Advances in Mathematical & Computational Sciences Journal,
Vol. 8 No.1, March 2020

Article Citation Format
Salako, E. A., Muhammed, B.A. & Solomon, A. A. (2020): Development of a Vehicle Driving Authorization Permit and Fake Driver Detection System Using Fingerprints Techniques. Journal of Advances in Mathematical & Computational Sc. Vol. 8, No. 1. Pp 1-14

Article Progression Time Stamps

Article Type: Research Article
Manuscript Received 19th November, 2019
Final Acceptance: 3rd January, 2020
Article DOI: dx.doi.org/10.22624/AIMS/MATHS/V7N3P1

Development of a Vehicle Driving Authorization Permit and Fake Driver Detection System Using Fingerprints Techniques

[1]Salako, E. Adekunle, [2]Muhammed, B. Abdullahi & [3]Solomon, A. Adepoju
[1]Department of Computer Science, FCT College of Education, Zuba, Nigeria.
[2&3]Department of Computer Science, Federal University of Technology Minna, Nigeria
E-mails: kunlesky2@gmail.com; el.bashir02@gmail.com; sa.adepoju@gmail.com

ABSTRACT

The world at large is characterized by the rising of vehicle thefts thereby leaving many owners of vehicles helpless in the hand of thieves and unauthorized drivers. The safety of the vehicle has become a matter of major significance to the owners. Among the issues of concern that could easily lead to stealing of vehicle or driving by the unauthorized drivers is the lack of good parking spaces in offices arena or residential areas and lack of availability of sophisticated security devices. As a technological approach to providing the solution to the aforementioned problem, this research was on the development of a vehicle driving authorization permit and fake driver detection system using fingerprint technique. The system had majorly three modules, namely enrolment, driver's, authentication and Global System for Mobile (GSM). An enrolled driver sent a destination code from a registered mobile number to the authentication module before the commencement of the journey that would be used for the authentication at the various checking points. The developed system was designed and implemented using C# and SQL programming languages. Eight biometric standard metrics were used to evaluate the system. Series of tests were carried out in five different towns in five states of Nigeria. The developed system was able to suitably identified fake drivers and permitted genuine drivers to proceed on the journey earlier specified. The result of the analysis showed an excellent system accuracy value of 96.25% with a lower Equal Error Rate of 3.75% with the mean-time of 49 seconds to create a reference template.

Keywords: Vehicle, Authorization Permit, Fingerprint, Fake Driver, Detection

1. INTRODUCTION

The significance of vehicle to convey people and goods cannot be over-emphasized. Vehicles are used by the owners for different reasons. For instances, vehicles can be used to transport peoples from one geographical location to the other, convey goods to different places, and advertising services to mention but few. The driving of vehicles simply involves starting the engine with the key [1]. This means that anyone with the key can start the vehicle and use it either lawfully or illegally. Vehicle usage has become important everywhere in the world and also preventing it from theft is required [2].

Automobile manufacturers are incorporating security features into their products by introducing advanced automated technologies to avoid stealing by thieves. Security features are provided by biometric and non-biometric methods [3]. Sometimes security systems fail due to hacked password and encryption of decrypted data, but it is almost impossible to make a duplicate of distinctive characteristics [4]. Biometric systems are modern and techniques like fingerprint recognition, iris recognition and facial recognition towards prevention of illegal use. According to [3], people could easily be identified with fingerprint recognition and detection systems. These days, automobile burglary cases are increasing day by day, it has gotten to be difficult to give a vehicle outstanding security with the main focus being kept on the burglary gadget [5]. According to [6], passwords are the weakest element of many important security systems that could easily be guessed or detected by fraudsters for stealing sensitive properties. Reference [3] stated that the objective of the vehicle security system is to prevent the theft of the vehicle and ensure safe driving.

2. LITERATURE REVIEW

The key goal of the system developed by [7] was to protect the vehicle from any unauthorized access, using fast, easy-to-use, clear, reliable and economical fingerprint recognition technique. The vehicle security system intimated the status of the vehicle to the authoritative person (owner) using the Global System for Mobile (GSM) communication technology. The model for the security system was built on the embedded platform using PIC Microcontroller which controlled all the processes. The driver of a vehicle scanned the enrolled fingerprint to gain access to use drive the vehicle if there was a match in the database. By using GPS technology, the location of a vehicle could be identified very easily. However, in [7], there was a high likelihood of fingerprint's fooling to gain access to drive the vehicle illegally. This problem allowed the thieves to steal a vehicle and passed the police officers at the checking points.

The research of [8] was focused on protecting cars from unauthorized drivers and to prevent the vehicle from theft. Using biometric fingerprint security system, only authorized drivers could start the vehicle. The research dealt with the development of the antitheft system using ATmega 328. A fingerprint sensor which was kept inside the vehicle was used to sense the fingerprint of a driver. A successfully authenticated driver could start the engine of the car. An intruder who had un-matched fingerprint could not start the engine. The problems identified included reprogramming of the ATmega 328 microcontroller and fingerprint fooling by thieves and fake drivers. These problems allowed thieves to steal a vehicle and passed the police officers at the checking points. This new technology did not use any microcontroller and the driver of the vehicle was in person required to scan the live fingerprint.

To prevent non-licensees from the stolen vehicle, an advanced automobile system was proposed by [9]. While issuing the license, the specific driver's fingerprint was saved in the database. In the proposed system, every automobile had a fingerprint reader device. A driver who wanted to drive the vehicle swiped his/her finger (license) in the vehicle. If the fingerprint image stored on the smart card and swiped in the device matches, the driver could proceed for ignition, otherwise, the ignition system would not work. The possibility of fingerprint's fooling was high to start the engine, as no officers available to monitor and prevent the scanning of the fooled fingerprint (fake fingerprint). In addition, thieves could threat a genuine owner of a car with guns to start a vehicle and the stolen vehicle could pass the police checking points without any detection of robbery. This is possible because there was no authentication mechanism at the checking points for authentication.

Reference [10] was on a prototype model of a fingerprint-based security system for vehicles with the aim at improving the level of security in automobiles. The system used Arduino Uno, a Fingerprint Micro Switches LCD Display, Servo Motor, I2C Backpack and Sensor Module. A driver could start the vehicle, but only upon fingerprint authentication could the driver put the vehicle into motion. In recognition of the fingerprint, the valve fixed in the outlet of the fuel tank opens, thereby allowing the flow of fuel to the engine. The problems identified included reprogramming of the memory of Arduino Uno and fingerprint fooling by thieves and fake drivers. Upon compromising these measures, thieves could steal a vehicle and passed the police officers at the checking points without any detection. How could security agents identify a stolen vehicle at the checking points when the real owner had been threatened with dangerous weapons to starts the vehicle? This new technology did not use any microcontroller and the driver of the vehicle was in person required to scan the live fingerprint.

2.1 Research Motivation

The vehicles are generally operated by turning the ignition key to start the engine. Once the engine starts, setting the vehicle on motion becomes easier for any driver to drive the vehicle. This implies that an unauthorized driver or a thief with an ignition key could steal and drive the vehicle. The cases of armed robbery in Nigeria are rampant that require urgent but technological intervention. Security gadgets provided by many security firms have been compromised thereby allowing fake drivers (armed robbers) to drive a vehicle without the real owner's consent and even passed the police officers at the checking points. The paper-based identification approached had not yielded any significant results in the prevention of theft. A genuine driver could easily be impersonated by the paper-based technique. In addition, the use of a password is the weakest component of many important security systems [6].

The password of the genuine driver could be guessed, making stealing by a thief easier and driving by an unauthorized driver is inevitable. However, [3] developed a multi-level authentication ignition system, where the driver's fingerprint was embedded in a smart card to turn ON the ignition system. The problems with the [3] system were the fingerprint fooling, high cost of smart-card production and shimming of smart cards. Therefore, this research attempted to solve the aforementioned problems through the development of a vehicle driving authorization permit and fake driver detection system using fingerprint technique.

2.2 Research Objectives

The specific objectives of this research are to:

1. design a vehicle driving authorization permit using fingerprint technique towards fake driver detection,
2. implement the designed vehicle driving authorization permit model and
3. evaluate the performance of the developed model.

2.3 Significance of the research

The significance of this research are:

1. Detection of fake drivers and armed robbers;
2. Faster driver's identification than the current paper-based approach;
3. Moderate in the cost of implementation and
4. Highly secured against impersonators.

3. METHODOLOGY

The development of a vehicle driving authorization permit using fingerprint technique towards fake driver detection was detailed as follows:

3.1 Architectural Diagram

The architectural block diagram of the developed system is illustrated in Figure 1. The vehicle theft detection and authorization system had three fundamental modules. The modules were enrolment, driver's, authentication and Global System for Mobile (GSM).

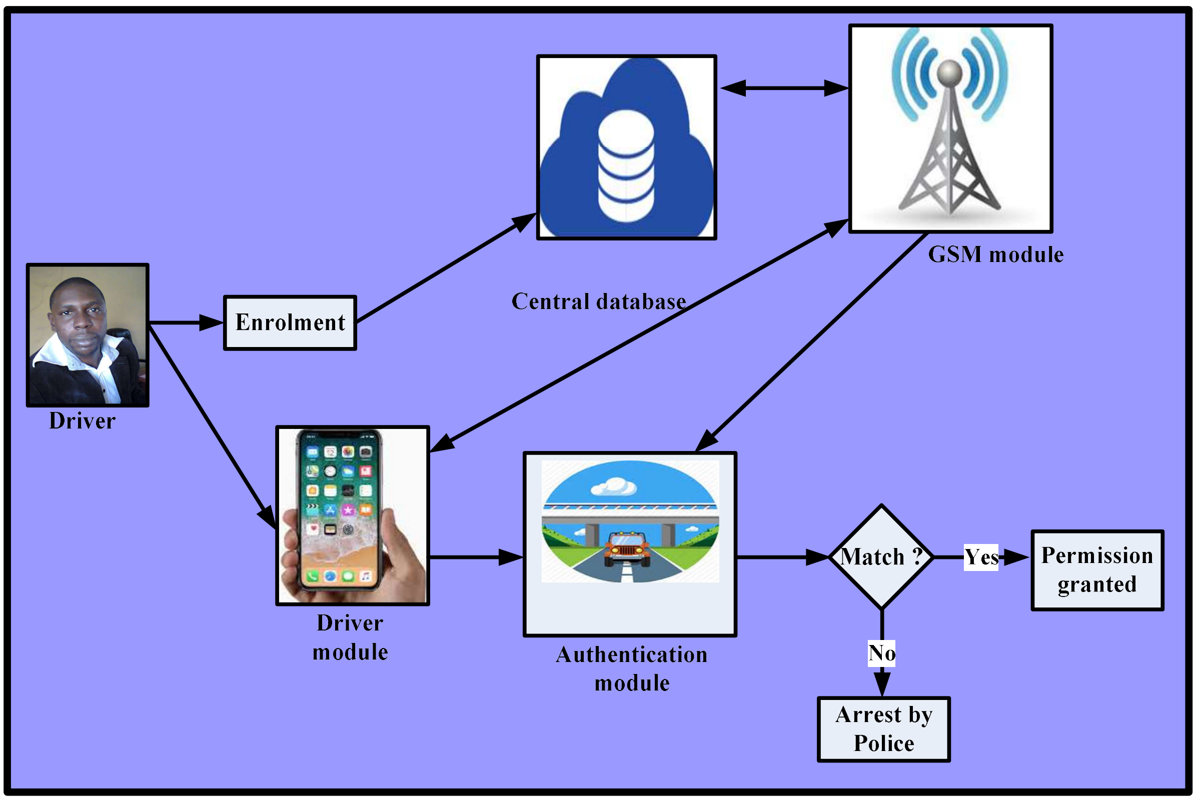

Figure 1: Architectural diagram

i. Enrolment Module

The enrolment module allowed the real owner and an additional four authorized drivers to enrol into the database for the permission to drive a registered vehicle. A particular vehicle was assigned to a maximum number of five to drive the vehicle. However, in case of an emergency, where the real owner and other authorized drivers were not available, the real owner requested an authorization code for the emergency driver. The emergency driver was a driver who had been enrolled with a particular vehicle into the database as an emergency driver and had the authorization to drive a vehicle.

The developed system allowed only the real owner of the vehicle to request for a new driver through a registered mobile number. Also, if the real owner died, the other four authorized drivers assigned to the vehicle of the deceased had to report in persons to the nearest office for notification and re-assignment of ownership. During enrolment, drivers' fingerprints, vehicle chassis number, drivers' GSM number were significantly required for the enrolment among others particulars.

ii. Fingerprint Minutiae Points Analysis

The ridge-ends and ridge bifurcations detection analyses were performed on the drivers' fingerprint image acquired. The fingerprint pre-processing involves Normalization, Segmentation, Fingerprint Image Enhancement and Binarization as illustrated in Figure 2. Figure 3 shows a local neighbourhood of each pixel of a driver's ridge-ends and ridge bifurcations and Figure 4 shows ridges end and bifurcations characteristics.

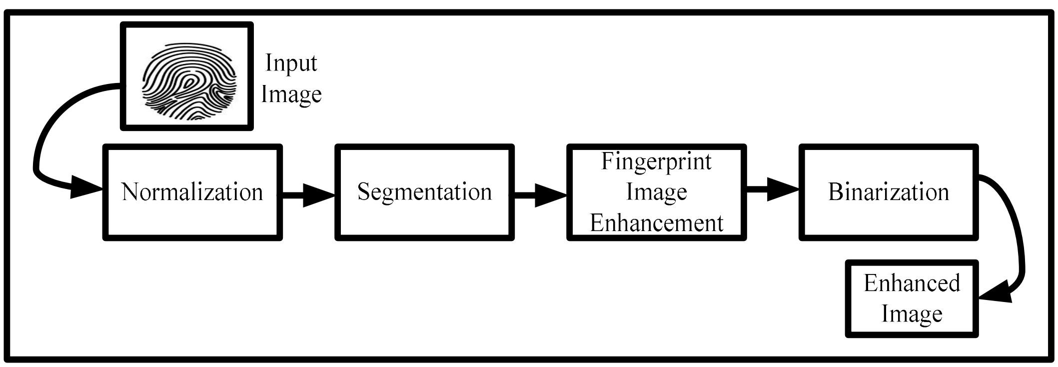

Figure 2: Fingerprint pre-processing

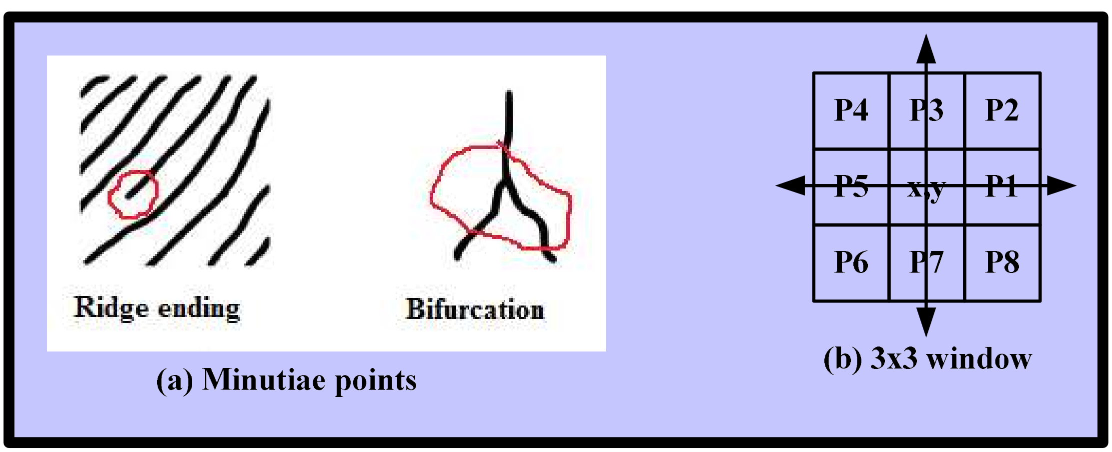

Figure 3: Local neighbourhood of each pixel of ridge-end and bifurcation

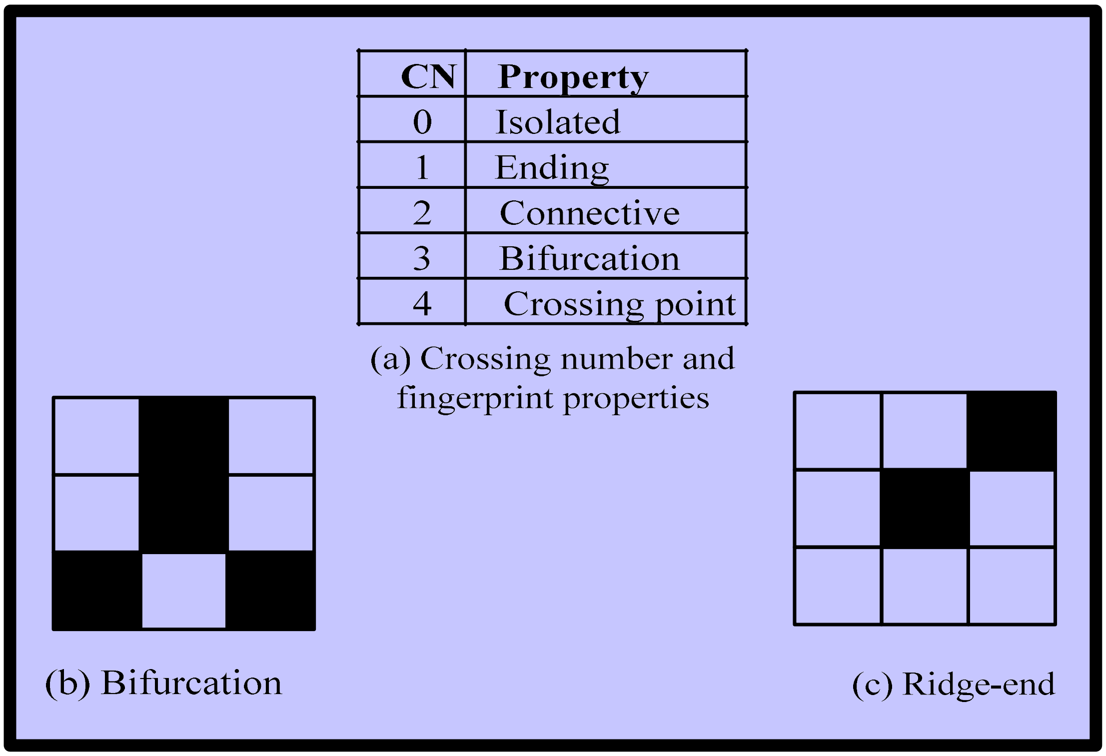

Figure 4: Ridges end and bifurcations characteristics

To identify the ridge–end and bifurcation point, a crossing number (CN) identification technique used in Olagunju (2018) was adopted:

$$CN = \frac{1}{2}\sum_{i=1}^{8}|P_i - P_{i+1}| \qquad \text{..........................(1)}$$

In equation 1, $P_9 = P_1$.

Therefore, the attribute of the driver's fingerprint features was represented by D_{fT} and it was expressed as:

$$D_f = \frac{D_{f1}}{\sqrt{D_{f1} + D_{f2}}} \text{..(2)}$$

Where D_{f1} and D_{f2} were the fingerprint ridge and bifurcation scores respectively. The D_f was the driver's fingerprint template score during enrolment stored in the database for reference use. The decimal representation of letters in the chassis number was used in the fusion technique.

Mathematically, the driver's fingerprint details (ridge and bifurcation) and the vehicle chassis number (VCN), (V_{Cn}) were fused during enrolment as follows:

$$D_{ET} = f(D_f, V_{Cn}, \beta) = \frac{8.2(V_{Cn} * D_f)}{D_f} + \left(\frac{1}{\beta}\right) \qquad \ldots\ldots\ldots\ldots(3)$$

Where The Beta β was a mathematical constant and it was used as a driver's sensitivity that controlled the difference in the scores between a genuine driver and fake driver. The D_{ET} was the ticket generated during the enrolment and it was stored in the database for authentication. After successful enrolment, the driver was presented with a card that had the driver's photography and vehicle details.

Iii Drivers' module

The drivers' module allowed any of the enrolled vehicle's drivers that wanted to use the vehicle to identify the destination, send the destination code to the central database and received a confirmation of the destination through a registered mobile number prior to the commencement of the journey. The driver's request on the destination was transferred to the authentication module for adequate identification and fake driver (thief) detection. This technique was used to authenticate the driver's identity at the checking points located along the road specified by the driver. Importantly, the driver could have a change of destination as the vehicle moved from one geographical location to another. The developed system allowed diversion even if one destination had earlier been identified. To achieve a successful authentication at the checking point for the new destination, the driver needed to send a new destination code to the authentication module.

iv. Authentication module

The authentication module used the driver's fingerprint and the chassis number of the vehicle to verify the driver. The checking points for authentication were located at the entrance and exit of identified towns and on the major highways. At the checking points, the driver's fingerprint and the chassis number of the vehicle were scanned and verified. The result of the scanning was used to either grant or deny permission to proceed to the specified final destination. When there was a match of the driver's fingerprint with the record in the database, the driver's photography, vehicle name, model, type, colour and chassis number were displayed. In any case, where there was a repudiation to proceed on the journey, the driver was arrested and handed over to the police for interrogation.

The disparity in the record stored in the database with respect to the vehicle showed that the vehicle was in the hand of the fake driver. This authentication technique was used to detect fake drivers and theft. Anytime the destination code was not received at the checking point, the driver was charged to be a fake driver. The confirmation received through the registered mobile phone of the driver signified that the destination code was received and readily available at the checking point for authentication as the vehicle moved from one town to another until the final destination was reached.

To achieve a moderate acceptance and rejection rates of the diver's fingerprint during the authentication, a threshold value D_{fh} was computed as follows:

$D_{fh} = 0.78(D_f)$ ....(4)

This equation implies that seventy-eight per cent (78%) of the driver's fingerprint features were used to obtain a value, D_{fh}. The value of D_{fa} was the fingerprint's score of a driver during authentication at the checking point and it was computed using Equation 2. In line with the threshold value, fuzzy logic was used for the decision on the acceptance and rejection of the driver at the checking point. Fuzzy logic is a computational technique that deals with the "degrees of truth" not the Boolean logic of either "true" or "false" (0 or 1) on which the modern computer is designed and developed.

Therefore, if
$D_{fh} \leq D_{fa} \leq D_f$ ....(5)

then the driver's fingerprint was accepted.
$D_{fh} > D_{fa} > D_f$ ....(6)

then the driver's fingerprint was rejected.
At the authentication stage, let the matching score of the driver's fingerprint be D_{fa}, as computed in Equations 5 and 6, and the vehicle chassis number (VCN) be V_{Cna}. Therefore, the driver's ticket D_{AT}, for permission to proceed on the journey was computed and generated by fusing D_{fa} and V_{Cna} as follows.

$D_{AT} = f(D_{fa}, V_{Cna}, \beta) = \frac{8.2(V_{Cna} * D_{fa})}{D_{fa}} + \left(\frac{1}{\beta}\right)$ ....(7)

The D_{ET} was the driver's ticket generated during the enrolment and the D_{AT} was the driver's ticket generated during the authentication. Mathematically, the D_{TA} may not be equalled to the D_{TE} before the driver was permitted to proceed to drive the vehicle from the checking point. However, the value of D_{AT} must not be lesser than the value of D_{ET}. As long as the threshold value, D_{fa} was satisfied and the V_{cna} was correct, the driver was granted permission to proceed on the journey.

v. GSM module
The GSM module received the destination code from the driver, retrieved the driver's details from the central database and transferred the same destination code to the authentication module at the checking point. The enrolled drivers of the vehicle used the registered mobile number to send the code and received a confirmation of the destination.

3.2 Algorithm
The algorithm used for the software development of the vehicle driving authorization permit using fingerprint technique is depicted on the next page.

Start
Select an operation; //operation on the homepage
Form1: Enrolment;
Form2: Edit Driver's/Vehicle details;
Form3: Authentication;
Case Form1:
Start
Enrol driver's details, d; //i.e Name, mobile number
Acquire, process and store driver's fingerprint features, D_f; //fingerprint at enrolment
Enrol the vehicle's particulars, Vp; // model/type, colour
Enrol the chassis number, Vcn ; // Chassis number at enrolment
$D_{ET} = \left(\left(8.2(V_{Cn} * D_f)\right)/(D_f)\right) / \left({}^{1}/_{\beta}\right)$; //Fuse D_f and Vcn
Save D_{ET}, d, Vp and Vcn; // save the records
End; // End the new enrolment
Case Form2:
Start
Open the driver's details, d, D_f; // including other records
Open the vehicle's details, Vp, Vcn;
Confirm and delete d, D_f, Vp, Vcn;
Open new enrolment page;
Enrol driver's details, d; //i.e Name, mobile number
Acquire, process and store driver's fingerprint features, D_f; //fingerprint at enrolment
Enrol the vehicle's particulars, Vp; // model/type, colour
Enrol the chassis number, Vcn ; // Chassis number at enrolment
$D_{ET} = \left(\left(8.2(V_{Cn} * D_f)\right)/(D_f)\right) / \left({}^{1}/_{\beta}\right)$; //Fuse D_f and Vcn
Save D_{ET}, d, Vp and Vcn; // save the records
End; // End the Re-enrolment
Case Form3:
Start
Input chassis number, Vcna; // Chassis number at authentication
Acquire, process and compare driver's fingerprint, D_{fa}; //fingerprint at authentication
$D_{AT} = \left(\left(8.2(V_{Cna} * D_{fa})\right)/(D_{fa})\right) / \left({}^{1}/_{\beta}\right)$;; //Fuse D_{fa} and Vcna
String message1 = " SUCCESSFUL ";
String message2 = " PERMISSION to proceed is GRANTED ";
String message3 = " NOT SUCCESSFUL ";
String message4 = " ARREST….THIS FAKE DRIVER ";
If
Start
$D_{ET} = D_{AT}$;
Show (message1, message2);
Else
Show (message3, message4);
End; // End the if….else condition
End; // End the Authentication
End

3.3 Software development

The source code of the vehicle driving authorization permit using fingerprint technique towards fake driver detection was developed using Visual C# in Microsoft visual studio 2010 ultimate version and Microsoft SQL Database was used for the database management system to store all the data. Figures 5, 6 and 7 were the screenshots of the developed application for the vehicle driving authorization and fake driver detection.

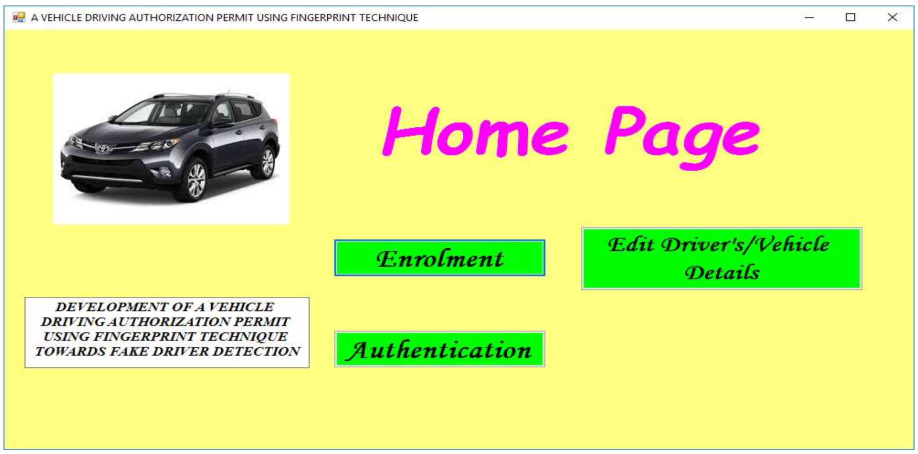

Figure 5: Homepage of the system

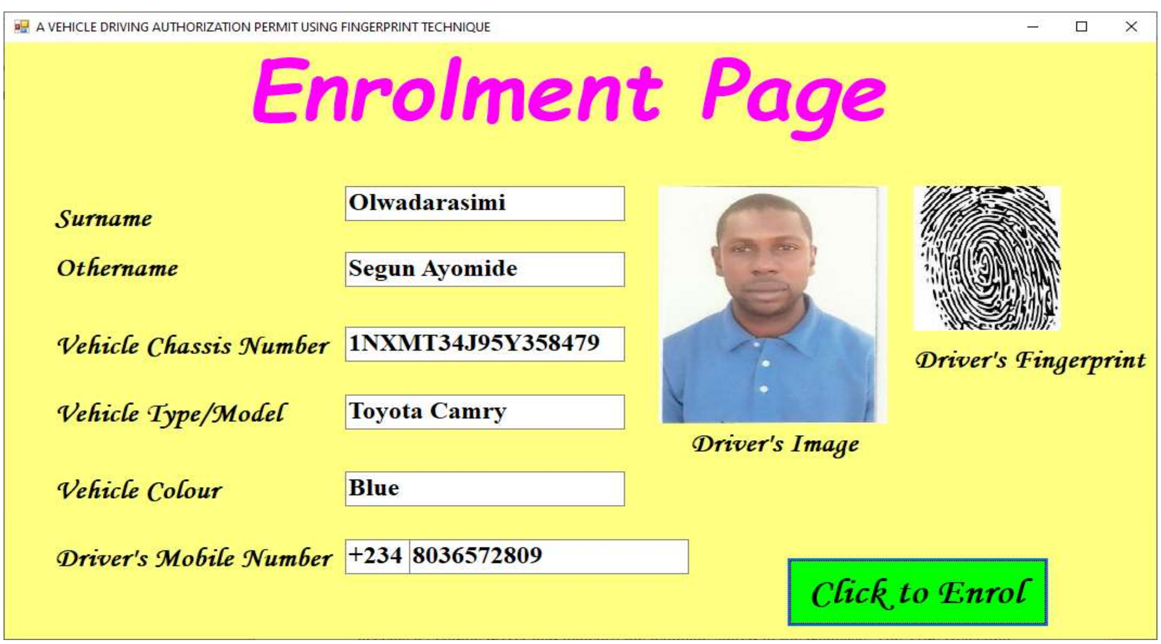

Figure 6: Enrolment page of the system

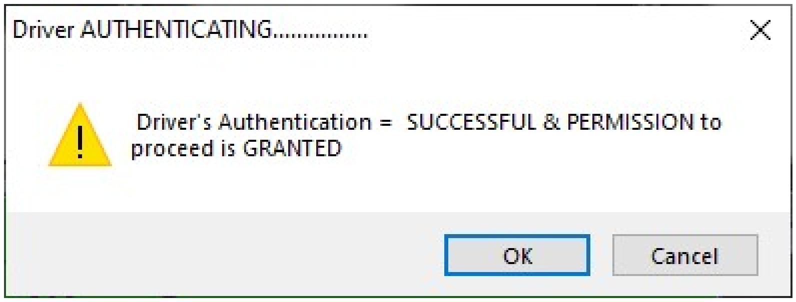

Figure 7: Driver's authentication status

3.3 Standard Metrics for System Evaluation

The standard metrics explained below were adopted to evaluate the system performance. These metrics are:

1. **The True Acceptance Rate (TAR)** refers to the likelihood that the biometric system correctly accepts a genuine driver and matches the template stored in the database.
2. **The True Rejection Rate (TRR)** refers to the probability that the biometric system correctly rejects a fake driver (imposter) and there is no match of a template stored in the database.
3. **The False Acceptance Rate (FAR)** refers to the likelihood that the biometric system incorrectly accepts a fake driver (imposter) and incorrectly matches a template stored in the database.
4. **The False Rejection Rate (FRR)** refers to the likelihood that the biometric system incorrectly rejects a genuine driver and there is no match of the template of the genuine in the database.
5. **The Mean Time-to-Enrol (MTTE)** refers to the mean-time required by the biometric system to collect, process and create a reference template for a driver and successfully store in the database.
6. **The Equal Error Rate (EER)** refers to the point or value where FRR and FAR are equal at a specific threshold value. The lower the value of EER, the better is the accuracy of the system.
7. **The Total Success Rate (TSR)** refers to the number of attempts that are successfully achieved in true acceptance and true rejection. The accuracy refers to the degree of correctness of a biometric true value of individual acquired, measured, processed and stored with a biometric system.

3.4 Research Design and Sample

An experimental design was adopted and two groups were randomly selected for testing the system. The first group comprised of the genuine drivers and the second group included fake drivers that were distinguished with tags. A purposive sampling technique was used to select forty (40) genuine drivers and twenty (20) fake driver from each of the five towns. Therefore, a total of one hundred and fifty (200) genuine drivers and one hundred (100) fake drivers.

4. EXPERIMENTAL RESULTS

A series of pilot experiments were conducted to determine a suitable threshold value for authentication. At 0.78 (78%) threshold value, an Equal Error Rate (EER) of acceptance and rejection of the diver's fingerprint during the authentication was achieved as illustrated in Figure 8.

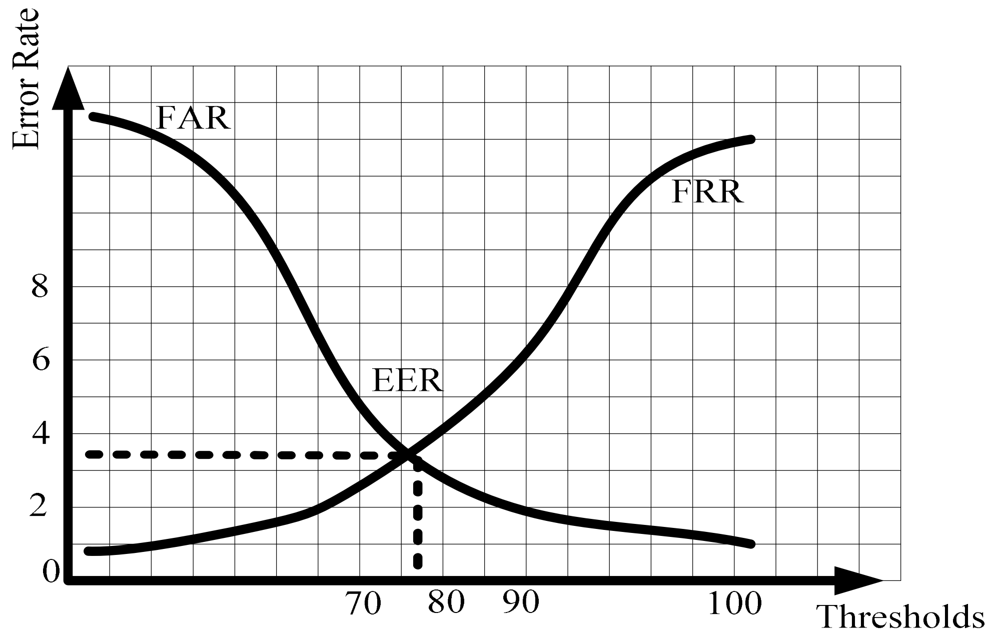

Figure 8: Error Tradeoff curve

After the pilot experiments, the developed system was then tested in five towns from five different states in Nigeria. The towns were Oro, Akure, Gwagwalada, Minna and Ile-Ife.

Individual	Accept	Reject	Total
Genuine	TA	FR	GT
Imposter (Fake driver)	FA	TR	IT
Grand Total	A	R	G

=

Individual	Accept	Reject	Total
Genuine	193	7	200
Imposter (Fake driver)	4	96	100
Grand Total	197	103	300

1. True Acceptance Rate (TAR) = $\frac{\text{Total True Accept}}{\text{Total True Attempts}} = \frac{\text{TA}}{\text{GT}} = \frac{193}{200}$ = 0.965
2.
3. True Rejection Rate (TRR) = $\frac{\text{Total True Reject}}{\text{Total False Attempts}} = \frac{\text{TR}}{\text{IT}} = \frac{96}{100}$ = 0.96
4.
5. False Acceptance Rate (FAR) = $\frac{\text{Total False Accept}}{\text{Total False Attempts}} = \frac{4}{100}$ = 0.04
6.
7. False Rejection Rate (FRR) = $\frac{\text{Total False Reject}}{\text{Total True Attempts}} = \frac{7}{200}$ = 0.035
8.
9. Equal Error Rate (EER) = $\frac{\text{FAR+F}}{2} = \frac{0.04 + 0.035}{2}$ = 0.0375 (3.75%)
10.
11. Total Success Rate (TSR) = $\frac{\text{TAR + TRR}}{2} = \frac{0.965 + 0.96}{2}$ = 0.9625
12. Accuracy = 1 – EER = $1 - 0.0375 = 0.9625$ (96.25%)
13. Mean Time-to-Enrol (MTTE) = 49 seconds

The proposed system of [11] was used for comparison as indicated in Table I.

Table I: Performance comparison

S/n	Parameters	Ref [11]	Developed System
1	Number of features	250	300
2	TAR	0.93	0.965
3	TRR	0.78	0.96
4	Mean-time	1mins 13sec	49 sec

The False Rejection Rate (FRR) of the developed system was 0.035, the Total Success Rate (TSR) was 0.9625 (96.25) and the time of processing reduced from 1 minute 13 seconds in the existing system to 49 seconds in the developed system.

5. CONCLUSION

In conclusion, vehicle driving authorization permit and fake driver detection using fingerprint technique was designed, developed, tested and evaluated. The developed system was able to suitably identified fake drivers and permitted genuine drivers to proceed on the journey that was earlier specified. The result of the analysis of the data obtained showed an excellent system accuracy value of 96.25% with a lower Equal Error Rate of 3.75% and the mean time required by the biometric system to collect, process and create a reference template was 49 seconds.

REFERENCES

[1] Ramya, V., Palaniappan, B., & Karthick, K. (2012). Embedded controller for vehicle in-front obstacle detection and cabin safety alert system. International Journal of Computer Science & Information Technology (IJCSIT), 4(2), 117-131.

[2] Chen, P., & Jiang, X. (2008). Design and implementation of remote monitoring system based on GSM. Computational Intelligence and Industrial Application, 1, 678-681.

[3] Surendra, K., Suman, K. R., & Raj, P. (2014). Biometric authentication based vehicular safety system using arm processor. International Journal of Engineering Science & Advanced Technology (IJESAT), 4(5), 410–413.

[4] Alexe, A., & Ezhilarasie, R. (2011). Cloud computing based vehicle tracking information systems, International Journal of Computer Science and Technology, (IJCST), 2(1), 67-75.

[5] El-Medany, W., Al-Omary, A., Al-Hakim, R., Al-Irhayim, S., Nusaif, M. (2013). A cost effective real-time tracking system prototype using integrated GPS/GPRS module," International Journal of Computer Science, Engineering and Applications (IJCSEA), 3(3), 20–25.

[6] Joel, S., & Kiran, R. G. (2016). Anti-Theft System For Vehicles Using Fingerprint Sensor. International Journal of Scientific & Engineering Research, 7(7), 1436 – 1441.

[7] Kiruthiga, N., Latha, L., & Thangasamy, S. (2015). Real-time biometrics based vehicle security system with GPS and GSM technology. Procedia Computer Science 47, 471–479

[8] Brijet, Z., Santhoshkumar, B., & Bharathi, N. (2016). Vehicle anti-theft system using fingerprint recognition technique. Journal of Chemical and Pharmaceutical Sciences, 9, 78–82.

[9] Ajay, S. P., Sayli, A. P., Shrinath, B. P., & Vishal, M. (2016). Fingerprint authorization based license checking system for auto-mobile. International Journal on Recent and Innovation Trends in Computing and Communication, 4(4), 487 – 492.

[10] Saritha, A. & Arun, P. (2018). Fingerprint-based security system for vehicles. International Journal of Advance Research, Ideas and Innovations in Technology (IJARIIT), 4(4), 370–372.

[11] Garba, S., Salako, E. A., Abdulraheem, O. U., & Lawal, A. L. (2019). Examination impersonation system (EIS) using fingerprint biometric technique: case study of FCT College of Education, Zuba-Abuja. Proceedings of the 3rd International Conference on Intelligent Computing and Emerging Technologies (ICET-2019), School of Computing and Engineering Sciences, Babcock University, Nigeria, 3, 46–53.