NEXT GENERATION ENGINE IMMOBILISER

Sagnik Basu Choudhuri[1], B Venkatesh[2], G Ramasubramaniam[3], J Sam Jeba Kumar[4]

[1, 2, 3]B.Tech, Students, [4]Assistant Professor, Department Of Instrumentation and Control Engineering, SRM University, Chennai, India

Abstract

Technological innovation in Automotive Electronics has led to the development of Engine Immobilisers. The present day Engine Immobiliser based on Radio Frequency Identification Device (RFID) are growing unsafe as professional hackers have been able to break into them. In 2005, a group of students in the Johns Hopkins University, USA hacked an RFID Engine Immobiliser and stole the vehicle in under twenty minutes. It is disturbing that almost a decade later the field of Engine Immobilisers has seen very little advancement. As a result the number of vehicle theft cases has risen exponentially in the past decade globally. The need of the hour is to design a system which enhances the security of the vehicle removing the drawbacks of the existing RFID system. We propose a system which replaces the prevalent technology with a Face Recognition System. Additionally, the system gives the owner remote access to the vehicle's ignition system further reducing chances of vehicle theft. Measures are also taken to enhance passenger safety. Ease of operation is supplemented through a Keyless Entry module.

Keywords: *RFID; Face Recognition; NI LabVIEW; Keyless Entry; Arduino UNO.*

----------***----------

1. INTRODUCTION

To avoid theft of a vehicle a device called Engine Immobiliser was introduced. The existing system uses a Radio Frequency Identification Device (RFID). A chip fit in the key fob of a modern car broadcasts an encrypted radio signal of specified length to the car as the driver starts the vehicle. If the signal is recognized by the car's receiver, it responds by sending an encrypted signal to the Engine Control Unit (ECU), which allows the car to start. If the driver tries using the incorrect car key fob, the ECU locks down the engine.

For over a decade and a half, Engine Immobilisers have played a crucial role in reducing car theft. But the proprietary encryption keys used to transmit data between the key fob, receiver and engine are so poorly implemented on some cars that they can be easily cracked [1]. Hence, the Engine Immobilisers are failing in their basic task to protect against car theft.

Further, it takes an Indian car manufacturer an average of Twenty days to replace the keys if the original keys and the duplicate get lost. The car stays in the lockdown state for that duration hampering the daily activities of the owner and his family.

2. IMAGE ACQUISITION

The first step of the system is to acquire an image of the driver and compare it to the stored templates to see if the driver is authorised to drive the vehicle. There is a provision to store three templates with which the live feed from the camera is compared. If need be more than three images can be stored. The acquired image is fed to NI LabVIEW with the help of Vision Acquisition Express, which is an additional tool to acquire, save and display images. We can use NI-IMAQ to acquire from analog, parallel digital, Camera Link camera & NI Smart Camera. It can also be used with NI-IMAQdx with USB3 Vision, GigE Vision, IP (Ethernet) & IEEE 1394 devices [2].

In our prototype, we are acquiring the images from an Android mobile phone's camera. The images taken from the camera are feed into NI LabVIEW Vision Acquisition Software (VAS) using an Android application called "Smart Cam". To set the mobile phone camera as the image source, we have to select the Smart Cam Camera option in the Camera device list of the NI Vision Acquisition Software.

3. SELECTION OF LIGHT SOURCE

The system that we are proposing has to work seamlessly in both the day and the night condition. Hence, we have to select a light source that enables image processing in the night as well with approximately equal efficiency.

Due to the differences of the spectral absorption, scattering, reflectance, transmittance of human skin and blood, the human face texture imaging clarity will be affected [3]. According to the study by Li Queyu et al, with increasing wavelength, the skin reduces spectral absorption [4].

The incident light must have very good penetration of the skin of the face. Medical studies have shown that near-infrared light compared to other bands of light, such as

visible light on human skin has a strong penetrating power, and better absorption by haemoglobin, so the near-infrared light is used in imaging of the human body vein as the best fill light source [5].As the 850nm near-infrared light on skin penetration ability, and relative to the other band near-infrared light can be better absorbed by haemoglobin, and least absorbed by other organizations [3].

4. IMAGE PROCESSING

The three main stages of Face Recognition are:

- Image pre-processing
- Template Storage
- Template matching
- Authentication

The Image Processing is achieved using the NI LabVIEW Vision Development Module (VDM).

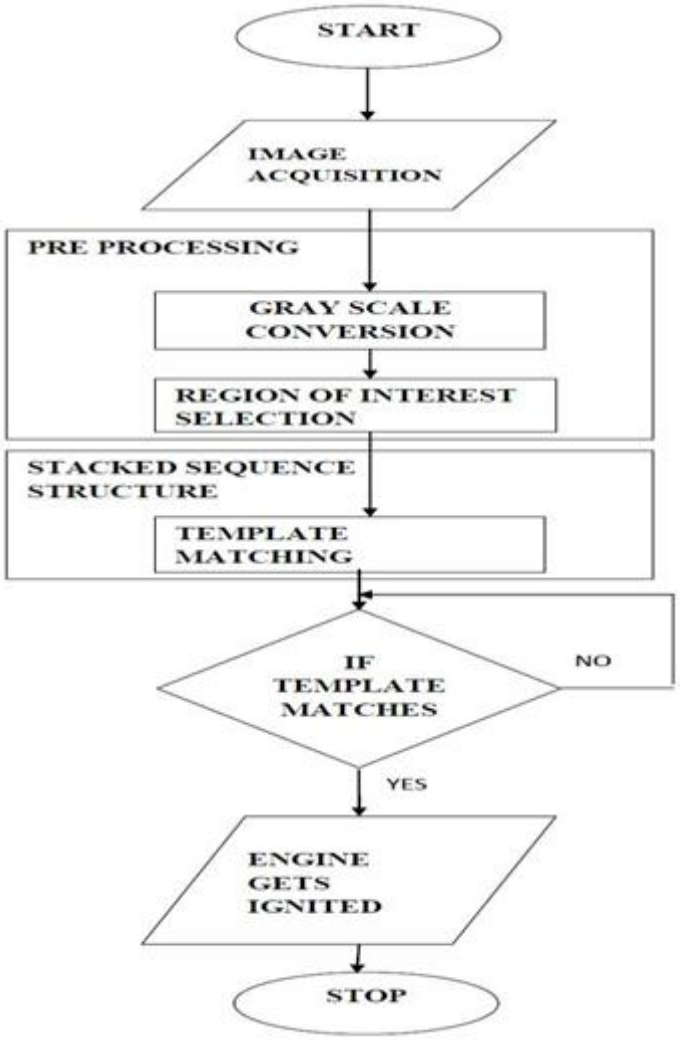

Fig -1: Flow Chart of Image Processing

4.1 Image Pre-Processing

The image obtained from the camera has to be pre-processed in order perform template matching namely reducing the Region of Interest (ROI) & Gray scale conversion.

4.2 Template Storage

Images are taken of three people who are authorised to operate the car and are stored as template in the database.

4.3 Template Matching

Pattern recognition is a common technique that can be applied for the detection and recognition of objects. The algorithm not only searches the exact apparition of the image but also finds a certain grade of variation with respect to the pattern

4.4 Authentication

If the face recognition is successful then the engine of the car starts else it does not.

5. THE STATE MACHINE

The state machine is an integral part of the project. In terms of LabVIEW, a State Machine is a combination of a While Loop having a set of Shift Registers along with a Case Structure. The State Machine evaluates the input of the user and it executes the case which corresponds to that particular input.

The major types of State Machine supported by LabVIEW are [6]:

- Enumerated And Type Definitions State Machine
- Sequence Type State Machine
- Test Executive Type State Machine
- Classical Style State Machine

For our model we have selected the Enumerated and Type Definitions State Machine.

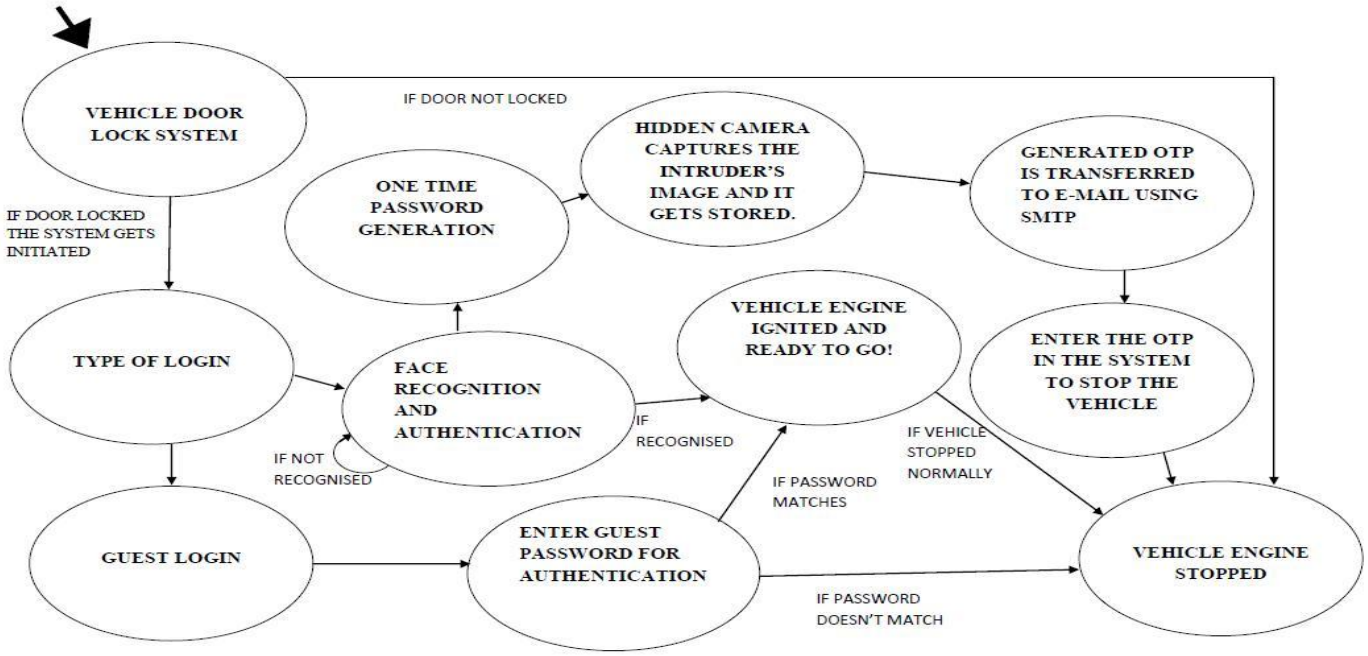

Fig 2: The basic flow diagram describing the State Machine

6. THE BASIC PROCESS

The state machine first waits for the user's input. If the user selects the Face Recognition Method then the State Machine executes the cases which belong to that particular function. After receiving the input from the user, the State machine executes the image processing cases where it is ascertained whether the user is an authorized driver or not. If yes the car engine starts else it does not. The system has provision for a Guest Login where a third party user can run the car after authentication from the owner. The authentication is a specific Password which only the owner knows. If the Guest Login Password is authentic, the car starts else it does not.

We have also introduced a system which stops the car if a thief manages to steal and run the car. In case a thief steals the car there is a separate system which generates a unique One Time Password (OTP). The OTP is mailed to the registered mail id of the owner using Simple Mail Transfer Protocol (SMTP), present in LabVIEW. The system also switches on a hidden camera when the OTP is generated. The hidden camera will take a set number of images of the thief without his knowledge. The image of the thief is stored in the memory which can be retrieved later and can be handed later to the concerned authorities.

The system enables remote switching of the car's engine off through the NI Data Dashboard App (Version 2.2), which helps us to remotely control a process [7]. This app enables the owner to feed in the Guest Login password or the OTP from a remote location. Alternatively, both the passwords can also be entered from an Internet Browser providing additional security. This helps us to stop the car in the event of a theft.

Regarding the safety of the passenger we have also designed a system which does not allow the car to switch on unless and until all the doors of the car are latched. In case any of the doors open while the car is running, the car will come to a halt.

7. THE IMMOBILISING ACTION

Most cars nowadays have an Electric Fuel Pump [8]. The main method by which we plan to immobilize the car is to control its fuel pump. It will be easy to switch off the fuel pump as and when the LabVIEW state machine executes that command.

Further, the Engine Control Unit (ECU) of a car are interconnected by the Controller Area Network Bus (CAN Bus) [9]. The other prospective method to immobilize the car would be to disable the ECU. This can be achieved by connecting the LabVIEW system to the CAN Bus of the car.

8. KEYLESS ENTRY

The system also incorporates a Keyless Entry system.

In our prototype we have used an Android app called Arduino Bluetooth Control which establishes connection with a Bluetooth module. An Arduino UNO works as the

body controller which is a computer in the car. When the power door locks, the body controller monitors all of the possible sources of an "unlock" or "lock" signal. It monitors a door-mounted touchpad and unlocks the doors when the correct code is entered from the mobile. When it receives a signal from the mobile, it provides power to the actuator that unlocks or locks the doors [10].

The range of the Bluetooth system can be increased using a Class 1 Bluetooth device which transmit at 100mW and have a standard range of approximately 100 meters or 328 feet. The range is comparable to that of an 802.11b WLAN device [11].

9. CONCLUSIONS

The primary testing that we have done on the on all the sub systems of the LabVIEW code have yielded a perfect result.

We are convinced that the Engine Immobiliser that that we wish to implement will bring down the number of car theft cases keeping passenger safety in mind.

REFERENCES

[1] Criminals find the key to car immobilisers http://www.newscientist.com/article/mg20827894.500-criminals-find-the-key-to-car-immobilisers.html#.UyC7AvmSxiZ

[2] NI Vision Acquisition Software http://sine.ni.com/nips/cds/view/p/lang/en/nid/12892

[3] Weiqi Yuan, Yonghua Tang, "Driver authentication device based on the characteristics of Palm print and Palm Vein", International Conference On Hand-based Biometrics(ICHB), The Hong Kong Polytechnic University, Hong Kong, China, 2011

[4] Q. Y. Li, Y, Wang. And Y. L.Zhang, "VIVO determination of the absorbance spectra of human skin", Photon Journal, vol.31, no.11, pp. 1321–1324, 2002.

[5] Guotian Yang, "Palm vein image acquisition and recogniton system research", Master Dissertation of Shenyang University of Technology, 2010

[6] Rick Bitter, Taqi Mohiuddin, Matt Nawrocki, LabVIEW: Advanced Programming Techniques, Second Edition

[7] Enhancements to the Data Dashboard for LabVIEW app http://www.ni.com/white-paper/14033/en/

[8] Are RFID ignition systems secure? http://electronics.howstuffworks.com/gadgets/automotive/rfi d-ignition-system.htm/printable

[9] Controller Area Network (CAN) Understanding the basics and its role in Automotive diagnostics http://www.warwickcontrol.com/ata/Infobackup_and_librar y/Basicbus

[10] How Power Door Locks Work http://auto.howstuffworks.com/power-door-lock1.htm

[11] Dispelling Common Bluetooth Misconceptions http://www.sans.edu/research/security-laboratory/article/bluetooth

BIOGRAPHIES

Sagnik Basu Choudhuri B. Tech Fourth Year, Instrumentation and Control Engg

B. Venkatesh, B. Tech Third Year, Instrumentation and Control Engg.

G. Ramasubramaniam, B. Tech Third Year, Instrumentation and Control Engg

Mr. J Sam Jeba Kumar, Assistant Professor, Instrumentation and Control Engg