License and Fingerprint Detection for Security Purpose in Automobiles

Deepak.S[1], Dinesh Kumar.G[2], Hariharan.M[3], Prema.V(AP-Sr.G)[4]
[1, 2, 3 & 4] *Department of CSE, SRM Valliammai Engineering College, Kattankulathur, TamilNadu, India*

ABSTRACT

This paper deals with driver License and fingerprint detection. A vehicle accident and theft is becoming very common nowadays, which is one of the main issues for a person having car or bike. The design of a fingerprint and RFID tag (License) based authentication for a vehicle is explained. Fingerprint identification gives the biometric based authentication and RFID tag (License) gives a user authentication for a vehicle. So inorder to avoid vehicle accident and theft the proposed system is designing a user authentication system for a vehicle instead of going with security based authentication system; it also provides a user based authentication which is a fingerprint of a person. A person, who wishes to drive the vehicle, first step is to verify with their RFID tag (License) whether the person who wish to Drive the vehicle is allowed to drive or not; by checking the fingerprint, once verification done then ignition unit of vehicle will starts automatically. If the person fingerprint is not valid in the Fingerprint Module then the vehicle will not get started.

Keyword: *Fingerprint Sensor, RFID tag, Arduino Uno, LCD Display, DC Motor.*

1. INTRODUCTION

Fingerprint refers to the identification or verification of a Person based on valid user or not. The paper presents the designing of fingerprint identification in vehicles which is a biometric authentication, to avoid road accident which includes the RFID tag (license) for user authentication of a vehicle. Fingerprint identification is one of the most honest and dependable personal fingerprint identification methods. The proposed system was designed on vehicle user authentication instead of going with security based authentication system. It is providing a system based on driver authentication. A person who choose to drive the vehicle in order to verify with their fingerprint and then second step is to check whether the person is having RFID tag (license) or not, once the verification is cleared then ignition unit of vehicle is started automatically. If the person fingerprint is not valid on the Fingerprint Module then the vehicle will not get started, hence RFID tag (license) verification is not needed to show. For this purpose security it requires an "RFID" tag and a "fingerprint" scanner, the following shows the required configuration of the system. This paper aims to introduce a hardware architecture which detects the fingerprint as well as the valid of the user authentication of the driver and takes a robust decision to turn on or off the ignition system based on the valid user. Firstly it describes about the fingerprint matching algorithm followed by RFID tag (License) authentication and in last it describes about the system architecture.

2. BLOCK DIAGRAM AND SYSTEM DESCRIPTION

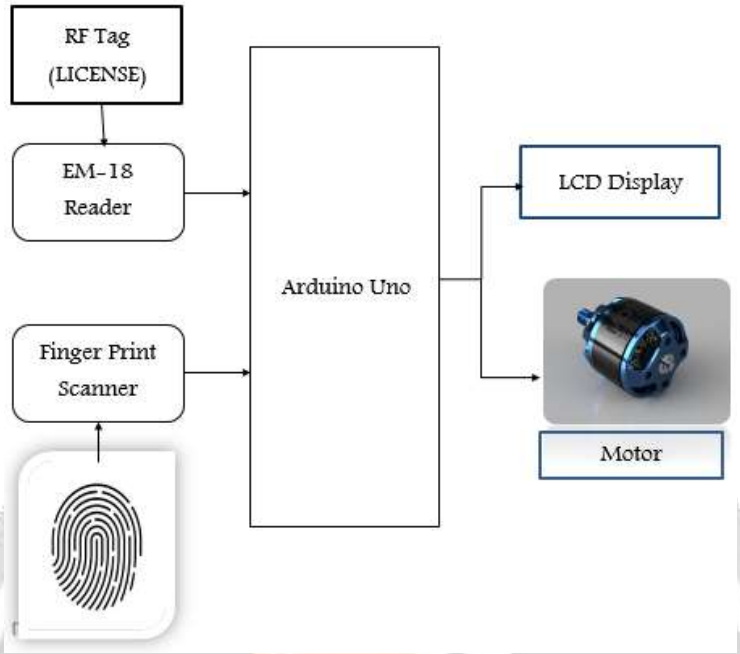

Fig -1: Block Diagram

Analysis of Hardware Structure

1) **Fingerprint Sensor Module *:***

A Fingerprint Sensor is an electronic device, which are used to apprehend a digitalized image of the fingerprint pattern. The apprehend image is called as a live scan. The following figure 2 shows the image of the fingerprint Sensor module R305 model. This live scan finger is followed by digital processing to create a biometric template (a stockpile of Deduced features) which is stored and used for matching purpose.

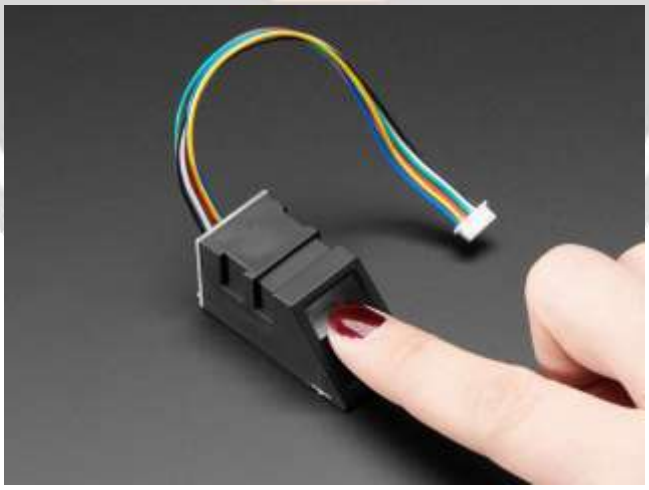

Fig -2: Fingerprint sensor

The complex circuits only easy circuits and fingerprint module can enhance the paper into fingerprint authentication power. It is universally used in different areas like electronics business, information security, access control, identity authentication and other security industry.

- Hardware connection

serial interface is the fingerprint module may communicate with MCU of 5V power: TD (transmitter) connects with RXD (receiving), RD (receiver) connects with TXD (transferring). This connection was added for level converting circuit, between the Module and PC.

- Serial communication protocol

This mode is a semi duplex asynchronies serial communication, and it has some default baud rate of 57600bps. The baud rate can be rooted in 9600~115200bps.Transferring frame format is 10 bit: the low-level starting bit, 8-bit data with the LSB first and an ending bit, and there is no check bit.

2) **RFID Reader Module (EM-18):**

Radio-frequency identification (RFID) is a wireless identification. The figure 3 shows the RFID tag module of the system. An RFID tag is an object that can be implemented to or assimilated into a product, animal, or person for the cause of identification using radio waves.

Fig -3: RFID Reader

RFID tags contain at least two parts:

- An integrated circuit for storing and processing the information of identification, modulating the signal and demodulating the radio frequency signals.
- An antenna for receiving and transmitting of the signal.

Radio Frequency Identification (RFID) involves a contactless reading and writing of data into an RFID tag's non-volatile memory through an RF signal unlike barcodes which are printed on product and read by the laser scanner which is a high cost process. An RFID system consists of an RFID reader and an RFID tag. The reader emits an RF signal and data is exchanged when the tag comes in the range of the reader signal. The RFID contains antenna in which consists of a coil and a capacitor for tuning the circuit to the nominal carrier frequency of 125 kHz.

3) **Arduino Uno Module:**

This microcontroller is based on the ATmega328P. Arduino Uno board as 20 pins (0-19) out of which 6 are analog inputs, 14 are digital input output pins(6 pins provide PWM voltage) a power jack and a reset button. It has an operating voltage of 5V. It contains everything needed to support a microcontroller which is shown in figure-4. The board having the fowling features.

Fig -4: Arduino Uno

4) **LCD Display:**

Liquid Crystal Display consists of 16 columns and 2 rows. The library that is used is <liquidcrystal.h>.

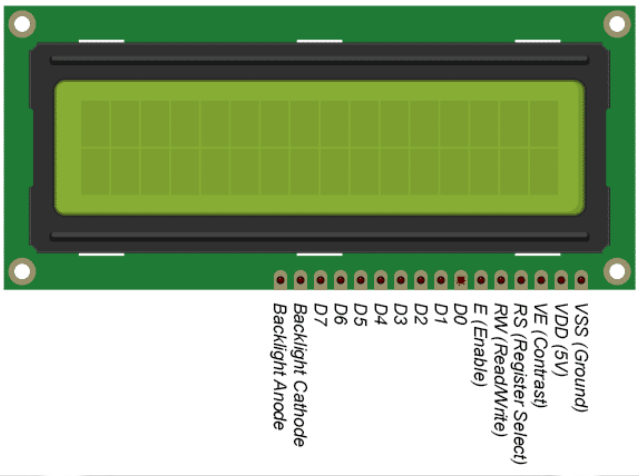

Fig -5: LCD Display

These are specialized for being used with Arduino, They are used for display different messages on a miniature LCD.

5) **DC Motor***:*

DC motor is an electric device that runs on direct current power. In any electric motor is rotate clockwise and anticlockwise direction.

Fig -6: DC Motor

Software Used for the programming

1) Arduino IDE

This software program for verification using in Arduino programming language called Processing. Arduino Uno is programmed used in Arduino IDE. Upload the code with the help of USB cable. It is an open source software that is mainly used for writing and compiling the code. It support both c and c++ language.

2) Embedded C

Embedded **C** is a set of language which is an extension for the C Programming language by the C Standards committee to address common issues that are existed between C extensions for different embedded existed between C extensions for different embedded systems. In early times, the C Standards Committee extended the C programming language for addressing these issues by providing common standards for all the implementations to cling to its commonality. In embedded C language it has a more number of features that are not available in normal C language, such as, fixed-point arithmetic, named address spaces, and basic I/O hardware addressing. Embedded C follows the most basic syntax and semantics of standard C language, in the time of beginning years of microprocessor based systems, programs are used to develop in the assemblers and agglutinated into the EPROMs. There are no mechanisms which are used to find what exactly the program was doing because there are no displays to read. Instead they use LEDs, switches, and etc. to check for correct execution of the program within a device. Some 'very fortunate' developers had simulators like In-circuit Simulators (ICEs), but they are way too costly to purchase and also not quite reliable for the outcomes. Afterwards C is the most universally used programming language for embedded processors/controllers. Assembly is also used but it is implemented when the portion of the code requires very high timing accuracy, code size efficiency, etc. for the ultimate requirements. As assembly language programs are specific to a processor, assembly language didn't offer any portability across the systems. To overcome this drawback, several high level languages, including C, came up. Some other languages like PLM, Modula-2, Pascal, etc. also came into existence but couldn't find any wide acceptance. Amongst those, C language got the full-fledged acceptance for not only embedded systems, but also for desktop applications. Even though C language might have lost its gleam as mainstream language for general purpose applications, it is still having a strong-hold in embedded programming language. Due to the wide acceptance of C language in the embedded systems, various kinds of supporting tools like compilers & cross-compilers, ICE, etc. become highlighted and all this facilitated development of embedded systems using C language. Assembly language later seems to be an obvious alternative for programming into embedded devices. However, use of assembly language is confined for developing an efficient code in terms of size, speed and accuracy. Also, assembly codes become costly software development tool to purchase and code portability is not there. Developing small codes is not exactly the main problem, but to make large programs/projects have become increasingly arduous to maintain in assembly language. Finding good assembly program developer is also becoming big issue nowadays. Hence high level languages for device are preferred for embedded systems programming.

3. METHODOLGY AND BACKGROUND

Fingerprint matching is achieved by minutia matching of the pattern. It is classified into two stages, they are pre-processing stage matching stage, both the are converted to polygons in polar coordinate system and a matching algorithm. In this pattern approach, the graphical center of the fingerprint image is located at the center point. The cropped region is stored for matching. Minutiae based algorithms are pre-processing and image enhancement techniques to improve perception.

Termination : A ridge comes to an end.

Bifurcation : A ridge divides into two separate ridges.

Binarization : The process of converting the original image to a black-and white image.

Thinning : Reduce the width of each ridge to one pixel

Matching Ratio : It will decide to allow access to an (FMR) imposter is given in an equation (1)

$$FMR = \frac{FalseMatches}{\mathrm{Im}\, posterAttempts} \quad \text{---------- (1)}$$

It is matching each input image with all the template images.

False Non Matching Ratio (FNMR): It is denies access to an approved user is given in an equation (2)

$$FNMR = \frac{FalseNonMatches}{EnrolleAttempts} \quad \text{---------- (2)}$$

Matching Score: It is score between the input and data is given in an equation (3)

$$Matchingscore = \frac{MatchingMinutiae}{Max(NT, NI)} \quad \text{------ (3)}$$

Minutiae Extraction: The minutiae points are classified as Termination, Normal ridge and Bifurcation respectively, is shown in figure-7.

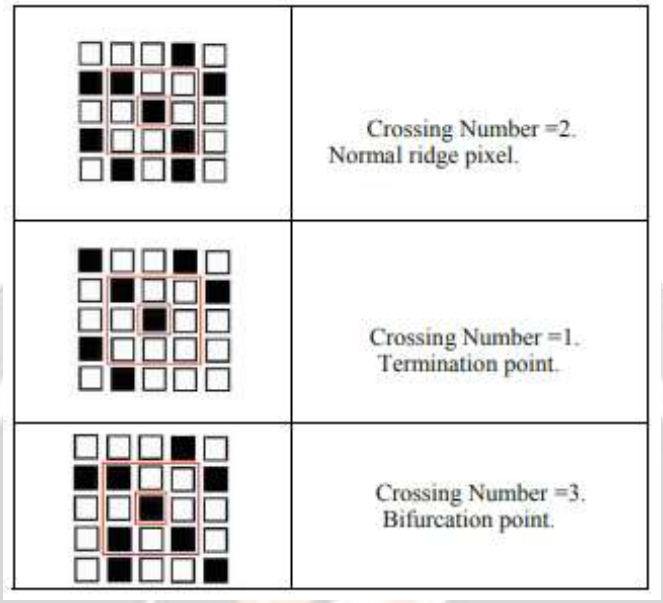

Fig -7: DC Motor

4. BUILDING THE PROTOTYPE SYSTEM

STEP 1: A Person who wishes to drive a vehicle to place the finger on the fingerprint scanner. If the placed finger matches with the fingerprint enroll then it goes to step 2. Otherwise it will show an error message display like please place valid fingerprint and again displays please enter a valid fingerprint. In case the fingerprint accessing process is failed for more than three times than process for fingerprint will go to the initial condition i.e.; place a valid fingerprint. *STEP 2:* In this step the user has to show a valid RFID tag (license) of that particular vehicle, if it is not a valid identification then it will display an error message like it is an invalid RFID tag (license) please show a valid RFID (license) and again it displays like waiting for valid RFID to show. In this process if the RFID tag shown fails for more than three times, then as in the step1 after the process of fingerprint the RFID tag process will move to the initial condition i.e.; fingerprint placing step. If a valid RFID tag is shown it will forward to the next step.

STEP 3: In this step a person who wishes to drive a vehicle then step1 is processed and after the validation of step1 it will proceed to step 2. After step 2 validation finally the last step which is after fingerprint scan and RFID tag (license) verification, the kit is proceeding for the ignition of the system. If all of the process fails to do this process then the ignition system will not work.

STEP 4: If the fingerprint matches and the RFID (license) of the vehicle is verified then the ignition system will start and the user can drive the vehicle and the process goes on. If the fingerprint does not matched with the first taken fingerprint then the controller gives an error message to process the verification and set back to its initial step 1. Figure 8 shows the complete system operation flow.

We are going for basic hardware usage as an interfacing device to scan the data from the fingerprint and read the data from the card. The task of the fingerprint scanner is to read the finger placed on it and for card reader is to read a twelve digit unique RFID tag and it is displayed on the screen. So each fingerprint scanned has unique template identification for single user and a RFID tag card has a film with a 12 digit unique RFID and the number is printed on the card itself for recognition purpose.

5. SYSTEM OPERATION WORK FLOW

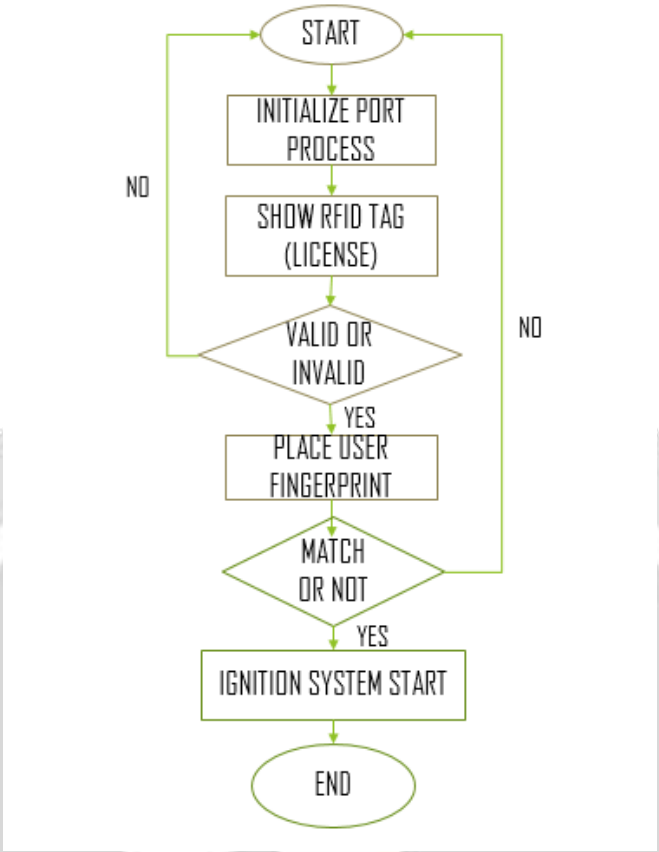

Fig -8: System Operation Flow

When power supply is switched on, first it displays "MOTOR CONTROL" in LCD. After some delay it displays "WAITING FOR LICENSE" in LCD display, through the driver authentication user shows the RFID tag at the RFID tag reader module. If the user shows the wrong RFID tag then it displays "INVALID LICENSE PLEASE SHOW VALID LICENSE" in LCD display but if it is valid RFID tag and then user their fingerprint on the fingerprint module. If the placed finger is invalid then it will displays "PLACE A VALID FINGER" in LCD display. If the placed finger is valid then it will display "FINGERPRINT VERIFIED" in LCD display and then the finally the DC motor will be started.

Fig -9: Practical Implementation on Kit

5. CONCLUSION

A minutiae approach in designing the Authentication System were implemented using Fingerprint and RFID tag gives security to the users' vehicle system and provides safety for the ignition system using a finger print scanner and RFID tag for the authentication of the ignition system. The result obtained in providing the security gives quite reliable in all the different modes of the paper. The system has successfully gain mastery over some of the aspects existing with the present technologies, by the use of finger print Scanner and RFID tag identification as the authentication Technology.

6. ACKNOWLEDGMENT

The authors would like to thanks for the Department of Computer Science & Engineering of SRM Valliammai Engineering College (Autonomous), SRM Nagar, Kattankulathur, Tamil nadu, India, for allowing us to explore this innovative idea.

7. REFERENCES

[1] Dinesh Singh and Chalavadi Krishna Mohan, Deep Spatio-Temporal Representation for Detection of Road Accidents Using Stacked Autoencoder, 28 May 2018, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTION SYSTEM

[2] Afaf Bouhoute , Rachid Oucheikh, Karim Boubouh, and Ismail Berrada, Advanced Driving Behavior Analytics for an Improved Safety Assessment and Driver Fingerprinting, 06 June 2019, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTION SYSTEM

[3] Jennifer Howcroft , Bruce Wallace , Rafik Goubran, Shawn Marshall, Michelle M. Porter, and Frank Knoefel, Trip-Based Measures of Naturalistic Driving: Considerations and Connections With Cognitive Status in Older Adult Drivers , 07 July 2019, IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT.

[4] P. Yankov, Olsen, Mikkel B. Stegmann, Søren Sk. Christensen, and Søren Forchhammer, Fingerprint Entropy and Identification Capacity Estimation Based on Pixel-level Generative Modeling, 04 August 2019, IEEE TRANSACTIONS ON NETWORKING

[5] Abdellah El Mekki , Afaf Bouhoute , and Ismail Berrada, Improving Driver Identification for the Next-Generation of In-Vehicle Software Systems, 08 August 2019, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY

[6] B. I. Kwak, J. Woo, and H. K. Kim, "Know your master: Driver profilingbased anti-theft method," in Proc. 14th Annu. Conf. Privacy, Secur. Trust, 2016. MEKKI et al.: IMPROVING DRIVER IDENTIFICATION FOR THE NEXT-GENERATION OF IN-VEHICLE SOFTWARE SYSTEMS 7415

[7] E. Romera, L. M. Bergasa, and R. Arroyo, "Need data for driver behaviour analysis? Presenting the public UAH-DriveSet," in Proc. IEEE 19th Int. Conf. Intell. Transp. Syst., Nov. 2016, pp. 387–392.

[8] E. Carvalho et al., "Exploiting the use of recurrent neural networks for driver behavior profiling," in Proc. Int. Joint Conf. Neural Netw., Anchorage, AK, USA, 2017, pp. 3016–3021, doi: 10.1109/IJCNN.2017.7966230.