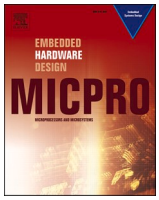
Microprocessors and Microsystems 96 (2023) 104728

Contents lists available at ScienceDirect

Microprocessors and Microsystems

journal homepage: www.elsevier.com/locate/micpro



Development of surveillance robot based on face recognition using Raspberry-PI and IOT

Houda Meddeb [a,*], Zouhaira Abdellaoui [b], Firas Houaidi [b]

[a] Automatic Research Center of Nancy, CRAN, UMR 7039, Cosnes and Romain, Nancy, France
[b] Communication Systems Research Laboratory SYSCOM - LR-99-ES2, University of Tunis El-Manar, National Engineering School of Tunis – ENIT, Tunis-Belvédère, BP 1002, Tunisia

ARTICLE INFO

Keywords:
AI
Face recognition
IoT
Raspberry PI
Robot
Surveillance

ABSTRACT

The advancement in recent technologies such as artificial intelligence (AI), computer vision (CV) and internet of things (IoT) extends to various areas, especially surveillance systems that require real-time facial recognition processing to ensure safety. In fact, mobile robots are widely used in surveillance systems to perform dangerous tasks that humans cannot.

In this context, we propose a prototype of a low-cost mobile surveillance robot based on Raspberry PI 4 which can be integrated into any industrial area. This intelligent robot checks about the presence of intruder using IoT and face recognition technology.

The system is equipped with passive infrared (PIR) sensor and camera to record live streaming video and photos, which are transmitted to the room control via IoT.

Thanks to facial recognition algorithms, the system can distinguish between company personnel and intruders. Haar Cascade Classifier and LBPH (Local Binary Pattern Histogram) algorithm are used in image processing to detect and identify individuals. When a stranger is detected, alert notifications and email with captured image are sent to the room control via IoT. A web interface was developed to remotely control the designed robot via a WiFi connection. This application allows monitoring of a wide area and can improve the robot's perception system. Performance evaluations will be conducted to demonstrate the effectiveness and robustness of the face recognition algorithms used in this framework.

1. Introduction

In recent years, surveillance has become a vital necessity to protect lives and assets. The integration of mobile robots in surveillance is the most flexible and cost-effective solution to increase safety in many fields such as industries, military and home automation. In fact, they can take the place of humans in dangerous ambiance or manufacturing processes.

Intelligent security robotics are equipped with cameras and several sensors which are used to monitor continuously the area with minimal human intervention, detect intrusions or problems and alert the surveillance personnel in real time and with great reliability. Consequently, surveillance mobile robots become an area of great research interest [1–5].

With the advancement in recent technologies such as Artificial intelligence (AI), computer vision (CV) and internet of things (IOT) we are able to improve the quality of surveillance robotic and augment its performance in terms of quality of service, quality of video transmission, speed, accuracy and robustness.

Facial recognition technology is one of the most important topics in computer vision and biometrics systems after fingerprint [6]. It is capable of recognizing digital images of human faces using computer technology as well as various vision devices such as (camera, 3D scans, …) to capture and process faces [7]. This method is used to identify ordinary people and strangers. Today, facial recognition technology has become an exciting area of research for surveillance applications such as smart home and cities [8–10] and robotic systems [11,12].

IoT is newly introduced in the field of surveillance to enhance security and to offer personal protection. In this concept, many physical devices around the world are connected to the internet to collect and exchange data without human intervention. The advantages of IoT: are fast operation, automation and control, easy access to information and saving money.

It is necessary to utilize facial recognition and IoT to improve the

* Corresponding author.
E-mail addresses: meddebhouda@gmail.com (H. Meddeb), zouhaira.abdellaoui@enit.rnu.tn (Z. Abdellaoui).

https://doi.org/10.1016/j.micpro.2022.104728
Received 4 September 2022; Received in revised form 10 November 2022; Accepted 19 November 2022
Available online 22 November 2022

Nomenclature

Abbreviation

AI	artificial intelligence
CV	computer vision
CNN	convolutional neural network
FN	false negative
FP	false positive
FNIR	false negative identification rate
IoT	Internet of Things
LBPH	local binary patterns histograms
PIR sensor	passive infrared sensor
RTP	real-time transfer protocol
SVM	support vector machine
TN	true negative
TP	true positive
TPIR	true positive identification rate
VNC	virtual network computing

quality of surveillance robots and develop rapid response systems.

In this paper, a prototype of a low-cost mobile surveillance robot is proposed. The designed model is easy to install and can be used in various fields. The intelligent security system is controlled by Raspberry Pi 4 model B which provides high performance computing processor unlike others Pi versions or others microcontrollers such as Arduino Uno/Mega.

The proposed robot is equipped with PIR sensor and a USB camera to check about the presence of intruders in a specific area using IoT and face recognition technology. When a PIR sensor detects a person, the system triggers the camera to record live streaming video and photos, which are transmitted to the room control via IoT.

Facial recognition technology is used to distinguish known persons from intruders. There are many algorithms that can run face recognition models. In this work, Haar cascade technique is used for face detection, while the local binary pattern histogram (LBPH) algorithm is used for feature extraction and image recognition. Haar Cascade Classifier and LBPH were chosen for their speed and high accuracy . Furthermore, they are suitable for Raspberry Pi based frameworks as they are capable of detection and identification with very little computational complexity.

When an intruder (unknown person) is detected, an email with captured image and alert notification are sent to room control using IoT. A web interface was developed to receive data and to remotely control the movements of the designed robot via a Wifi connection.

Using mobile robots wirelessly controlled through web application can allow monitoring a wide range of areas and can improve the perceiving system by reducing the distance from the camera to the target and recording photos and videos of higher quality. Furthermore, the robot does not move continuously which allows avoiding power supply problems. In addition, this smart system has a quick video transmission via IoT and a high quality of live feeds since it depends on the resolution of camera utilized as well as the internet speed at the Raspberry Pi's.

Overall, a set of numerical results are presented to evaluate the performance of the proposed face recognition algorithm, and comparison with other methods is discussed.

The work is structured as follows: Section 2 discusses related work. Section 3 describes the hardware components and software methods used in mobile robots. Section 4 presents the flowchart of the system. Section 5 is dedicated to face recognition algorithms. Finally, a prototype of the monitoring robot will be implemented and performance evaluated.

2. Related works

Several projects and systems have been proposed in order to develop a mobile surveillance robot using various processors and features.

The authors in [2] designed and implemented an intelligent surveillance robot using a Raspberry pi 3 model B that can be remotely controlled via Internet. A camera is installed on the robot and wirelessly transmits live video to the website using Wi-Fi technology. The obstacle avoidance module is used to detect and avoid obstacles. A metal sensor is connected to raspberry Pi to detect metal.

A Raspberry Pi 3 based spy robot is developed in [3], which remotely monitors and controls algorithms via IoT. The system can be used in the military field to detect suspicious persons in war zones. The spy robot system consists of multiple sensors (PIR, LDR, IR) and a PI camera. When the PIR sensor detects an object, the PI camera captures the moving object, which is also displayed on the web page. The robot can avoid obstacles detected by infrared sensors. The movement of the robot can also be manually controlled via buttons on the web page. LDR sensor is used to flash the camera at night.

In [13], the authors present surveillance robot based on Raspberry Pi 3 Model B which can be integrated into household. A webcam is attached to the Pi to monitor the area and stream live videos. When the system detects movement, an email notification is sent to the user. The motion detection algorithm is written using Simple CV. The robot is controlled to perform its function by pressing the appropriate key selected from the keyboard.

The authors in [14] developed a surveillance robot for domestic use. This system is controlled by Raspberry pi board and equipped with camera, PIR sensor, buzzer and GSM module attached to the Node MCU. When the PIR sensor detects a person, the buzzer starts sound and GSM module notifies about the presence of intruder. The camera captures video and sends it back to controller's device via the internet. This robot is operated from a PC or an Android phone connected to the internet via a website.

In [15], a spy robot car was developed using IOT technology and Arduino UNO. The robot is suitable for continuous surveillance in hazardous environments. The system consists of cameras and various sensors such as PIR sensors, ultrasonic sensors and gas sensors. The Android application based on Blynk software can control the navigation of the robot from a long distance through WiFi communication. The movements of the robot depend on visual feedback from the camera. The spy bot monitors and transmits live streaming information to connected Android devices. However, the system does not send an alert message to the user.

The surveillance robots proposed in [2,3,13–15] are designed to detect human movements or objects. But, any facial recognition method is used to distinguish between authorized and unauthorised people.

A surveillance robot system with facial recognition is proposed in [11] to detect the presence of an enemy or any unusual events. The system provides the live streaming of surveillance data to the operator using Raspberry Pi 3 and VNC Viewer. Flame and gas sensors are mounted to the system to check for the presence of fire and gas. If gas/fire is detected an alert message is sent to the operator. Haar Cascade classifier and LBPH algorithms are used to recognize whether the detected person is known or unknown. If the detected person is unknown, the robotic system will stop and the relay will activate the laser gun aimed at them or the LED will turn on. However, the authors have not developed a web or Android application to obtain information and control the robot remotely. As a result, the system is constantly moving to monitor the surrounding area, which can cause problems with the robot's power supply system. Also, the system cannot record video and take pictures.

In [12], the authors integrated a developed face recognition software into a mobile robot, aiming to analyze the performance of the detection range and detection speed of the face recognition algorithm in a mobile environment. The face detection method chosen for this analysis is the

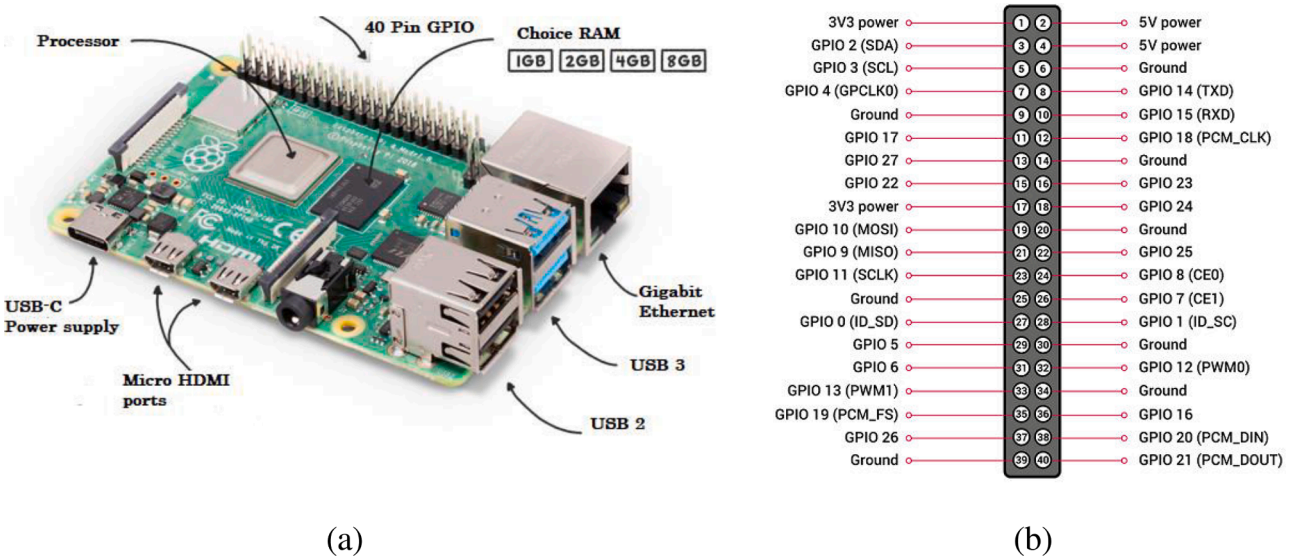


Fig. 1. (a) Raspberry PI 4 model B, (b) The forty pins GPIO.

PCA-Eigenface method from the OpenCV library. In this system, a simple webcam is connected to the robot which is controlled by an Arduino Uno. A phone application was used to manually control the robot's movements.

A novel holistic Unmanned Aerial Vehicles (UAVs)-enabled multi-target tracking and sensing framework is proposed in [16]. A reputation model is introduced to evaluate the targets' potential in offloading useful data to the UAVs. Based on this model and while considering UAVs and targets tracking and sensing characteristics, an intelligent matching mechanism between the UAVs and the corresponding targets is performed to decide the targets to be tracked by the UAVs. In this work, a Stackelberg game-theoretic approach is developed in order to determine the targets' optimal amount of offloaded data and the effort-based price that the UAVs offers to collect the targets' data.

In this paper, we aim to fill these implementation gaps by presenting a surveillance robot controlled by Raspberry Pi 4 model B, the latest and most efficient version of the low-cost Raspberry Pi computer. This smart security robot uses IoT and facial recognition technology to verify the presence of intruders.

When the PIR sensor detects abnormal motion, the Raspberry Pi immediately triggers the USB camera to take a picture and live stream the video, which is transmitted to the room control via IoT. Due to facial recognition methods, the intelligent robot is able to distinguish known person from intruders. In the case of a stranger, the system will use IoT to send an email with captured images and alert notifications.

The system features fast video streaming and high-quality live feeds via IoT, as it depends on the resolution of the camera used and the speed of the internet on the Raspberry Pi. Additionally, a web interface is being developed to receive data over a WiFi connection and remotely monitor the navigation of the surveillance robot. This application is used to make objects near the robot more visible and to avoid power problems due to discontinuous movement of the robot.

A detailed set of numerical results is provided to evaluate the performance and robustness of the face recognition algorithms used in this work. The robot is easy to install, has low operating costs and can be used in many areas to improve safety.

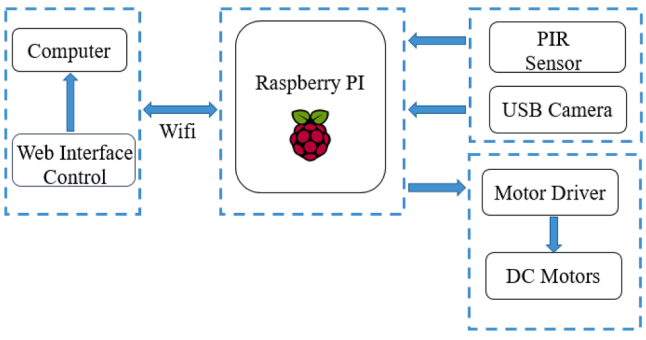


Fig. 2. Block diagram.

3. Materials and methods

In this section, we will present the hardware components and the software methodology used for the realization of a mobile surveillance robot.

3.1. Hardware design

This surveillance robot is composed of the main parts detailed below:

- **Mechanical structure:** in our case, it is represented by the chassis of the mobile robot and wheels.
- **Control part:** This allows the robot to analyze data from the sensors and send commands to the motors. In this work, the control part is physically implemented by a Raspberry PI 4 Model B, a small computer with a Linux operating system for embedded computing applications. It works efficiently when running games, image files and documents. It operates at 1.5 GHz and 8 G and is capable of outputting 4 K video at 60 Hz or powering dual monitors [17]. The Raspberry PI board contains 40 input/output pins as shown below (Fig. 1):
- **Motors:** They enable the robot to perform its actions. They are interactively controlled with the information transmitted by the sensors. In this case, four DC motors (12 V) were selected. The speed of the motor can be changed by varying the input voltage.
- **Motor drivers:** The motor requires a power interface to provide sufficient power and current at the proper polarity. The motor driver contains the H-bridge connection required for bi-directional control of the motor. This is important so that the robot can reach all directions. The motor driver used in this project is the L298N, which can control two motors simultaneously [18].
- **Sensors:** Different types of sensors are used to improve the perception capabilities of robots, such as ultrasonic, infrared and many

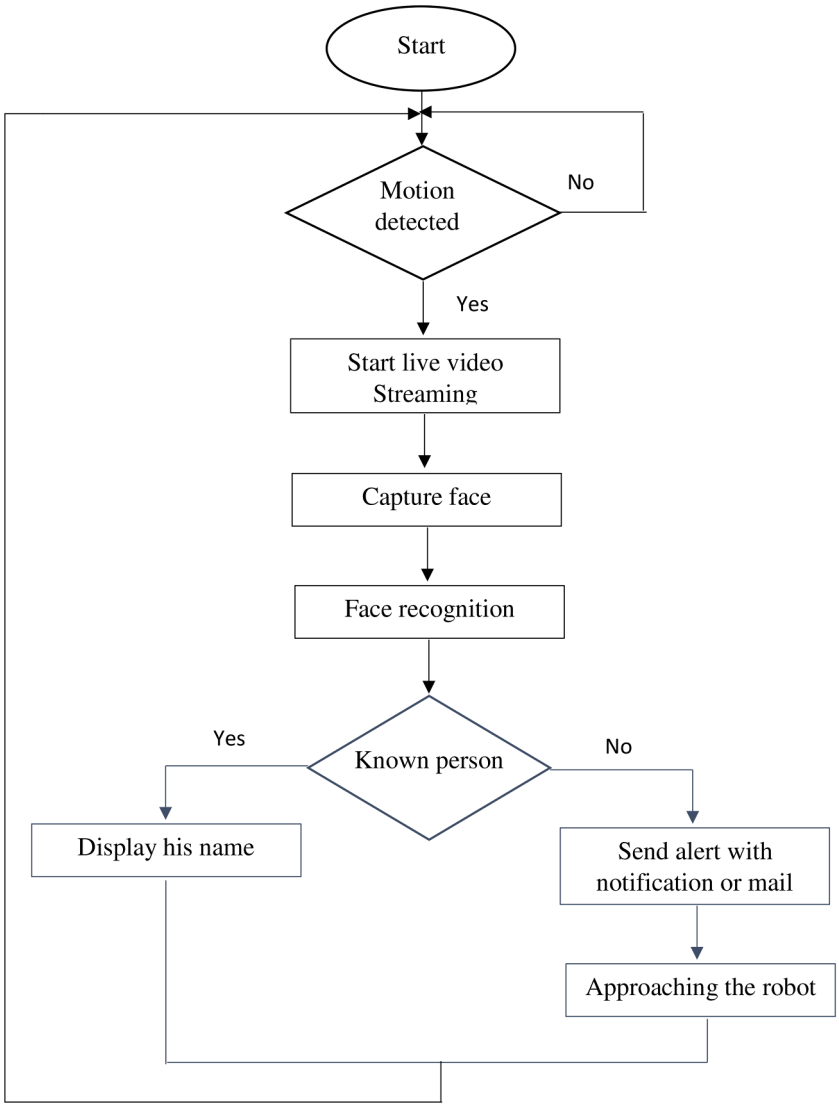


Fig. 3. Flowchart of surveillance robot.

others. We use a PIR sensor to detect human motion with a sensitivity range of about 7 m

- **USB camera:** the camera is frequently used in surveillance systems. It is used in this project for streaming live video to the user in remote location and for capturing the image of the intruder when motion is detected.
- **Power supply:** Power can be in the form of batteries or accumulators, taking into account the characteristics of the robot. The power source for the motors is a 12 V battery which is supplied appropriately to the motors using the motor driver. A power Bank is used to power the Raspberry pi.

The block diagram of the robot system is given by the following (Fig. 2,).

3.2. Software design

For coding, Python language [19] and Open CV (Open Computer Vision) library are utilized to record video, analyze and manipulate the images captured by the camera. It provides a set of computer vision algorithms that can perform a range of image processing: color extraction, facial detection, shape, application of filters. Open CV is widely used in academia and industry [20,21]. In our project, Open CV is used as it contains the necessary face recognition algorithms. Additionally, VNC (Virtual Network Computing) is used to remotely access the Raspberry PI graphical desktop.

On the other hand, the HTML language is implemented to design web interfaces by using various available tags along with Flask, which provides useful tools and functions to facilitate creating web applications in Python and sending requested data in a framework [22].

In addition, Fritzing software is exploited for electrical circuit design of the surveillance robot.

4. Flowchart of surveillance robot

4.1. Operation

The designed robot is remotely controlled via Wifi connection and a web application to communicate with the robot and manipulate its movements. The web interface contains two areas:

- The command area which contains four buttons that allow us to move the robot to the desired destination.
- The display area that displays the live videos taken by the camera which ensures surveillance and safe movement of the robot.

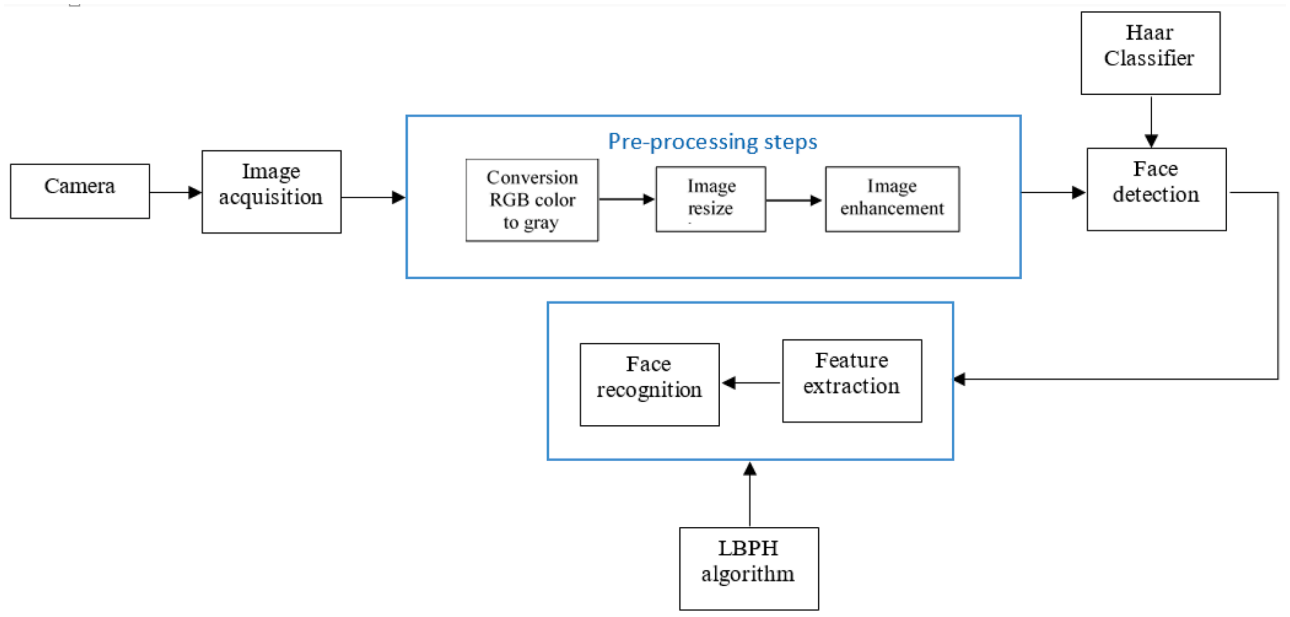


Fig. 4. Flowchart of face recognition.

It is assumed that the system monitors a well-defined area in a company and checks the presence of humans by using motion sensor and camera. Based on facial recognition algorithms and IoT, the robot can instantly transmit videos, photos and notifications via message or email, thereby distinguishing company personnel from intruders in real time with high reliability and alerting room control.

4.2. Video stream transmission and data import

The transmission of the stream live video is an essential task of any monitoring system, it consists in viewing the camera remotely in order to ensure the control of the robot. For this task, a client-server system developed in HTML based on RTP (Real-time Transfer Protocol) and Flask was utilized. To stream video content from the server, the client sends a request to start the camera and begin the transfer. The server treats the request by checking the supported format and it creates an RTP session to transmit the video to the client's IP address.

Each time a moving object is detected, an image recording of that scene is automatically launched, giving the control center a chance to import and display the recorded files. After the transfer is complete, the control station can view all the videos sent by the server (robot).

4.3. Alert system

The main purpose of the alert is to caution security guards when an intruder enters the company. This typically involves IoT technology, which is widely used nowadays in several areas such as smart city [10], automobile field [23], farming, smart grids.... IoT is defined as a system of interrelated computing devices, mechanical and digital machines allow transferring data over a network without requiring human-to-human or human-to-computer interaction.

In this work, the web application allows to send notifications and emails to smart phone and home control. The data is processed by the Raspberry Pi board which is connected to a Wi-Fi module.

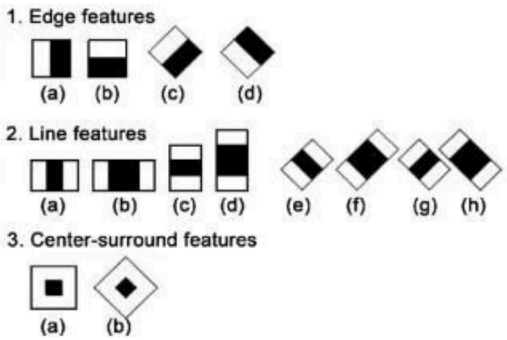


Fig. 5. Haar-like Feature [25].

4.4. Flowchart

When the PIR sensor detects the presence of a person, whether stored in the database or not, the robot will start live-streaming the video and taking pictures. With the help of face recognition algorithms, the system can determine whether an identified face is that of a known or unknown person by comparing the received image with the data already stored in the database. If a person is detected as an intruder, the system sends an immediate notification to the room control, and can also send an email with a photo of the person. If it is a known person, it will give his name.

In addition, the web application is developed to remotely control the robot in order to approach to the person for better visibility and take high quality pictures and videos. Note that the robot can be used as a fixed surveillance system. The flowchart of the surveillance robot is shown in Fig. 3.

5. Face recognition

Face recognition is a technology combining biometric techniques, artificial intelligence, 3D mapping and Deep Learning to verify faces. The process of identifying a person is divided into the following steps: face detection, feature extraction and face recognition.

Face detection is the basic task on face recognition which detects the presence and location of faces in images or videos without identification. The next step is to extract features from faces in a vector containing unique numeric values. In the identification step, the system checks whether the displayed face model corresponds to one of the models stored in the database. There are different face recognition algorithms such as LBPH, Eigenface and Fisherface [24,25]. In this work, Haar Cascade Classifier and LBPH algorithms are used for image processing to detect faces and recognize people, respectively. Fig. 4 shows the flowchart of face recognition.

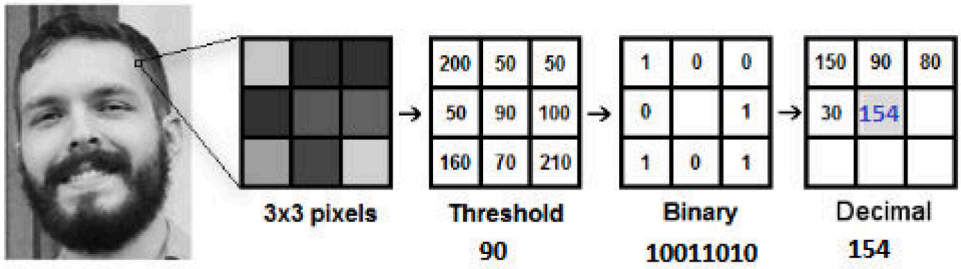


Fig. 6. Greyscale value calculation for sub matrix [24].

5.1. Face detection with Haar classifier

Object detection using Haar feature-based cascade classifiers is one of the popular face detection algorithm proposed by Paul Viola and Michael Jones in [26]. It is a machine learning based approach where a cascade function is trained from a large set of positive images (images with face) and negative images (images without face).

The Haar features are the calculations that are performed on adjacent rectangular one light and the other is dark, at a specific location in a detection window. Features from a Haar cascade are shown below (Fig. 5)

Every Haar feature is a single value obtained by subtracting the average of pixels in light rectangle from average of pixels in dark rectangle. Consequently, the Haar pixel value can be calculated by using Eq. (1).

$$Pixel\ Value = \frac{\text{Sum of the dark pixels}}{\text{Number of dark pixels}} - \frac{\text{Sum of the light pixels}}{\text{Number of light pixels}} \quad (1)$$

Haar features are considered present if the difference is above a threshold (set during learning). For large images, these features can be difficult to determine, as a result, Violas and Jones used a technique called integral images [25].

AdaBoost is a machine learning algorithm used to train classifiers with only the best features. A cascaded classifier is a concatenation of several classifiers arranged one after the other. It makes a lot of small decisions to indicate that an object has been found (positive) or moved to the next area (negative). The structure of the cascade classifier is a degenerate decision tree.

When the cascade classifier detects a face, the image is processed for face recognition, where the image is compared to a collection of face samples. OpenCV already contains Haar cascade classifier and several pre-trained models for face recognition, ready to use. According to [27], Haar cascade classifier has higher accuracy than the LBP classifier.

5.2. Facial recognition with LBPH algorithm

LBPH is a face recognition algorithm for recognizing faces. It uses 4 parameters, namely Radius, Neighbors, Grid X and Grid Y [8,24]. Radius is used to construct a circular local bit pattern and represents the radius around the center pixel. Neighbors are multiple sample points used to create a circular binary pattern. Grid X is the number of cells in the horizontal direction, and Grid Y is the number of cells in the vertical direction.

For feature encoding, the image is divided into multiple cells (3×3 pixels) as shown in Fig. 6. The central pixel (90) which is the threshold is used to define new values from 8 neighbors. Each pixel value is compared with the central pixel. If the value is greater or equal to central pixel, the result is '1' otherwise, the result is zero.

By accessing clockwise a binary value for the cell (10,011,010) is generated. Thereafter, the binary code is converted to a decimal value (154) indicating the LBP value of the center point.

Using the Grid X and Grid Y parameters, the resulting image is divided into grids and a histogram is created for each grid. Then a new bigger histogram is created by concatenating each small histogram. These steps are illustrated in Fig. 7.

Based on the comparison of the histograms, the algorithm will be able to identify the images. There are various approaches to compare histograms; a commonly used approach is the Euclidean distance. Considering the two histograms of LBP H1 and H2, the Euclidean distance is given in Eq. (2) below.

$$D = \sqrt{\sum_{i=1}^{N} (H1_i - H2_i)^2} \quad (2)$$

5.3. Performance evaluation

Face recognition algorithms generate two types of errors: false positives (FP) and false negatives (FN). The FP situation occurs when the algorithm thinks there is a positive match between two facial images, but there is actually no match. The second case happens when the algorithm returns results that there is no match, but really there should be one. The complement of these two parameters is a true positive (TP) when the algorithm correctly identifies a face and a true negative (TN) when there is no match between two face images and the algorithm confirms this result.

Therefore, false negative identification rate (FNIR) and true positive identification rate (TPIR) can be calculated to evaluate face recognition

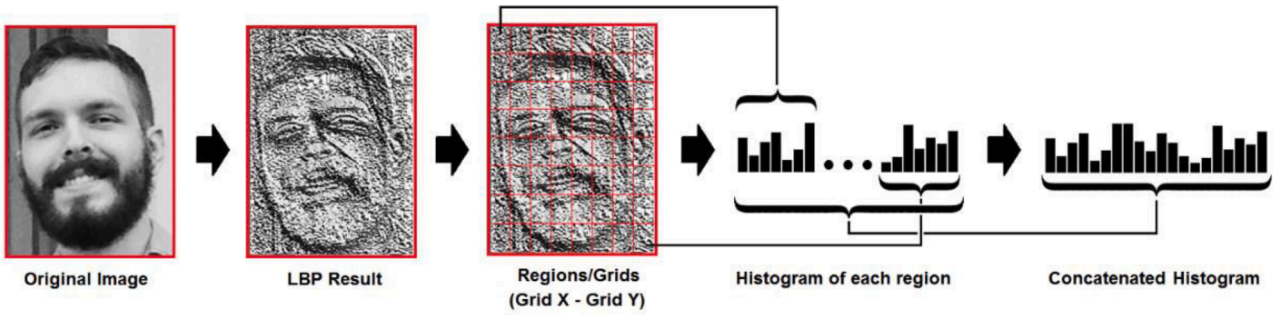


Fig. 7. Procedure for building the big histogram.

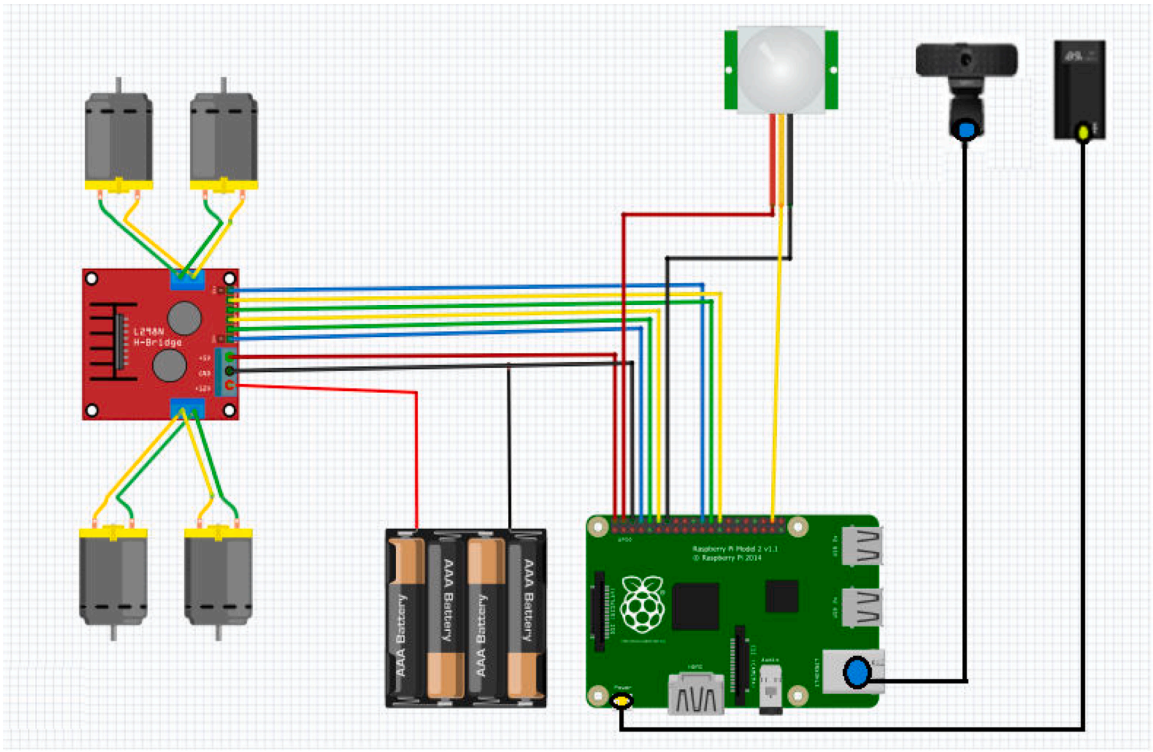


Fig. 8. Electrical circuit of the robot.

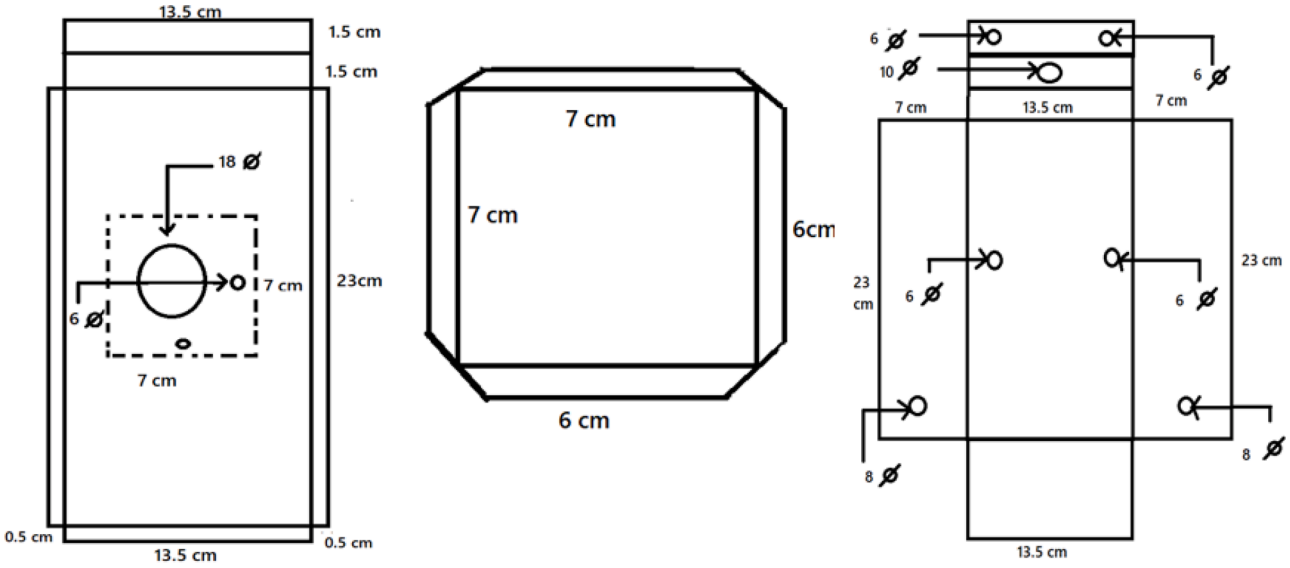


Fig. 9. Mechanical design of the robot.

algorithm [27,28]. FNIR and TPIR are given respectively in Eqs. (3) and (4).

$$FNIR = \frac{FN}{FN + TP} \tag{3}$$

$$TPIR = \frac{TP}{TP + FP} \tag{4}$$

Accuracy equation is deduced.

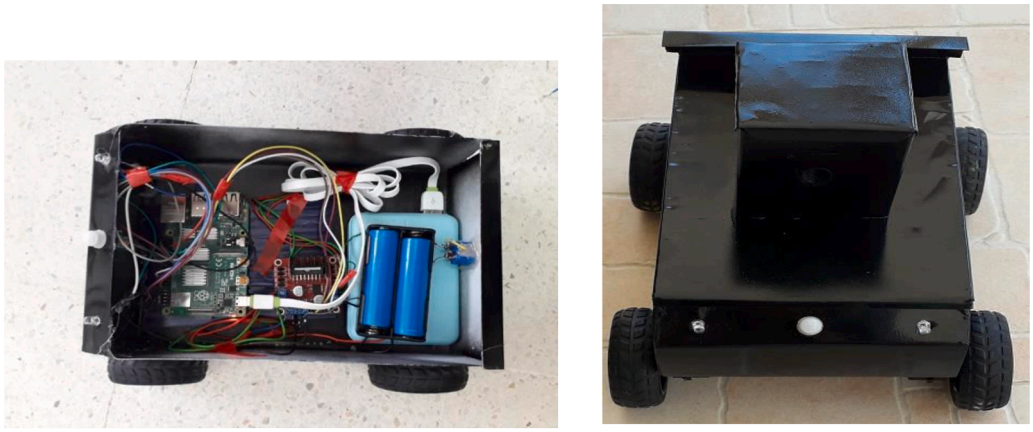
$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)} \tag{5}$$

6. Implementation

6.1. Mechanical and electrical design

In this section, electrical and mechanical design of the robot is presented. The schematic diagram of the proposed system designed using Fritzing software includes the following components:

- Four DC motors,
- L298N Dual H-Bridge,
- PIR sensor,



(a) (b)

Fig. 10. (a) Top view of the surveillance robot, (b) front view of the surveillance robot.

Table 1
The cost of HD-Guard robot.

Component	Price (Euro)
Raspberry PI 4 model *B* +Sd card 32GB	160
PIR Sensor	6
4 DC Motors + 4 wheels	48
USB Camera	18
Motor drivers L298n	7
2 rechargeable batteries	60
Power bank	25
Connection wires.	3
Total price	**327**

Note that the total cost of implementation is much lower than existing monitoring systems.

- Raspberry pi4,
- USB camera,
- Power supply (power Bank and batteries),
- Connection wires.

The electrical circuit of the surveillance robot is exposed in Fig. 8.

After completing the development of the circuit and control application, the mechanical structure of the robot is made. The designed model of the system is called HD-Guard. The robot architecture is divided into three main parts: bottom, top and hat containing camera. A front view of these components is shown below: (Fig. 9)

The realized prototype of the surveillance robot is shown in Fig. 10.

6.2. Implementation cost

Implementation cost can be estimated as the total cost of hardware implementation and software development. To take advantage of the implementation cost of the framework, only the total hardware cost is considered. After specifying the price of each component, the total cost of the HD-Guard robot is shown in Table 1.

6.3. Results and simulation

When the PIR sensor detects human motion, a live streaming video is

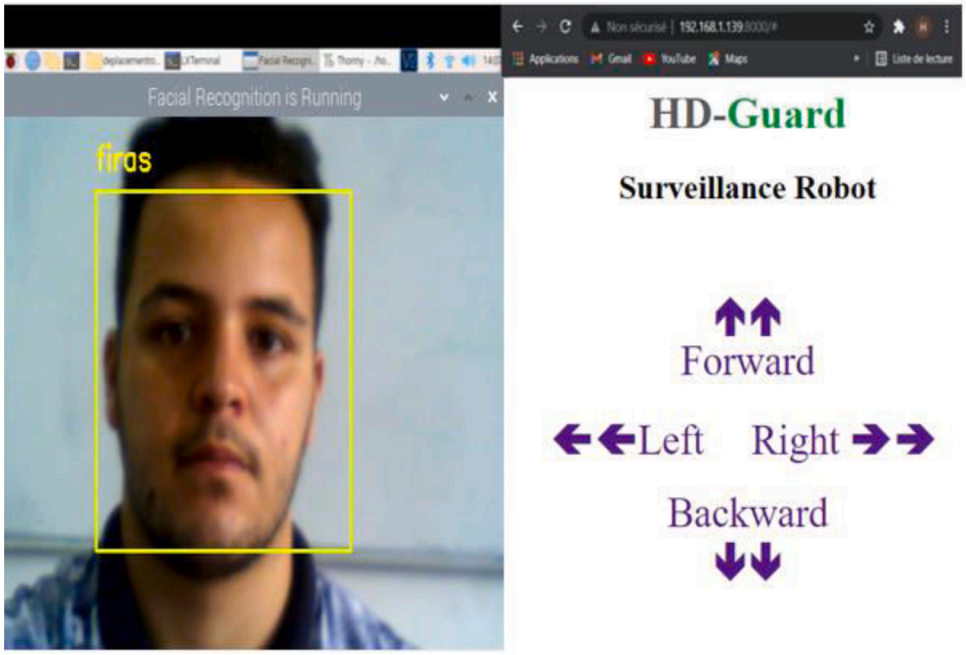
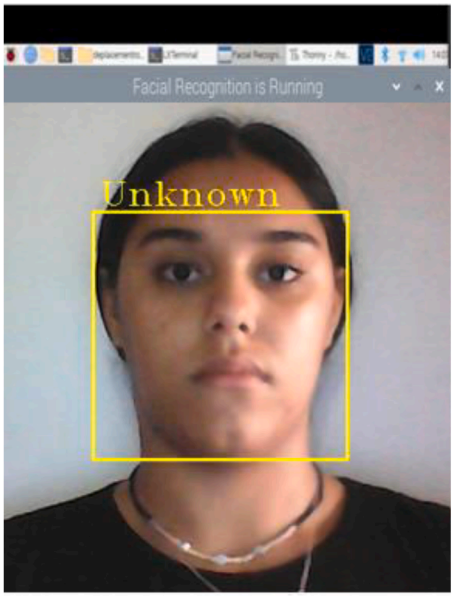
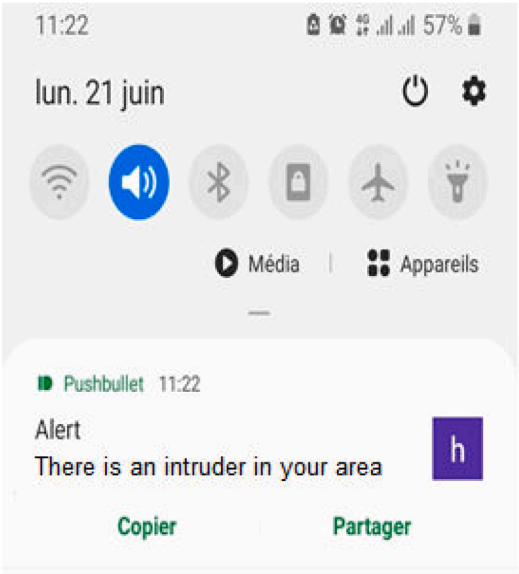


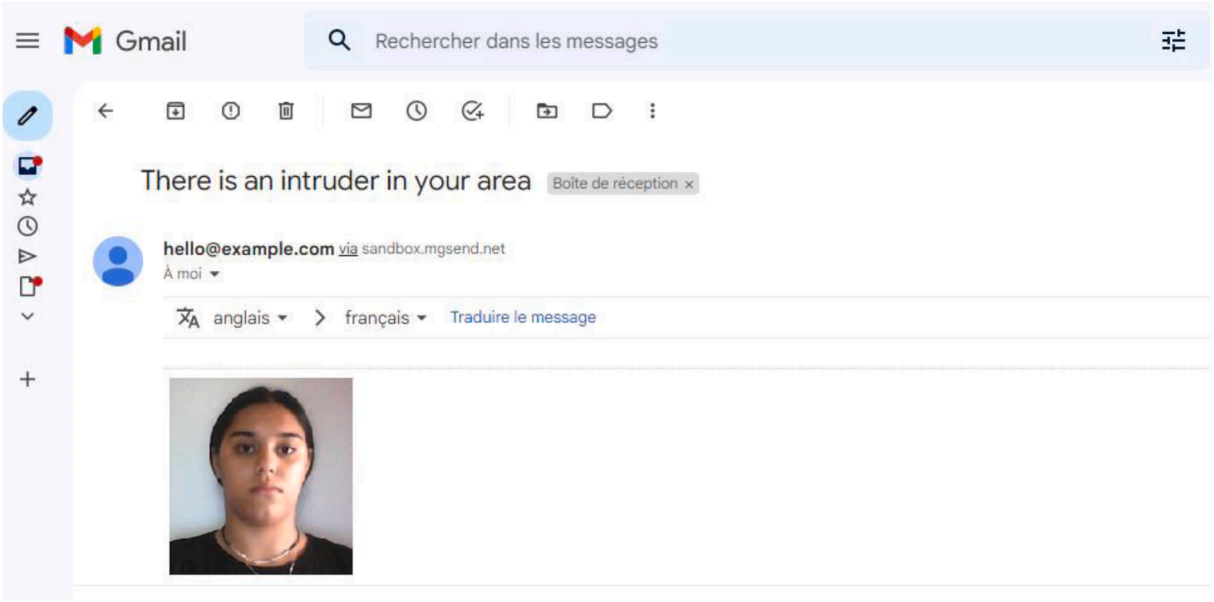
Fig. 11. Web interface and face recognition.



(a)



(b)



(c)

Fig. 12. (a) An intruder detected by the system, (b) An alert notification, (c) Email containing the person's photo sent when the system detects an intruder.

triggered and the system verifies the presence of personal facial data. If the detected person is known, the system displays his name, as shown in Fig. 11.

If the face data of the portrait does not match the database, the monitoring system will display "unknown" as shown in Fig. 12a), and send an alarm notification and email with captured image to room control as shown in Fig. 12b) and c) respectively.

In this work, we stored 30 images in a database and tracked the evolution of the algorithm during face detection and recognition by calculating the distance rate between detected faces and those stored in the database. The figures below show the results obtained in different situations.

The evolution of distance rate for different cases corresponding to known and unknown faces is shown in Fig. 13.

Fig. 14 presents the distance rates for two known faces. The first corresponds to image 3 (distance rate = 0.3950) and the second corresponds to image 20 (distance rate = 0.3758).

Fig. 15 shows the distance rates for two known and unfamiliar faces. For unknown face, the distance rate is greater than 0.6, therefore, the algorithm does not recognize it. The second face matches frame 5 (distance rate = 0.3428).

6.4. Discussion

A series of tests were then run to evaluate facial recognition algorithms for identifying personal. We point out that robot does not necessarily recognize faces simultaneously. Table 2 contains the number of detected faces, FP, TN, FN, TP, FNIR, TPIR and accuracy percentage.

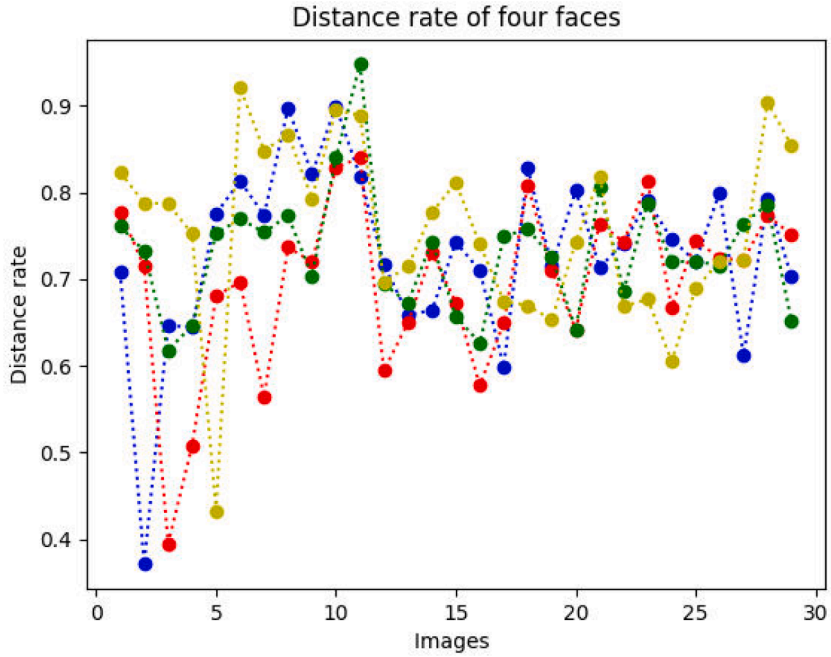


Fig. 13. Distance rate for different cases.

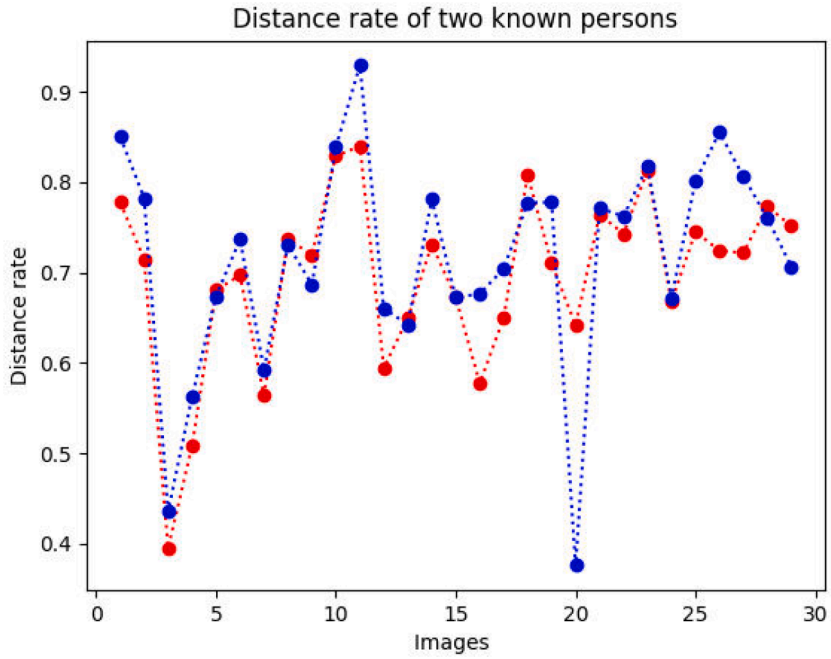


Fig. 14. Distance rate of two known faces.

Fig. 16 illustrates the scoring parameters of the face recognition algorithm in three graphs. The X-axis represents the number of detected faces, and the Y-axis represents FNIR or TPIR or percent accuracy.

We found that the FNIR value varies between 0 and 0.06, the TPIR value varies between 0.85 and 1, and the accuracy rate is greater than or equal to 90%, so we came to the conclusion that the face detection algorithm works very effectively on a sample of 30 frames.

6.5. *Comparison with other approaches*

Many other algorithms have been proposed to achieve the best accuracy for face recognition. There are two types of algorithms: non-deep learning, such as Eigenfaces, Fisherface, and Support Vector Machines (SVM), and deep learning: Convolutional Neural Networks (CNN).

A comparative study of non-deep learning and deep learning approaches for face recognition is discussed in [29]. The experiment was applied to a database consisting of 15 different subjects (faces). Table 3 presents the results showing the accuracy of different algorithms.

In this work, the LBPH method is also applied to 5, 10, 15 and 20 subjects (faces), and according to Table 2, the accuracy of 15 subjects is 93.33%. This percentage is similar to the accuracy reported by the CNN algorithm and better than the results of the non-deep learning algorithms. This again demonstrates the efficiency of the method used in this paper.

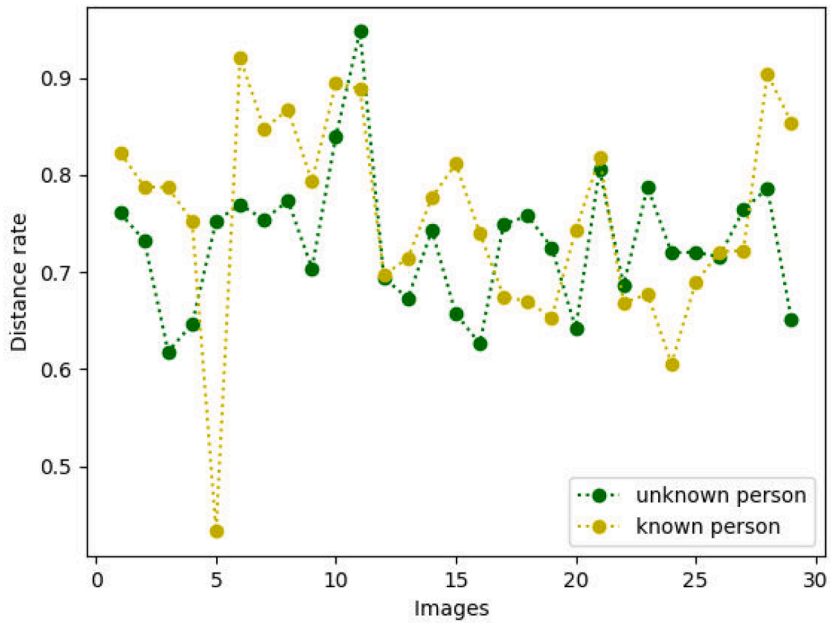


Fig. 15. Distance rate of known and unknown faces.

Table 2
Evaluation of face recognition algorithm.

Number of detected faces	5	10	15	20
FP	0	1	1	1
TN	2	3	4	4
FN	0	0	0	1
TP	3	6	10	14
FNIR	0	0	0	0.06
TPIR	1	0.85	0.90	0.93
Accuracy	100%	90%	93.33%	90%

Note that FNIR, TPIR, and Accuracy are calculated from Eqs. (3), (4), and (5), respectively. For clarity and readability, the results in Table 2 are shown in Fig. 16.

7. Conclusion and outlook

This article presents a mobile surveillance robot based on Raspberry Pi 4 and IoT. The smart system, called HD-Guard, can be controlled remotely via a web interface and WiFi connection. The designed robot continuously monitors a defined area and provides live streaming video

Table 3
Rate of recognition of different methods [29].

Method	Accuracy rate(%)
Eigenface	77.9
Fisherface	85.2
SVM	90.6
CNN	93.3

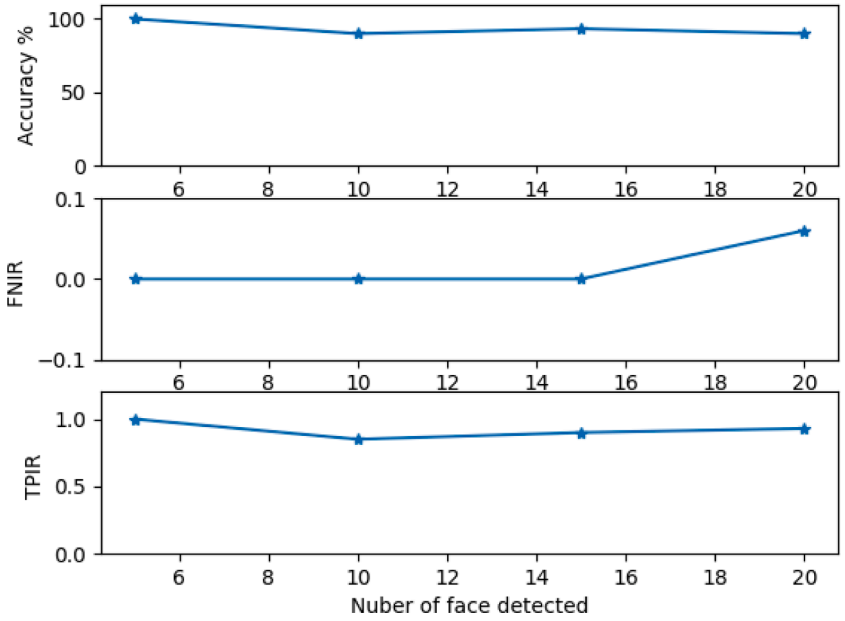


Fig. 16. TPIR, FNIR and accuracy of face recognition algorithm.

when human motion is detected. Thanks to the face recognition algorithms, the proposed surveillance robot can identify whether the detected person is familiar or unfamiliar. If the detected person is an intruder, the system will send alert notifications and emails via IoT. A performance evaluation is conducted to demonstrate the effectiveness and robustness of the face recognition algorithm used in this framework. Due to these features, the designed robot is suitable for surveillance applications in any area. This work can be extended to:

- The creation of a mobile security robot able to move autonomously, avoid obstacles and choose the optimal trajectory to follow.
- The use of more efficient facial recognition algorithms to enable robots to recognize vehicles license plates.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability

No data was used for the research described in the article.

References

[1] S. Patel, R. Sanyal, T. Sobh, RISCBOT: a WWW-enabled mobile surveillance and identification robot, J. Intell. Rob. Syst. 45 (2006) 15–30, https://doi.org/10.1007/s10846-005-9014-4.

[2] A.P. Raut, A. Raj, S. Patil, A. Katkar, Internet controlled techrobot using raspberry Pi, Int. J. Eng. Res. Technol. (IJERT) 9 (8) (2020) 594–600, https://doi.org/10.17577/IJERTV9IS080275.

[3] G.O.E. Abdalla, T. Veeramanikandasamy, Implementation of spy robot for a surveillance system using internet protocol of raspberry Pi, in: Proceedings of the 2nd IEEE International Conference on Recent Trends in Electronics Information & Communication Technology, Bangalore, India, 2017, pp. 86–89, https://doi.org/10.1109/RTEICT.2017.8256563.

[4] N. Hossain, M.T. Kabir, T.R. Rahman, M.S. Hossen, F. Salauddinv, A real-time surveillance mini-ROVER based on openCV-python-JAVA using raspberry Pi2, in: Proceedings of the IEEE International Conference on Control System, Computing and Engineering, Penang Malaysia, 2015, pp. 476–481.

[5] T. Kaur, D. Kumar, Wireless multifunctional robot for military applications, in: Proceedings of the 2nd International Conference on Recent Advances in Engineering and Computational Sciences (RAECS), Chandigarh, India, 2015, https://doi.org/10.1109/RAECS.2015.7453343.

[6] A.M. Martinez, Face recognition, overview, Encycl. Biom. (2015) 355–359.

[7] J. Galbally, S. Marcel, J. Fierrez, Image quality assessment for fake biometric detection: application to iris, fingerprint, and face recognition, IEEE Trans. Image Process. 23 (2014) 710–724.

[8] J.J. Lin, S.C. Huang, The implementation of the visitor access control system for the senior citizen based on the LBP face recognition, in: Proceedings of the International Conference on Fuzzy Theory and Its Applications (iFUZZY), Pingtung, Taiwan, 2017, https://doi.org/10.1109/iFUZZY.2017.8311817.

[9] T.S. Gunawan, M.H.H. Gani, F.D.A. Rahman, M. Kartiwi, Development of face recognition on raspberry Pi for security enhancement of smart home system, Indonesian J. Electr. Eng. Inf. (IJEEI) 5 (4) (2017) 317–325, https://doi.org/10.11591/ijeei.v5i4.361.

[10] M. Sajjad, M. Nasir, K. Muhammad, S. Khan, Z. Jan, A.K. Sangaiah, M. Elhoseny, S. W. Baik, Raspberry Pi assisted face recognition framework for enhanced law-enforcement services in smart cities, Fut. Gener. Comput. Syst. (2017).

[11] R. Bhavyalakshmi, B.P. Harish, Surveillance robot with face recognition using raspberry Pi, Int. J. Eng. Res. Technol. (IJERT) 8 (12) (2019) 648–651, https://doi.org/10.17577/IJERTV8IS120298.

[12] J.S. Quah, M.M. Ghazaly, Development and analysis of face recognition system on a mobile robot environment, J. Mech. Eng. 15 (2) (2018) 169–189. https://ir.uitm.edu.my/id/eprint/36336.

[13] R. Harshitha, M.H. Safwat Hussain, Surveillance robot using raspberry Pi and IoT, in: Proceedings of the International Conference on Design Innovations for 3Cs Compute Communicate Control, Bangalore, India, 2018, https://doi.org/10.1109/ICDI3C.2018.00018.

[14] M. Sunitha, P.V.S.S. Datta Vinay, V.S.N. Lokeshand, B. Dinesh, Kumar IP based surveillance robot using IOT, in: Proceedings of the IEEE 4th International Conference on I-SMAC, Palladam, India, 2020, https://doi.org/10.1109/I-SMAC49090.2020.9243519.

[15] T. Akilan, S. Chaudhary, P. Kumari, U. Pandey, Surveillance robot in hazardous place using IoT technology, in: Proceedings of the 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India, 2020, https://doi.org/10.1109/ICACCCN51052.2020.9362813. DOI:.

[16] N. Patrizi, G. Fragkos, K. Ortiz, M. Oishi, E.E. Tsiropoulou, A UAV-enabled dynamic multi-target tracking and sensing framework, in: Proceedings of the IEEE Global Communications Conference, Taipei, Taiwan, 2020, https://doi.org/10.1109/GLOBECOM42002.2020.9322567.

[17] H.D. Ghael, L. Solanki, G. Sahu, A review paper on raspberry Pi and its applications, Int. J. Adv. Eng. Manag. (IJAEM) 2 (12) (2021) 225–227, https://doi.org/10.35629/5252-0212225227.

[18] G. Balaji, L.R. Haritha, M. Mahesh, A.R. Kannan, Web controlled raspberry Pi surveillance robot, Ann. Rom. Soc. Cell Biol. 25 (3) (2021) 8582–8589. https://www.annalsofrscb.ro/index.php/journal/article/view/2402.

[19] J. Yates, Python Practical Python Programming For Beginners and Experts, CreateSpace Independent Publishing Platform, 2016.

[20] J. Howse, OpenCV computer vision with python, Packt publishing, BIRMINGHAM – MUMBAI, 2013.

[21] R. Puri, V. Jain, Barcode detection using OpenCV-python, Int. Res. J. Adv. Eng. Sci. 4 (1) (2019) 97–99.

[22] M. Grinberg, Flask Web Development, O'Reilly, Tokyo, 2014.

[23] V. Sanjay Kumar, S. Nair Ashish, I.V. Gowtham, S.P. Ashwin Balaji, E. Prabhu, Smart driver assistance system using raspberry pi and sensor networks, Microprocess. Microsyst. 79 (2020), https://doi.org/10.1016/j.micpro.2020.103275.

[24] A.M. Jagtap, V. Kangale, K. Unune, A study of LBPH, eigenface, fisherface and haarlike features for face recognition using OpenCV, in: Proceedings of the IEEE International Conference on Intelligent Sustainable Systems, Palladam, India, 2019, https://doi.org/10.1109/ISS1.2019.8907965.

[25] K. Kadir, M.K. Kamaruddin, H. Nasir, S.I. Safie, Z.A.K. Bakti, A comparative study between LBP and Haar-like features for face detection using OpenCV, in: Proceedings of the IEEE International Conference on Engineering Technology and Technopreneuship, Kuala Lumpur, Malaysia, 2014, https://doi.org/10.1109/ICE2T.2014.7006273.

[26] P. Viola, M. Jones, Rapid object detection using a boosted cascade of simple features, in: Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR 2001), Kauai, HI, USA, 2001, https://doi.org/10.1109/CVPR.2001.990517.

[27] A.B. Shetty, D. Bhoomika, J. Rebeiro, Ramyashree, Facial recognition using Haar cascade and LBP classifiers, in: Proceedings of the Global Transitions Proceedings, 2021, pp. 330–335, https://doi.org/10.1016/j.gltp.2021.08.044.

[28] M.D. Coco, P. Carcagnì, Face recognition algorithms: performance evaluation. Institute of Applied Sciences and Intelligent Systems, Dhitech scarl Campus Universitario, Italy, 2016.

[29] S. Setiowati, E.L.F Zulfanahri, I. Ardiyanto, A review of optimization method in face recognition: comparison deep learning and non-deep learning methods, in: Proceedings of the 9th International Conference on Information Technology and Electrical Engineering (ICITEE), Phuket, Thailand, 2017, https://doi.org/10.1109/ICITEED.2017.8250484.

Houda MEDDEB received her PHD diploma in Automation, Signal and Image Processing and Computer Engineering from Lorraine University, France, 2017. She carried out her research works in Automatic Research Center of Nancy (CRAN). She obtained her National Engineering Diploma, 2007 and Master's degree, 2008 from INSAT, Tunisia, in Industrial and Automatic Computing. Her research interests include System Control, Robotic, Artificial intelligence, Embedded System, Optimization algorithms and Wireless communication.

Zouhaira Abdellaoui received her PHD diploma in Telecommunications from the National Engineering School of Tunisia (ENIT) within the Sys'Com Laboratory in 2016, received the engineering degree in Electrical Engineering from the National Engineering School of Tunis, Tunisia, in 2010 and a master degree in Automatic and Signal Processing in the same institute, in 2011. Her current research interests are performance evaluation of Middleware on Real-time vehicular networks, optical networks wireless communication technologies, Robotic, Artificial intelligence and Embedded System.

Firas Houaidi received his Licence degree in Industrial and Automatic Computing from ISSATM, 2021, Tunisia. He is currently pursuing his Master of computer science at National Engineering School of Tunisia (ENIT).