Automobile Anti-Theft System

Thripthi A H
Dept of CSE, AIET, Mijar,
Karnataka, India

Shetty Niketha Sadhu
Dept of CSE, AIET, Mijar,
Karnataka, India

Shreyas C Rao
Dept of CSE, AIET, Mijar,
Karnataka, India

Rajarajeshwari B B
Dept of CSE, AIET, Mijar,
Karnataka, India

Vivek Sharma S
Dept of CSE, AIET, Mijar,
Karnataka, India

***Abstract*—Every day the number of crimes in the country is increasing at a significant rate. This alarming rate calls for some innovative ideas for increasing the security of the systems. Of all the crimes one of the most trending is the theft of Automobiles. Here we propose a Fingerprint Detection System to unlock and use the automobile. The owner of the automobile will be able to unlock his/her car only after authentication through an application on his/her phone. The data is verified every time they have to use the vehicle. The owner has an option to make multiple accounts on the application as well.**

***IndexTerms*—Fingerprint Recognition and Authentication, Biometrics, Anti-Theft System**

I. INTRODUCTION

In this 21st century various kinds of luxurious and comfort- able automobiles have been invented by mankind. However there is least security provided for these systems. Here we come up with the antitheft system which uses biometric techniques. With the advancement of biometrics in this period, iris recognition and fingerprint recognition techniques have become major research fields. Iris recognition and fingerprint techniques works on certain algorithm which will restrict the access for all the users. Fingerprint recognition refers to the automated method of identifying or confirming the identity of an individual based on the comparison of two fingerprints. Optical readers, capacitive readers, ultrasound readers and thermal readers are four types of fingerprint reader hardware. Here we use R307 fingerprint read/sensor module which is a type of optical reader.

only under the worst of cases. Biometrics has now grown into a separate industry whose standardization has made exponential advancements [1]. In Fig. 1 we can see that fingerprint recogni- tion has high universality, very much convenient, high stability, high reliability and also cost efficient. It is implemented in PDA's, cellular phones and smart phones.

IV. IMPLEMENTATION

The final and important phases in the system life cycle are the implementation of the new system. Implementation is the realization of the application, or execution of a plan, idea, model, design, specification, standard, algorithm or policy. In computer science, an implementation is a realization of a technical specification or algorithm as a program, software component or other computer system. Many implementations may exist for a given specification or standard.

A. Platform Used for Implementation

An integrated development environment (IDE) is a software application that provides comprehensive facilities to computer programmers for software development. The Arduino Integrated Development Environment or Arduino Software (IDE) contains a text editor for writing code, a message area, a text console, a toolbar with buttons for common functions and a series of menus. It connects to the Arduino and Genuino hardware to upload programs and communicate with them.

II. Motivation

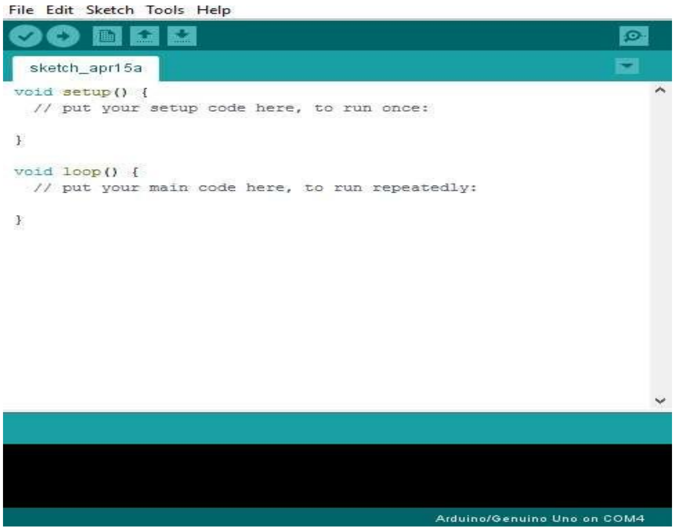
In this 21st century security has become must in everybody's life. Automobile theft has drastically increased from the previous decade. As per the crime report of India, there were 213765 incidents and 214009 victims of auto theft reported in India during 2016. The top 10 States having highest cases of auto theft in India during included, Delhi, Haryana, Chandigarh, Manipur, Rajasthan, Puducherry, Mad- hya Pradesh, Maharashtra, Karnataka and Uttar Pradesh . Approximately 4 vehicles were stolen every hour in Delhi. Security systems for automobiles currently depend on sensors which are very expensive. So there is a need for a greater level of security in a cost effective manner.

III. Available Technology

Biometric technology have great scope in the current chang- ing world. Biometrics of a person is something which changes Fig. 1 shows the window when we open the Arduino IDE software. Programs written using Arduino Software (IDE) are called sketches. These sketches are written in the text editor and are saved with the file extension .ino. The message area gives feedback while saving and exporting and also displays errors. The console displays text output by the Arduino Software (IDE), including complete error messages and other information. The bottom right hand corner of the window displays the configured board and serial port.

B. Language Used for Implementation

Although Arduino Software (IDE) is written in program- ming language Java, it supports the languages C and C++ using special rules of code structuring. Programs for embedding software with hardware can be written using programming languages like embedded C in the IDE. The proposed system is coded using both C++ and C as programming languages, mostly using C++.



```
void setup() {
  // put your setup code here, to run once:

}

void loop() {
  // put your main code here, to run repeatedly:

}
```

Fig. 1. Arduino IDE

C. Hardware Implementation

The hardware implementation of the project is as shown in Fig. 2. The 230V power supply input is converted to 12V, 1A using an adapter. 7812 for 12V is used. 12V from adapter is passed to each regulator. The regulators share a common ground connection. The regulator in turn passes 12V and 5V to capacitors. All the components used in the project require AC current. Hence, capacitors are used along with the 2 regulators. Capacitors are used to filter out all the DC current and give AC current as output. The capacitors used in the system are rated 47microF. The 12V from 7812 is forwarded to a DC motor controller. The DC motor controller is L293D which is a driver. The DC motor controller is connected to a 45rpm motor. The 15V from 7805 is forwarded to the Arduino board.

The DC motor controller has 4 control pins I1, I2, I3 and I4. In the project, I1 and I2 are connected to the Arduino's digital pins. I1 from DC motor controller is connected to Arduino's digital pin 4 and I2 to digital pin 5. The Arduino board has 10 digital pins out of which 8 are used in the project. The project requires 2 Fingerprint sensors; one for the door lock module and other for the ignition module. An R307 Fingerprint sensor is used; it consists of 4 control pins. These pins are connected to Arduino via connecting wires. In the door lock module, Vin is connected to the 5V supply of the Arduino, the Gnd pin is connected to the ground pin of the Arduino, RX pin of R307 is connected to the digital

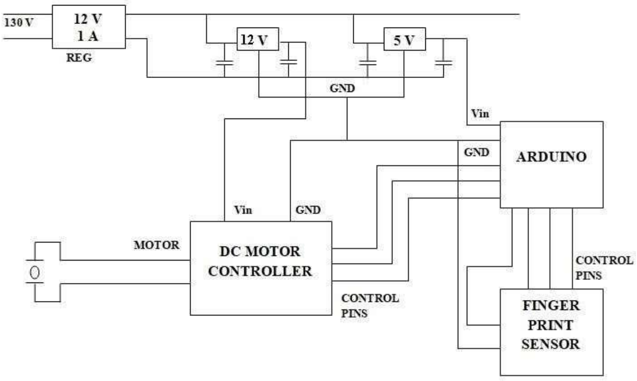


Fig. 2. Hardware Implementation of Ignition System

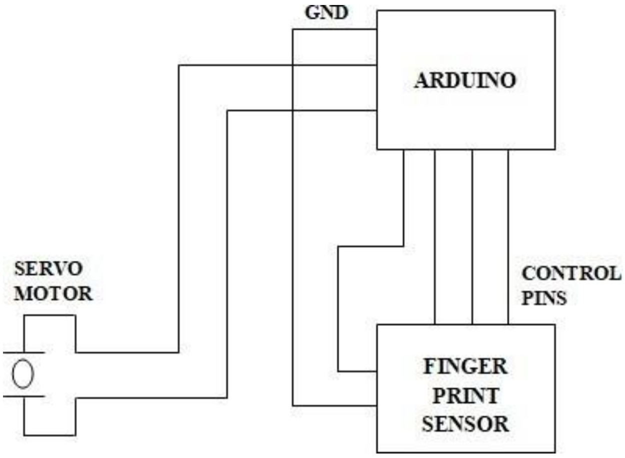


Fig. 3. Hardware Implementation of Door Lock System

pin 8 of the Arduino and TX pin of R307 is connected to the digital pin 9 of the Arduino so that to establish a serial communication through which there will be a communication between the Fingerprint sensor and the Arduino. In the ignition module, Vin is connected to the 5V supply of the Arduino, the Gnd pin is connected to the ground pin of the Arduino, RX pin of R307 is connected to the digital pin2 of the Arduino and TX pin of R307 is connected to the dīgital pin 3of the Arduino. The digital pin 10 of the Arduino is connected to a servo-motor. The R307 fingerprint scanner has 2 buffers inside it which is used in the project.

There is an H-bridge consisting of 2 vertical terminals. It is used to send data clockwise or anticlockwise from one terminal to other. In the project, the first terminal is the Arduino board from where data is sent to the other terminal which is the DC motor controller. If a signal 10 (1 for high and 0 for low) is sent, the motor turns clockwise and if signal 01 is sent, the motor turns anticlockwise. The Arduino comprises of a serial monitor. This serial monitor is used to display the menu with 3 options; Register new user, Unlock/Lock car and Exit. The Fingerprint scanner has 2 different functions, namely enrolling a new user and authentication of users. First, let’s see the enrollment or registration process.

The registration of a new fingerprint is done in 2 steps. First, the sensor takes the scanned image of the fingerprint and stores it in buffer 1. After the image is stored, another function will create a feature template using the image in buffer 1 and store this template in buffer 1. When this process is successfully completed, a message is thrown on the serial monitor saying “image converted”. The Fingerprint sensor requires one more scanned image of the same fingerprint for successful registration. So, in the second step, the scanner takes the image and stores it in buffer 2. The same process is repeated for the second image and template is stored in buffer 2. The user is registered successfully, only if the two templates match. A fingerprint model is created a soon as the user is registered and is stored in the database. There will be an id associated with each fingerprint model in the database and it ranges from 0 to 127.

The next is the authentication process. For authentication, the serial monitor will be waiting for a user input and will display “waiting for a valid fingerprint”. The valid fingerprint here represents an enrolled fingerprint. The sensor will take the scanned fingerprint and store in any of the 2 buffers depending on the availability. A feature template will be created for the image and in turn a fingerprint model is created and stored in buffer. When the model is successfully created, a function fastSearch() is called which will compare the models in buffer and database. If the models match, the function returns the success status code “FINGERPRINT_OK”. For the door lock module, the servo-motor starts running on return of success status code. For the ignition module, the dc-motor starts running on return of success status code. Since there are 2 modules, there are 2 flags (1 for each module) which act as switch. These flags are used for lock and unlock or start and stop switching. If the models do not match, the function returns the failure status code “FINGERPRINT NOTFOUND”. On the return of failure code, the control returns to the waiting stage and waits for user input again.

The images in the Fingerprint sensor are acquired and processed in different steps to create a feature template. The basic steps for digital image processing in Fingerprint Identification involve acquiring, storing and analyzing the fingerprint data. Fig. 4 shows the fingerprint image with ridges and valleys on it.

The first step involves acquiring fingerprint image from different sensors like - Optical or Capacitive Sensor. The

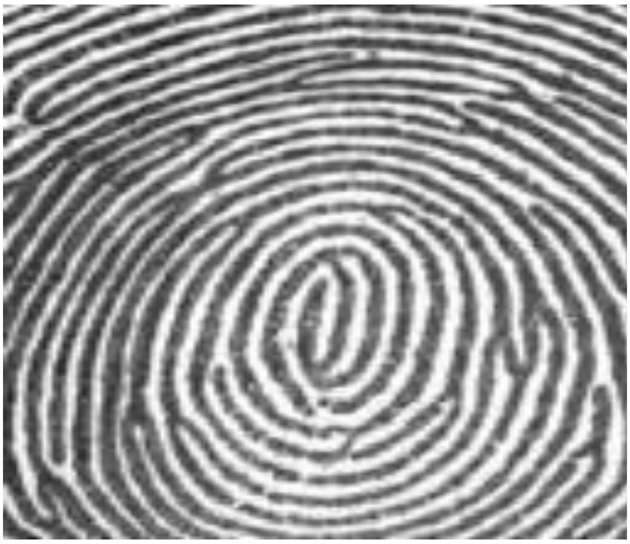


Fig. 4. Ridges and Valleys in a Fingerprint

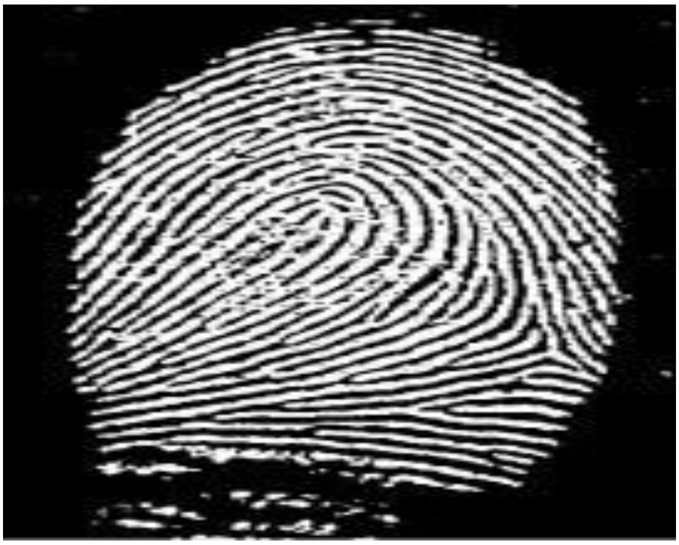


Fig. 5. Normalized Image

charged and coupled device present in the optical scanner consists of light sensitive diodes which emit electrical signals when illuminated. These tiny dots when hit a target spot form the pixels and an array of pixels form the image. Once the finger is placed on the monitor, the image is acquired by illuminating the ridges of the finger.

The second step involves storing and processing the images using the below given steps:

- Image Segmentation: It involves removal of unwanted features from the acquired image. Procedure followed is Thresholding, wherein the pixels having intensity (gray level value) greater than a particular threshold is con- sidered, whereas those having intensity lesser than the threshold value are removed or deleted.
- Image Normalization: It involves obtaining a uniform intensity pattern for the whole image. This is done so that the image pixels are in a desired range of gray values. Fig. 5 shows a normalized image.
- Image Orientation: The image is formed by calculating the orientation at each point. The orientation is in turn de- termined by calculating the average of vector orthogonal to the gradient of each pixel at X and Y directions.
- Image Filtering: This involves using various techniques like Gabor or Butterworth filters to remove unwanted noise. Fig. 6 shows the filtered image.
- Image Binarization: This involves conversion of the fil- tered image to binary image using Thresholding tech- nique, to improve the contrast. It utilizes global Thresh- olding technique, wherein pixel value greater than the threshold is set to 1 and pixel value less than the threshold is set to 0.

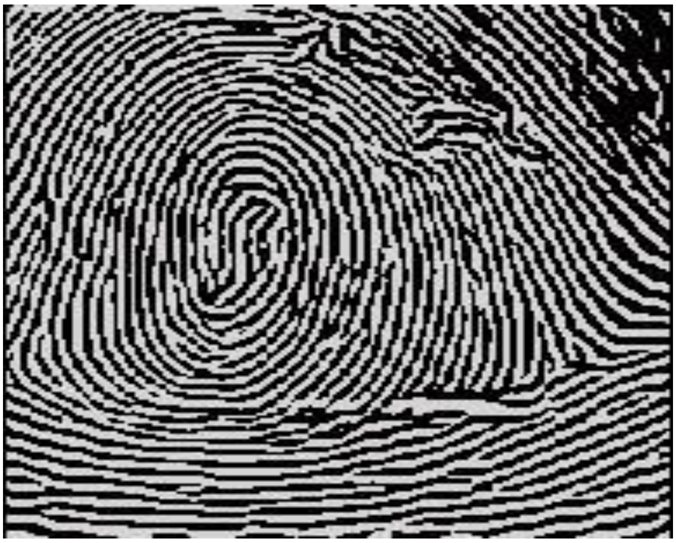


Fig. 6. Filtered Image

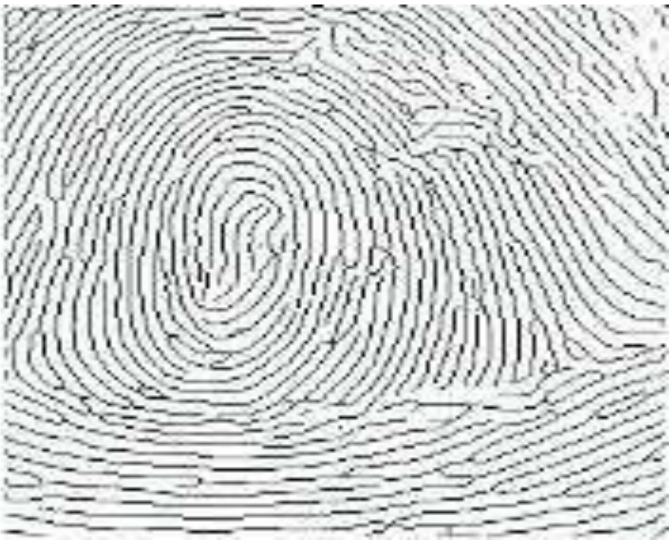


Fig. 7. Thinned Image

- Image Thinning: This is done to preserve connectivity of the ridges and involves eliminating foreground pixels. Fig. 7 shows the thinned image.

The third step involves analyzing the images, by extracting minutiae details from the processed image and then comparing these details with those of the already stored templates. This is achieved by calculating the crossing number (half of sum of differences) between pair of pixels in an eight-connected neighborhood. This gives a unique identification for each characteristic of the fingerprint. This creates a feature template which is stored in the database as a fingerprint model. This model is used for the authentication process of fingerprint as described earlier.

V. Conclusion

Security is becoming essential in all kind of applications. The aim of the project is to explore the area of Iot and biometric sensors, and contribute to the reduction in auto- mobile thefts and thus, the project aims at improving the security level of automobile industry. As the fingerprint is a promising biometric pattern for personal identification in terms of both security and ease of use, we implement the system using a fingerprint sensor. This is a unique method of designing and assembling a low-cost, compact theft control system for an automobile.

The system ensures that nobody other than the owner can use the car without his/her authentication. Project presents the performance analysis for fingerprint biometric. It presents apparent advantages over password and token-based security. The proposed security system can be used to reduce the increased vehicle theft. This system provides a greater extent of security compared to the existing system.

VI. Future Work

The project has a vast scope and can be developed numerous ways for effective and efficient use. A face biometric sensor can be implemented from which the vehicle can be started. In the next stage of work a GSM module can be added through which if an unauthorized person places the finger, then a message will be sent to the registered mobile number. A GSM-GPRS module could also be placed which also send the location coordinates along with the message. Also in the future we can implement iris scanning instead of fingerprint or add it as a two-step authentication process.

References

[1] Zhaoxia Zhu and Fulong Chen. Fingerprint Recognition-Based Access Controlling System for Automobiles, 2011.
[2] Biometrics (Fingerprint Sensor) on http://www.atmel.com/products/Biometrics/, 2007-04-10
[3] P Marwedel. Embedded System Design. Springer, 2006.