Automobile Intrusion Avoidance Using Face Detection and Finger Print

HamidKaashif S, Henrick John Antony J, Saravana Raj R & Nithya D

Department of Electronics and Communication,
Panimalar Engineering College, Anna University, Chennai
E-mail : hamidkaashif@gmail.com, anthenjohn@gmail.com, sharavan21@gmail.com, nithya_do@yahoo.co.in

***Abstract* - The incontrovertible fact in the world is that the number of automobiles particularly cars are exponentially increasing in terms of production as well as theft attempts. Even though lot of automobile manufacturing industries took efforts to produce high quality automobile anti-theft systems, it does not end the theft of automobiles. An aberrant fact is that for every six minutes a vehicle is stolen from India. This paper focuses on automobile security which consists of two-step verification. Face Recognition using Matlab is followed by Finger print recognition using Microsoft Visual Basic.**

Keywords - Haar Wavelet, Weber Law, GSM, GPS, MMS, Matlab, Visual Basic.

I. INTRODUCTION

Security on any product is one of the major concerns today. For automobiles, some of the following measures like Face recognition, Voice recognition, Finger print scanning, Retinal scanning and keypads are used for security purposes, but each measure has its own pros and cons. This paper uses two of the following techniques to prevent automobile theft: Face recognition and Fingerprint recognition. Some of the other measures are complicated and the efficiency is low. The purpose is to prevent the theft of automobile by using Bio-Metric equipment and Wireless Communication Techniques. Initially the portrait image of the person in the driver's seat is captured and verified with the pre-stored images in the database. In case of a match, the finger print is then verified. On positive matches on both, the car engine starts. In case of a mismatch of anyone one of the above, the captured image of the person is sent via MMS to the owner's personal mobile number and also the GPS coordinates of the automobile is sent to the same. If the owner recognizes the image of the person and sends a positive message via a SMS, which is a prescribed code, then the ignition takes place. In case of a different code, no ignition takes place.

II. LITERATURE SURVEY

A. Commonly used tools by automobile racketeer

- Slide hammers puller to break into the door locks and the cylinder lock.
- Multi-meters or a test light to find a power source.
- Spare wires or a screwdriver to connect the power source to the ignition and starter wires.
- A generic rod and hook tool kit to slip between the car window and car frame and to open the lock behind the window. A common one is called the "Slim Jim".
- Many keyless ignition/lock cars have weak or no cryptographic protection of the unlock signal. Proof-of-concept "thefts" of top-of-the-line luxury cars have been demonstrated by academic researchers using commercially available tools such as RFID microreaders, but is unknown whether the attack has been used for actual theft.
- A firearm or other weapon such as a baseball bat, or a utility knife or a box cutter to break open a window or threaten a passenger if inside the car.

B. Existing Systems

There are various methods of prevention to reduce the likelihood of automobile getting stolen. These include physical barriers, which make the effort of stealing the vehicle more difficult. Some of these include:

- Devices used to lock a part of the vehicle necessary in its operation, such as the wheel, steering wheel or brake pedal. A popular steering wheel lock is The Club.
- Immobilizers, allowing the vehicle to start only if a key containing the correct chip is present in the ignition. These work by locking the steeringwheel and disabling the ignition.
- Chances of heist can also be reduced with various deterrents, which give the impression to the thief that he/she is more likely to get caught if the vehicle is stolen. These include:

➢ Car alarm systems that are triggered if a breaking and entry into the vehicle occurs [1].

➢ Microdot identification tags which allow individual parts of a vehicle to be identified. A microdot is text or an image substantially reduced in size onto a small disc to prevent detection by unintended recipients. Microdots are normally circular around one millimeter in diameter but can be made into different shapes and sizes and made from various materials such as polyester and also metal.

➢ Kill switch circuits are designed to frustrate or slow down the efforts of a determined car thief. Kill switches are often located between crucial parts of the starting system, between the battery source and the coil, or the fuel pump. A car cannot start without first flipping these kill switches to closed position. Savvy car owners hide these kill switches in obscured areas, under the dashboard, beneath the seat, behind a chair, etc.

➢ Signage on windows warning of the presence of other deterrents, sometimes in absence of the actual deterrents.

Recently, face recognition was used as security measure. Algorithms like PCA (Principle Component Analysis) [2], LDA (Linear Discriminant Analysis) [3], DCT (Discrete Cosine Transform) SVDA (Support Vector Discriminant Analysis) were used. But, the accuracy is low, and many factors are needed to be considered. Some of the performances of each algorithm are shown below:

- *Performances obtained for ORL Database[4]*

Algorithm	Performance
PCA (Principle Component Access)	71.38%
DCT (Discrete Cosine Transform)	67%
Hybrid Method (DCT + PCA)	72.77%

LBP (Local Binary Pattern) is used with any one of the above algorithms to improve the efficiency [5].

- *Performances obtained for JAFFE Database[6]*

Algorithm	Performance
LBP + SVDA	69.3%
LBP+PCA	63.7%
LBP+LDA	64.3%
PCA	56.3%
LDA	58.2%
2DPCA	63.1%
2DLDA	60.5%

Background colorsplay a major role on use of these algorithms. A minor change would give an erroneous output. Time for processing the images with the above algorithms isalso quite high. To overcome these drawbacks, the proposed system uses a combination of the following algorithms; Haarcascade and Weber Law.

III. PROPOSED SYSTEM

The proposed system consists of a face recognition module to get real time image of the driver, a finger print module to scan the finger print of the driver, a Global Positioning System module to keep track of the automobile's location, a Global System for Mobile communication module to send MMS and SMS to the owner's mobile, a Relay, an Embedded control platform to interface the relays and a Power supply unit (Fig 1) and are explained below.

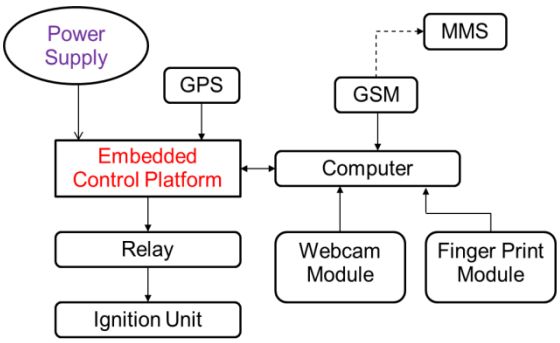

Fig 1 : Block diagram of proposed system

A. *Embedded Control Platform*

ARM7 (Advanced RISC [Reduced Instruction Set Computer] Machine) microprocessor is used in the embedded control platform. LPC2148 (Low Power Consumption) is the IC used. ARM7 has two UART's (Universal Asynchronous Receiver/Transmitter), it is connected to the computer and the GPS module.

Frequency of 32MHz with a DC power supply of 3.38V is used to run the processor. Motor of the automobile is connected to port 0 of the processor.

- *Serial Communication:*

The serial communication unit contains MAX 232 IC and two serial UART ports. It uses a single data line for transmitting and one for receiving data. Most often 8-bit data is transferred, as follows: 1 start bit, low level, 8 data bits, 1 stop bit, and high level. The low level start bit and high level stop bit mean that there's always a high to low transition to start the communication.

- *Power Supply:*

The AC voltage, typically 220V rms, is connected to a transformer, which steps that ac voltage down to the level of the desired DC output. A diode rectifier then provides a full-wave rectified voltage that is initially filtered by a simple capacitor filter to produce a DC voltage. This resulting DC voltage usually has some ripple or AC voltage variation.A regulator circuit removes the ripples and has the same DC value even if the input DC voltage varies, or the load connected to the output DC voltage changes.

B. Global System for Mobile Communication (GSM)

GSM modem consists of a slot to fix a SIM card (Subscriber Identity Module) to send MMS (Multimedia Messaging Service) containing the image of the driver. Additionally, a SMS (Short Message Service) containing the GPS coordinates of the automobile position is sent to the owner's mobile phone. Baud rate of 19,200 bits per second is set here.

C. Global Positioning System (GPS)

This module provides the latitude and longitude values, which is sent as SMS to the owner's mobile phone. Baud Rate of 4800 bits per second is used here [7]. GPS works on a process called trilateration were at least four satellites combine to generate the GPS values.

For Example, Latitude and Longitude values generated during an experiment are:

Latitude: 13.028098

Longitude: 80.228884

- *Coordinate Conversion*

	Degrees	Minutes	Seconds
Latitude	13	1	41.1522
Longitude	18	13	43.9818

D. Webcam and Fingerprint Module:

A webcam is a video camera that feeds its image in real time to a computer or computer network. A webcam with a resolution of 640x480 is used to capture a high quality image.

A fingerprint scanner system has two basic functions - it needs to get an image of a finger, and it needs to determine whether the pattern of ridges and valleys in the image matches the pattern of ridges and valleys in pre-scanned images.

Working of proposed system

As soon as the driver enters the automobile and closes the door, a portrait is captured and compares with the image which is stored in the database. If the image matches with the database, then fingerprint is scanned and verified. On a positive match, DPDT switches and the automobile engine ignites. On the contrary if any of the scan either face or fingerprint mismatches, then the RGB image of predefined resolution is sent as MMS to the owner's mobile phone along with the GPS values. If the owner recognizes the image, then a short command is sent by the owner to the GSM module in the car, the automobile engine ignites. If the owner doesn't recognize the image, he can inform the police and necessary action would be taken by them. The working process is clearly shown in the flow chart shown below (Fig 2).

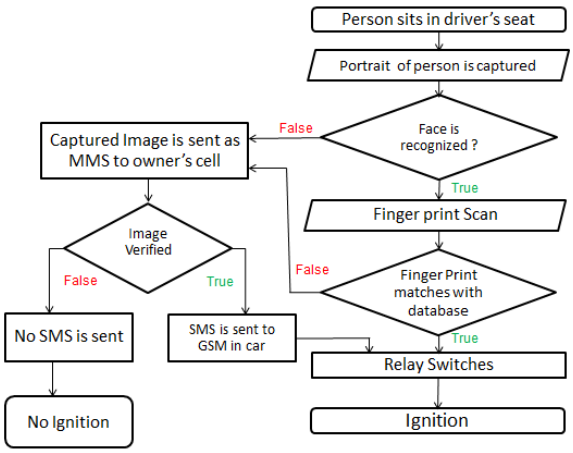

Fig 2 : Flow Chart of the process

IV. FACE RECOGNITION

Enrolment Stage is a onetime process where the owner's image is captured, then processed and stored in a database.

Authentication stage is a process where the driver's image is captured and then compared with the owner's image stored in the database.

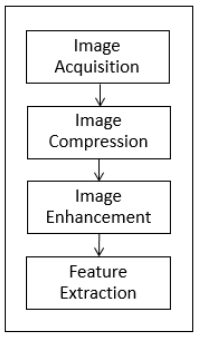

Fig 3. Image Processing Steps

A. Image Acquisition:

This is the first step which includes capturing the RGB image of the driver using a webcam attached to the sun shield. Various parameters like color space, resolution and adaptors are specified to make the processing ease.

B. Image Compression:

Image compression is done by converting the image in RGB to gray scale to reduce the size of the image, make the processing faster. The size of the image is reduced by three times; for example, a RGB image is 3 MB, after converting to gray scale would result in an image which is 1 MB.

C. Image Enhancement:

Image enhancement is done to highlight the required attributes. Haar cascade is used to crop the image and resize the image to a smaller resolution which contains attributes for the feature extraction. The function shown below is used for the enhancement process.

```
Face = FaceDetect('haarcascade_frontalface_alt2.xml',A);
```

- *Haar Wavelet Transform*

The Haar wavelet is a certain sequence of rescaled "square-shaped" functions which together form a wavelet family or basis [9]. Wavelet analysis is similar to Fourier analysis in that it allows a target function over an interval to be represented in terms of an orthonormal function basis.

The Haar sequence is now recognized as the first known wavelet basis and extensively used as a teaching example in the theory of wavelets.

The Haar wavelet's mother wavelet function ψ(t) can be described as:

$$\psi(t) = \begin{cases} +1; & 0 \le t < \frac{1}{2} \\ -1; & \frac{1}{2} \le t < 1 \\ 0; & Otherwise \end{cases} . \qquad (1)$$

And it's scaling function

$$\phi(t) = \begin{cases} 1; & 0 < t < 1 \\ 0; & Otherwise \end{cases} . \qquad (2)$$

Haar used these functions to give an example of a countable orthonormal system for the space of square-integral functions on the real line.

D. Feature Extraction:

Features are extracted using low pass filter. The image is filtered five times. The high frequency components containing noises and edge informationare removed. The lowest frequency component*LLLLLLLLLL*(Fig 4) contains the features. This process is called as sub band image decomposition (Weber's Law).

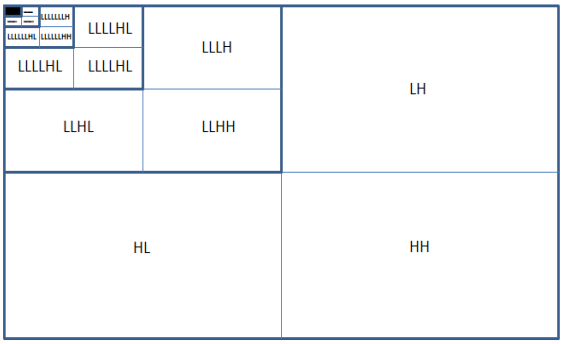

Fig. 4 : Sub band Image Decomposition (Weber's Law)

- *Weber's Law*

Weber's law has a logarithmic relation. Weber's law states that the relationship between the physical magnitudes of stimuli and the perceived intensity of the stimuli is logarithmic. This technique is applied to image processing to enhance the image effectively [8]. Weber's law is defined as:

$$C = k \log L + b \quad (L>0) \qquad (3)$$

Weber's law can be best understood from the following example. Consider a photo taken in a dark room. The obtained photo actually consists of 2 different things. One is what we visually perceive in that image and the other is what that is actually present in the image. Weber's law simply states that the relation between these two is logarithmic.

Enrolment Stage

Initially, RGB image of the owner is captured with a resolution of 640x480(Fig 5a). Image is converted to gray scale (Fig 5b), then the face is detected and cropped using Matlab functionwith a resolution of 256x256 (Fig 5c).

Fig 5. a) RGB Image, b) Gray Scaled Image, c) Cropped Image

Authentication Stage

During the authentication stage, a portrait image is captured and features are extracted (Fig 6) and verified with the database image.

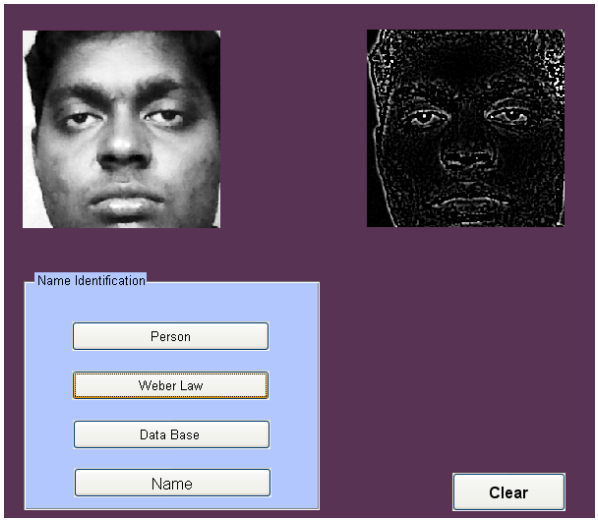

Fig 6. Feature Extraction from Image

The function below is used to extract the features.

y1=weberlaw(nn,alfa,sigma,X);

In the above function,

nn=9;

alfa =2;

sigma =1;

X is the image captured.

Only one image can be stored in the database. Driver's image is shown twice (Fig 6). One image shows the cropped grayscale image, other shows the extracted feature of that image. Person is clicked to load the driver's image. Weber law is clicked to extract features from the image. Database can only be accessed by the owner which contains the driver's image and his extracted features.

V. FINGERPRINT RECOGNITION

A fingerprint is the pattern of valleys and ridges on the surface of a fingertip. No two individuals have common fingerprints. The local ridge characteristics andtheir relationships contribute to the uniqueness to each individual. A total of 150 different local ridge characteristics (islands, short ridges, enclosure, etc.) have been identified. These local ridge characteristics are not evenly distributed. Most of them depend heavily on the impression conditions and quality of fingerprints and are rarely observed in fingerprint [10].

The two most prominent localridge characteristics, called minutiae, are

- *Ridge ending* is defined as the point where a ridge ends abruptly.
- *Ridge bifurcation* is defined as the point where a ridge forks or diverges into branch ridges.

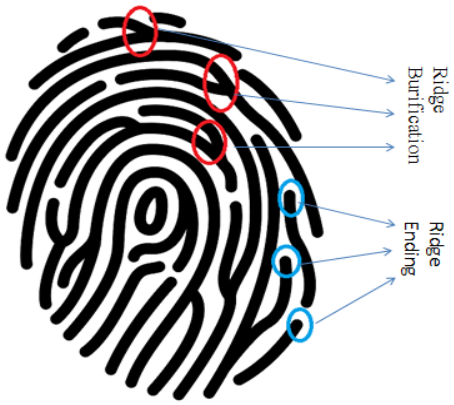

Fig 7. Prominent Local Ridge Characteristics

Algorithm for Feature Extraction

1) Subject the gray scale texture image to 2- level discrete wavelet transform decomposition.

2) At each level, the wavelet transform decompose the given image in to three directional components, i.e., horizontal, diagonal and vertical detail sub bands in the direction of 0,45 and 135 respectively apart from theapproximation (or) smooth sub band. For the second level LL sub-image compute the following three features.

- Standard deviation

The standard deviation of the image gives a measure of the amount of detail in that sub band.

- Kurtosis:

It measures the peaked ness or flatness of the

Distribution and is given by

$$K = \frac{1}{N}\sum_{i=1}^{N}\left(\frac{x_i - \mu}{\sigma}\right)^4 \quad . \qquad (4)$$

where μ is the sample mean of the N pixels within the image and σ is standard deviation.

- Skewness

Skewness is a measure of the asymmetry of the data around the sample mean, denoted by g1.

$$g1=\frac{m_3}{m_3^{3/2}}*\frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})^3}{\{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})^2)\}^{\frac{3}{2}}}. \quad (5)$$

Where, x_i is the ith value, $\bar{x}$ is the sample mean, m_3 is the sample third central moment, and m_2 is the sample variance. Given samples from a population, the equation for the sample skewness g1 above is a biased estimator of the population skewness. A distribution that is skewed to the left (the tail of the distribution is heavier on the right) will have a negative skewness. A distribution that is skewed to the right (the tail of the distribution is heavier on the left), will have a positive skewness.

3) Compute the three features for original image also. Thus the length of the feature vector is: 3 features * [(3*10) + original image] = 93.

VI. CONCLUSION

In this paper, we propose a low-cost high security system which consists of a face detection subsystem, a GPS module, a GSM module, a control platform and a fingerprint module. Comparing with traditional car security system, this system does not need any sensor, and cost much less.

Experiment results prove that this proposed security system works well, and can be put forward to practical application. From the paper, we conclude that face recognition and fingerprint scanning techniques can provide important highly accurate and cost efficient measures required for the authentication of the user and as a result avoid automobile theft. It ultimately protects the vehicle from the usage of unauthenticated users.

We are considering redesigning the system replacing ARM 7 processor with FPGA (Field Programmable Gate Array) and GPS with IRNSS (Indian Regional Navigational Satellite System) to extend the applications of our proposed system.

VII. REFERENCES

[1] Pang-Chieh Wang, Ting-Wei Hou, Jung-Hsuan Wu, and Bo-Chiuan Chen, "A Security for Car Appliances"; International Journal of Aerospace and Mechanical Engineering.1:3 2007.

[2] K. Sangeetha, S. Arulraj, G.Aravind, M.M. Vignesh; "Intelligent Vehile Theft Prevention and Location Finding system using Face Detection based on Image Processing", International Journal of Communications and Engineering; Volume: 1, Issue: 3 -2012.

[3] Yu Bing, Jin Lianfu, Chen Ping, "A New LDA-based Method for Face Recognition"; IEEE 2002.

[4] M. A Anjum, M. Y. Javed, and A. Basit, "Face Recognition Using Double Dimension Reduction"; World Academy of Science, Engineering and Technology4, 2007.

[5] Anagha V. Malkarpurkar, RupalPatil, Prof. SachinMurarka; "A New Technique for LBP Method to Improve Face Recognition"; International Journal of Emerging Technology and Advanced Engineering; Volume 1, Issue 1, November 2011.

[6] V.Gomathi,Dr.K.Ramar, and A. SanthiyakuJeevakumar, "Human Facial Expression Recognition using MANFIS Model"; World Academy of Science, Engineering and Technology26 2009.

[7] Muruganandham, P.R.Mukesh, "Real Time Web based Vehicle Tracking using GPS"; World Academy of Science, Engineering and Technology37 2010.

[8] Jie Chen, Shiguang Shan, Guoying Zhao, Xilin Chen, Wen Gao1, MattiPietikäinen, "A Robust Descriptor based on Weber's Law"; IEEE Computer Vision and Pattern Recognition, 2008.

[9] P. Raviraj and M.Y. Sanavullah, "The Modified 2D-Haar Wavelet Transformation in Image Compression"; Middle-East Journal of Scientific Research 2 (2): 73-78, 2007.

[10] Lin Hong, Yifei Wan, and Anil Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation"; IEEE transactions on pattern analysis and machine intelligence, Vol. 20, No. 8, August 1998.

[11] K.Thaiyalnayaki, S. Syed Abdul Karim, P. VarshaParmar, "Finger Print Recognition using Discrete Wavelet Transform"; 2010 International Journal of Computer Applications (0975-8887) Volume 1 – No. 24.

◈◈◈