2nd International Conference on Information and Communication Technology and Its Applications (ICTA 2018)
Federal University of Technology, Minna, Nigeria
September 5 – 6, 2018

Fingerprint Based Driver's Identification System

O. C. Inalegwu, D. Maliki, J. Agajo, L. A. Ajao, and A. D. Abu
Department of Computer Engineering, Federal University of Technology, Minna, Nigeria
ogbole.inalegwu@futminna.edu.ng

Abstract— **This design work presents a proposed replacement to the current system used by the Federal Road Safety Commission (FRSC) for checking licensed/unlicensed drivers. It gives a faster and less tedious way of identifying registered and licensed road users using biometric captures. The system employs the use of an Arduino board to control and process the functioning of other peripherals: the fingerprint scanner and the Organic Light Emitting Diode (OLED) screen connected to it to achieve its purpose. The prototype system developed was able to displays driver's information on the OLED screen (Age, Name, Sex and License ID); the average response time of the system was also calculated to be 1.41 seconds, which is a good response time considering the system in question. The false accept rate and false reject rate were relatively low (after a sample test with 25 individuals); at 4% and 8% respectively. Also, for its implementation, the components are readily available, relatively cheap and the system is one that can be easily adopted by the FRSC if access to their already existing database is granted. Consequently, it is safe to say that the developed system measured up to the design expectations; it meets the aim of a proposed replacement for the present analogue and easy to beat system employed by the FRSC.**

Keywords- Arduino; fingerprint; biometrics; license

I. INTRODUCTION

The road Traffic Act was annunciated on the 1st of January, 1949 and is available in the Traffic Act Chapter 548 Laws of the Federation of Nigeria (1990) [1]. In Nigeria, the three arms of government agencies that handle or are in charge of vehicle licensing, registration and control are: The Federal Road Safety Commission (FRSC), the Vehicle Inspection Officer (VIO), and the state Board of Internal Revenue. Necessary payments are made to all three institutions providing the personal information, collection of documents and also plate numbers. The Driver's License in form of an identification card is also issued after registration to every individual. The driver is expected to be in possession of this license at all times while driving any vehicle, and a failure to do so attracts a penalty. In Nigeria, according to the FRSC, a driver's license violation is a 10-point offence and the present punishment for this is the payment of a sum of 10,000 Naira.

In the world now, consumers accept the use of biometrics such as fingerprint in everyday business because it is a secure way to verify individual's identity.

Biometrics uses some manner of human physiology, behavioral traits or some deep-rooted skill [2]. Biometric recognition is linked to each individual as the physiological traits cannot be the same or shared between individuals [3]. For these reasons, biometric recognition is considered the best choice for any identity system as it is reliable and unique [4]. A biometric system is basically a pattern-recognition system that distinguishes an individual from another based on a feature vector gotten from a particular physiological or behavioral characteristic unique to that individual [5]. The physiological characteristics include: the face, fingerprint, iris, hand geometry, DNA, while behavioral include: signature, keystroke, voice etc.

Fingerprint Recognition is the process of acquiring a digital depiction of an individual's fingerprint and matching it to an existing digital version of it. The digital images of the fingerprint are reproduced based on either the electrical characteristics of the finger's ridges or valleys or based on the reflection of light on the finger's ridges and valleys. When the pictures are now processed, the final results are the distinct features of the finger contained in digital templates. As applied in [4], individual fingerprints can now be stored in a database as digital templates and this can replace the use of passwords in security applications.

In Nigeria, the Federal Road Safety Commission has a great deal of work on their hands as there is a continuous increase in the number of drivers on the road. The FRSC officials need to check the drivers on the road to ascertain if they are registered. The method of identification being used currently is the driver showing his/her driver's license, this method though somewhat effective, still needs a more efficient alternative due to various reasons. Thus, the need to design a fingerprint-based driver's identification system that would verify if the driver is registered or not and also give other relevant information. This is more efficient in terms of speed and reliability of the information. The fact that the drivers have to stop for license to be checked and the ratio of the number of officials to the number of drivers at any given time makes "a holdup" imminent. This system will provide additional information of the driver, like the name, age, sex, license class and expiring date. This will increase efficiency in FRSC's service beyond what is presently obtainable.

II. RELATED WORKS

Fingerprint technology is the most widely accepted biometric technique and its deployment is easy and a good security measure. Although fingerprints are first captured, the images are not what are stored; the fingerprints are changed into templates that contain the fingerprints [6]. Research in this area has attracted a lot of interest lately. In the design in [7], the project handled the construction of fingerprint identification in cars to avoid automobile theft with the use of GSM and FPGA technologies. This system is basically a security system for automobiles. The prototype of this system was designed as a keyless car, making the authentication biometric based. The security measures of the system are top notch including the fact that an SMS and MMS are sent to the owner of the car when the alarm is triggered. However, the system does not consider a means to ascertain the location of the intruder after he/she must have triggered the alarm [7]. The authors in [8] developed a system that could quickly identify an individual via a mobile phone by just capturing a person's fingerprint. The purpose of the mobile phone is to connect to a database of fingerprints stored on a computer by use of an internet connection, and to send the individual's fingerprint for checking. The system is very effective as it interacts with the database in real time but that is also dependent on how reliable the network is at that particular location. Furthermore, in [9] we see a design of a security system for automobiles which involved the design of a smart card capable of storing the vein image of the driver with vein reader in the car. The driver vein must match the stored image before the car can be started. The system handles the checking of status of the license, whether expired or not. The system considered in [10] handled the confirmation; whether a driver is registered or not by use of a fingerprint scanner linked to a database of registered drivers. When the fingerprint is captured, the system gives a positive ID if the driver's fingerprint has a match in the system's database and gives no result if there is no match. The U4000B miniature fingerprint scanner was used and was connected to a computer. It also used the Biokey SDK development tool. In addition, the system used a "liveness" detection feature which prevented the use of fake fingers. The works in [11]-[14] also presents various ways by which fingerprint biometric has been adopted for improved efficiency and security of biometric embedded systems.

III. SYSTEM DESIGN

The main components of the system are a fingerprint sensor, an Arduino microcontroller unit and an OLED display. The Arduino Integrated Development Environment (IDE) was used to program the fingerprint sensor and to also display how the components will interact based on the program written to the Arduino board. On Arduino, messages to prompt the user for input or for debugging are sent through the hardware serial port and displayed on the serial monitor. The Arduino Uno has a single hardware serial port, so a software serial port must be set up to be used for communication between the Arduino and the fingerprint module All registered drivers' fingerprints are added into the database by using the enroll function on the fingerprint sensor. A numerical ID is given to each fingerprint to be stored on the sensor. To enroll a fingerprint, one must have the finger scanned twice, with an image generated each time to make sure the image is clear enough before it is finally stored. If the two captured pictures are not clear enough, the fingerprint will not be stored and the process has to be repeated. After enrollment, when a driver is stopped, his/her fingerprint is captured on the sensor and is compared with the already stored images looking for a match. It conducts one-to-many comparisons to establish the identity of the driver. If there is a match, the numerical ID of that driver's fingerprint and the driver's name is displayed on the OLED screen and an error is displayed if there is no match. Figure 1 gives a flowchart of the process involved in the enrollment.

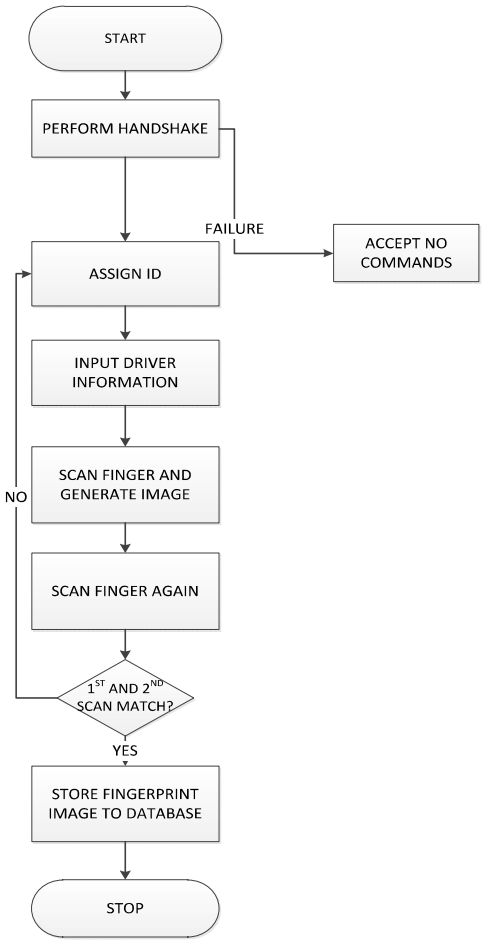

Figure 1. The Flowchart of the Enrollment Process

From Figure 1, the process starts with the assignment of a numerical ID that will be used to store the particular fingerprint to be captured. The driver's information is then inputted next; driver's name, age, sex, license ID, class and the expiry date is registered. When all the information has been successfully typed in, a prompt will show asking that the fingerprint be placed on the sensor. The fingerprint is captured twice before it is stored, and if the first and second one is not a match, the process is started all over again from the point of assigning a numerical ID.

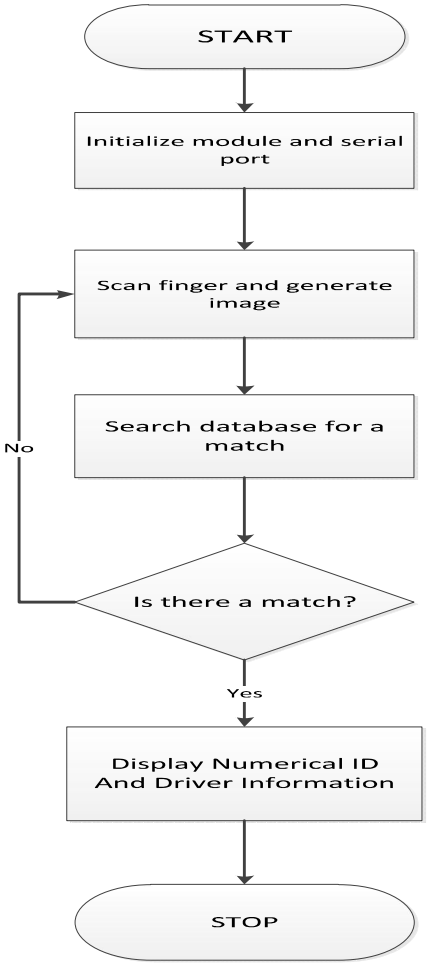

Figure 2. Flowchart of the Proposed System

Next, as shown in Figure 2, the system is powered ON and the OLED screen comes on and displays that the fingerprint sensor is found; it waits for a finger to be placed on the sensor. Once the finger is scanned, a search is conducted to see if there is a match. If there is a match, confirmation is given and the driver's information is also displayed. If there is no match, 'Driver not Licensed' is displayed on the screen.

The generic architecture of any fingerprint recognition system consists of five main modules. There are:

The Capture module: This acquires the individual's fingerprint and assigns it a numerical value. This value is used for the enrollment and identification.

Image processing module: It allows the reduction of the extracted numerical representation in order to optimize the quantity of data to be stored during the enrollment phase, or to facilitate the processing time during the verification and identification phases.

Storage module: Stores the captured fingerprints into templates.

Matching module: The captured fingerprint is compared to the already stored templates. After matching, the level of similarity between the two fingerprints is also determined.

Decision module: This module determines if the amount of similarity is sufficient enough to identify the individual or not.

IV. RESULT AND DISCUSSION

Once the system is powered, the OLED screen comes on and displays 'Place Finger to Confirm'. Once a finger is placed on the sensor, in less than five (5) seconds the OLED gives a response. If the finger is stored, it will display 'Driver is licensed', the numerical ID and level of confidence (how accurate the fingerprint is to the stored fingerprint). The driver's name, age, sex and license ID and expiry date are displayed. For the case of an unregistered driver, the screen will display 'Driver not Licensed'. Figure 3, 4 and 5 shows a snapshot of the prototype for the various displays just discussed.

These results show the model testing. Testing is necessary before the deployment of the developed system in order to ensure the proper working of the system.

Problems that could be encountered during the enrollment process are: Wrong placement of finger; making it difficult for the first and second capture to match. Also, if the finger is wet the sensor will not save the fingerprint.

Figure 3. OLED Indication of a Licensed Driver

Figure 4. OLED Display of a Registered Driver's Information

Figure 5. OLED Display of an Unregistered Driver

A. Performance Evaluation

The main objective of performance evaluation is to provide a certain measure of efficiency, effectiveness and reliability of the system that has been developed.

The two metrics used for evaluation are the False Accept Rate (FAR) and False Reject Rate (FRR). Twenty-five (25) participants were considered for the evaluation.

1) False Accept Rate

FAR = FP/ (number of genuine users) (1)

The number of genuine users are the number of people registered successfully in the system.

Where FP = False Positive (number of impostors that have been authenticated).

FAR = 1/25

FAR = 0.04 =0.04 x 100

FAR = 4%

2) False Reject Rate

FRR = number of users that have not been properly authenticated/ (number of genuine users) (2)

Number of genuine users = 25

FRR = 2/25

FRR =0.08 = 0.08 x 100

FRR = 8%

3) Response Time

The response time to be considered in this work is the time taken for the fingerprint sensor to give a response when an individual's finger is placed on the sensor. The graph in Figure 6, shows the readings gotten when the response time was measured after ten (10) different attempts.

TABLE I. RESPONSE TIME FOR TEN (10) TRIALS

Attempts	Response time (sec)
1st	1.36
2nd	1.39
3rd	1.69
4th	1.72
5th	1.16
6th	1.17
7th	1.29
8th	1.21
9th	1.56
10th	1.55

Average Response Time = Total response times recorded/Number of times response time is recorded. (3)

Av. Response Time = (1.36 + 1.39 + 1.69 + 1.72 + 1.16 + 1.17 + 1.29 + 1.21 + 1.56 + 1.55)/ 10

= 14.1/10

=1.41 seconds

A line diagram is given below to illustrate the changes in response time after successive attempts.

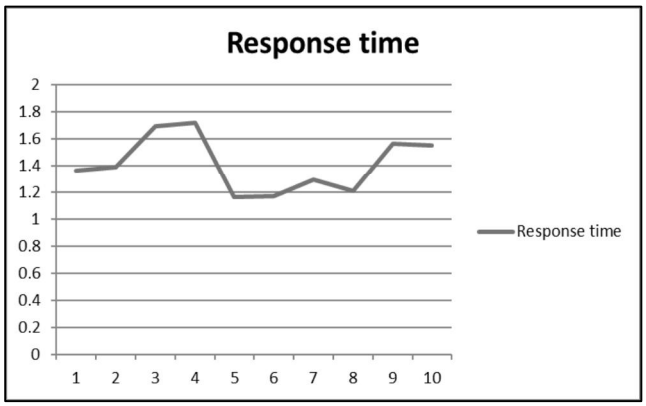

Figure 6. Graph of the Response Time Distribution

The FAR and FRR calculated were high compared to the FAR and FRR given by the manufacturers in the datasheet. The number of people considered for this project is low and that could be the reason why the FAR and FRR are high. Since the number of people considered by the manufacturers is unknown as well. The higher the FRR, the more ineffective is the system as more individuals are incorrectly identified. For the FAR, as the FAR increases the more unsecure the system. This is due to the fact that it recognizes unregistered individuals. The documented response time (search time) was given as less than a second (< 1 second). The average response time was 1.41 seconds which is obviously higher than what was expected but this response time is still a very good response nonetheless. From figure 4, there is a non-uniform change in the response time after ten readings were taken.

V. CONCLUSION

At the end of the process of system development, the results were obtained and stated objectives were achieved. The developed system was tested and its performance evaluated to determine if the system works as was intended. The system was designed to make identification of registered drivers on the road easier and to also give personal information of each registered driver. Compared to the previous method of identification, this system will make it less tedious. Applicants who wish to register would have to go to the FRSC office where their biometric data is captured and added to the database. Since the driver's fingerprint capture is what is being used to identify him/her, the issue of a driver not being with his/her driver's license is eliminated.

REFERENCES

[1] O. Ikechukwu, "Online Motor Vehicle Licensing System," Department Of Computer Engineering, Caritas University, Amorji-Nike, 2012.

[2] Y. R. Dileep Kumar, "A Brief Introduction Of Biometrics and Fingerprint Payment Technology," International Journal of Advanced Science and Technology, pp. 1-2, 2009.

[3] S. Mayhew, "History Of Biometrics," 14 January 2015. [Online]. Available: http://www.biometricupdate.com/201501/history-of-biometrics. [Accessed 23 February 2016].

[4] P. M. S. M. V. S. Smita S. Mudholkar, "Biometric Authentication Technique for Intrusion Detection Systems Using Fingerprint

Recognition," International Journal of Computer Science, Engineering and Information Technology(IJCSEIT), vol 2, p. 8, 2012.

[5] S. P. k. J. Salil Prabhakar, "Biometric Recognition: Security and Privacy Concerns," in Biometrics, IEEE Computer Security, 2003, pp. 33-34.

[6] A. K. Ojha, "ATM Security using Fingerprint Recognition," International Journal of Advanced Research in Computer Science and Software Engineering, pp. 1-2, 2015.

[7] S. R. K. M. Vijay Kumar, "Fingerprint Based Licensing System for Driving," Internatonal Journal of Advanced Research in Computer and Communication Engineering, p. 3, 2014.

[8] C. A. a. P. P. Tomas Bulka, "Secure Mobile Fingerprint Identification System," Santa Clara University, Santa Clara, 2005.

[9] S. P. D.Divya, "Finger Vein Based Licensing and Authentication Scheme using GSM," International Journal Of Computer Engineering, p. 1, 2013.

[10] M. K. B. K. K. M. J.Angeline Rubella, "FINGERPRINT BASED LICENSE CHECKING FOR AUTO-MOBILES," in Fourth International Conference on Advanced Computing, Chennai, 2012.

[11] F. A. T.-h. K. a. D. B. Ishani Sarkar, "Palm Vein Authentication System: A Review," International Journal Of Control and Automation, pp. 1-6, 2010.

[12] D. V. T. H. Mr. Shriram D. Raut, "Biometric Palm Prints Feature Matching for Person Identification," InternationalJournal Modern Education and Computer Science, pp. 1-2, 2012.

[13] D. K. Mary Lourde .R, "Fingerprint Identification in Biometric Security Systems," International Journal of Computer and Electrical Engineering, p. 1, 2010.

[14] S. V. L. Rajasekar, "Wireless Fingerprint Attendance System Using Zigbee Technology," International Journal of Power Control Signal and Communication, p. 1, 2012.