VOL. 14, NO. 23, DECEMBER 2019 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

DEVELOPMENT OF VEHICLE IGNITION USING FINGERPRINT

Jamil Abedalrahim Jamil Alsayaydeh[1,2], Win Adiyansyah Indra[1,3], Adam Wong Yoon Khang[1,3], Vadym Shkarupylo[4] and Dhanigaletchmi A. P. P. Jkatisan[1]
[1]Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, Durian Tunggal, Melaka, Malaysia
[2]Center for Advanced Computing Technology, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, Durian Tunggal, Melaka, Malaysia
[3]Center for Telecommunication Research and Innovation, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, Durian Tunggal, Melaka, Malaysia
[4]Department of Computer Systems and Networks, National University of Life and Environmental Sciences of Ukraine, Heroyiv Oborony str., Kyiv, Ukraine
E-Mail: jamil@utem.edu.

ABSTRACT

This paper is about building a prototype of vehicle ignition using fingerprint sensor. This system can prevent the vehicles from being stolen. It is developed to control the ignition of the vehicle through the fingerprint scanner. This system consists of GSM SIM 900 that connects to the Arduino which is the microcontroller of the project. To make sure the system is secure, only authorized fingerprint is paired with the Arduino to start the ignition. Vehicles ignite when the enrolled fingerprint is matched against the fingerprints in the database while users with no match in the database are prevent from igniting the vehicle. A theft alarm from buzzer, a notification to the owner's mobile phone via GSM SIM 900 and status display in the LCD are the appropriate signal to the owner. This article describes briefly in detail about the design and implementation of the ignition system.

Keywords: vehicle ignition, article, camera-ready format, arduino, GSM, paper specifications, fingerprint.

INTRODUCTION

Biometric technology is a method that requires the physical presence of the identified person. It is a new state of art method for security systems. Fingerprint recognition is one of the most widely used biometric system and also the oldest method which is dated back to 2200 BC [1]. The use of fingerprints as personal code was also in tradition method. Developing a prototype with biometric system will serve a robust and embedded real time fingerprints-based ignition systems in vehicle.

This project focuses about developing a prototype of vehicle ignition using fingerprint. According to [2] this system has a potential to avoid the vehicle from being stolen. This lock security is developed to control the ignition of the vehicle by using fingerprint. The existing lock at the vehicle is not highly secured which consist of handle lock and standard switch lock. To overcome this, there are variety of security lock system that can be added to the vehicle. By creating this prototype, security level of the vehicle ignition is highly protected and could help to decrease theft. The main idea of this project is a fingerprint scanner will detect the authorized or an unauthorized user and alert the user via GSM.

In the current era, there is high demand for robust security systems in vehicles. So, the designing and developing a biometric security system using fingerprint technology to prevent unauthorized vehicle is easy and very useful.

Vehicle ignition

Ignition system basically is used to initiate a car's 12-volt battery and send it to each sparkplug in turn, starting the air fuel mixture in the engine's combustion chamber. It then produces high voltage arcs at the spark plug electrode. By using ignition coil, high voltages are produced where it is supplied with lower voltage battery. The basically, ignition system consists of ignition switch, relay, starter motor, battery and fuse.

The ignition system works when low voltage in the battery goes through the primary coil. Wire connects to the kick starter using a wire from the battery while the other wires attach to the kick starter to the key system. When the car key switch on the system once, two wires from the kick starter to key system are connected. This results the engine to be in on condition. Followed by the next turning of the key is where the third wire connects the other two joined wires which cause the voltage to flow from the battery to the respected vehicle parts so that the vehicle gets to move.

Vehicle ignition using fingerprint system is known as security system to prevent vehicle theft. Vehicle usage is basically a necessity for everyone in current era. Nowadays, vehicle security system depends on sensors that are way too costly and high efficient. This system is developed to cut cost for the technology like only the premium car makers are imposing this in the market. Thus, developing vehicle ignition using fingerprint would be efficient and low cost for users who own vehicle to keep secure their vehicle without any worries. Fingerprints biometric system is cheaper compared to the rest of the biometrics and there is also high usage among users [3].

Classifications of Arduino

Arduino is one of the platform used for this project. It is a software feature which enables experienced programming designers to utilize the Arduino code to converge with the current programming language libraries can be broadened and changed. It is an awesome tool for

individuals with all ability levels. Both physical programmable circuit board and programming is in Arduino. It continues running on PC which is utilized to compose and exchange PC code to the physical. Arduino has capacity such as interacting with light on a sensor, a finger on a button, running a motor, switching on an LED and distributing something online. In addition, Arduino doesn't need a separate piece of hardware, to load a new code onto the board since it can utilize it with a USB cable. The most utilized ones are Arduino Uno and Arduino Mega. Arduino IDE is utilized to program an Arduino and it utilizes a straightforward version of C++. This makes the program to be learnt less demanding. Rajan *et al.* proposed the product which is good with a wide range of working frameworks like Windows, Linux, and Macintosh and so on indistinct vague unclear vague [4].

Global system for mobile (GSM)

Global System for Mobile communications is a digital cellular technology used for data services and transmitting mobile voice. Variation of time division multiple accesses (TDMA) are used the most used from the three digital wireless telephony technologies (TDMA, GSM, and CDMA). GSM packs the information digitizes, at that point sends it down a channel with two different streams of user data, each in its own time slot. GSM has few services which are tele services, data services and supplementary services. Tele services includes mobile phones, data services consist of short message services and supplementary services for incoming and out coming calls, call forwarding, call waiting, call hold and conference. This device supports voice calls and information transfer speeds of up to 9.6 kbps, including the transmission of SMS. GSM operates in 900MHz or either 1.8GHz recurrence band. GSM first launched at Finland 1991.In current era, more than 690 mobile networks provides GSM services across 213 countries.

Many network operators have signed agreements with foreign operators, so this makes the user continue to use their mobile phones even while travelling. A Worldwide system for Mobile (GSM) is more known as second era telecom framework standard that was worked to deal with the crack issues of the main cell structures. Beforehand it was known as Group Special Mobile. They chamber took up the task of demonstrating an ordinary Mobile correspondence structure for Europe the 900 MHz band [5] [6].

Table-1. Worldwide development of mobile telephone systems.

Year	Mobile System
1981	Nordic Mobile Telephone (NMT) 450
1983	American Mobile Phone System (AMPS)
1985	Total Access Communication System (TACS)
1986	Nordic Mobile Telephone (NMT) 900
1991	American Digital Cellular (ADC)
1991	Global System for Mobile Communication (GSM)
1992	Digital Cellular System (DCS) 1800
1994	Personal Digital Cellular (PDC)
1995	PCS 1900-Canada
1996	PCS-United States

Retrieved on April 2017 from book "Global System for Communication" [7].

Table-2. GSM milestone.

Year	Milestone
1982	GSM formed
1986	Field test
1987	TDMA chosen as access method
1988	Memorandum of understanding signed
1989	Validation of GSM system
1990	Pre-operation system
1991	Commercial system start-up
1992	Coverage of larger cities/airports
1993	Coverage of main roads
1995	Coverage of rural areas

Retrieved on April 2017 from book "Global System for Communication" [7].

Liquid crystal display (LCD)

A 16x2 LCD is used to display the output of the project. Pin 1, 2, 3, 4, 5, 6, 7, 15 and 16 are utilized to interface with the LCD. It is a dot matrix display that is used to display characters, alphanumeric characters and symbols. The LCD will receive codes from the microcontroller and displays it to its display data RAM. This will then transform the character code into character pattern and display the characters in the LCD. The LCD can display the option to add and delete the user. It will also show the status if authorized user is detected and reject if it is an unauthorized user. The LCD will be display the message accordingly as per programmed.

PIN MODULES AND ITS FUNCTIONS

Table-3. Pin Modules and its functions.

Pin Modules	Functions
Pin 1	Connects to VDD
Pin 2	Connects to power supply
Pin 3	Used to adjust the contrast of LCD
Pin 4	Used for selecting register
Pin 5	Used to select read or write signal
Pin 6	Enable the signal
Pin 7 to in 14	Data pins
Pin 15	Increase backlight of the LCD
Pin 16	Decrease the backlight of the LCD

FINGERPRINT SENSOR

Fingerprint biometric are first used in China. It is proposed in Europe in the year 1858 and implemented in Germany in 1903. In the field of biometrics, fingerprints are the most used and most researched recognition. Fingerprints are basically unique where up till now there is no any two fingerprints matched together are found. Even an identical twin, the fingerprints are not the same. Fingerprints are the representation of an epidermis layer of finger. Fingerprints are basically used to reduce the search time of an activity. Fingerprints consist of ridges and valleys. Ridges are the curved segment consisting the dark area while valleys are the area in between of two adjacent rings of the white area. Minutiae is the major feature of a fingerprint that defines the point of the ridges lines end of fork. Based on (Mridula, 2014) [8] the patterns of the fingerprints are classified as arch, tented arch, right loop, left loop and the whorl. Arches are basic type of fingerprints formed by ridges. It enters at one side and exits at another side. This is the same for the plain arch and also the tented arch. Whorls contains at least one of the ridge that makes a whole circuit and loops are one or more ridges entering from one side of the print, recurving and existing at the same side of the print. After a fingerprint picture is obtained by the fingerprint reader equipment, this fingerprint must be interpreted. It must be prepared such that read-outs can be effectively thought about and coordinated against each other. Two sorts of coordinating software exist, which is minutiae matching and pattern matching. There are two types of fingerprint sensor used mostly is capacitive and optical fingerprint sensors.

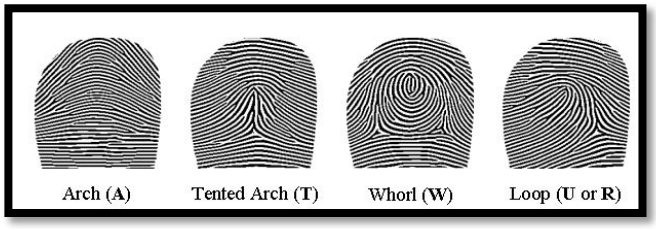

Figure-1. Patterns of fingerprints.

A person's weight, eye color, and hair color can change or be changed, but his fingerprints cannot be altered. They are unique to each individual, and can be differentiated and identified based on certain distinctive patterns made by the ridges. The following are some of the commonly used fingerprint patterns that have been identified and used in the process of fingerprinting.

There are basically three main forms of patterns that are made by the ridges of fingerprints.

a) **Loops:** Loops make up almost 70 percent of fingerprint patterns. They originate from one side of the finger; curve around or upward, before exiting out the other side. A loop pattern always comprises one delta, which is roughly a triangular formation in the pattern.

b) **Arches:** Arches are encountered in only 5 percent of the patterns, and comprise lines that slope upward and then down, similar to the outline of a small hill. There is generally no delta.

c) **Whorls:** Whorls constitute around 25% percent of all patterns. They are circular or spiral patterns, similar to eddies. A pattern that contains 2 or more deltas will always be a whorl pattern.

Figure-2. Minutiae patterns.

CLASSIFICATION OF FINGERPRINT SENSORS

Capacitive sensor

This is a CMOS reader that uses capacitors and an image is formed using electrical current. It is more expensive compared to optical readers. The advantage of using capacitive sensor it requires a real fingerprint shape, not only a visual image. This is the reason for CMOS to be harder to get tricked. It is embedded in a Silicon chip composed of 2D array of micro capacitor. Between the finger surface and the Silicon plates, electrical charges are created. Plates leads to pattern of distinguished capacitances are respected with the distance of variation of ridges and valleys.

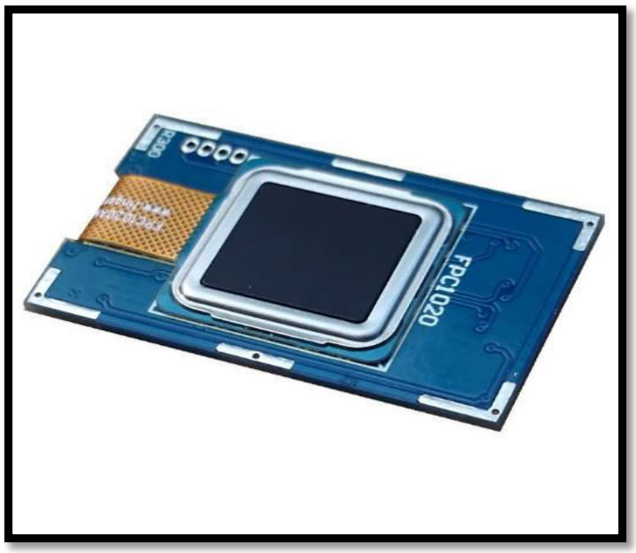

Figure-3. Capacitive sensor.

Optical sensor

Manikandan *et al*. proposed a 4 pin device that is used for various applications such banks, safety deposits and access control, this sensor requires the visual image of the fingerprint.3. Dimensional image is recorded by using this sensor and stored into the microcontroller. Light incident on detector will convert the energy first to electrical charge. This is one of the most commonly used fingerprint sensor, process starts when the user places their finger on top of the glass. The scanner will not function if the image placed on top of the glass is too dark. This senses difference of the intensity of reflected light from valleys and ridges; normally one fingerprint is scanned at a time [9].

Figure-4. Optical sensor.

FACE RECOGNITION BASED CAR IGNITION AND SECURITY SYSTEM

Bhojane and Thorat, briefly discussed about how the car provides ignition to the engine. Literally this system replaces the key off a vehicle with specific user's face. In this paper, a facial recognition system by embedding face detection and face tracking system algorithm found in MATLAB with the use of Raspberry Pi B is discussed. The purpose of this system to prohibit vehicles getting steal from thieves. Owners of the vehicles face towards technology as an anti-robbery system by developing this face recognition system.

With the knowledge and applications of large amount embedded techniques, car security program study and analyses are consistently improving. Many trendy techniques, a well-known as biometric passport campaign, perception processing technique, communication technique thus, have been entire into car security systems. At the same anticipate, the approach to the cars remains valuable. So, one efficient car security program should be sensible, competent and reliable. So to prohibit vehicles stealing from thieves, owners of the automobiles are facing towards technology as an anti-robbery system.

In this paper, use of Haar-like feature is been used to detect and recognize the face of the authenticated user. This is to achieve the secure environment for ignition and accessing the car a typical rectangular haar-like feature. Objective of this car ignition system is creating a secure environment associated with the face of the individual [10].

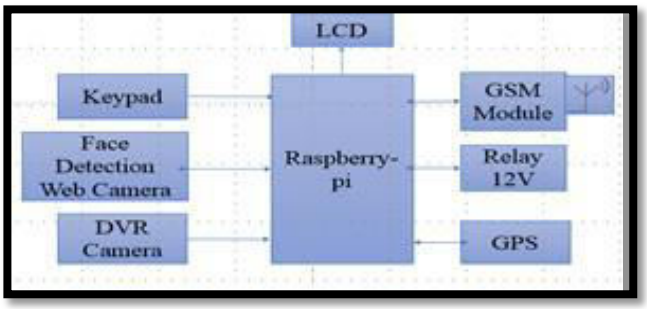

Figure-5. Architecture of face recognition-based car ignition system.

REAL TIME BIOMETRICS VEHICLE SECURITY SYSTEM WITH GPS AND GSM TECHNOLOGY

Kiruthiga *et al*. have been discussed about saving the vehicle from theft. This system is literally to defend the vehicle from any illegal access, easy to use, fast usage; clear, consistently good in performance and also reasonable fingerprint recognition technique. This development intimates the position of the vehicle to the authorized user by Global System for Mobile (GSM) technology. If an authorized person tries to access the vehicle, it is allowed meanwhile if an unauthorized person tries to access a message will be sent to owner of the vehicle and the engine will be immobilized. The GPS system is attached to know the position of the vehicle and its current location. In any cases the vehicle got towed or theft detection the location will be detected. If an engine is switched off, but the GPS changes significantly a message will send to the authorized user to alert them. Besides that, PIC16F877a is used as the main platform of the security system which monitors all the input and output of the system. Status of the system will be displayed on LCD and SMS will be sent to notify the authorized user [11].

RESULTS AND DISCUSSIONS

Here is a sample result for this illustrative project. Some discussions are added up as an example of real feedback from design and testing activities.

RESULTS

The system has been tested to demonstrate the project delivery's functionality as in presented design. The combination of the software applications and hardware components has enabled the application operating as planned or labelled on the designed interface.

The data are taken from different fingerprints in order to examine the accuracy and consistency of the system. Table and Figure method are used to interpret data that collected from the prototype of vehicle ignition using fingerprint. Application used in this project is interfaced together with Arduino software to control the commands. Application used is to notify the owner on the usage of the vehicle.

The projects have been successfully created including the operation along with explanations of the different functions used for the application software and hardware systems work.

DESIGNING

Process flow to complete this project successfully is included with input, process and output of the system. Fingerprint is scanned to activate the ignition when the authorized user fingerprint is detected. Adding or deleting a fingerprint option is included in this project. In the case of adding or deleting a fingerprint, a master fingerprint will be set as an ID first. When the master fingerprint ID is authorized, then only user can be added to be an authorized user or deleted from the list. Followed by the Arduino which will interpret the received message from the fingerprint scanner. The results will display the status of the user in LCD. If the fingerprints are matched, the ignition system of the vehicle will turn on. If an unauthorized fingerprint is detected, the buzzer will turn on and an alert message is sent to the authorized user. Upon receiving the SMS using GSM technology, the user will know that the vehicle is being operated by someone else.

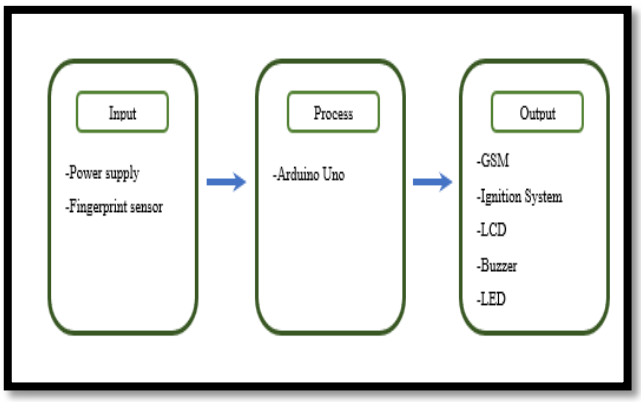

Figure-6. Flowchart of the system.

BLOCK DIAGRAM FOR FINGERPRINT RECOGNITION PROCESS

First the individual must register themselves in the biometric system database. This begins as the fingerprint of an individual is acquired by a scanner. Followed by the verification task that will identify the individuals. The biometric reader will take note on the individual's fingerprint so that could be determined and converts it to a digital format. Final task is identification which the system differentiates the input of the biometric in the system database. The result is either identified of an authorized user or alert as an unauthorized user.

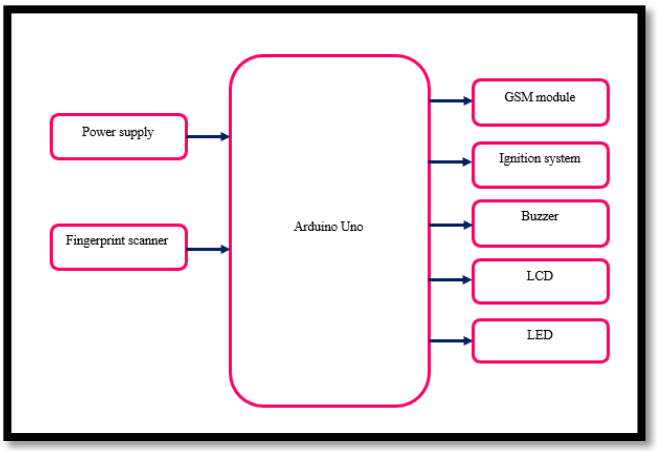

Figure-7. Block diagram of the system.

HARDWARE SETUP

Hardware circuit connection

Connection of all the hardware's are done accordingly. LCD pins are connected to A0, A1, A2, A3, A4, A5, fingerprint scanner connected to pin 2 and 3, GSM to pin 10 and 11 (RX, TX), push button pin 4, 5, 6 and 7, relay to pin 12 and buzzer to pin 13.

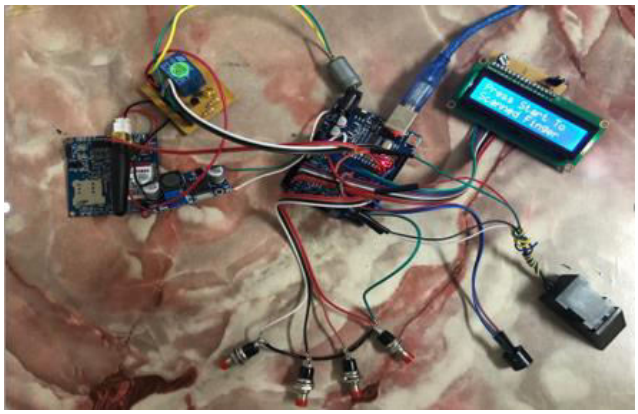

Figure-8. The connection of LCD, GSM, relay, fingerprint scanner, buzzer and push button on the Arduino Uno board.

Performance analysis

For verification on the functionality correctness of the developed product, a series of testing operation took place as the final step of the project work. The tests showed successful results for the different appliances when switched ON and OFF using the apps that has been developed. Some of the functionality testing details are given in pictures by next paragraphs.

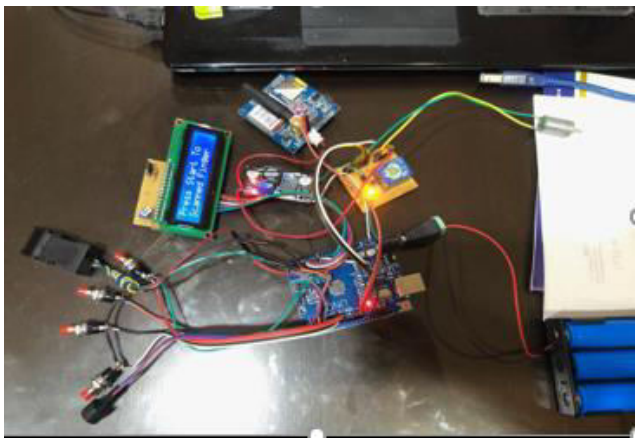

Figure-9. The yellow LED will turn ON when the ignition starts.

Project development is the final step to make sure the project functions properly. The result has been tested to make sure all the components are connected properly and is attached to work together with Arduino code. Figures (9 & 10) show the successful hardware connection of the project and the successful message received by the owner through the GSM SIM900.

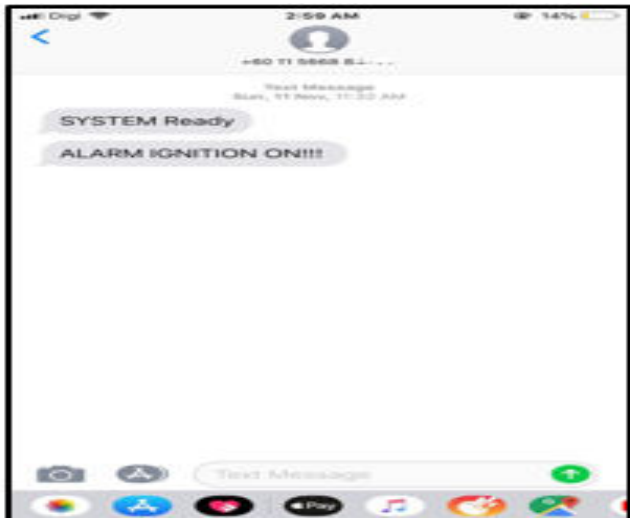

Figure-10. GSM SIM900 Module sent SMS to Mobile phone.

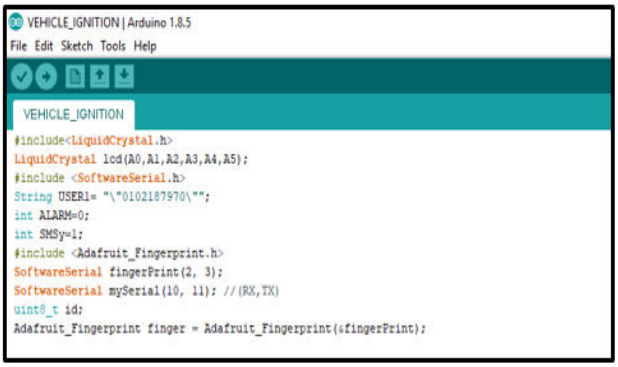

Figure-11. The library of the code program.

Figure-12. Result of initializing system.

This void Enroll functions to add in fingerprints in a specific location or a specific Id. The enroll process works when the fingerprints are first placed on the scanner to be read, remove and the place it for the second time for confirmation of the fingerprints. Once the fingerprints are read, it will store in Arduino and displays as "Stored" while if no fingerprints detected it displays as "No Finger".

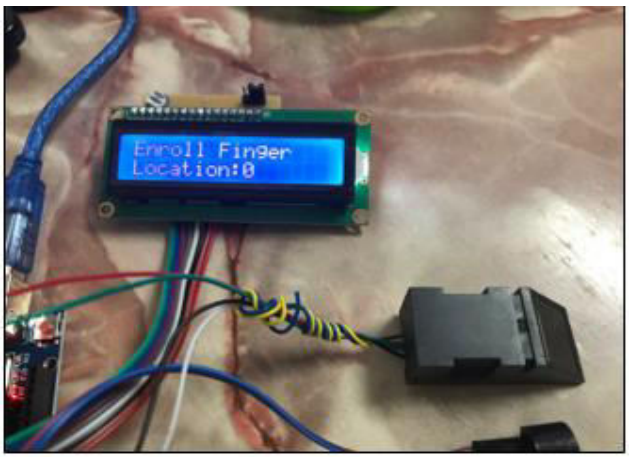

Figure-13. Enroll Finger for the first time.

Figure-14. Enroll Finger for the second time for confirmation.

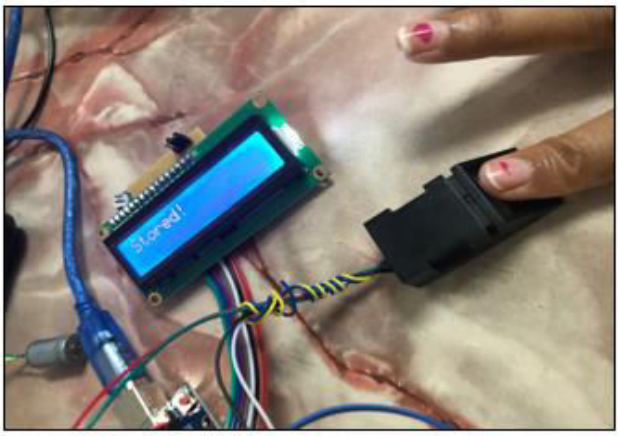

Figure-15. Fingerprints stored.

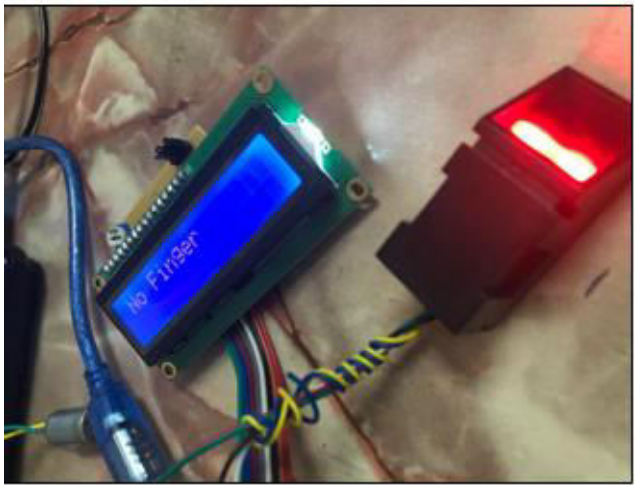

Figure-16. If no fingerprint detected.

Analysis of this project is done by scanning the fingerprint of registered users. The project's result is obtained after making sure all the components in the project functions fine. Five registered users attempt to run the ignition has been recorded. All the five fingerprints have different confidence level. Higher confidence is the better match. Average reading of all the five users is recorded as per shown in the table below.

Table-4. Average fingerprint sensor reading of fingerprint ID.

Fingerprint ID	Average fingerprint sensor reading
1	251.0
2	154.4
3	131.6
4	117.2
5	239.6

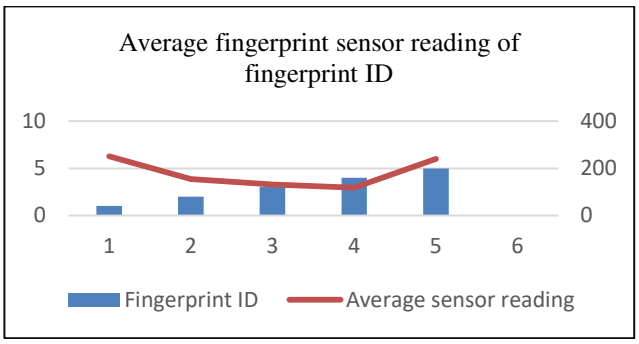

Figure-17. Fingerprint ID vs average fingerprint sensor reading.

Figure-18. Final output when the authorized user is detected.

Successful output of the ignition system is shown in the LCD as per figure above. When the authorized user is detected, LCD user displays the status, along with LED yellow ON and motor starts ignition. The reading of the fingerprint sensor will not be always the same since it depends on the fingerprint's condition as well as the scanner. Somehow, the fingerprint scanner will detect the authorized user's fingerprints detail and allow the vehicle to start.

CONCLUSIONS

The project's objectives for development of vehicle ignition using fingerprint have been successfully developed. In a nutshell, this prototype of vehicle ignition using fingerprint scanner is successfully developed. This system operates fine in regard of enrolling new user and deleting registered user. Appropriate steps to notify the authorized user via SMS using GSM is successfully done in this project. SMS's are sent to the owner when the vehicle is turned on and when an unauthorized user is detected. Besides that, the status of the user is displayed in LCD. LCD displays the status of the vehicle when the vehicle is on, ready to start and fingerprint's condition. Output of this system is revealed through LED and motor for a successful user attempt. LED will light on and the dc motor will start running saying the ignition is successful while the buzzer sounds showing the attempt of unauthorized user is failure. This fingerprint technology focuses on automobile and is only possible for the authorized user to use. In the case of implementing this system on locally manufactured vehicles will make the car security system tight which will be also cheap.

ACKNOWLEDGMENT

The authors would like to thank for the support given to this research by Ministry of Higher Education Malaysia and Universiti Teknikal Malaysia Melaka (UTeM) under the Grant PJP/2019/FTKEE (6A)/S01659. We thank also those who contributed in any other forms for this paper.

REFERENCES

[1] Omidiora E. O., Fakolujo O. A., Arulogun O. T., Aborisade D. O. 2011. A Prototype of a Fingerprint Based Ignition Systems in Vehicles. 62(2): 164-171.

[2] Kumar B. S. and Engineering I. 2017. Vehicle Anti-Theft System Using Fingerprint Recognition Technique Microcontroller Interface. 1(1): 7-12.

[3] Arora R. and Kumar K. 2015. Start-Up the Engine Using Fingerprinting. IX(X): 21-24.

[4] C. Rajan, B. Megala, A. Nandhini, C. Rasi Priya. 2015. A Review : Comparative Analysis of Arduino Micro Controllers in Robotic Car. 9(2): 371-380.

[5] Gill K. R. and Sachin J. 2016. Vehicle Ignition using Fingerprint Sensor. IJIRST –International Journal for Innovative Research in Science & Technology. 2(12): 357-363.

[6] Jamil Abedalrahim Jamil Alsayaydeh, Vadym Shkarupylo, Mohd Saad bin Hamid, Stepan Skrupsky and Andrii Oliinyk. 2018. Stratified Model of the Internet of Things Infrastructure. Journal of Engineering and Applied Sciences. 13: 8634-8638.

[7] Consortium E. 1982. Global System for Mobile Communication (GSM). The International Engineering Consortium. pp. 1-19.

[8] Mridula P. 2014. A Review on Classification of Fingerprint Images. 9(3): 61-66.

[9] N. Manikandan, K. Manikandan, K.E. Vishn, R. Thirumoorthi Raja, K. Kanthaboopathi, T. Senthilnathan. 2018. Biometric vehicle security system and pollution monitoring. pp. 1126-1131.

[10] Bhojane K. J. and Thorat S. S. 2018. A review of Face Recognition Based Car Ignition and Security System. pp. 532-533.

[11] Kiruthiga N., Latha L. and Thangasamy S. 2014. Real time biometrics based vehicle security system with GPS and GSM technology. Procedia Computer Science. Elsevier Masson SAS. 47(C): 471-479. doi: 10.1016/j.procs.2015.03.231.