Simulation and Construction of Fingerprint Vehicle Starter System Using Microcontroller

Samson Dauda Yusuf [*1], Ahmed Dalhatu[2], Ibrahim Umar[3], Abdulmumini Zubairu Loko[4]

[1,3,4]*Department of Physics, Nasarawa State University Keffi, Nigeria*

[2]*ICT/Technical Service Department, News Agency of Nigeria, Abuja, Nigeria*

**Correspondence*

Abstract: **The rising number of vehicle thefts is becoming an issue particularly in Nigeria where the security system is porous. Vehicle security system has become very important and vital in providing personal security for our cars. In this study, simulation and construction of a fingerprint vehicle starter system was carried out using Arduino Uno ATmega328 microcontroller. The circuit was simulated using Proteus ver8.0 via Arduino compiler programming language using embedded C language. The stages of the circuit consisting of regulated power supply, fingerprint module, microcontroller, LCD, motor output driver, and buzzer unit. The hardware prototype of the circuit was constructed on a PCB board and performance evaluated test was carried out with 150 trials in 5 stages, with 4 authorized users and 1 unauthorized user. The specificity, sensitivity and accuracy of the device was calculated. Results shows that, the sensitivity, specificity and accuracy were 96%, 97% and 97%. This implies that finger print vehicle detector will correctly accept and give access to 96% authorized users, correctly deny 97% unauthorized users, but will fail to accept 4% authorized users, and give access to 3% unauthorized users. Also, vehicle starting using the constructed device is only successful for authenticated users and we are 97% sure. Evaluation carried out under the measured performance metrics were able to be compared and analyze distribution scores of both authorized and unauthorized users with satisfactory result. The device can be recommended for vehicle security and other similar operations.**

Keywords: **Fingerprint module, vehicle starter, microcontroller, motor driver, Proteus design suit, Arduino Uno**

I. INTRODUCTION

The development of steam engine is one of the greatest technology of the 17th century and is the iconic invention of the industrial revolution [1, 2]. Though cars are an expensive commodity but they keep us on the road safely, gives us convenience, as well as style. Though, keys ought to be carried about and misplacing keys or losing them will result to multiple users using the vehicle without the owner's consent, or the car can be stolen if it falls in the wrong hands. In addition, keys may be duplicated and with the rising statistics of car theft, one tends to wonder if we are offering our cars enough protection [3]. In 2020, New Zealand had the highest car theft rate worldwide, with 1,172 occurrences per 100,000 inhabitants, followed by Uruguay, Italy and the United States [4]. In 2020 about 810,400 vehicles were stolen in the US amounting to $7.4 billion lost and there were 229,339 vehicle thefts with keys between 2016 and 2018 [5]. According to Kuadli [3], car break grew in statistics by 9% in 2018 In the UK, and between 2015 and 2017, 697,000 motor vehicles were stolen in the EU.

In the case of Nigeria, data from the National Bureau of Statistics (NBS) has shown that 2,544 vehicles were stolen between 2013 and 2015, out of which only 1,377 vehicles were recovered, while the unrecovered 1,167 stolen vehicles amounted to a loss of about N1.8 billion to the vehicle owners [6]. In addition, the level of insecurity is growing in an alarming rate as statistics have shown that as of March 2022, Nigerians reported to be most worried about muggers and robbers at a concern level about 66.04 points, while worries about car stolen stood at 59.92 points on a scale from zero to 100 [7]. Thieves are constantly devising new and sophisticated means and tactics of stealing autos including acquiring smart keys, which eliminated hot-wiring to steal cars; switching vehicle identification numbers; and using stolen identities to secure loans for expensive vehicles [5]. Even though, keys are being gradually replaced by push start buttons [8], automobile security system still remains an essential deal in this present days [9]. There is need for a more robust security in form of personal security system that is cheap and efficient to safeguard our vehicles from unauthorized access and thefts.

The uses of biometric based system have been in the increase especially in security systems where they are used to provide secured access to major functioning systems like ATM, cellular phones, cars, laptops, offices, and other systems that need authorized access [10]. Biometric have made significant changes in security systems because its chances of being duplicated are very less, relatively easier to maintain, efficient, and cheap, as such, making them more secure than before [10, 11]. Many methods are used in Biometrics, but the most important are: Palm, Fingerprint, Iris, Voice, and Face [12]. However, fingerprint sensors are quite cheap in comparison to other biometric sensors and they are relatively easier to maintain [13]. The biometric fingerprint security system is widely used due to its accurate identification, easy to use, low cost, high performance, customizable and reliability [14]. The use of biometric-based security for automotive industry ensures that car hijacking or snatching on highway, car theft due to easy access to a car's functional system can be reduced by using a biometric system for starting the car's engine as protection and access restriction [15]. The objective of this study is to simulate and

construct a fingerprint vehicle starter system using a microcontroller. Since naturally each person's fingerprint is different to another, the system will only allow authorized users to start the vehicle [16]. The study will be significant to individual vehicle owners for a more secured and reliable vehicle security system that economically cuts the technology cost and reduce car theft.

II. MATERIALS AND METHODS

A. Materials

The materials and their specification that were used for the simulation and construction of fingerprint vehicle starter system includes microcontroller ATMega328, IC7805 voltage regulator, IC L293D motor driver, 5V dc motor, BC547BP transistor, 5V piezoelectric buzzer, DT830D digital multimeter, computer laptop, 175x67x8mm Bread board, 100x86mm PCB, 116MHz clock, R305 fingerprint sensor, 12V battery, 2-30A relay, LCD LM16X212 display, Arduino Uno board, and Proteus 8.0 software.

B. Methods

The methods for implementation of the fingerprint vehicle starter system was carried out in three (3) parts including software design, hardware construction and circuit analysis (testing).

B.1 Software Design Method

The software design for the system includes circuit simulation, algorithm, flow chart, and choice of programming language.

B.1.1 Simulation Method

The simulation of the fingerprint vehicle starter system was carried out in Proteus ver8.0. The process was carried out according to the block diagram shown in Fig. I. The stages in the implementation includes regulated power supply, fingerprint module, microcontroller, LCD display, motor output driver, and buzzer unit.

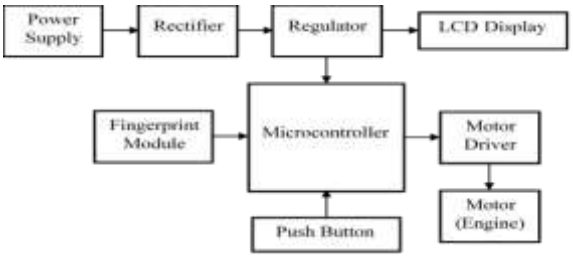

Fig. I Block Diagram of the proposed system

1) Power Supply Unit: The power supply is an electrical device that supplies electric power to an electrical load. The voltage from the main source is 220V AC but some sections of the circuit will need 5V DC. Therefore, a step-down transformer is needed to get 12V AC from 220V which can be rectified to 12V DC using a rectifier. The result of the rectifier still comprises of some distortions despite that it is a DC signal and as such it is called as fluctuating DC. The ripples will be removed to realize a smoothened signal using DC power filter circuits. 12V is used to power the relay/motor unit with 12V but regulated to 5V to power the microcontroller. The power supply unit is shown in Figure II.

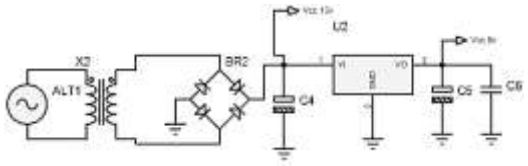

Fig. II The regulated power supply unit

2) The Fingerprint Module Unit: The fingerprint sensor/ module is an electronic device used to capture a digital image of the fingerprint pattern [17]. Types are; optical, capacitive, mechanical, thermal and dynamic output constructed in either stagnant or moving form. An optical biometric fingerprint reader (R305) module with TTL UART interface for direct connections to a 3.3v or 5v microcontroller was used in this work. The user can store the fingerprint data in the module with the aid of a powerful Digital Serial Port (DSP) in its core and can be configured in 1:1 or 1: N mode for identifying the person. We can communicate with it using a packet of hex codes in a specific format but commands for operation can vary from module to module. Pins 1 – 4 are for serial communication with default baud rate of 57600bps. Pins 5 – 8 are for USB communication [18, 19]. The module pins function is shown in Table I. The module has power DC 3.6V-6.0V, working current 100mA, character file size: 256 bytes, image acquiring time: <0.5s, storage capacity: 256, security level: 5 (low to high: 1, 2, 3, 4, 5), False Accept Rate (FAR): <0.001%, False Reject Rate (FRR): <0.1%, average searching time: < 0.8s, window dimension: 18mm*22mm, baud rate is (9600*N) bps, N = 1 – 12 (default N = 6). Therefore, user may set the baud rate in 9600 – 115200bps [19, 20]. The fingerprint module unit is shown in Fig. III.

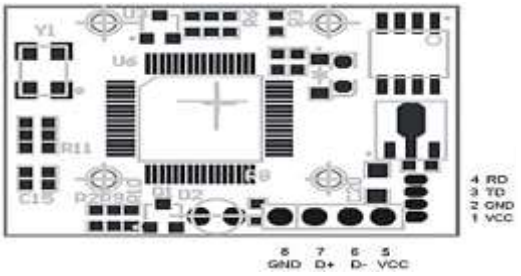

Fig. III The R305 fingerprint module unit [18]

Table I. The R305 Module Pins Function [18]

Pin No.	Name	Function
1	VCC	Power Input
2	GND	Signal Ground
3	TD	Data Output TTL Logic
4	RD	Data Input TTL Logic
5	VCC	+5 VDC
6	D-	Data -
7	D+	Data +
8	GND	Ground

3) Liquid Crystal Display Unit: The Liquid Crystal Display (LCD) screen is an electronic display module. A 16x2 LCD display LM16X212 was used. It displays 16 characters per line and there are 2 such lines. Each character is displayed in 5x7 pixel matrix. The 16x2 intelligent alphanumeric dot matrix display is capable of displaying 224 different characters and symbols [21]. This LCD has two registers, namely, Command and Data registers. Command register accepts and stores various commands or instructions given to the LCD while data register stores data to be displayed by the LCD. In Arduino project, Liquid Crystal Library simplifies the process of controlling the display, hence, there is usually no need to know the low-level instructions [22]. However, the contrast of the display can be adjusted by adjusting the potentiometer to be connected across VEE pin. The LCD is used in this study to displays the state of the motor and user authentication. Fig. IV shows the 16x2 LCD unit.

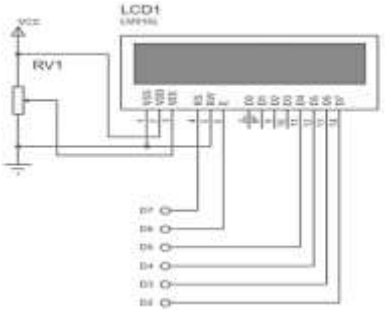

Fig. IV The LCD LM16X212 Unit

4) The Buzzer Unit: This is an audio signaling device, which may be mechanical, electromechanical, magnetic, electromagnetic, electroacoustic or piezoelectric [28]. An active buzzer, piezoelectric type, which will buzz at a predefined frequency (2300 tolerance of 300Hz) on its own when a steady DC power is applied, is used in this work since its element may be driven by an oscillating electronic circuit or another audio signal source, driven with a piezoelectric audio amplifier. A beep will indicate unauthorized, or unregistered or unauthenticated fingerprint. The buzzer circuit is shown in Fig. V.

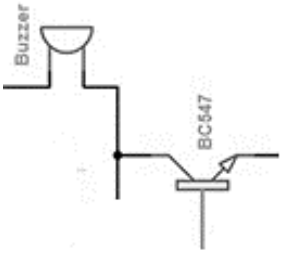

Fig. V The buzzer unit

5) The Microcontroller Unit: The Arduino is an open source platform used for building electronics projects, it consists of a physical programmable circuit board (often referred to as a microcontroller) and a piece of software, or IDE (Integrated Development Environment) that runs on your computer, used to write and upload computer code to the physical board. The Arduino IDE uses a simplified version C++, making it easier to learn the program [23]. In this work, the Arduino Uno based on Atmel ATmega328P was used. It is a high performance, low power, 32K 8-bit microcontroller based on the AVR architecture. Comprising 131 instructions executed in a single clock cycle, providing a throughput of almost 20 MIPS at 20MHz. It comes in a PDIP 28 pin package suitable for use on our 28 pin AVR development board. It has 32kB of programmable flash, 1kB of EEPROM, 2kB SRAM, 10,000 write and erase cycles for flash and 100,000 for EEPROM, and data retention for 20 years at 85°C and 100 years at 25°C [24]. The microcontroller unit is shown in Fig. VI.

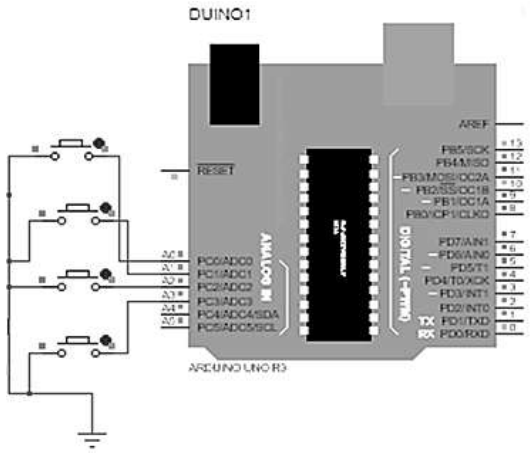

Fig. VI Atmel ATmega328P Microcontroller unit

6) The Motor Output Driver Unit: The motor driver is a device or group of devices that serves to govern in some predetermined manner the performance of an electric motor. It is an integrated chip that is usually used to control motors in autonomous robots. It acts as an interface between Arduino and the motors [25]. A Motor Driver IC L293D was used in this system. It is a dual H-bridge motor driver integrated circuit (IC). Motor drivers act as current amplifiers since they take a low-current control signal and provide a higher-current signal. This higher current signal is used to drive the motors [26, 27]. A simple 5V DC motor used in this work to serve as an illustration of vehicle to generate rotational motion. The circuit diagram of the motor output driver is shown in Fig. VII.

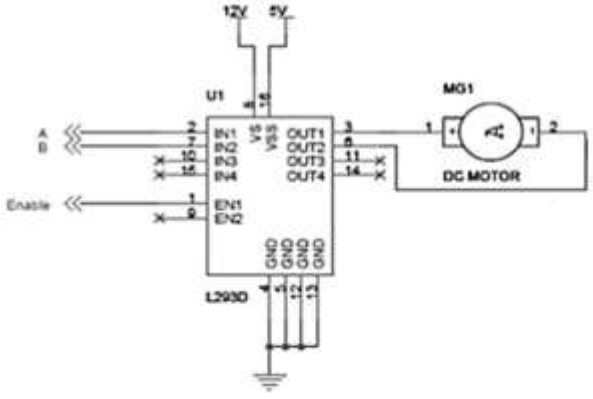

Fig. VII The Motor driver IC L293D [27]

B.1.2 Flowchart

The flowchart for the fingerprint vehicle starter system is shown in Fig. VIII.

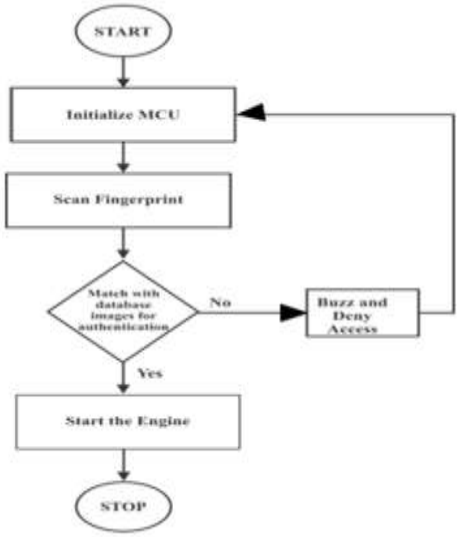

Fig. VIII Flowchart of the proposed System

B.1.3. Algorithm

The algorithm that explains the flowchart for the fingerprint vehicle starter system is presented as follows:

1. Start
2. Press Enter button
3. Place finger to scan fingerprint
4. If the image match with pre-loaded image, then start the engine
5. If not, go back to no.1 and give no output
6. Stop

B.1.4. Choice of Programming Language

The basic software program is written via the Arduino programming language using embedded C language. The choice of C language programming was chosen because it is more compatible with the Arduino programming software. This is widely used in programming language for embedded microcontrollers. C language is also used mainly to implement those portion of the code where very timing accuracy, code size efficiency are key requirements.

B.1.5. Fingerprint Registration

In setting up the input of the fingerprint, a fingerprint must be registered (entered) twice by the same finger. The two are stored as a template, to improve the system's fault tolerance [29]. In the two entry process, in case the deviation of the contact occurs in the fingers and the entry slot becomes too large, the system will deny registration and consider them as a different fingerprint. Also if two finger entry positions change a little, the system may collect them exactly as same fingerprint and deny the registration.

B.1.6. Fingerprint Detection

The fingerprint detection method in this study is the pattern and minutia algorithms method, where the fingerprint pattern is determined by the pattern algorithm from one of the three options; an arch, a loop, or a whirl. The fingerprint ridges themselves are analysed by the minutia algorithm, which involves ridge endings, or where the ridges end, bifurcation, or where ridges split, whether short or dot ridges, which are shorter than the average ridge size. According to Maio and Maltoni [30], automatic minutiae detection is an extremely critical process, especially in low-quality fingerprints where noise and contrast deficiency can originate pixel configurations similar to minutiae or hide real minutiae. Although, different from each other, all these methods transform fingerprint images into binary images. Comparing with original technique, based on ridge line following, the minutiae are extracted directly from gray scale images and the results achieved are compared. Despite a greater conceptual complexity, the method performs better in terms of efficiency and robustness.

B.2. Hardware Construction Method

The circuit construction was carried out in stages according to the block diagram shown in Figure I. The components were first assembled on electronics breadboard to ensure proper terminal connections and then transferred on to a PCB board for permanent soldering using the soldering iron and MBO 1mm wire lead solder, +183°C melting point. However, too much Lead was avoided to prevent clumsiness and bridging of the component to each another.

B.3. Circuit Testing Method

Components testing was carried out before fixing them on the PCB board. Also Continuity test and Power ON test were carried out during construction to ensure proper functioning of the circuit and to ensure that no components in the circuit undergo heating when the device is in use and also to avoid loading and impedance mismatch of one stage and another.

B.3.1. Continuity Test

This test is performed to find any electrical open paths in the circuit after the soldering. The continuity test was carried out to make sure no cable or line jammed and all lines have free flow of electrons. It helps the researcher to check and see if current flows in the constructed circuit or the lines are continuous. The test can be performed by using a multi meters which measure current and specialized continuity testers which are cheaper, or generally with a simple light bulb that lights up when current flows or even a piezo electric speaker. If electron flow is inhibited by broken conductors, damaged components, or excessive resistance, the circuit is "open". We used a multi meter to perform this test in this study.

B.3.2. Power ON Test

This test is carried out to ascertain whether the voltage at the different terminals is according to the requirement or not. It was carried out without microcontroller to protect the

microcontroller from damage by any excessive voltage and possible heat [31]. In this study, a multi meter was used to carry out this test.

B.3.3. Performance Evaluation Test

The performance evaluation was carried out to ascertain the functionality of the constructed device. This was carried out to test the working condition of the fingerprint module for various authentication conditions and the true positive, false negative, true negative and false positive were determined.

True Positive (TP) = Number of authorized users that are correctly accepted by the system.

False Negative (FN) = Number of authorized users that are incorrectly denied by the system.

True Negative (TN) = Number of unauthorized users that are correctly denied by the system

False Positive (FP) = Number of unauthorized users that are incorrectly accepted by the system

The result obtained was used to calculate specificity, sensitivity and accuracy of the device as follows:

Specificity, $S_p = \frac{TN}{TN+FP} \times 100$ (1)

Sensitivity, $S_e = \frac{TP}{TP+FN} \times 100$ (2)

Accuracy, $Acc = \frac{TP+TN}{TP+FN+TN+FP} \times 100$ (3)

III. RESULTS

A. Simulation Result

The Simulation was carried out in stages according to the block diagram in Fig. I to observe the behavior at different levels and finally carried out on the full schematic system and the results are presented in Fig. IX to XII.

Figure IX is the simulation result showing the complete circuit at initialization stage when powered ON with the LCD displaying ‘’fingerprint-based car access’’. The probe between V1 and BR1 shows 12.17Vac input that is fed to the rectifier circuit. Another probe between D3 and voltmeter indicates 4.85Vdc output to the other parts of the system, the same with the voltmeter display. The probe at the base terminal of the transistor indicates 2.303V. LED D3 glows to indicate voltage output. Other indicators blue, grey and red colors indicate signal flow. An Analog graph can be observed at the left bottom indicating a sinusoidal signal of the input voltage and next is a digital graph displaying output DC voltage on load from the regulator at approximately 4.8Vdc.

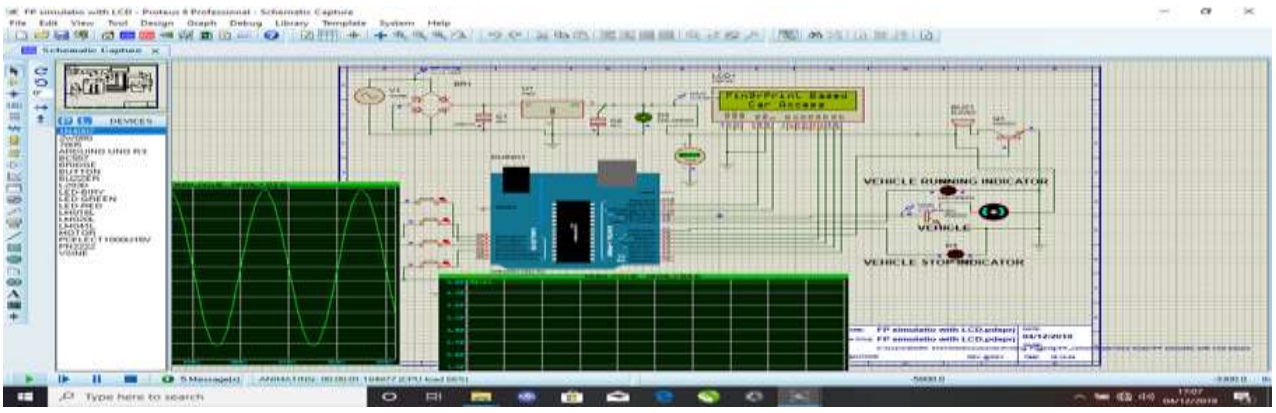

Fig. IX simulated general circuit in idle state initializing

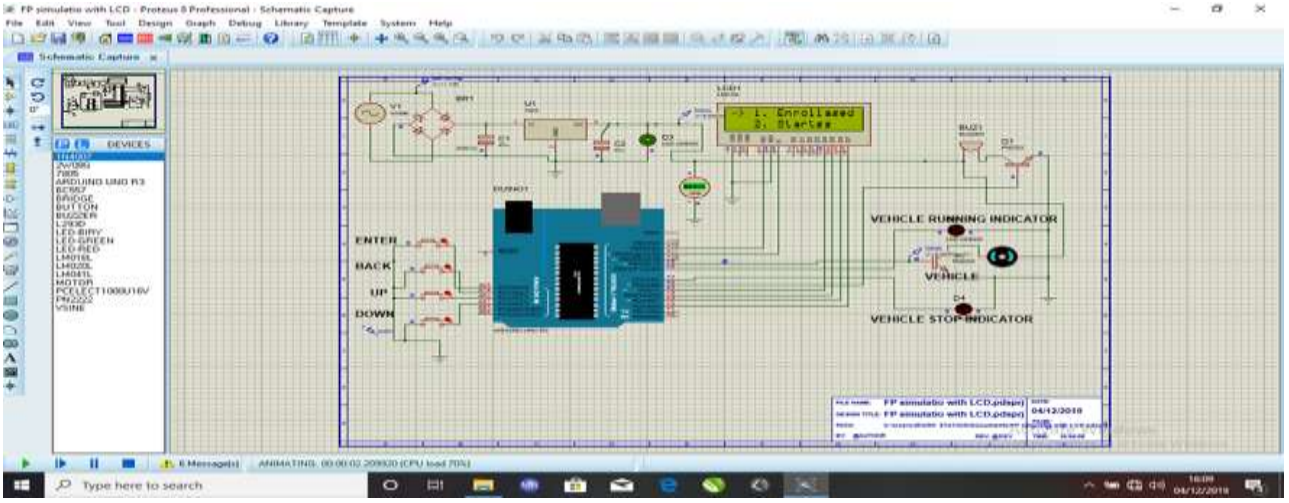

Fig. X simulated result showing system menu

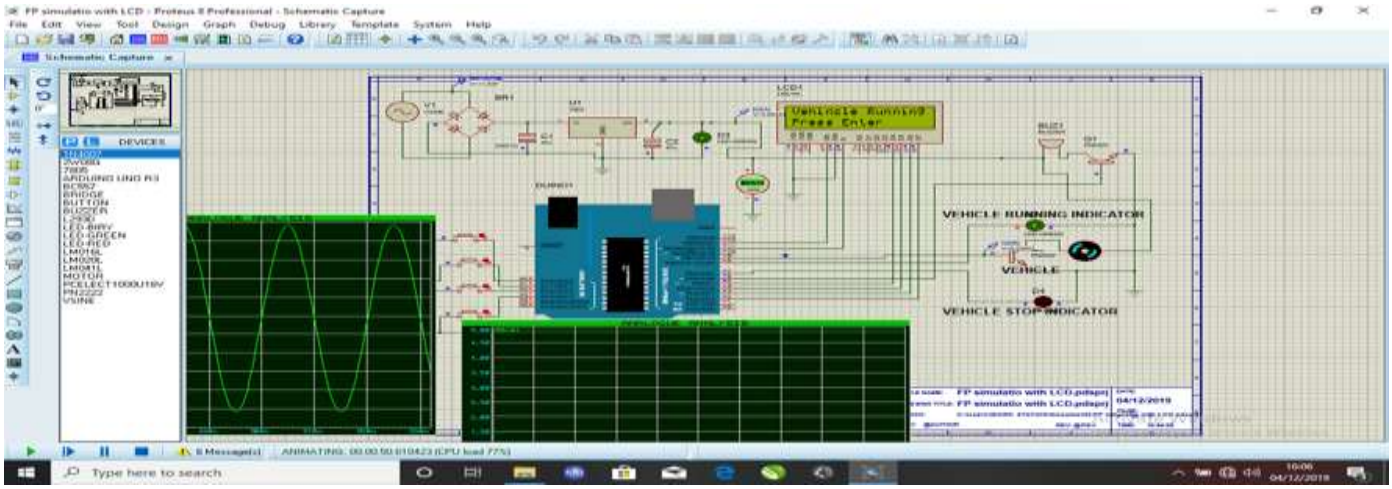

Fig. XI simulated result showing authorized user

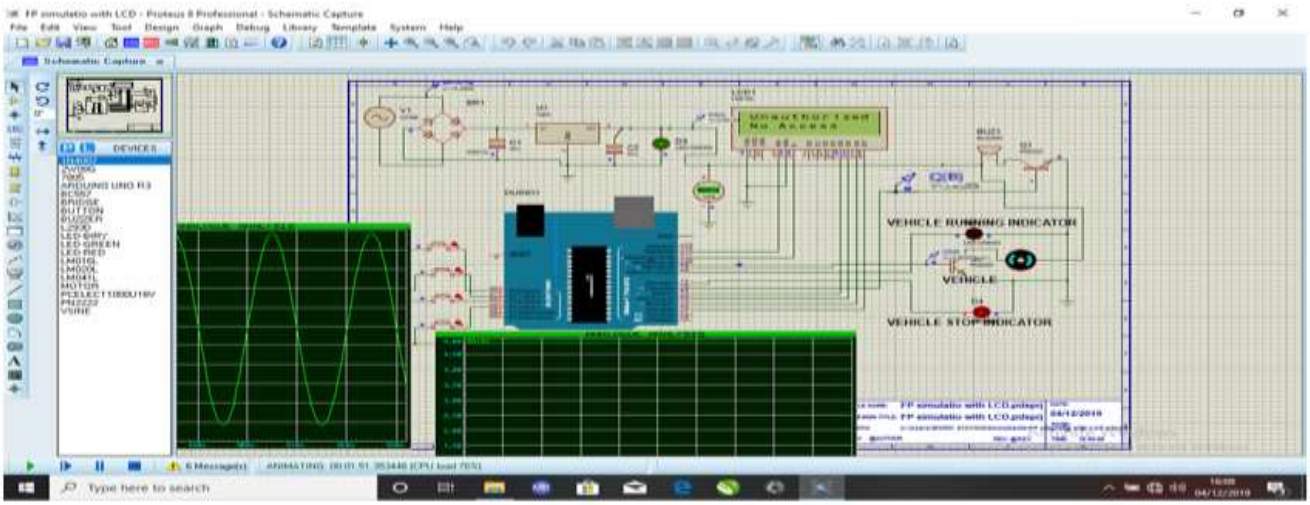

Fig. XII simulated result showing unauthorized user

Fig. X presents the simulation result of the system menu for selection between Enroll and Start. Enroll is when you intended to register the user(s) while start is when a user(s) intended to operate the vehicle either to start or to stop it. The arrow indicates the direction of start. It can be redirected between start and enroll by using Up and Down push bottom switches. At this very moment, the motor remains stationary.

Fig. XI presents the simulated result of authorized user showing vehicle running when the system has authenticated an authorized user and started the vehicle. The user selects ‘’Start” from the menu by pressing Enter switch, capture the fingerprint by placing a finger on the scanner and the system compares the captured fingerprint with the image stored in its memory, if a match is found, it then displays “authenticated” and allow the user to start the vehicle.

Fig. XII presents the simulated result of unauthorized user showing vehicle stop when the system has denied an unauthorized user and the vehicle refused to start. The system compares the captured fingerprint with the image stored in its memory, if no match is found, it then displays “user not authorized”, denies the user to start the vehicle and the buzzer sounds.

B. Hardware Construction

B.1 Circuit Construction

The construction was carried out first on a bread board to ensure that the circuit is working as required, then transferred to the PCB board for permanent soldering. The constructed circuit showing the top view of the device on PCB board with user authenticated and user not authorized is shown in Fig. XIII and Fig. XIV.

Fig. XIII Top view showing user authenticated

Fig. XIV Top view showing user not authorized

B.2 Casing and Packaging

A casing measuring 15cm x 15cm x 5cm was finally provided to the system for mechanical protection. It is provided with 5no. of 0.5cm diameter hole for the push bottom switches (Enter, Back, Up, On and Reset), 4no. of 0.25cm diameter hole within 0.5cm diameter groove the edges of its top side for screw lock, 1no. of 0.5cm diameter hole for the power switch tighten by 1.5cm diameter nut and 1no. of 1cm diameter hole for the motor tighten by 2cm diameter nut. Others are 2no. of 0.25cm diameter hole spaced apart 0.5cm for LED indicators (Red for power and Yellow for DC motor), 1no. of 7cm x 2.3cm hole for LCD and 1no. of 3cm x 2cm hole for the Fingerprint sensor. Finally, provision has been made for the system ventilation. The complete isometric diagram of the casing showing its three views (Front, Side and Top) and the various dimensions is shown in Fig. XV, while the complete packaged device with full casing showing its top and side view is shown in Fig. XVI.

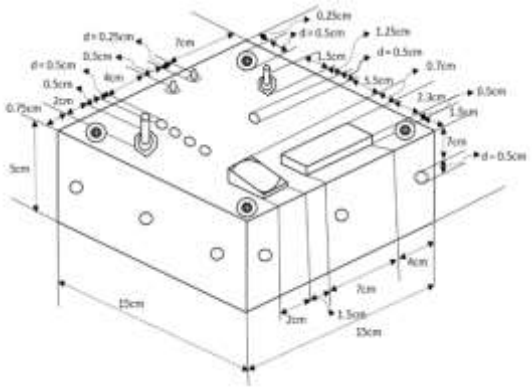

Fig. XV The isometric diagram of the casing

Fig. XVI Top view of complete packaged device with full casing

C. Testing and Analysis

C.1 Continuity Test

In this study, the multi meter was used to perform this test. The multi meter was set at the continuity mode and the two ends of the probe was placed at the ends of a particular wire that is being checked for continuity, if there is a negligible resistance between the ends of the wire or path or the multi meter buzzer sounds then, the ends or path is continuous. Test results shows that the soldering was perfectly done as there were no short circuits along the paths, or broken conductors, damaged components, or excessive resistance along the circuit.

C.2 Power ON Test

In this test, we took a multi meter and put it in voltage mode and the output of the transformer was checked for 12V AC. This voltage was then applied to the power supply circuit and the output of voltage regulator was checked and ascertained to be 5V output. This 5V output is fed to the microcontroller at the 40th pin. The voltages at the other terminals were also checked and ascertained to be as required from the specification in the simulated circuit.

C.3 Performance Evaluation

To ascertain the functionality of the constructed device a performance evaluation test was carried out for various authentication conditions i.e. authorized and none authorized users. Multiple users (up to 162) can be registered and unregistered whenever the need arises through id No. or by resetting the system, like in the case of a change of car ownership. However, five (5) fingerprints (four (4) authorized and one (1) unauthorized users) were selected at random to operate the system. A total of 150 trials were made in 5 different stages of 10, 20, 30, 40, and 50 trials. The number of true positive (TP), false negative (FN), true negative (TN), and false positive (FP) were recorded and presented in Table II.

Table II. Performance Evaluation Test Result

Stage	No. of Trials	True +ve (TP)	False – ve (FN)	True – ve (TN)	False +ve (FP)
1	10	10	0	10	0
2	20	20	0	20	0
3	30	30	0	30	0
4	40	38	2	39	1
5	50	46	4	47	3
Total	150	144	6	146	4

Table II presents the outcome of performance analysis. It was observed that out of 150 trials in 5 stages, the TP was 144, FN was 6, TN was 146, and FP was 4. These result was used to calculate specificity (Sp), sensitivity (Se) and Accuracy (Acc) and the results are presented as follows:

For the Specificity test, equation 1 was used as follows:

$S_P = \frac{\text{[illegible]}}{\text{[illegible]}} \times 100 = 97\%$

For the Sensitivity test, equation 2 was used as follows:

$S_e = \frac{\text{[illegible]}}{\text{[illegible]}} \times 100 = 96\%$

Also for the Accuracy test, equation 3 was used as follows:

$Acc = \frac{\text{[illegible]}}{\text{[illegible]}} \times 100 = 97\%$

Further analyses were carried out to compare TP and TN and the result is presented in Fig. XVII.

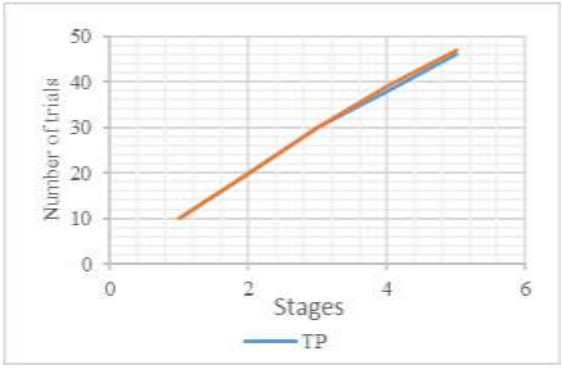

Fig. XVII Comparison between true positive and true negative

The comparison between TP and TN rates as indicated in Fig. XVII shows that for the five (5) selected users making 7 attempts each which is 35 trials, the system was observed to be very significant in user authentication. However, immediately after 35 total trials, the system starts miss-authenticating users. This behavior is an indication of the system threshold. However, as more trials increases, fewer imposters' attempts will be falsely considered matches, at the same time more genuine attempts will be falsely classified as non-matches. This means that the system can take a maximum of 35 users conveniently.

D. Comparison with Other Fingerprint Algorithm Detection

The present system was compared with previews studies on fingerprint detection and the results are presented in Table III and IV. Comparing the threshold, storage capacity and speed with similar module is shown in Figs. XVIII, XIX and XX.

Table III. Comparison Between R305 And R307 Module

Fingerprint Module	R305	R307
Storage Capacity (Fingerprints)	250	1,000
False Accepted Rate (FAR)	≤0.0001%	<0.001%
False Rejected Rate (FRR)	≤0.1%	<1.0%
Work environment	-20 to 55℃	-20 ℃ - +40 ℃
Scanning speed	<0.5 second	<0.3 seconds
Template size	512bytes	512bytes
Security Level	5 (1, 2, 3, 4, 5 (highest))	5 (1, 2, 3, 4, 5 (highest))

Table IV. Comparing Present System with Other Fingerprint Algorithms Detection

Fingerprint Application	**Sensor Module**	**Micro-controller**	**GSM/GPRS**	**Threshold Value Set**	**Fingerprint Application**	**Specificity**	**Sensitivity**	**Accuracy**
Present Study	R305	ATmega 328	×	30%	Vehicle Starter	✓	✓	✓
Jain et al [15]	✓	PIC 18F4620	✓	Unstated	✓	×	×	×
Gill & Sachin [11]	✓	AT89S52	✓	Unstated	✓	×	×	×
Brijet et al [10]	✓	ATmega 328	✓	Unstated	✓	×	×	×
Ingashitula [32]	✓	ATmega 328	×	Unstated	Exam Hall Authentication	×	×	×
Vaishnavi et al [33]	R307	PIC18f4520	×	25%	Educational System	×	×	×
Swaroop et al [34]	✓	PCF8574	✓	Unstated	Access Door	×	×	×

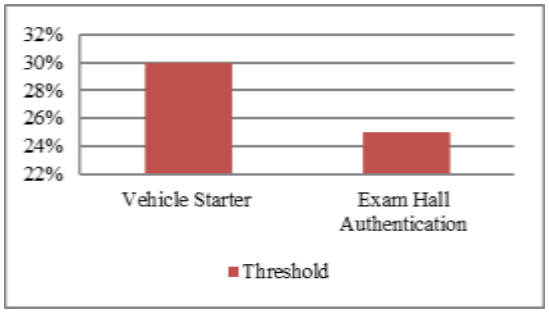

Fig. XVIII Comparison between thresholds

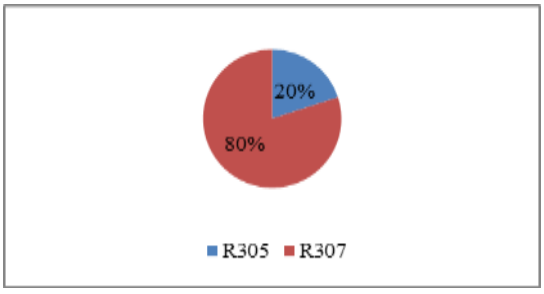

Fig. XIX Comparison between storage capacities

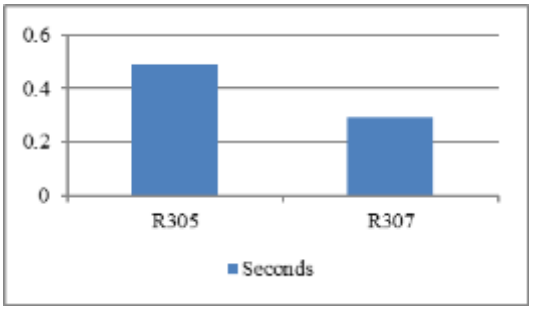

Fig. XX Comparison between speeds

IV. DISCUSSION

The constructed fingerprint vehicle starter subjected to various test have revealed vital information that ascertain its functionality. The continuity test revealed that the circuit was continue with no short circuits along the paths, or broken conductors, damaged components, or excessive resistance along the circuit and the soldering was ok. While the power ON test shows that, the voltage at the different terminals was according to the requirement and specification of the simulated circuit. Prototype was tested beyond reasonable doubt and found worthy to be implemented by car owners for vehicle protection. The device performances in terms of security level expectation is highly sensitive in authenticating authorized users, but it can neither track your vehicle nor arrest the thief.

The design is similar to that of Jain et al. [15] who designed and developed a fingerprint-based car ignition system using a fingerprint module and microcontroller, Brijet et al. [10] who developed a vehicle anti-theft system using fingerprint recognition technique and microcontroller, Ingashitula [32] who designed a fingerprint based exam hall authentication systems, though, his design was to assist in the elimination of examination impersonation, while the present study is on automobile users. Also, Gill and Sachin [11] developed a vehicle ignition system using a fingerprint sensor. Although, their system can either send an SMS or an email or give a call when someone tries to access the vehicle illegally, while the present study only employed a buzzer.

For the performance analysis on the device, findings from this study has revealed that the sensitivity, specificity and accuracy were 96%, 97% and 97%. This implies that finger print vehicle starter will correctly accept and give access to 96% authorized users, correctly deny 97% unauthorized users but will also fail to accept 4% authorized users, and give access to 3% unauthorized users. In addition, with an accuracy of 97%, we can say that vehicle starting using the constructed device is only successful for authenticated users and we are 97% sure. Performance evaluation has also revealed that the system can take a maximum of 35 users conveniently. Therefore, the device is found worthy to be implemented by car owners for personal vehicle security and protection against thefts. This can be a better substitute for key, push button, smartcard and password. The present study differs from all the previous studies in the addition of performance evaluation to calculate specificity, sensitivity and accuracy which was not done in previous studies. This reveals the additional contribution of this work to the existing literature.

However, this does not guarantee 100% security considering treats associated with single biometrics, such as spoofing, hacking, and non-universal biometric traits [35]. The observed errors of false rejects and false accepts could be due to some people have biometric features that were either hard to capture because of worn friction ridges following manual labour, dry skin due to cold weather and skin diseases or show few indications of unique characteristics like few minutiae in the ridge pattern, scar contours and edges, and failure to present finger proper part. For instance, the top of fingers has fewer characteristic structures. In addition, the vehicle may not be used in case of an emergency where the authorized user is incapacitated to start the system. The device may also develop a fault that can lead to memory loss and improper functioning due to electrical faults in the vehicle system.

VI. CONCLUSION

This study focused on vehicle security system using a simple biometric structure to protect vehicle owners from unauthorized access to their automobile. The fingerprint sensor match will activate the relay that controls the ignition system. It provides authentication to users and only genuine users can be permitted to start the vehicle. The system can be a better substitute for Key, smartcard and password, which could not eliminate impersonation. The device was simulated, prototype was constructed, tested and obtained satisfactory results. The system's performance was evaluated using a statistical measure for the performance of a binary classification test. Its future applications could be achieved in many areas for developing very high-security systems. These areas may include access control system, punch card system, ATM system, bank locker system, and vehicle's electronic safe.

REFERENCES

[1] Gambino M. A Salute to the wheel. Smith Sonian Magazine 2009. [Online]. Available: www.smithsonianmag.com/science-nature/a-salute-to-the-wheel-31805121/.

[2] Wilde R. Steam in the Industrial Revolution. Thought Co 2019. [Online]. Available: https://www.thoughtco.com/steam-in-the-industrial-revolution-1221643.

[3] Kuadli J. 25 Car Theft Statistics to Keep Your Ride Safe in 2022. Legal Jobs 2021. [Online]. Available: https://legaljobs.io/blog/car-theft-statistics/.

[4] Szmigiera M. Car theft rate globally 2018, by country. Statista 2021. [Online]. Available: https://www.statista.com/statistics/1238378/car-theft-rate-country/#statisticContainer.

[5] Insurance Information Institute (2022). Facts + Statistics: Auto theft 2022. [Online]. Available: https://www.iii.org/fact-statistic/facts-statistics-auto-theft.

[6] Sule T. Only 5 of every 10 stolen vehicles are recovered in Nigeria. Business Day 2016. [Online]. Available: https://businessday.ng/uncategorized/article/5-every-10-stolen-vehicles-recovered-nigeria/.

[7] Statista. Levels of concern related to different crimes in Nigeria as of March 2022. [Online]. Available:

https://www.statista.com/statistics/1200186/levels-of-worry-related-to-different-crimes-in-nigeria/.

[8] Susarla M, Akhil C, Reddy A, Rizwana S. Vehicle Ignition Using Biometric Data. Journal of Network Communications and Emerging Technologies (JNCET) 2018;8(5):21-23.

[9] Sundar R, Hebbar S, Golla V. Implementing intelligent traffic control system for congestion control, ambulance clearance, and stolen vehicle detection. IEEE Sensors Journal 2014;15(12):1109-1113.

[10] Brijet Z, Kumar BS, Bharathi N. Vehicle Anti-Theft System Using Fingerprint Recognition Technique. Open Academic Journal of Advanced Science and Technology 2017;1(1):36-41. DOI: 10.33094/5.2017.11.36.41.

[11] Gill KR, Sachin J. Vehicle Ignition using Fingerprint Sensor. International Journal for Innovative Research in Science & Technology (IJIRST) 2016;2(12):357–363.

[12] Ghayoumi M. A review of multimodal biometric systems: Fusion methods and their application. In Proceedings of the IEEE/ACIS 14th International Conference in Computer and Information Sciences (ICIS) 2015;131-136.

[13] Yang W. Security and Accuracy of Fingerprint-Based Biometrics: A Review. MDPI 2019. [Online]. Available: https://www.mdpi.com/2073-8994/11/2/141/pdf.

[14] Dermalog. The Fastest AFIS in the World 2019. [Online]. Available: http://dermalog.com/products/software/fingerprint-identification/?gclid=EAlalQobchMlr7rZgL.

[15] Jain A, Goswami A, Joshi P, Nag P, Saxen G. Design and development of fingerprint based vehicle starting system. National Journal of Advanced Research 2017;3(1):39-41.

[16] Townsend AM. Smart cities: Big data, civic hackers, and the quest for a new Utopia. W. W. Norton & Company, New York, USA, 2013, 1285.

[17] Pandit VR, Joshi KA, Bawane NG. ATM Terminal Security using Fingerprint Recognition. International Journal of Applied Information Systems (IJAIS)–ISSN 2249-0868 2013;14-18.

[18] Rhydolabz. Finger Print Sensor (R305) -TTL UART 2019. [Online]. Available: https://www.rhydolabz.com/miscellaneous-other-widgets-c-205_124/finger-print-sensor-r305-ttl-uart-p-1085.html.

[19] Sumit Electronics & Electricals. Finger Print Scanner R305. "India Mart" 2022. [Online]. Available: https://www.indiamart.com/proddetail/finger-print-scanner-r305-20147423648.html.

[20] Electro Peak. R305 Optical Fingerprint Scanner Sensor Module 2019. [Online]. Available: https://electropeak.com/optical-fingerprint-module-r305.

[21] Novoselov P, Aubert JE. Display device control method. U.S. Patent No. 9,589,530. Washington, DC: U.S. Patent and Trademark Office 2017.

[22] Atayero AA, Alatishe AS. Design and Construction of a Microcontroller-based Automatic Irrigation System. In Proceedings of the world Congress on Engineering and Computer Science 2015;1(1):21-23.

[23] Ojha M, Sheetal M, Shranddha K, Diksha T. (2016). Microcont Automatic Plant Watering System. International Academy of Science, Engineering and Technology 2016;5(3):25-43.

[24] Manjula M, Basha SM. Universal Remote Control for Home Appliances Using Arduino. International Journal of Research 2019;6(10):985-1005.

[25] Mraz S. What's the Difference between Motor and Drive? Machine Design 2015. [Online]. Available: www.machinedesign.com/motorsdrives/what-s-difference-between-motor-and-drive.

[26] Singh S. L293D Motor Driver IC. Include Help 2018. [Online]. Available: www.includehelp.com/embedded-system/1293d-motor-driver-ic.aspx.

[27] Nevon Projects. Fingerprint Vehicle Starter Project 2018. [Online]. Available: https://nevonprojects.com/fingerprint-vehicle-starter-project/.

[28] Electronic Projects Focus. What is a Buzzer: Working & Its Applications 2022. [Online]. Available: https://www.elprocus.com/buzzer-working-applications/.

[29] Piratheepan A, Sasikaran S, Thanushkanth P, Tharsika S, Nathiya M, Sivakaran C, Thiruthanigesan K. Fingerprint Voting System Using Arduino. Middle-East Journal of Scientific Research 2017;25(8):1793-1802.

[30] Maio D, Maltoni D. Direct gray-scale minutiae detection in fingerprints. IEEE transactions on pattern analysis and machine intelligence 1997;19(1):27-40.

[31] Jha DK. Computational Physics, 1st ed., Discovery publishing House PVT, Ltd., New Delhi 2016, 223-268.

[32] Ingashitula MS. Designing Fingerprint Based Exam Hall Authentication. BSc. Project Submitted to the Department of Networking and Security, International University of Management, Bachbrecht, Namibia (Published) 2017.

[33] Swaroop YJ, Kumar AT, Raju B, Chandramohan NL, Arshini G. Fingerprint Recognition Access Microcontroller-Based Doors. UGC Care Group I Listed Journal 2022;12(1): 662-666.

[34] Vaishnavi VK, Mangita SW, Supriya KG, Dananjay BS. Fingerprint Based Exam Hall Authentication. International Journal of Research in Engineering, Science and Management. 2019;2(10):787-789.

[35] Ross A, Jain AK. Multimodal biometrics: An overview. In Proceeding of the 12th European Signal Processing Conference 2004, 1221-1224.