, one of the leading causes of death has been because of auto accidents. Individuals who have never undergone testing driving prevailing and inexperienced drivers make up the majority of cases the cause. This essay tries to deter such motorists from getting behind the wheel, hence reducing the number of negligent drivers on the road and the frequency of everyday auto accidents. The main objective of this project is to develop a fingerprint authentication system that will be required in order to start an automobile, together with user authentication using A valid driver's license. With this double verification, the results are much more credible. Due to the use of biometrics, more verification than a single verification as well as the license that was issued by the government.

- In [19] considering the substantial rise in the number of automobiles the number of accidents on highways in large cities, and the number of traffic law violations are rising. Because the bulk of commutes is made in personalvehicles by the populace, it gets challenging to get a parking spot. At this time the parking and the toll systems are not entirely automated that is paper, a program that tries to lessen the traffic issue to completely end manual interventions and to reduce using a smartcard with the internet of things as the foundation is reviewed. The Internet of Things allows anything, including everyone and everything, to be connected. Smartcard with IIOT capabilities uses several sensors used to transmit device-related information supplying data to the internet.

- In [20] This essay offers an offline-based method to prevent unauthorized and ineligible users access to a car for driving, which no driver will be allowed to use the vehicle until he receives a legitimate driving permit, which prevents unauthorized drivers by providing a sign of his eligibility to drive. Those with driving licenses have access to cars, but the owner of the automobile does not want him to drive it. For the company that provides driver's licenses, it is leveraging hardware to access a driver's eligibility while utilizing protected data. Accessto the motor vehicle is controlled by a mobile communication application and a malicious mobile application. Itself. It is a functional offline. Model at theuses a but obtaining driving data from a secure web platform it is used to manage the licensing authority database. Mobile software. The key-based method isquite secure, and it will initially be used with the car, which is the main owner. The owner will obtain the names and phone numbers of the people he wishes to use cable and wireless interfaces for data transfer. Regarding the memory chip that is a part of the car's hardware module. It presently operates offline. The capability of this program to recognize the driver's sleep activities andadvise them of it.

- In [21] Verifying a driver's identity using driver authentication. In the modern automobile, identity plays a significant role. Based on his identity, and key, additionally, identification verification using fingerprints is possible. Camera mounted inside, employing a password and image-based technique-centered authentication. In this work, we outline a strategy. That uses a unique statistical feature set that is taken from the GPS information used to verify a driver's identity. Having such a unique feature set decreases computation and enhances accuracy and the capacity to understand the feature's proposed approach is enhanced by identifying and utilizing the most appropriate machine learning approach. Our approach is to increase particularity, sensitivity, and precision. The significant contribution of this method's reliability is indicated by the average area under the receiver operating characteristic curve (AUC) that was obtained, which is 0.9. this study presents a novel feature set for driver authentication. To verify the driver, we analyze the efficacy of various machine learning approaches algorithms, including SVM, random forest, Naive Bayes, and MLP.

- In [22] A vehicle identifying proof and driver's verification system is an excellent example of municipal enhancement. It includes a web and windows application where a consolidated data set of authorized automobiles is stored in addition, RFID labels for each user and vehicle will be present. This tag will be attached to a car to get the label for each user used. The

details on the RFID labels by examining the RFID tag's chronic number. The vehicle can be done successfully, but the public authority's task of vetting the driving permitframework is enormous. Numerous crimes might occur because of the when checking off the archives traffic control staff. If at all possible, the person putshis finger on the special mark scanner the device will reveal to you whether they have permission.

- In [23] Authorized driver's and permitted vehicles can access unrestricted areas of airports, as well as governmental, office, and private parking facilities. Private parking facilities, a system made up of a vehicle thanks to a system made up of a device mounted inside the car, as well as accompanying infrastructure. With the use of its own digital certificate, the device authenticates itself to the infrastructure, and the driver authenticates using a digital certificate on the smart card they have inserted into the device. With or without further biometric driver verification, the system can be designed to function.

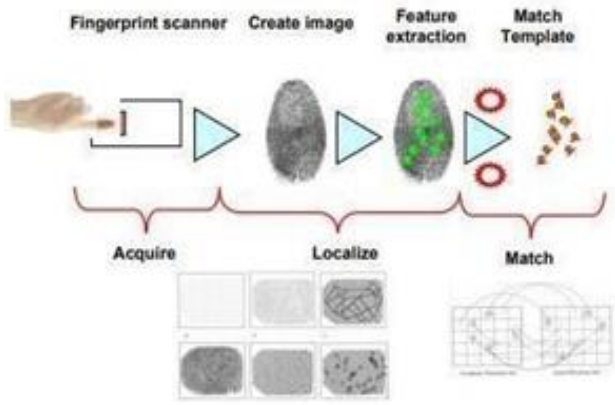

Fig 3 The Biometric Identity of the Driver is Checked by Matching Her/His Fingerprint with the One Stored on Card.

- In [24] An example of a smart city application is the automatic verification of insurance validity, license registration, emission testing, and vehicle registration difficulties. Both drivers and police officers find it quite bothersome when traffic police check these documents utilizing license plate scanning or validating documents after halting the driver. We offered a novel concept to accomplish this validation utilizing the vehicle's Global Positioning System (GPS) location in order to overcomethis difficulty.

IV. ALGORITHM

The Minutiae-based phase correlation fingerprint matching technique. A fingerprint's significant local ridge characteristics are called minutiae. The alignment stage and matching stage are the two phases of our matching method. After determining transformations like rotation and translation between two minutiae sets, the input minutiae set is aligned to models in order to measure similarity. In this study, we assume that because fingerprints are typically obtained at the same resolution,there is no scaling difference between the two fingerprints. The aligned input minutiae set and the template minutiae set are compared in the matching stage to assess how similar they are.

The phase correlation (PC) approach is a well-liked choice for image registration because of its dependable performance and simple computational construction. It is based on the well-known Fourier shift theorem. Consider two images, f1 and f2, which are different dueto translations dx and dy. The two photos' relationships will be explained by,

- $f2(x,y) = f1(x – dx, y-dy)$
- The relationship between their corresponding Fourier Transforms F1 and F2 is,
- $F_2(u,v) = e^{-j2\pi (udx/M+vdy/N)} F_1(u,v)$.

Table 1 Comparative Analysis of the Existing Methods

S No.	Name Of Authors, Paper Title,Year	Methodology And Problem Focus	Platform Used	Authentication Used
1.	Ganesh Sharma, Et.Al., E-Driving Licence And RC Book Verification System QR Code, 2017	The Riders's Identiry And That Of His Documents Are Verified Using QR Codes. It Is Not Required To Always Carry The Licence And All The The Supporting Documentation When Using Ths Software. All You Need To Do Is Have A Smartphone With A QR Code.	Android Application	QR Codes
2.	Bhavani Ratakonda, Ajay Therala, And Chanikya Kumar Hanumanthu, Driving License Detection Using QR Code,2020	With Their Login Information, Each Employee Of This System Can Create A QR Code, Enter The Applicant's Information, And Create A New License With A QR Code Attached. If The Information Collected From The QR Code And Tge Information On The License Don't Match Traffic Police Can Determine That The User Is A Fraudulent User By Scanning This QR Code Using A Mobile Phones's Scanner App.	Android Application	QR Codes
3.	Komal Chorghade, Piyush Dahiwele, Saurabh	Driver Will Sign Up For RTO Services, And Driver Will Be Given Login Information To Login. For His	Android Application	QR Codes

	Deshmukh, Prof. Prajakta Pise, RTO Automation Using QR Code, 2018	RTO Driving Licence, The Driver Will Create A QR Code. When The Police Scan The QR Code In The Application At The RTO Traffic Police's End, Data From The Server Is Fetched And License Details Re Displayed.		
4.	Kaveri Ningappa Gunjiganvi, Et.Al., Vehicle Document Verification Using Vehicle Number(VCOP-App), 2018	An App Is Used To Manually Enter The Vehicle's Licence Plate Number, Then Receive The Information From The Number Plate In Text Format. If The Documents Are Fraudulent Or Nor, The Police Can Confirm That. With The Help Of This Application, You Can Be Certain That All Of Your Papers, Including Your PUC, RC Book, And Insurance Papers, Re Manageable. Apolyibg Fine Details And Insurance Obligations Will Be Communicated To The Owner. A SMS Alert Will Be Sent To The Car Owner If Someone Other Than The Owner Operates The Vehicle.	Mobile Application Based On Linux Kernel And Java Developmen t Environment	Optical Character Recognition Algorithm
5.	Prof. Chandrakant Umarani, Et.Al., Smart RTO Web And Android Application, 2017	This Form Requests Registration For The Licence, Vehicle Registrations, And Other Paperwork. For The Use Of RTO Officials, This Programme Includes Investigative Functions Like Licencing And Document Checks. Traffic Police May Verify All Of A Person's And Vehicle's Details By Utilising This Android Application. RTO Administrator Keeps A Database With All The Data Pertaining To The Vehicle And The Driver.	Web Based Android Application	License Number
6.	Electronic Secure Vehicle Verification System Using Prof. C.S. Pagar, Et.Al., Advanced RTO System, 2020	An Advanced RTO Scheme That Is Used For Vehicle Verification Mechanisms For Fixing Real-Time Issues Takes Secure Custody Of The Necessary Files, Such As Driving Licenses, PÚCS, Insurance, RC Boojs, Etc. That Electronically Verify The Vehicle User, Resulting In A Lot More Transparency And Authenticity And Also Minimising The Corruption Of Fake Archives. It Also Lowers The Administrative Burden On RTO Administrative By Minimizing The Employ Of Human Resources.	Web Application	Optical Character Recognition, Algorithm, Hissing Codes
7.	Prof. Sindhu A S, Arpitha S. Bindushree C, Dhruvashree, Aishwariyaa V, Vehicle And License Authentication Using RFID And Finger Print, 2021	It Consist Of A Web And Windows Programme Where A Centralized Data Set Of Authorized Vehicles Is Stored. Additionally, It Has RFID Vehicle Label Per User. This Tag Will Be Attached To A Car. To Retrieve The Data From The RFID Labels, One Label Is Used Per User. By Examining The RFID Tag's Chronic Number. Vehicle Can Be Done Successfully. A Person May Also Be Responsible For The Wrong Doing. By Using A Second Small Finger Impression Scanner That Is Peovided To The Checkpoint Employees, This Problem Will Be Resolved.	Web And Windows Application	RFID Tags Finger Impression Scanner
8.	Sandeep Gupta, Attaullah Buriro, Bruno Cripso, Behavirol Driverauth: Biometric-Based Driver Authentication Mechanism For On-Demand Ride And Ridesharing Infrastructure, 2019	The Authors Introduce Driverauth, A Completely Open And Simple-To-Use Driver Authentication Method Based On Typical Behavioural Biometric Modalaties,Such As Hand Gestures,Swipes,And Touch-Strokes, While Drivers Interact With The Specific Smart Phone Based Application To Accept The Booking. A Viable Verification Mechanism For Smart Phones Is Provided In Preliminary Research Of Behavioural Biometric Based Techniques, And It Could Be A Way To Increase Passenger Safety In The Developing On-Demand Transport And Rideshare Infrastructure.	Web And Windows Application	Behavioral Biometrics Modalities

9.	Abraham Ziegen, Joel Manova M And Dr. A Akilandeswari, License Verification System With Face Recognition Using IOT, 2021	This Project Is Successful In Removing The Need For Hard Copies In Favour Of Digital Records. This Issue Will Be Solved By Implementing An IOT Based Facial Detection And Fingerprint-Based License Authentication System. The Brain Of This System,The Raspberry Pi, Aids With Face Detection And Recognition. The Raspberry Pi Is Interface With The USB Camera To Obtain User Data. These Data Are All Uploaded Via Nodemcu To The Cloud(IOT). It Is Used To Determine Whether A Person Has A License Or Not As Well As To Verify The Validity Of The Vehicle. The Display Displays That A License Is Invalid When The Holder Doesn't Have A Valid One, When It Has Already Expired, And Vice Versa.	Raspberry Pi, Node MCU, Iot	Face Recognition

V. CONCLUSION

Using fingerprint and driver's license technology, a vehicle security system was built for this thesis. With the help of this technology, car theft, and unauthorized driving are both avoided. It was accomplished using the setting type of driver's license whose holder permits the operation of a vehicle as well as an added layer of protection. The technology uses biometrics to provide entry to the vehicle, specifically fingerprint recognition. GSM module is used to send an SMS to the automobile owner informing him that an unauthorized driver's license has been used, preventing any potential vehicle theft. Additionally, the GSM module was used to send SMS reminders to the license holder.

REFERENCE

[1] K. S. Tamilselvan, G. Murugesan, and S. Sasikumar, "Design and Implementation of Biometric Based Smart Antitheft Bike Protection System," 2018 International Conference on Intelligent Computing and Communication for Smart World (I2C2SW), 2018, pp. 136-138, doi:10.1109/I2C2SW45816.2018.8997118

[2] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma, and K. -K. R. Choo, "Unified Biometric Privacy Preserving Three-Factor Authentication and Key Agreement for Cloud-Assisted Autonomous Vehicles," in IEEE Transactions on Vehicular Technology, vol. 69, no. 9, pp. 9390-9401, Sept.2020, doi: 10.1109/TVT.2020.2971254.

[3] Y. Xun, J. Liu, N. Kato, Y. Fang, and Y. Zhang, "Automobile Driver Fingerprinting: A New Machine Learning Based Authentication Scheme," in IEEE Transactions on Industrial Informatics, vol. 16, no. 2, pp. 1417-1426, Feb. 2020, doi: 10.1109/TII.2019.2946626.

[4] A. E. Mekki, A. Bouhoute and I. Berrada, "Improving Driver Identification for the Next-Generation of In-Vehicle Software Systems," in IEEE Transactions on Vehicular Technology, vol. 68, no. 8, pp. 7406-7415, Aug. 2019, doi: 10.1109/TVT.2019.2924906.

[5] S. Sharma, K. K. Ghanshala and S. Mohan, "A Security System Using Deep Learning Approach for Internet of Vehicles (IoV)," 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2018, pp. 1-5, doi: 10.1109/UEMCON.2018.8796664.

[6] R. A. Rashid, N. H. Mahalin, M. A. Sarijari, and A. A. Abdul Aziz, "Security system using biometric technology: Design and implementation of Voice Recognition System (VRS)," 2008 International Conference on Computer and Communication Engineering, 2008, pp. 898-902, DOI: 10.1109/ICCCE.2008.4580735.

[7] M. Ramesh, S. Akruthi, K. Nandhini, S. Meena, S. Joseph Gladwin, and R. Rajavel, "Implementation of Vehicle Security System using GPS, GSM, and Biometric," 2019 Women Institute of Technology Conference on Electrical and Computer Engineering (WITTON ECE), 2019, pp. 71-75, doi:10.1109/WITCONECE48374.2019.90 92918.

[8] H. Khalid, S. J. Hashim, S. M. S. Ahmad, F. Hashim, and M. A. Chaudary, "New and Simple Offline Authentication Approach using Time-based One-time Password with Biometric for Car Sharing Vehicles," 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), 2020, pp. 1-7, DOI: 10.1109/CSDE50874.2020.9411569.

[9] M. R. Pawar and I. Rizvi, "IoT Based Embedded System for Vehicle Security and Driver Surveillance," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), 2018, pp. 466- 470, doi: 10.1109/ICICCT.2018.8472984.

[10] P. Muddapu, "Camera and Biometric based Vehicle Monitoring System for Public Safety," 2020 IEEE-HYDCON, 2020, pp. 1-6,doi: 10.1109/HYDCON48903.2020.9242840.

[11] M. Ismail, S. Chatterjee and J. K. Sing, "Secure Biometric-Based Authentication Protocol for Vehicular Ad-Hoc Network," 2018 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS), 2018, pp. 229-234, doi: 10.1109/iSES.2018.00057.

[12] A. T. Noman, S. Hossain, S. Islam, M. E. Islam, N. Ahmed, and M. A. M. Chowdhury, "Design and Implementation of Microcontroller Based Anti-Theft Vehicle Security System using GPS, GSM, and RFID," 2018 4th International Conference on Electrical Engineering and Information & Communication Technology (IEEE ICT), 2018, pp. 97-101, DOI: 10.1109/CEEICT.2018.8628051.

[13] D. Mukhopadhyay, M. Gupta, T. Attar, P. Chavan and V. Patel, "An Attempt to Develop an IOT Based Vehicle Security System," 2018 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS), 2018, pp. 195-198, doi: 10.1109/iSES.2018.00050.

[14] J. Patel, M. L. Das, and S. Nandi, "On the Security of Remote Key Less Entry for Vehicles," 2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2018, pp.1-6, DOI:10.1109/ANTS.2018.8710105.

[15] B. Siregar, S. Efendi, C. Setiawan, and F. Fahmi, "RFID Wristband for Motorbikes Real-Time Security System," 2019 3rd International Conference on Electrical, Telecommunication and Computer Engineering (ELTICOM), 2019, pp. 116- 119, doi: 10.1109/ELTICOM47379.2019.8943903.

[16] S. Khan, O. Rahman and M. Ehsan, "Design and fabrication of a password protected vehicle security and performance monitoring system," 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), 2017, pp. 560-563, DOI: 10.1109/R10-HTC.2017.8289022.

[17] N. Ramakumar, P. S. N. Reddy, R. N. Naik and S. A. K. Jilani, "Authentication based systamatic driving license issuing system," 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), 2017, pp. 1327-1331, doi: 10.1109/ICCONS.2017.8250685.

[18] Pradesh, R. B S, N. Nagabhushan and T. Madhavi, "Fingerprint-based Licensing for Driving," 2021 6th International Conference for Convergence in Technology (I2CT), 2021, pp.DOI6, DOI: 10.1109/I2CT51068.2021.9418134.

[19] K. Chopra and K. Gupta, "Smart Vehicle Card Using IoT," 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), 2019, pp. 20-24, DOI: 10.1109/COMITCon.2019.8862210.

[20] J. B. K. Gangone, "An Ineligible and Unauthorized Motor Vehicle Driver Access control and Sleep State Alert System: An Offline based Model," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019, pp. 1-6, DOI: 10.1109/ICCCNT45670.2019.8944492.

[21] T. Banerjee, A. Chowdhury, T. C, Chakravarthy, and A. Ghose, "Driver authentication by quantifying driving style using GPS only," 2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2020, pp. 1-6, DOI: 10.1109/PerComWorkshops48775.2020.9 156080.

[22] https://ijarcce.com/wpcontent/uploads/2021/08/IJARCE.2021. 10770.pdf.

[23] A. Makarov, M. Španović and V. Lukić, "Authenticating vehicles and drivers in motion based on computer vision and RFID tags," 2012 IEEE 10th Jubilee International Symposium on Intelligent Systems and Informatics, 2012, pp. 419-424, doi: 10.1109/SISY.2012.6339556.

[24] K M Farhat Snigdah. Md Gulzar Hussain,"Smart Traffic Vehicle Monitoring & Authenticating System using GPS" 2019 Conference: International Conference on Sustainable Technologies for industry 4.0 (STI), doi:10.13140/RG.2.2.10237.92642

[25] D. Mukhopadhyay, M. Gupta, T. Attar, P. Chavan and V. Patel, "An attempt to develop an iot based vehicle security system", 2018 IEEE International Symposium on Smart Electronic Systems (iSES) (FormerlyiNiS), pp. 195-198, Dec 2018

[26] Ganesh Sharma, et.al., E-Driving License and RC Book Verification System Using QR Code, International Journal of Advances in Electronics and Computer Science, Volume-4, Issue-1, pp. 1-2, Jan2017

[27] Kaveri Ningappa Gunjiganvi, et.al., Vehicle Document Verification using Vehicle Number (VCOP-App), International Journal of Engineering Research and Technology (IJERT), ICRTT 2018 Conference Proceedings,Volume 6, Issue 15, pp. 1

[28] Prof. C. S. Pagar, et.al., Electronic Secure Vehicle Verification System using Advanced RTO System, International Research Journal of Engineering and Technology (IRJET), Volume 7, Issue 4, pp. 5330-5336, Apr 2020

[29] Dr.A.Srinivasarao, S.Gopiraju, M.Raghavendra, E-Driving License Authentication System, International Journal for Research in Engineering Application & Management (IJREAM), pp. 176-178, 2018

[30] Abraham Ziegen, Joel Manova M and Dr. A Akilandeswari, License Verification System with Face Recognition Using IOT, International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Volume 4, Issue 2, pp. 656-670 , April 2021

[31] Sandeep Gupta, Attaullah Buriro, Bruno Crispo, DriverAuth: Behavioral biometricbased driver authentication mechanism for the on-demand ride and ridesharing infrastructure, The Korean Institute of Communications and Information Sciences (KICS) published by Elsevier, Science Direct, ICT Express, Volume 5, pp. 16-20, 2019.

[32] Dr.A.Srinivasarao,S.Gopiraju, M.Raghavendra, E-Driving License Authentication System, International Journal for Research in Engineering Application & Management (IJREAM), pp. 176-178, 2018.