Research Article

Ahmed A. Elngar* and Mohammed Kayed

Vehicle Security Systems using Face Recognition based on Internet of Things

<https://doi.org/10.1515/comp-2020-0003>

Received Sep 15, 2019; accepted Nov 12, 2019

Abstract: Nowadays, the automobile sector is one of the hottest applications, where vehicles can be intelligent by using IoT technology. But unfortunately, these vehicles suffer from many crimes. Hence it has become a big challenge for the IoT to avoid such these crimes from professional thieves. This paper presents a proposal for the development of a vehicle guard and alarm system using biometric authentication based on IoT technology. Whereas, for vehicle security issues; the proposed system *VSS – IoT* gives only full access for authorized vehicle's driver based on the interface of a *Raspberry Pi 3 Model B+* development board, Pi camera, *PIR* sensor, and smart-phone. Therefore, if the proposed system detects an unauthorized person inside the vehicle, then the system will notify and send his image to vehicle's owner and/or to a police workstation through the Internet, as well as, its location in case the vehicle is stolen or damaged. The proposed system is tested on two datasets that are ORL dataset and our dataset. The experimental results of the *VSS – IoT* showed that the accuracy is 98.2% on ORL dataset, whereas 99.6% when applied on our dataset. Besides, the *VSS – IoT* enhances the sensitivity to 97.7% which is important for real-time. As well as the result demonstrated that the proposed system took shorter time 0.152 sec under different illumination conditions, when the value of the threshold is 3×10^3 and 3.50×10^3 . Therefore, the *VSS – IoT* is very robust and reliable for face recognition when deployed on the low-power processor.

Keywords: Internet of things, face recognition, haar-cascade, principle component analysis, vehicle security systems

1 Introduction

In recent years, the popularity of the automobile sector is increasing all over the world [1]. But unfortunately there exist an exponential increase in vehicles crime [2]. At the present time, most vehicles are controlled via using mechanical keys, security cards, and password/pattern. But, with the development of *IoT* technologies and many embedded mechanisms, the vehicle security systems are continuously improving [3]. These improvements are depending on the vehicle's owners and police workstations requirements [4]. Whereas, they are not only concerning with the theft of vehicle contents, but also the loss of vehicles and the personal security requirements of the vehicle's owner[5].

Many well-known biometrics-based identification and verification techniques existed. Fingerprints, facial features, and iris have been employed in various security applications. Face recognition is considered a good choice biometric technique For vehicle security and alarm systems because it based on human face feature information and can work under different conditions [6]. Therefore, most of the face recognition techniques have been developed to achieve a higher rate of discrimination [7].

Meanwhile, the face recognition process uses some complex calculations, this paper proposes a reliable *VSS – IoT* system based on a low power processor as a guard against vehicle theft [8]. This system converts the images captured by the USB camera installed in the vehicle to gray-scale images to detect and recognize faces in real-time. Where the combination of *AdaBoost* algorithm with *Haar – Cascade* classifier improves face detection accuracy [9]. Then the proposed system employs the *PCA* algorithm to recognize drivers' faces [10].

This paper aims to employ the proposed face detection and recognition method for vehicle security systems through the interfaced of *IoT* technology with some sensors shielding. Whereas, the system is based on *Raspberry Pi 3 Model B+* development board and a smart-phone to implement the idea. The *Raspberry Pi 3 Model B+* development board can be interfaced with a motion sensor, servo motor and USB

*Corresponding Author: Ahmed A. Elngar: Faculty of Computers and Artificial Intelligence, Beni-Suef University, Beni-Suef, 62511, Egypt; Email: elngar_7@yahoo.co.uk

Mohammed Kayed: Faculty of Computers and Artificial Intelligence, Beni-Suef University, Beni-Suef, 62511, Egypt; Email: mskayed@gmail.com

camera. Also, a *Raspberry Pi 3 Model B+* can be programmed, so can be able to send an email to a prescribed *mailhub*, retrieve and send data to *Firebase* server which connected with Android mobile application for real-time video analysis.

By using this system, when unauthorized person face is found; the system will analyze it and send his/her image to the vehicle's owner and/or police workstation through *IoT* networks. Hence, the experimental results of the *VSS-IoT* showed that the accuracy is 98.2% on ORL dataset, whereas 99.6% when applied on our dataset. Besides, the *VSS-IoT* enhances the sensitivity to 97.7% which is important for real-time. As well as the result present that the proposed took less time 0.152 sec under different illumination conditions when the value of the threshold in 3×10^3 and 3.50×10^3 compared to other systems.

Energy conservation is one of the prominent issues to build smart vehicle security systems. Thus, a low power processor becomes an interesting topic to be investigated and evaluated by face recognition performance. Therefore, the proposed system provides low *CPU* utilize and low memory usage 76% and 53.5%, respectively, depending on the camera pixels used.

The rest of this paper is organized as follows: Section 2 gives the problem formulation. Section 3 gives a literature survey. Section 4 introduces the proposed (*VSS-IoT*) system for vehicle security. Section 5 gives the implementation results and analysis. Finally, Section 6 contains the conclusion remarks.

2 Problem formulation

Access rejection to the vehicle security system from the unauthorized person is a problem, but unfortunately, the actual problem is how to identify him/her face. Most robbed vehicles systems will help to get recovered, but the crime has already happened. Therefore, a good vehicle systems should be developed to offer a security based on new technologies like the Internet of Things (*IoT*) [11]. The vehicle system must employ user authentication for access control using biometric authentication based on *IoT* in a real-time. Moreover, the system should monitor the vehicle for any suspicious activity inside it [12]. The surveillance system must keep the vehicle secured by notifying the authorized driver via his/her Mobile Application/Email in case of any unauthorized person, or any intrusion try to access the vehicle security system. Also, the system should provide some extra features like vehicle location, within the

same hardware without increasing complexity and cost [13].

Let z_t be set of surveillance system sensors values acquired at time t .

$$z_t(a) = D_t[b_t](a), \forall a \in A \quad (1)$$

Where,

D_t denoted as a transforming factor of the original record b_t , and $a \in z^2$ indicates the sensors values that belonging to the regular record $A \subset z^2$. As far as there is no suspicious activity.

$$D_t[b_t](a) = b_t(a) + \eta_t(a), \forall a \in A \quad (2)$$

Where,

η_t is a random variable estimating for record noise values, and b_t are acquired from the same sensor even though typically $b_t \neq b_{t-1}$; because values of surveillance system record are changed.

When at time τ^* an external disturbance introduces a suspicious, the record b_t is degraded by an unauthorized person or unknown suspicious activity and z_t becomes:

$$D_t[b_t](a) = \int b(e)h_t(a, j)d_j + \eta_t(a), \forall a \in A, t \geq \tau^* \quad (3)$$

Where,

$h_t(a, j)$ is the value-spread function at value $a \in A$.

The proposed *VSS-IoT* is a system used to analyze a sequence of $\{z_t, t = 1, \dots, \text{number of sensors}\}$ to detect and recognize any unauthorized/intrusion face and time instant τ^* when suspicious activity occur as in equation 3. We assume that T_0 is suspicious-free values are provided for training.

3 Literature survey

The *IoT* performs intelligent functions, which lead to avoid vehicle theft [14]. Many authors have been working on vehicle security systems to provide the best mechanisms not only concerning with the theft of vehicle contents but also the loss of vehicles, and the personal security requirements of the vehicle's owner. According to their works; they have developed a vehicle security systems based on "Biometric Authentication" type such as eye, finger, face recognition, etc [15] [16]. This section describes some relevant collaborations which are proposed in recent years.

Authors in paper [1] propose anti-theft and driver surveillance embedded system. They used biometric authentication to access the vehicle. Authors claimed that

the system deploy *LBPH* algorithm for face recognition. Also, they showed that the system was simple and provided better results in various light conditions.

As stated by [17], authors presented an embedded vehicle security system called "POLLUX". The security of the system based on machine vision technology. It acts as a new level of preventing the theft which protects the vehicle in a manner that does not intrusive the drivers. The system used a neural network (*NN*) as face detection and used support vector machines (*SVM*) for face recognition.

The main aim of the work in [18] is offering advanced security system in the vehicle. The program consists of a password custom to meet face detection/recognition program, a GSM module and a control platform. Also, face detection system uses the optimized Local Binary Pattern (*LBP*) algorithm to detect the face of the users. In addition, the system used the *PCA* algorithm as face recognition.

Authors mentioned in [6] that they proposed a security system based on wireless communication and Bluetooth module. They tried to use the *GSM* module for sending messages. The vehicle's owner can control the engine/ignition and turn it off at any time. Authors also suppose the system can use a password through the keypad (with ≤ 3 chances) which controls the safety of vehicle locker door and wearing of a seat belt. Also, The controller is connected to a Bluetooth module.

According to [7], authors proposed a low-cost expendable framework for embedded smart vehicle security system. In which authors claim that the system consists of a face detection subsystem, a *GPS module*, a *GSM module* and a control platform. The optimized Haar cascade algorithm is used in face detection subsystem. Also, it can recognize faces in the vehicle, and make an alarm soundlessly.

Authors in [19] presented a design and develop face recognition system. They use a Haar cascade in detecting faces from a given image. Then, the system employ an Artificial Neural Networks *ANN* for face recognition. Authors claimed Upon system experimentation; it can recognize human faces with an accuracy of 88.6 %.

In [12], Authors claim that a multi-stage model for face detection is used as an integration based on Viola and Jones algorithm, Gabor Filters, and Principal Component Analysis *PCA*. Then they use an Artificial Neural Networks *ANN* for face recognition which give an accuracy 90.3%.

4 The proposed vehicle security system VSS – IoT

This section describes the idea behind the proposed *VSS – IoT*. So, the main aim of the proposed system is to detect and recognize the faces of professional thieves. Moreover, our proposed system provides a low cost, increase the simplicity and user-friendly is the most important to implement an embedded real-time vehicle security system. Therefore, the system must get the identity of owner vehicle's driver first, then provide him an authorization to access his/her vehicle system. The proposed system has a combination of biometric techniques, embedded devices and *IoT* technologies to design effective surveillance and alert vehicle security system. Besides, the system can be efficiently done by composed of two parts: design hardware architecture and design software architecture.

Figure 1 below presents the basic flowchart of the entire vehicle security system. It illustrates the series of events starting from intrusion event up to the point when it sends out an alert.

Figure 1: Basic flowchart of entire *VSS – IoT* system

4.1 Hardware system architecture

The hardware architecture of the proposed VSS – IoT composed of : *Raspberry Pi 3 Model B+* controller, *PIR* motion sensor, USB 3G Modem flash Pi USB camera module, MicroSD card, Servo Motor, power supply, owner mobile device, police workstation, and vehicle control unit. The proposed components connected wired and wirelessly, where the police workstation and actual owner terminals are connected wirelessly to *Raspberry Pi 3 Model B+* controller, but the rest of all devices will be interfaced using wired media as shown in Figure 2.

Figure 2: Hardware architecture of VSS – IoT

- The *Raspberry Pi 3 Model B+* : This model has a lot of merits over other models. Since it has a large of USB ports and *GPIO* pins. Moreover, it uses "Raspbian" operating system which has a very good integration with the hardware and it has a GUI with development tools.
- The Internet connection: is a necessary component in this work; so that the *Raspberry Pi 3 Model B+* can communicate over IoT-network protocols. The architecture in 2, show that it was necessary to change the IP address of the *Raspberry Pi 3 Model B+* from static to dynamic. This was done by editing the network interfaces file using the command (sudo nano /etc/network/interfaces).
- USB Camera : This is the camera made specifically for the *Raspberry Pi 3 Model B+*. It was hooked to the *Raspberry Pi 3 Model B+* through the USB port which is extremely fast. Therefore, to configure and

enable the camera, the following commands were executed at the *CLI* of the *Raspberry Pi 3 Model B+* (Sudo apt-get install fswebcam).

- Passive Infrared Sensor: The device used here was *HC501SR* passive infrared sensor. The detection range is 7 meters by 140(degrees) coning angles. It has a delay time of 16 sec but adjustable. The ambient temperature is 253K – 323K. It was powered directly from the *Pi* through the 5V *dc* supply pin. Its output was connected as the input to the programmable *GPIO* pin.
- Servo Motor : This component used to control Fuel injector. It was designed to be controlled through the action of system when unauthorized person detected.

4.2 System initialization and configuration

This subsection focuses on system initialization and configuration which all nodes are established to connect. The proposed system network should consist of the *IEEE802.15.4* which used in the physical layer to provide wireless communications, such that the bits of data after they have been converted into signals can be transmitted to the vehicle's owner and/or police workstation. Moreover, in the data link layer, *6LoWPAN* is used as (adaptation layer) where; the adjustment from *IPv6* to *IEEE 802.15.4* is done. Also, the Internet Protocol *IPv6* is used for addressing and routing of data. In which, we can assign every node a unique *IPv6* address. The next layer is a transport layer, where *UDP* is used for the carriage of the data. Finally, in the application layer, the *CoAP* protocol is used. The proposed system' network also connects to other networks via *Wi-Fi*. Also, this system executes the following tasks:

- **Importing python libraries and packages:** These libraries are predefined and help to make the interface modules work properly.
- **USB Camera setting and configuration :** After these configuration settings of USB Camera, the system was rebooted. This was done to ensure that the camera was allocated enough space in memory. The camera takes 5MP image and it has a resolution of 640 × 480. The following command was used (fswebcam image.jpg) on the image.
- **GPIO settings and pin initialization:** The channel was set using the *BCM* channel numbering. Passive infrared pin channel was set to read mode; so to read the value of any *GPIO* pin,

simply type; `GPIO.input(channel)`. While the led channel was set to drive/write mode. Therefore, to drive the channel of `GPIO` pin, type; `GPIO.output(channel, status)`.

- **Generating and sending e-mail :** It is necessary to generate and send the Email to the predefined subscriber After configuring the system. Multipurpose Internet Mail Extension (*MIME*) package used to generate the attachment mail. *MIME* supports characters and non-text attachments like (audio, video and application programs), etc. Also, the Simple Mail Transfer Protocol (*SMTP*) program is used to deliver the email from the *Raspberry Pi 3 Model B+* to the configured *mailhub*. This can be summarized using the Algorithm below:

Start the system.

Send out E-mail with boot IP assigned to a mailhost

Check the status of GPIO pin.

IF (the input of GPIO pin is Low).

Then GPIO pin output 13 is Low and system is Idle.

Else the input of GPIO pin suddenly goes HIGH.

Then Interrept event happend.

ENDIF

WHILE (the value of input GPIO is High).

Set the output of GPIO pin 13 to be High.

Call the function to start the Camera.

Camera detect and Recognize the face.

IF (An Authorized Person detect and recognize).

Then Open the servo motor.

Else Unauthorized Person detect and recognize.

Close the servo motor and Check the Internet.

ENDIF

IF (Internet Available).

Then (Close the servo motor and Generat the MIME message contract with attachment and mobile notification).

Call SMIP server to send alert with attachment.

Call firebase and pusher to push notifiction.

GPIO clean up and repeat the loop.

Else Rechcking agin after 0.5 second.

ENDIF

ENDWHILE

This sequence of events can be elaborated well using the block diagram below 3.

Figure 3: System initialization and configuration

4.3 Software design of VSS – IoT system

This subsection gives an overview of the software design of our VSS – IoT system which based on major Face detection and recognition system modules. This system developed by *Raspberry Pi 3 Model B+* Board with the newest operating system version called "*Raspbian*" which connected to some sensors and actuators. If a thief is trying to access the vehicle body, the vehicle security system will be turned on automatically. Then, all sensors of the security system will be actuated, such that if the *PIR* motion detection sensor detects sudden any movement, since it considered as the first line of defense, then it will change its idle state to active state. Moreover, when the thief is seated on the driver's vehicle seat, his/her face image will capture via hidden USB camera which is located at the top front of the driver in such manner that it can easily take the image. Once the image is captured, it will be sent to the controller device and convert it into a compatible format. Where the controller will make a comparison between f_n (represents the amount of pixels for the captured image) and f_{n-1} (represents the amount of pixels for the per-stored images of the vehicle' owner in its database images). Therefore, if there exists a true match, then the controller will allow to the vehicle' owner to access the vehicle motor system, otherwise, the controller will detect the captured image as an unauthorized person and will not give him access to the vehicle system. Hence, the security system will notify the owner and/or police workstation via different channel; like mobile application and email channels. All these

changes in the state will interrupt the controller instantly and it will give a command to the control of the vehicle's engine by turning it off at any instant. Figure 4 shows that some functional phases whose responsibility are given below:

Figure 4: Software system design of VSS – IoT system

4.3.1 Acquisition and preprocessing phase

The aim of image acquisition is to obtain the video images of vehicle driver face in real-time using an ip camera and stored in the database for the training and testing process. In this phase, the images are normalized and enhanced to improve the ability of the detection/recognition phases. Therefore, some metric property performed under different conditions like climatic, without/with glasses, genders, and ages, etc. which help to produce feature distinguishable in the image processing phase. Hence, after the images are acquiring, the system will encounter some challenges like fickle lighting, variable background, and other some obstacles. Therefore, image preprocessing will normalize the image intensity, uniform size, and shape. Whereas, image preprocessing is a technique to enhance raw images/signals received from cameras/sensors placed in the vehicles. Thus, The preprocessing steps should implement are as follows:

- Start the camera and set to capture video stream.
- Grab a frame from the video stream. If frame is grabbed, continue with the process.
- Else stop and Initialize the frame as the current frame
- Conversion of gray-scale image: gray-scale images means that the image color information is missing and it converted into grayscale format repre-

sented as a number from decimal 0 to 255, or binary 00000000 to 11111111.

Definition:

Let V be a set of values for any image

Let image with values E in V

Therefore, $I : E \rightarrow V$,

Where,

$I(x)$ is called the value of pixel x for I

Let K the set of all images with integers values in E . So, image in $I(k)$ is also called the value of gray-scale pixel of the image.

- Image blurring: blurring concept means that the image looks more detailed if we can perceive all the objects and their shapes correctly in it. Blurring can be achieved in many ways. Gaussian blur technique (also known as Gaussian smoothing) is used to blur the image. It is used to reduce noise in the image. Moreover, Gaussian smoothing is used as a Preprocessing stage to enhance image structures at different scales. The equation of a Gaussian function is 4:

$$G(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{x^2}{2\sigma^2}} \quad (4)$$

- Capture another frame and repeat the above steps.
- Check for pixel threshold if enough to call motion detected function
- Then draw a rectangle around the region where motion was detected

4.3.2 Face detection phase

Various approaches in the field of face detection are developed in recent years. Such as surveillance system and gender classification are using face detection technology as a part of face identification. Whereas, Face detection techniques focused on determining the frontal of human faces like locations and size in any digital image. Hence, it detects only the facial expression then treat with the rest of the image as background. This paper present a robust vehicle security system using rapid face detection technique *Haar cascade*. It considers as a machine learning object detection algorithm used to identify objects in image or video based on the concept of Haar feature which proposed by viola and Michael [20]. The most aim of the *Haar cascade* Classifier is that it reject the regions that unlikely to have consisted in the digital image. This algorithm divides into four stages:

- **Haar feature selection:** the core step of Haar cascade classifier is to collect the Haar Features.

Where a Haar feature considers adjacent rectangular groups of pixels at a specific location in a detection region. Then sums up all pixel intensities in each region and calculates the variance between these sums to determine relative light and dark regions. I.e.

$$f(x) = \text{Sum}_{\text{black rectangle}}(\text{pixel intensities}) - \text{Sum}_{\text{White rectangle}}(\text{pixel intensities})$$

Some different types of haar feature are shown in Figure 5:

Figure 5: Different types of haar features

- **Creating integral images :** for rapid computing of these features; the integral image is done. Equation 5 shows the calculation of the sum of all pixels inside any given rectangle. It needs only four-pixel values, which start from top left of the cornered pixel (x, y) .

$$p(x, y) = \sum_{x' \leq x, y' \leq y} i(x', y') \quad (5)$$

- **AdaBoost training:** The next step to construct *Haar cascade* classifier to select the important Haar features is using *AdaBoost* learning algorithm. It is used to detect the faces in the digital image by extracting the best features. A combination of weak classifiers can produce a strong classifier as shown in the following equation:

$$S(x) = a_1 w_1 + a_2 w_2 + \dots + a_n w_n \quad (6)$$

Where,

w_n are n weak classifiers defined as in 7 which used to construct a $S(x)$ strong classifier.

$$w_j = \begin{cases} 1 & P_j f_j \leq P_j \theta_j \\ -1 & \text{otherwise} \end{cases} \quad (7)$$

Such that

P_j : is the bias direction.

θ_j : is the threshold.

f_j : is a characteristic function.

- **Cascading classifiers:** the Haar cascade classifier is a series of stages. Each stage contains a weak classifier which trained to be strong. Therefore, if the image passes all stages then the image said to be a human face, otherwise, means it is not a human face.

4.3.3 Face recognition phase

Face recognition is considered an important phase in security systems. Whereas, many techniques focus to intend better recognition within a real-time when applied on high-speed computer. But, fortunate, a real-time processing for face recognition in-vehicle security systems may not be mandatory where the crimes were done on the street. Therefore, the vehicle security system will have enough time to verify the driver. Since, face recognition in-vehicle security system is implemented on low power processor, such as *Raspberry Pi 3 Model B+* board, so choosing a proper algorithm is very important. This research work investigates to employ the Principal Component Analysis (PCA) algorithm [21] in recognizing faces which applied on low power processor. PCA is a mathematical method that expressed as transformation W^t of high-dimensional facial images n into few-dimensional principal components m called Eigenface where $m < n$. In our *VSS - IoT* system; we have 10 vehicles, each vehicle has 5 authorized driver. While for each driver, our system will gather 10 images to be trained as eigenfaces. These images have been normalized as 64×64 pixels. The training results are saved and sorted in template file as those with the largest eigenvalues. The PCA algorithm in the system is shown in the following steps:

- **Step 1:** Let I is an image with size $(N \times N)$.
- **Step 2:** Convert I to Γ of size $(P \times 1)$, s.t. $P = (N \times N)$.
- **Step 3:** Suppose we have training set : $\Gamma' = [\Gamma'_1, \Gamma'_2, \dots, \Gamma'_M]$
- **Step 4:** Calculate the average by $\psi = \frac{1}{M} \sum_{i=1}^M \Gamma'_i$
- **Step 5:** Calculate the differs for each face $\Phi_i = \Gamma'_i - \psi$, then the difference matrix define as $A = [\Phi_1, \Phi_2, \dots, \Phi_M]$.
- **Step 5:** Compute the covariance matrix by $C = A A^T$ with size $(P \times P)$, then reduce the size using $L = A^T A$, with size $(M \times M)$.
- **Step 6:** Calculate the eigenvector by $A^T A X_i = \lambda_i X_i$, where, $U_i = A X_i$ is the eigenvector, and λ_i is the eigenvalue.
- **Step 7:** Compute the projected face image by $\Omega_k = U_k^T \Phi_i$.
- **Step 8:** Now test image Γ'_t using $\Phi_i = \Gamma'_t - \psi$
- **Step 9:** Compute the projected for test image using $\Omega = U_k^T \Phi_t$.
- **Step 10:** Compute the Euclidean distance to find the minimum distance between the test image and training image using $\varepsilon_k^2 = \|\Omega - \Omega_k\|^2$, then, if $\varepsilon_{k(\min)} \geq \Theta$ then the image is unknown, also if $\varepsilon_{k(\min)} \leq \Theta$ then the image is known face.

4.3.4 Face labeling phase

The result of the recognition phase will be used in this phase. Since the image is converted into binary form; so, this label is used to assess a specific value and matching it to the value of a person's name in the firebase database. Therefore, if the value match, then the name will successfully be returned. Otherwise, the system will return predefined as "unknown name" as shown in Figure 6.

Figure 6: successfully recognized a face of authorized person

4.4 Mobile application control and e-mail notification

In this subsection, *Raspberry Pi 3 Model B+* connect with the android application through firebase server to create a mobile application for the person who is an actual authorized driver. Such that, *Raspberry Pi 3 Model B+* send data to firebase database and pusher take action like send notification (thief image along with the message) to the android application named "Car Locked" to alert vehicle's owner as shown in Figure 7.

The next steps show how to create this mobile application:

- create java code and connect it with firebase database as shown in Figure 8
- Design user interface by XML as shown in Figure 9.

On the other hand, to allow email notifications sends to the police workstation. Simple Mail Transfer Protocol (SMTP) is a program that allows a system to send/received emails from a computer to *mailhost*. Thus, SMTP is an ideal protocol used for these situations where alerts are needed to be sent along with thieves image.

Figure 7: Mobile application control

Figure 8: Java code with firebase

Figure 9: Design user interface of mobile application

5 Implementation results and security analysis

The proposed *VSS – IoT* is evaluated on two face datasets which are ORL dataset [22] as shown in Figure 10 and our dataset which were collected from 10 vehicles, each vehicle has 5 authorized drivers. Whereas, for each authorized driver, our system will gather 10 images to be trained as eigenfaces. Then every authorized driver was tested; 100 times without glasses and 100 times with glass. Also, for every vehicle, we test on 5 unauthorized person where everyone was tested 100 times. All experiments have been performed using Intel Core i7, 4 GHz processor with 4 GB of RAM. The experiments have been implemented using python language environment with firebase database and *Raspberry Pi 3 Model B+* micro-controller and java language using some sensors.

Figure 10: Some samples of ORL database

5.1 Performance measurements

The recognition effectiveness of the proposed *VSS – IoT* is measured in terms of accuracy, sensitivity, specificity and precision are calculated based on the values of (*TP*), (*TN*), (*FP*), and (*FN*) as shown in equations 8, 9, 10 and 11 respectively. While equation 12 show that how equations 9 and 10 are effected on the accuracy in the way that they are multiplied in equations 13 and 14.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (8)$$

$$Sensitivity = \frac{TP}{TP + FN} \quad (9)$$

$$Specificity = \frac{TN}{TN + FP} \quad (10)$$

$$Precision = \frac{TP}{TP + FP} \quad (11)$$

$$Accuracy = Prevalence \times Sensitivity + (1 - Prevalence) \times Specificity \quad (12)$$

Where,

$$Prevalence = \frac{Positive}{Positive + Negative} \quad (13)$$

$$1 - Prevalence = \frac{Negative}{Positive + Negative} \quad (14)$$

Where,

True negatives (TN): shows the number of normal events is successfully labeled as normal.

False positives (FP): refer to the number of normal events being predicted as abnormal.

False negatives (FN): Represent the number of abnormal events is incorrectly predicted as normal.

True positives (TP): refer to the number of abnormal events is correctly predicted as abnormal.

Prevalence: is the number of positive samples to all samples.

1-Prevalence: pretend to the number of negative samples to all samples.

5.2 Experiment results

In this system before using the *Haar – Cascade* classifier was applied as face detection and *PCA* for face recognition. Therefore, the parameters used in our system are as follows:

- Scale increase rate: this parameter aims to balance between the number of the pass between the Haar detector and the accuracy. If the sitting is high, then the detector run fast with missing faces. Thus, the parameter value should be 1.2 out of these values 1.1, 1.2, 1.3, and 1.4, which lead to run a moderate number of passes to present better accuracy.
- Minimum neighbors threshold: the target of this parameter is to find the minimum-neighbors threshold which leads to decide for discarding or keeping the group of the rectangle as a face or not. Since the parameter range values from 0 to 10. In this work, we choose the minimum neighbors, which have the highest probability to be identified as a "face".
- Minimum detection scale: the next parameter is to find the smallest size of the face by changing the Haar cascade classifier values in XML file. To get the best results we set this value to 25×25 in our experiments. But we need to assure that the ratio of width to height should be the same as the default.

- Threshold: the maximum value between the testing images values and training images values evaluated by Euclidean distance function is called Threshold. At different values of threshold all experiments were done by 5 authorized drivers; 100 times without glasses and 100 times with glasses. Also, the system evaluated by 5 unauthorized person 100 time. From our experiments, recognition rate increased by using trial and error of the threshold value which is taken using $\Theta_{new} = 0.8 * \Theta_{old}$ of the maximum value of minimum Euclidian distances of each image from other images see subsection 4.3.3.

The results of our experimental demonstrated on our dataset as follows : Where, *CR* denoted as Correct Recognition, *FR* describe as False Recognition and *Not R* defined Not Recognized.

Table 1: Correct recognition of authorized driver No. 1 without/with glasses

threshold	driver without glasses			driver with glasses		
	C R	F R	Not R	C R	F R	Not R
$1.5 * 10^3$	92	1	7	87	3	10
$2 * 10^3$	92	2	6	89	5	6
$2.25 * 10^3$	94	0	6	92	0	8
$2.50 * 10^3$	96	1	3	91	0	9
$2.75 * 10^3$	94	1	5	92	5	3
$3 * 10^3$	100	0	0	98	2	0
$3.50 * 10^3$	100	0	0	99	0	1
$4 * 10^3$	99	0	1	77	13	10
$4.50 * 10^3$	87	8	5	70	17	13
$5 * 10^3$	80	15	5	75	12	13

As observe from Table 1 a good value of the threshold is $3 * 10^3$ and $3.50 * 10^3$ which give us a high accurate face recognition 100% and 99% even if the authorized driver No. 1 *without/with* glasses respectively. Also, as threshold value increased, the false recognition and not recognized increased, which means it gives a bad performance.

Table 2 shows that the best performance obtained for authorized driver No. 2 when the value of the threshold in $3 * 10^3$ and $3.50 * 10^3$.

Table 3 describe that the excellent value of the threshold was $3 * 10^3$ and $3.50 * 10^3$ which provide the best performance and give an efficient correct face recognition for authorized driver No. 3.

Table 4 demonstrate that the high accurate threshold value was $3 * 10^3$ and $3.50 * 10^3$ for correct recognize the authorized driver No. 4 even without/with glasses.

Table 2: Correct recognition of authorized driver No. 2 without/with glasses

threshold	driver without glasses			driver with glasses		
	C R	F R	Not R	C R	F R	Not R
$1.5 * 10^3$	5	0	95	4	0	96
$2 * 10^3$	21	8	71	18	0	82
$2.25 * 10^3$	49	5	46	41	0	59
$2.50 * 10^3$	77	3	20	72	20	18
$2.75 * 10^3$	89	6	5	89	1	10
$3 * 10^3$	99	0	1	94	0	6
$3.50 * 10^3$	100	0	0	99	0	1
$4 * 10^3$	97	0	3	79	2	19
$4.50 * 10^3$	86	4	10	70	14	16
$5 * 10^3$	78	12	20	81	9	10

Table 3: Correct recognition of authorized driver No. 3 without/with glasses

threshold	driver without glasses			driver with glasses		
	C R	F R	Not R	C R	F R	Not R
$1.5 * 10^3$	10	13	7	8	0	92
$2 * 10^3$	19	1	80	12	0	88
$2.25 * 10^3$	20	9	71	18	3	79
$2.50 * 10^3$	96	4	0	80	11	9
$2 * 75^3$	80	13	7	79	1	20
$3 * 10^3$	98	1	1	98	0	2
$3.50 * 10^3$	99	1	0	97	1	2
$4 * 10^3$	77	3	20	80	13	7
$4.50 * 10^3$	86	9	5	75	15	10
$5 * 10^3$	83	7	10	60	23	17

Table 4: Correct recognition of authorized driver No. 4 without/with glasses

threshold	driver without glasses			driver with glasses		
	C R	F R	Not R	C R	F R	Not R
$1.5 * 10^3$	86	2	12	72	0	28
$2 * 10^3$	80	12	8	70	1	29
$2.25 * 10^3$	87	3	10	75	13	12
$2.50 * 10^3$	93	7	0	90	3	7
$2.75 * 10^3$	95	2	3	93	2	5
$3 * 10^3$	100	0	0	96	1	3
$3.50 * 10^3$	99	1	0	82	8	10
$4 * 10^3$	81	10	9	99	0	1
$4.50 * 10^3$	66	20	14	60	3	37
$5 * 10^3$	72	21	7	75	0	25

The results of Table 5 documented that; the test of the system on authorized driver No. 5 it gives us more accuracy than the other thresholds when the threshold value $3 * 10^3$ and $3.50 * 10^3$ even with his/her without/with glasses.

Table 5: Correct recognition of authorized driver No. 5 without/with glasses

threshold	driver without glasses			driver with glasses		
	C R	F R	Not R	C R	F R	Not R
$1.5 * 10^3$	30	26	44	27	33	40
$2 * 10^3$	69	20	11	60	28	12
$2.25 * 10^3$	50	33	17	42	0	58
$2.50 * 10^3$	93	4	3	90	0	10
$2.75 * 10^3$	93	7	0	92	4	4
$3 * 10^3$	99	0	1	98	0	2
$3.50 * 10^3$	99	1	0	99	1	0
$4 * 10^3$	67	13	20	65	5	30
$4.50 * 10^3$	86	0	14	80	11	9
$5 * 10^3$	87	0	13	8	5	15

Table 6: Correct recognition of unauthorized driver test

threshold	C R	F R	Not R
$1.5 * 10^3$	100	1	0
$2 * 10^3$	100	0	0
$2.25 * 10^3$	100	0	0
$2.50 * 10^3$	100	0	0
$2.75 * 10^3$	99	1	0
$3 * 10^3$	100	0	0
$3.50 * 10^3$	100	0	0
$4 * 10^3$	100	0	0
$4.50 * 10^3$	92	8	0
$5 * 10^3$	87	13	0

The result of this Table 6 shows that the 100% of unauthorized drivers denied by this proposed specially with the threshold values $3 * 10^3$ and $3.50 * 10^3$.

Table 7 shows the performance of the proposed system comparing to common models when applied on the two datasets. Where the recognition accuracy based on *PCA* stand-alone is 87.9% on ORL dataset, where as it gives 95.2% when applied on our dataste. but with *Fisher*, and *ANN* algorithms the face recognition performance 85.2% and 86.7% are achieved respectively on ORL dataset, whereas they are giving 96.2% and 96.8% respectively too when applied on our dataste. Authors in [23] proposed a recognition system with average accuracy of 74.4%, and authors in [24] gives a proposed system with average accuracy of 90.3% based on ORL dataset. Finally, our proposed system with hybrid (*Haar Cascade + PCA*) provides a face recognition of 98.2% on ORL dataset and 99.6% when applied on our dataset.

Table 8 compares the performance evaluation between our proposed and the existing algorithms in terms

Table 7: Comparison of average accuracy

author/technique	average accuracy	
	ORL dataset	Our dataset
PCA	87.9%	95.2%
Fisher	85.2%	96.2%
ANN	86.7%	96.8%
[23]	74.4%	–
[24]	93.3%	–
Proposed	98.2%	99.6%

Table 8: sensitivity, precision, and specificity comparison

author/technique	sensitivity	precision	specificity
PCA	0.911	0.955	0.948
Fisher	0.899	0.942	0.881
ANN	0.906	0.916	0.935
our Proposed	0.977	0.979	0.992

Table 9: Face recognition on computer v.s. low power processing

author/technique	R T	R T
	on computer (s)	on LPP (s)
PCA	2.862	10.132
Fisher	2.997	23.279
ANN	2.942	19.680
our Proposed	0.093	0.152

of sensitivity, precision, and specificity by observing the values of *TP*, *TN*, *FN*, and *FP* outcomes during the experiments using our dataset. It is clear that the proposed system works extremely effectively and gives better performance.

Table 9 pretends the results of Recognition Time (*R T*) comparison between the proposed system and other algorithms when implementing on computer and Low Power Processing (LPP) respectively using our dataset. Where The results presented that face recognition execution time on the computer was not more than 3 seconds. While the execution time of these popular methods when implemented on low-power processor was not appropriate due to it takes a long execution time. As well as the results showed that the proposed system took a shorter time, so it is proper for face recognition when applied on a low-power processor.

Table 10 shows how much *CPU* utilized and memory usage of face recognition based on different cameras resolution. Therefore, the results presented that 640×480 gave better memory space and *CPU* Utilization more than other cameras pixel size. To calculate *CPU* Utilization and mem-

Table 10: CPU utilized and memory usage of our proposed

Cameras Pixel	CPU Utilized (%)	Memory Usage (MB)
1024 × 768	85	69.6
960	80	64.9
640 × 480	81	60.1
320 × 240	84	55.2
160 × 120	76	53.5

ory usage in percentage were calculated as following formula 15, 16 respectively :

$$U = \frac{R}{C} * 100 \quad (15)$$

Where,

U= Utilization

R= Requirements, means the CPU (BUSY TIME)

C= Capacity, means (BUSY TIME + IDLE TIME)

$$\frac{\text{Result}}{\text{Total Physical Memory}} * 100 \quad (16)$$

$$= \text{Total Physical Memory}$$

$$- (\text{Memory Free} + \text{Memory Buffers} + \text{Cache Memory})$$

5.3 Security analysis

The security is an important issue for vehicle security systems. So, this subsection showed the security of the proposed system and other approach based on some criteria. The experiments were conducted to perform a comparison between our the proposed system and the AR – 837E access controller [25].

Table 11 gives a comparison results of recognition rate, efficiency, security, and price. The proposed system was better than AR–837E. Where, AR–837E does not have the face recognition ability, and it has mid security compared to our proposed system. Moreover, without the magnetic card, our proposed system does not have a problem if the

magnetic card is stolen. Also, The most important criteria are that the deploying cost; whereas, the proposed system is less price than the AR – 837E.

6 Conclusions

This paper proposed a new intelligent vehicle security system called VSS – IoT using a secure, efficient, low-cost, and Low Power Processing chip with the Internet as its important part. Moreover, this paper employed a hybrid mechanisms (*Haar Cascade* + *PCA*) for face detection and recognition of the captured image by a USB camera. Whereas, the *Haar cascade* Classifier can be used to reject the regions that unlikely to have consisted in the digital image. Also, it is used to detect the faces in the digital image by extracting the best features. While *PCA* is a mathematical method that expressed as a transformation of high-dimensional facial images into few-dimensional principal components called Eigenface which used to recognize faces in the digital image. According to the primary and earlier experimental results compared with other existing systems, the proposed VSS – IoT achieved the best accuracy rate 98.2% on ORL dataset, whereas 99.6% when applied on our dataset to identify the authorized and unauthorized people. Also, the VSS – IoT enhances the sensitivity to 97.7% which is important when the system work under different illumination conditions hen the value of the threshold is $3 * 10^3$ and $3.50 * 10^3$. As well as, the proposed VSS – IoT enhanced the time compared with other systems which achieved 0.152 sec. Besides, the results presented that cameras pixel size 640×480 gave better memory space and CPU utilization more than others 76% and 53.5 MB respectively which is important for the real-time vehicle security systems. Therefore, due to its low-cost and high performance, it is very suitable for improving the security of the automobile sector.

Acknowledgement: The author gratefully acknowledge the editor and the anonymous reviewers for their valuable comments.

Table 11: Security analysis comparison

Criteria	Proposed System	[25] AR-837E
Identify Accuracy	High	Absence
Efficiency	High	High
Security	High	Mid
Price	USD\$80	USD\$200

References

- [1] Mahesh R. P. , Imdad R. , "IoT Based Embedded System for Vehicle Security And Driver Surveillance", Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT 2018), IEEE Explore Compliant - Part Number: CFP18BAC-ART; ISBN:978-1-5386-1974-2.

- [2] Vivek K. S., Soumitra M., and Harshit M., "Car Security using Internet of Things", 1st IEEE International Conference on Power Electronics Intelligent Control and Energy Systems (ICPEICES-2016), 978-1-4673-8587-9/16/31.00 ©2016 IEEE.
- [3] Tabassum J. Kh., M.R.Bhadange, Pooja S. P., Vinaya S., "Smart Vehicle Monitoring System Using Raspberry Pi", Spvryan's International Journal of Engineering Sciences and Technology (SEST), 3 (2), PP. 1 of 7, 2016.
- [4] Liu Z., Zhang A. and Li S., "Vehicle anti-theft tracking system based on Internet of things", Vehicular Electronics and Safety ("ICVES"), "IEEE International Conference" on, Dongguan, 2013, pp. 48-52., doi: 10.1109/ICVES.2013.6619601.
- [5] ArunSasi and Lakshmi R. N., "Vehicle Anti-Theft System Based On An Embedded Platform", in IJRET: International Journal of Research in Engineering and Technology, 2 (9), 2013.
- [6] Tahesin A., Prajakta Ch., Vidhi P., Megha G., Debajyoti M., "An Attempt to Develop an IoT based Vehicle Security System", 2018 IEEE International Symposium on Smart Electronic Systems (ISES) (Formerly iNiS), 0-7695-6618-9/18/31.00, 2018 IEEE, DOI 10.1109/ISES.2018.00050.
- [7] Jian X. and Haidong F., "A Low-cost Extendable Framework for Embedded Smart Car Security System", Proceedings of the 2009 IEEE International Conference on Networking, Sensing and Control, Okayama, Japan, March 26-29, 2009.
- [8] Shruthi K., Ramaprasad P., Ray R., Naik M. A. and Pansari S., "Design of anti-theft vehicle tracking system with a smartphone application" 2015 "International Conference on Information Processing" (ICIP), Pune, 2015, pp. 755-760. doi:10.1109/INFOP.2015.7489483.
- [9] Narayan T. D. and Ravishankar S., "Face Detection and Recognition using Viola-Jones algorithm and fusion of LDA and ANN", IOSR Journal of Computer Engineering (IOSR-JCE), 18(6), PP 01-06, 2016.
- [10] Kumar K. S., Shitala P., Vijay B. S., Tripathi R. C., "REAL TIME FACE RECOGNITION USING ADABOOST IMPROVED FAST PCA ALGORITHM", International Journal of Artificial Intelligence and Applications (IJAIA), 2(3), July 2011.
- [11] Shaik M. A. et al. "An Inexpensive Security Authentication System Based on a Novel Face-Recognition Structure", International Journal of Engineering Trends and Technology (IJETT), 4(9), 2013.
- [12] Mohammad D., Amin A. and Olivier D., "Face Detection using Viola and Jones Method and Neural Networks", International Conference on Information and Communication Technology Research (ICTRC2015), pp. 40-43, 978-1-4799-8966-9/15/31.00, IEEE 2015.
- [13] Ahmed A. E., "IoT-based Efficient Tamper Detection Mechanism for Healthcare Application", International Journal of Network Security, 20(3), PP.489-495, May 2018 (DOI: 10.6633/IJNS.201805.20(3).11).
- [14] Siddarth R., Dattatreya P. and Sadique N., "Face recognition using PCA and LDA: Analysis and comparison", IEEE International Conference on Advances in Recent Technology in communication and Computing, pp. 6-16, 2013.
- [15] Varsha G. and Dipesh Sh., "A study of various Face Detection Methods", International Journal of Advanced Research in computer and communication Engineering, 3(5), May 2014.
- [16] Bavya R. and Mohanamurali R., "Next generation auto theft prevention and tracking system for land vehicles", "Information Communication and Embedded Systems"(ICICES), International Conference on, Chennai, 2014, pp. 1-5, doi: 10.1109/ICICES.2014.7033987.
- [17] Zhixiong L. and Guiming H., "A Vehicle Anti-theft and Alarm System Based on Computer Vision", IEEE International Conference on Vehicular Electronics and Safety, 2005. DOI: 10.1109/ICVES.2005.1563666.
- [18] Sarvesh V. A., Chetana R., "Face Recognition System for Unlocking Automobiles Using GSM and Embedded Technology", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, (An ISO 3297: 2007 Certified Organization), 5(7), July 2016.
- [19] Christina Ma., Fernandez D., Kristina J. E. G., Aubrey R. M. L., Ron J. J. R., Argel A. B. and Elmer P. D., "Simultaneous Face Detection and Recognition using Viola-Jones Algorithm and Artificial Neural Networks for Identity Verification", pp. 672-676, 2014 IEEE Region 10 Symposium, 2014.
- [20] Viola P. and Jones M., "Rapid Object Detection using a Boosted Cascade of Simple Features", ACCEPTED CONFERENCE ON COMPUTER VISION AND PATTERN RECOGNITION 2001.
- [21] Turk M. A. and Pentland A. P., "Eigenfaces for Recognition", Journal of Cognitive Neuroscience, 3(1), PP. 71-86, 1991.
- [22] The ORL face database: <http://www.cl.cam.ac.uk/Research/DTG/attarchive/facedatabase.html>.
- [23] Ebrahimpour R., Nazari M., Azizi M. and Amiri A., "Single Training Sample Face Recognition Using Fusion of Classifiers", International Journal of Hybrid Information Technology, 4(1), January, 2011.
- [24] Novosel R., Meden B., Emersic Z., Struc V. and Peer P., "Face recognition with Raspberry Pi for IoT Environments", International Electrotechnical and Computer Science Conference ERK 2017, At: Portorož, Slovenia, September 2017.
- [25] AR-837E Access card reader, Available at: <http://www.soga.com.tw/content/product/180/index.html>.