International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 2 Issue: 3 553 – 556

Third Party Anti Theft Automobile Security System

[1]Akash M. Marathe, [2]Mihir S. Samak,
Department Of Information Technology,
Trinity College of Engineering and Research,
Pune, India.

[3]Prof. Sudhanshu Gonge, Assistant Professor,
Department Of Information Technology, Trinity College of Engineering and Research,
Pune, India
[4]Mr. Samir Kulkarni,

Responsible- Productivity & FE, Automotive SBU, KPIT Technologies Ltd., Hinjewadi, Pune.

***Abstract*—** In India, a vehicle is stolen every six minutes an alarming statistics, that is forcing the government to consider making it mandatory for all two, three and four-wheeler makers to fit their products with a hi-tech anti-theft security systems. Security system providers are interested in making their mark. These day's vehicle theft cases are higher than ever, giving our vehicles an excellent protection with many reliable anti-theft devices. Anti theft security systems ensure the best guarantee to protect the vehicle from different kinds of theft cases. It is a vehicle security device that offers excellent protection to the vehicle.

Keywords- *Biometric Fingerprint Scanner, Raspberry Pi, Raspbian Linux OS, LCD Display, Alpha-Numeric Keypad, GSM SIM 900.*

*****

I. INTRODUCTION

The motivation behind our proposed system is to provide maximum security in cars with easily available components and lower per-unit production costs. Many cases of car thefts and illegal use of cars are reported nowadays. So, the proposed system can help be a savior in some of these cases and bring down the crime rate in case of car robberies and thefts. So a more developed system makes use of an embedded system based on Biometric fingerprint authentication. The designed & developed system is installed in the vehicle. The main concept in this design is storing the fingerprint templates of the owner and all those persons the owner wants to give his car to ride to. A physical lock is fitted on the steering wheel key hole. So whenever a fingerprint is scanned and the template matched, the key hoe opens automatically, allowing the user to drive the car. But in case the input templates do not match, then the lock won't open forcing the user to not drive the car.

II. EXISTING SYSTEM

There are many anti theft security systems available out there in the market today. The main purpose of such systems is to thwart any attempts by the intruder/thief to try and steal the car. All existing systems are made by original equipment manufacturers (OEM). They are so designed to function with the working of the car. They are also costlier than the third party anti theft system proposed through this journal.

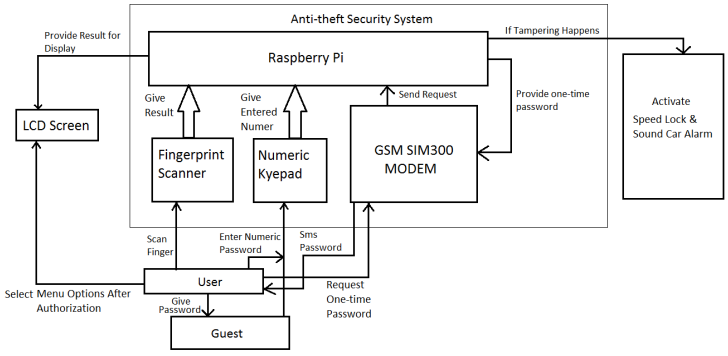

FIG 1: Proposed Third Party Anti Theft Security System Architecture Diagram.

The above figure depicts the architecture of a basic biometric system which is employed in the proposed anti theft security system for automobiles.

III. PROPOSED SYSTEM

Inspired by the existing systems, we have decided to develop a Third Party Anti Theft Security System for Automobiles which shall not interfere with the functioning of the car. The car shall have a Fingerprint sensor fitted on

the dashboard so that the owner can enroll his fingerprint and scan it whenever he/she wants access to the steering wheel of the car. Also, a GSM SIM 900 module shall be fitted so that when the owner wants to lend his car to some friend of his, he can request a special one-time password from the GSM Modem and forward it to the third person he/she wants to lend to. Additionally, a numeric keypad and 16X2 LCD panel shall be provided to interact with the anti theft security system.

IV. EXPERIMENTAL STUDY.

In this, we shall look at the four main design components for an automatic fingerprint identity authentication system.

A. Acquisition:

The two primary methods of capturing a fingerprint image are inked (off-line) and live scan (ink-less). The typical way of acquiring an inked fingerprint image is: A trained professional obtains an impression of an inked finger on a paper, and the impression is then scanned using a flat-bed document scanner. The live-scan fingerprint is a collective term for a fingerprint image which has been directly obtained from the finger without the preliminary step of getting an impression on a paper. Acquisition of inked fingerprints is a tough job in the context of an Identity-authentication system as it is both not feasible and socially unacceptable for identity verification. Optical frustrated total internal reflection (FTIR) concept is the most popular technology to obtain a live fingerprint scan. When a finger is placed on one side of a glass plate (prism), ridges of the finger are in contact with the plate while the valleys of the finger are not. The rest of the imaging system essentially consists of an assembly of a light emitting diode (LED) light source and a charge-couple device (CCD) placed on the other side of the glass plate. The glass gets illuminated by the laser light source at a certain angle, and the placement of the camera is such that it can capture the laser light reflected from the glass. The incident light on the plate at the glass surface touched by the ridges is randomly scattered, while the light incident at the glass surface in correspondence to valleys suffers total internal reflection, which results in a corresponding fingerprint image on the imaging plane of the CCD. Total internal reflection reflection plays a crucial role here.

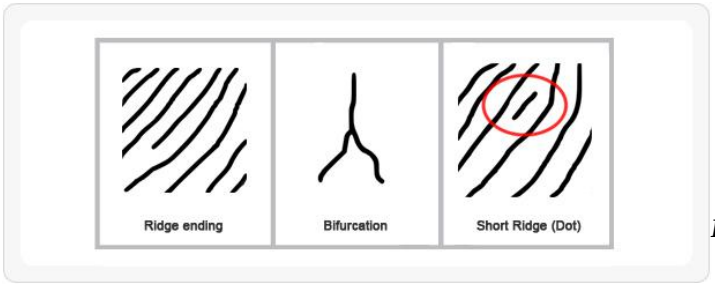

FIG 2: Types of Fingerprint Minutiae

B. Representation (Template):

There's a question to be answered here: which machine-readable representation completely captures the invariant and discriminatory information in a fingerprint image? The issue of representation constitutes the essence of fingerprint verification design and has far-reaching consequences on the design of the rest of the system. The unprocessed gray scale values of the fingerprint images are not invariant over the time of capture. There are many representations that rely on the entire ridge structure (ridge-based representations) and are largely invariant to the brightness variations but are significantly more sensitive to the quality of the fingerprint image than the landmark-based representations. This is because it is very easy to verify the fingerprints in the presence of a unique landmark.

C. Feature Extraction:

What the feature extractor does is that it finds the ridge endings and ridge bifurcations from the input fingerprint images. Minutiae extraction is just a trivial task of extracting singular points in a thinned ridge map, provided the ridges are perfectly located in an input fingerprint image. But in reality, however, it is not always possible to obtain a perfect ridge map. The performance of currently available minutiae-extraction algorithms depends heavily on the quality of input fingerprint images. Due to a number of factors like aberrant formations of epidermal ridges of fingerprints, postnatal marks, occupational marks, problems with acquisition devices, etc., fingerprint images may not always have well-defined ridge structures. Owing to such circumstances, reliable minutiae-extraction algorithms should not assume perfect ridge structures and should degrade gracefully with the quality of fingerprint images.

D. Matching:

A fingerprint matching module computes a match score between two fingerprints, which should be high for fingerprints from the same finger and low for those from different fingers. Fingerprint matching is a difficult pattern-recognition problem due to large interclass variations (variations in fingerprint images of the same finger) and large interclass similarity (similarity between fingerprint images from different fingers). Interclass variations are caused by finger pressure and placement—rotation, translation, and contact area—with respect to the sensor and condition of the finger such as skin dryness and cuts.

Some important features of the GSM SIM 900 Modem:

1. Quad Band GSM/GPRS: 850 / 900 / 1800 / 1900 MHz.
2. Built in SIM (Subscriber Identity Module) Card holder.
3. Built in Network Status LED.
4. LDB9 (Serial port) for interfacing.

Features of 16X2 LCD Panel compatible with raspberry pi:

1. Dimensions: 2.2" x 3.35"
2. Comes with a 16x2 Blue & White LCD
3. Plug and play with any Raspberry Pi
4. Uses only the I2C (SDA/SCL) pins
5. This board/chip uses I2C 7-bit address 0x20.

Features of Raspberry Pi Model-B:

1. Broadcom BCM2835 System on Chip.
2. 700 MHz ARM1176JZF-S Core CPU/
3. Broadcom Videocore GPU.
4. 512MB Memory (SDRAM).
5. Two USB2.0 ports.
6. Composite RCA, HDMI Video Output.
7. Raspbian OS (Linux based OS).

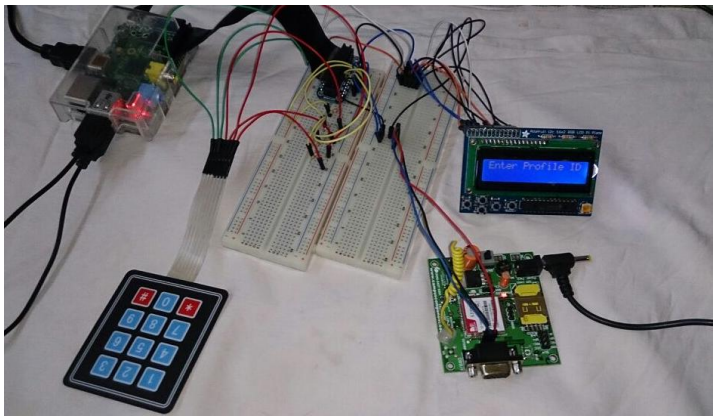

FIG 3: Theft Security System Hardware Assembly.

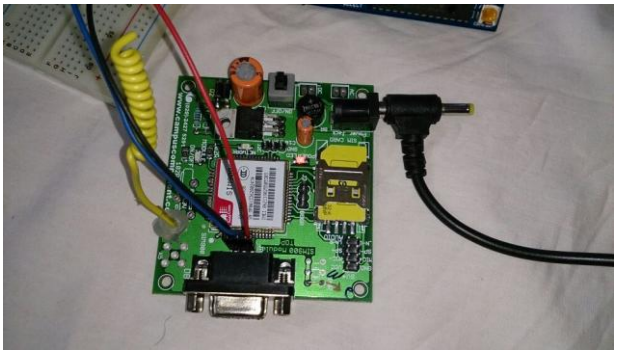

FIG 4: GSM SIM 900 Module.

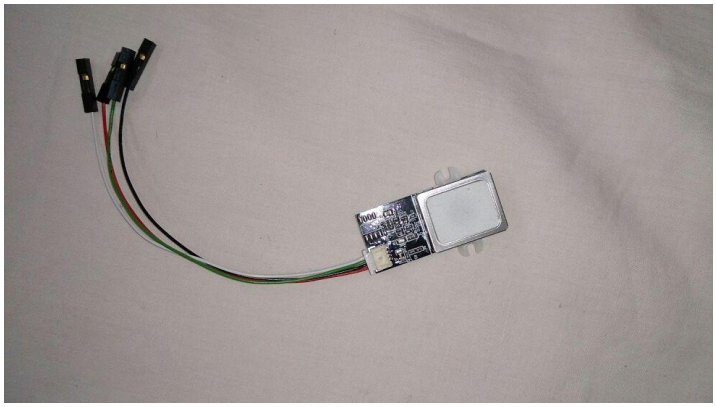

FIG 5: Fingerprint Scanner.

V. ADVANTAGES AND CONSTRAINTS

Advantages:

1. The first and foremost advantage of the proposed system is that none of the components would interfere with the functioning of the car. That way the engine won't be tampered with and warranty of the car won't be void.
2. *This is in accordance with the* third party- nature of the proposed system.
3. Nowadays, all the antitheft security systems that are out there depend on the car doors for entry of the intruder/thief. But the proposed system shall have an electro- magnetic switch fitted on the steering wheel key-hole. So even if the thief enters the car, he won't be able to drive it away since the electro-magnetic switch shall require a valid fingerprint ID/OTP to bypass it.
4. The system can be fitted in low-cost cars with price range from 1Lakh up to 5Lakh or more.
5. Very economical and user friendly.
6. Easy to operate and does not tamper with the engine at all.
7. The fingerprint scanner can store templates of up to 200 people at any given time.

Constraints/Limitations:

1. *A* limitation can be the availability of network coverage for the proper functioning of the GSM modem.
2. The power source for the Raspberry Pi has to be the secondary battery of the car. It should not draw power form the main battery.

VI. FUTURE ENHANCEMENTS

The proposed system can be further brought into serial production and used for regular customer sales. The per unit cost of the security system shall be very less than that of the one's provided by original equipments manufacturers (OEM).

VII. CONCLUSION

The proposed Biometric Fingerprint Based Anti-Theft Security System is perceived to be an upcoming technology which will make use of Biometrics in the most optimum manner. The system proposed, when put into proper functioning will revolutionize the Automobile Security Industry and will create scope for more employee and field of study. It will provide a cheap, reliable and efficient solution for automobile thefts which can be implemented by anyone on any car.

REFERENCES

[1] http://en.wikipedia.org/wiki/AntiTheftSecurity
[2] An Identity-Authentication System Using
[3] http://www.howstuffworks.com/antitheftsystemsin automobiles.htm

[4] Anil Jain, Lin Hong, Sharath Pakanti and Ruud Bolle, "*An Identity-Authentication System Using Fingerprints*" PROCEEDINGS OF THE IEEE, 0018–9219/97$10.00, VOL. 85, NO. 9. Year: SEPTEMBER 1997

[5] Raffaele Cappelli, Dario Maio, Davide Maltoni, James L. Wayman, and Anil K. Jain, "*Performance Evaluation of Fingerprint Verification Systems*", IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 28, NO. 1, Year: JANUARY 2006

[6] Robert W. Ives, Yingzi Du, Delores M. Etter and Thad B. Welch, *Senior Member,IEEE*,"*A Multidisciplinary Approach to Biometrics*", IEEE TRANSACTIONS ON EDUCATION, VOL. 48, NO. 3, Year: AUGUST 2005

[7] www.raspberrypi.org/forums

[8] [8]www.sparkfun.com

[9] www.adafruit.com

[10] www.stackoverflow.com