DETECTION AND RECOGNITION OF MOVING OBJECTS FOR PHYSICAL SYSTEMS PROTECTION IN NUCLEAR FACILITIES

Mohamed I. Gaber [1*], Ashraf A. M. Khalaf [2], Imbaby I. Mahmoud [3], and Mohamed S. El_Tokhy[1]

[1] Engineering Department, Nuclear Research Center, Egyptian Atomic Energy Authority, Egypt.

[2] Electric Communications and Electronics Department, Faculty of Engineering, Minia University, Egypt.

[3] National Center for Radiation Research and Technology, Egyptian Atomic Energy Authority, Egypt.

[*] Corresponding Author E-mail: doctor_moh_2020@yahoo.com

ABSTRACT

Recently, the nuclear applications and services are entering in several domains of our life. It is a mandatory direction to protect the physical systems against any malicious sabotage or threat. Human activity detection and recognition techniques have a significant role in the physical protection systems. It enhances the protection regime through anomalous activity detection and authorized human-computer interaction applications. This paper is aimed to demonstrate a real-time system for moving object\human detection and recognition in order to protect the physical systems. It integrates computer vision with Internet of Things (IoT) technologies for detecting and recognizing the moving humans with their occupation times at the camera field. The proposed system can introduce more reliable and active intrusion detection scenarios with simple and low cost implementation techniques. It provides high flexibility for securing access to the monitoring information with storing for the historian purposes. Through an internet environment, the system can monitor the sensitive areas through detecting the unknown faces and their occupation times via ThingSpeak channels. The monitoring information is tracked through web based dashboards and ThingView mobile application. The system can launch automatically the alert notifications through SMS, and e-mail messages. These notifications are received whenever detecting an intruder face and exceeding the occupation times of human motion. The results provide effective features for implementing real-time and low cost applications even with low resolution cameras.

1- Introduction

According to the sensitive nature of nuclear facilities, it is a big challenge to develop an intelligent protection system with the most recent technologies. The physical protection systems have an essential role to protect the assets of nuclear facilities against physical intrusion, malicious attack, sabotage, and theft scenarios [1]. Through integration of computer vision with internet of things technologies can implement a reliable detection and recognition system for the moving humans. It allows enhancing the efficiency and reliability of a security regime at the nuclear facilities especially the nuclear power plants.

At the nuclear facilities, there are many controlled areas which have a special nature regarding the radiation levels exposure and nuclear materials existence [2]. These areas aren't permitted for accessing by the unauthorized persons especially at the operation times. So, it is a crucial manner to detect any movement of humans and their occupation times at these areas. Also, one of the recognition systems should specify an intruder who accessing the restricted areas. The face of humans can be considered as the main recognition element for accessing any system. Most of the recognition systems use the human face to authorize the persons in many applications such as human-computer

interaction, access control, and identification systems. Computer vision mechanisms can use to detect any movement action of humans with recognizing their faces [3]. It allows detecting and recognizing an unauthorized person at the controlled area especially in the operation times. It provides high protection to the physical systems through IoT applications and services. It is simple, cheap, and more accurate comparing with others. So, it enters to several applications such as human computer interaction, home automation, access control, and criminal identification. Motion detection techniques can help to recognize the human activities with the authorized faces.

For human recognition, the earliest techniques were used routine inspection by specialist persons who causing many problems. So, all of the innovative techniques are configured to prevent the intrusion threats without any efforts from the operators. Background subtraction approach is used with Gaussian mixture model to detect the motion of objects at the monitoring area [4]. One of the features extraction techniques can use to recognize the detected faces. Internet of Things (IoT) technology is a service to share data between the devices which can access the same channel [5]. This channel allows collecting the monitoring information through internet environment. By using IoT platforms, operators can monitor and control the hardware devices of any IoT application [6].

ThingSpeak is one of the most reliable and intelligent IoT platforms. It is an IoT analytics platform service that allows collecting, visualizing, and analyzing online data streams in the cloud environment. It depends on an open Application Programming Interface (API) which provides instant visualization for the streaming posted data from IoT devices [7].

Also, it allows communicating with another open (APIs) to provide data analysis and processing services. These services will help the operators to take the suitable actions regarding the system design procedure. The monitoring information is stored at the created channels which can be a programmable element provides the control data and alert notifications.

These channels provide a secure monitoring tool for the monitoring information from any location at any time. At the nuclear facilities, monitoring the real-time behavior and classifying the motion of humans is a crucial trend. It helps the authorities to detect any abnormal work at the targeted monitoring area. The motion occupation time can use to classify the behavior of humans. The operation and maintenance routines can defines the normal times for occupation the controlled areas.

In this paper, an intelligent detection and recognition system is proposed for the moving humans. With the help of capturing video streams, it can catch any intruder to protect the physical systems and produce alert notifications whenever detecting unknown faces. Also, it can detect the motion of humans with their occupation times at the restricted areas. The detected information is monitoring through the private channels of ThingSpeak platform. Alert notifications are launched whenever the system detects any threat like exceeding the occupation times or catching intruder. These notifications can be SMS messages at mobile phones and e-mail messages.

As shown in Fig.1, it shows an example of the general architecture for one nuclear facility. It contains three main areas including: controlled area, non-controlled area, and clean rooms in the controlled area. At these areas, it is necessary to use the detection and recognition techniques of moving objects for many reasons. One of these reasons is aiming to protect the physical systems of nuclear facility from any sabotage. The other one is aiming to protect the workers from high radiation levels during the routine operation at the restricted areas [8]. These areas are the main target of intruders and external attacks which can threat the nuclear facilities.
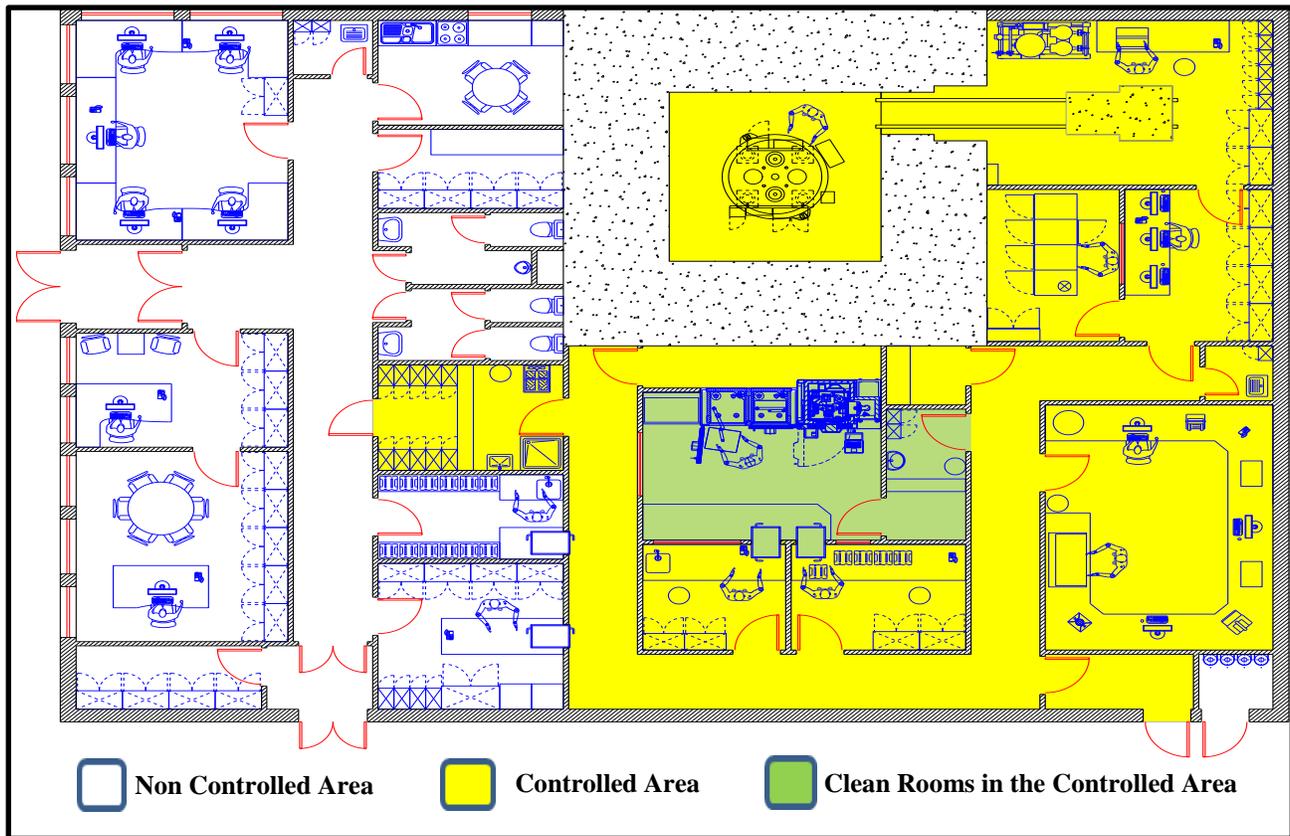
Fig. 1: An example of general architecture for a nuclear facility [33]

2- Related Works

Recently, the development trends of internet of things applications have motivated the researchers' interest. So, several research papers have found for studying the using of IoT devices and services in object detection and recognition mechanisms. These mechanisms are used for physical systems protection and intelligent intrusion detection applications.

For example, the authors of [1] proposed an efficient intrusion detection system which based on a convolutional neural network (CNN) to classify the moving objects with a virtual fence in active graphical user interface. It protects the facilities from an intruder by using the obtained images from the optical and thermal cameras. They used a training dataset with ten classes of intruders and animals classify the detected objects. Also, they develop a particle filter–based tracking algorithm to recognize the intruder's behavior through action recognition mechanism. They combined the different functions sensors to implement an efficient intrusion detection system in a nuclear power plant. In the same way, the authors of [2] presented a behavior recognition mechanism which is based on hand motion time series data analysis and use deep learning to explore insider sabotage detection. They classified five potential malicious motions using a test dataset with different motions including Pushing, Grasping, Cutting, Patting, and Turning. They verified the robustness against data loss by verification datasets at different data loss ratios. Their mechanism has accurate and real time characteristics for hand motion recognition which detecting the insider sabotage at the nuclear facilities. But, these systems have suffered from many defects regarding the extra expensive cost through using the highest cost cameras. Moreover, it used high computing and processing computers or servers for the training datasets.

The authors of [9] presented a method for tracking human motion through wide angle image distortion. It automatically estimates the transformation parameters needed to improve the accuracy of motion recognition; these parameters are applied to a distorted wide-angle image in every frame. It allows recognizing the motion of human in both work and protective clothing. They built new convolutional neural network (CNN) architecture for human pose estimation and human motion recognition with an ability to handle wide angle and close-range images. While, they didn't show the anomalies of the detected information regarding the proposed human motion recognition system

The authors in [10] presented a real-time system which counts the number of people in the main library of Inonu University. It used Internet of Things technology for monitoring the status of such library regarding the occupation of available places. They used counter through Thingspeak platform to show the counter information in internet environment. But, the implemented system didn't recognize the humans through any human recognition mechanism. Thus, it introduced low accuracy in comparison with the other security systems.

Another example for using IoT devices is introduced in [11] which applied a machine learning approach for Indirect Human Presence Detection. The authors used the obtained information from several home automation devices to detect the presence of a person in the monitoring area. They used supervised learning algorithms to train the models of presence detection. However, the concluded results have low precision and recall measurements for the presence class. In addition, this system didn't launch any automatically alert notifications regard to the adversary actions.

In [12], the authors used the object detection mechanism to develop a smart home automation system which based on model view controller (MVC) architecture. It depended on Cloud of Things (CoT) such as, Amazon Web Service (AWS) cloud for the remotely homes monitoring. They used OpenCV library as an image processing tool to evaluate the performance of object detection algorithm under different environmental conditions such as the light intensity level, distance of object from camera, and frame size of video. Their obtained results ensure that the performance of object detection algorithm is essentially dependent upon selected embedded device, camera model and object detection algorithm. However, they didn't introduce any solutions for remotely and real-time implementation in internet of things environment.

The authors of [13, 14] studied the background subtraction technique which comparing two different captured images using Pi-NoIR camera. They developed security system to detect the suspicious object through motion detection mechanism. They defined the best time limit for capturing videos which allowing the detection of sufficient information for a user to identify suspicious activities. Also, they did several tests for getting the suitable locations for installing the cameras. They used IoT devices to detect the motion by using captured video from an embedded camera.

These devices allowed sending a notification to users through Telegram application for accessing the system at any time and from any location. However, these studies didn't focus on monitoring the gathered information at any graphical interface to detect and show the intruder's activity. To overcome many limitations in the studied literature, our proposed system enhances the efficiency and reliability of the human activities detection and recognition systems through an active real-time monitoring. It used the low cost and open source components for detecting the objects occupation times and unknown faces at many conditions. It can develop the real time monitoring applications and frameworks in IoT environment. The major contributions of this work can be summarized as follows:

- The proposed system integrates computer vision techniques with Internet of Things technologies to present a reliable detection and recognition system for the moving humans.

- Detecting the movement of any object and their occupation times to monitor the restricted areas.

- Using the face recognition techniques for any authorized access and to analyze the activities through the video streams.

- Using ThingSpeak as internet of things platform for remotely real-time monitoring through the cloud servers and external (APIs).

- Alerting the operators by launching the notifications whenever the system detects any threat like exceeding the occupation times or catching an intruder face.

The rest of this paper is divided as follows. In section.3, the system architecture is explained with the methods of motion detection and faces recognition. The experimental results and their discussions are presented in Section 4. Section 5 concludes the study with an outlook to our future work.

3- System Architecture

As shown in Fig. 2, it illustrates the architecture of our proposed system. In the proposed system, a camera unit represents the sensing element for any motion objects. The motion detection module is launching after capturing the video streams. It uses background subtraction technique to detect any occupation from the moving objects. It detects the occupation time from the motion start time to end time with real-time monitoring. Also, it can record the motion durations and export their times at excel file for the historian purposes. Then, computer vision module is applied to detect and recognize the human faces [15]. The system will launch alert notifications in two main cases. The first one is whenever exceeding the threshold occupation time. The second one is whenever detecting unknown faces at the monitoring area. The system is very suitable for the real-time applications. Because, it can apply to real-time video streams and produce online monitoring information at ThingSpeak channels. Also, this information is tracking through mobile application at smart mobile phone.

In Fig. 2, the motion detection module detects any motion by using a high resolution camera with the background subtraction method. It finds the human faces and then the face recognition scenario can be processed to detect the known faces. Face recognition is used to classify the faces as known or unknown. It compares the invariant features got from the detected face with the stored features in system dataset. The detected motion time is calculated and recorded for analyzing in local and remote operation units. The alert notifications can be in many forms according to the permanent existence tools at the operation center with a redundant policy.
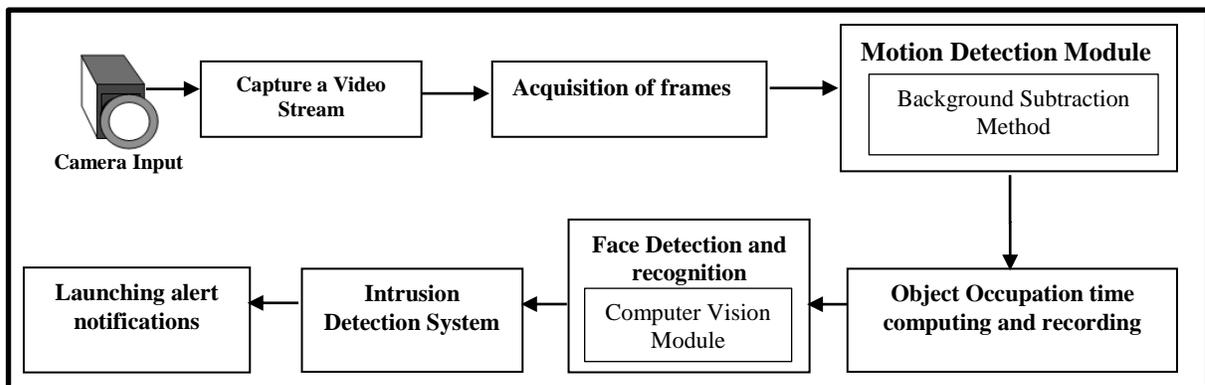
Fig.2: Block diagram of the proposed system architecture

3-1- Moving objects detection module

Motion detection module is depended on background subtraction method. It uses a main mathematical equation to subtract the intensity of two cascade images pixels. Background image is taken from the first frame in a captured video stream. The cascade images are considered from the next frames. Over the same pixels position, the current cascade image is compared with the background image. If the subtraction result is greater than threshold value, it identifies the intensity of moving objects pixels. Otherwise, it determines the background image pixels. The subtraction calculation can be concluded as:

$$DI(x, y) = \begin{cases} I_K(x, y) - I_{K-1}(x, y) > \text{Threshold} \\ \text{others} \end{cases} \quad (1)$$

Where $DI(x, y)$ is the subtraction result of image intensity for two cascade frames. $I_K(x, y)$ represents the image intensity for the current frame, and $I_{K-1}(x, y)$ represents the image intensity for the background or previous image frame. Threshold is a manually identified rate through the experimental results [16]. This method integrates image processing and computer vision to get foreground image for next object recognition processing. It helps to detect any motion and record its time occupation at the dedicated monitoring area.

As shown in Fig. 3, it shows the flow chart of motion detection and face recognition system. We proposed the system for any indoor facilities and at the same time presented use case for the critical infrastructures especially the nuclear facilities. The nuclear facilities can suffer from many threats through internal or external sabotage with their sensitive nature. Physical systems protection aims to prevent any sabotage at the nuclear facilities which can target the nuclear materials and radiological areas. It can also very useful to protect the workers from a high radiation dose at the restricted areas.

These facilities need continues monitoring for the human activities and intensive protection for the physical systems. Our work presents a suitable scenario for determining the detection and response time at any sabotage attempt from such adversary. Through the detection of both faces and occupation times for the humans, the operators can monitor remotely the physical systems via the secure channels of internet of things platform.
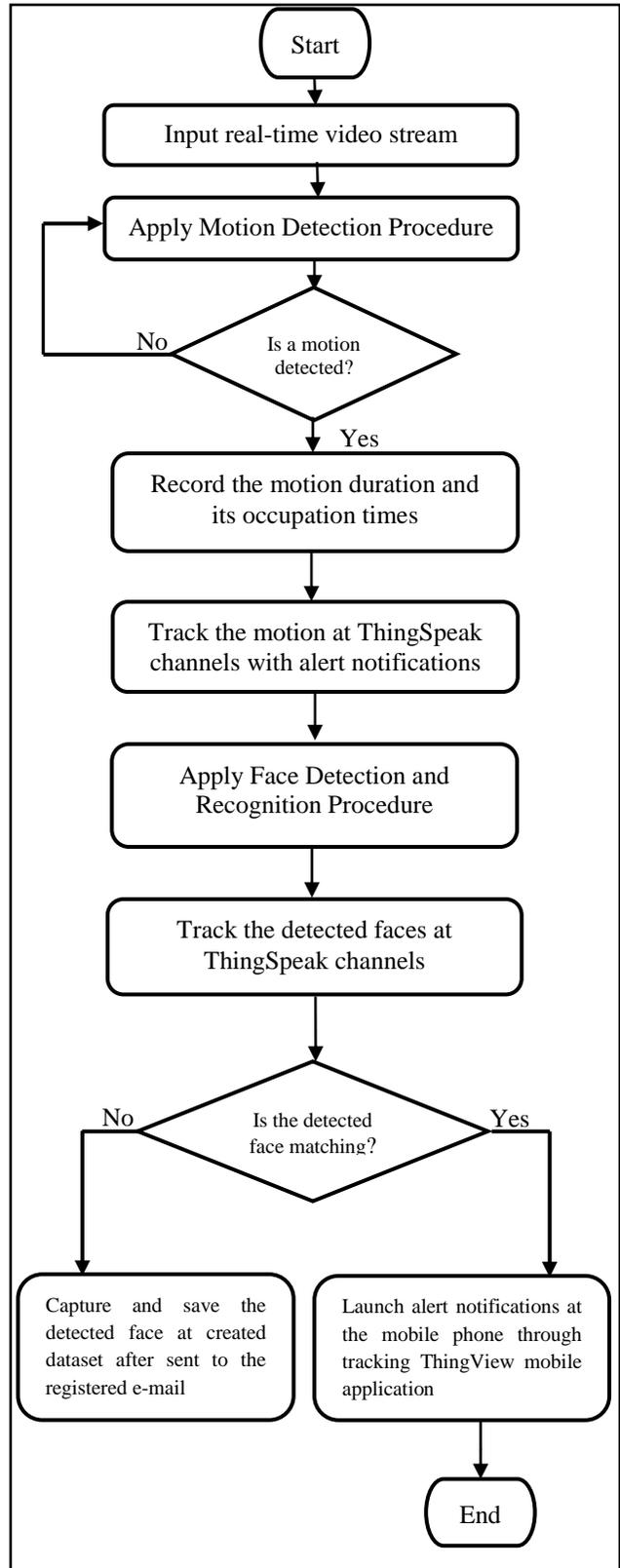
Fig.3: Flow chart of the moving object detection and recognition system

3-2- The physical systems protection scenarios

In particular, the nuclear facilities have suffered from many threats through internal or external sabotage with their sensitive nature. Physical systems protection aims to prevent any sabotage at the nuclear facilities which can target the nuclear materials and radiological areas [1, 2]. In this paper, an intelligent system for physical systems protection against the unauthorized motion and removal of nuclear materials or sabotage at the nuclear facilities based on IoT environment is introduced. Also, it can use to detect any human motion for avoiding the high exposure of radiation levels during the routine operation at the controlled areas of nuclear facility. The proposed system can monitor the behavior of real-time motion at nuclear facilities with time series data through IoT environment.

Detection of moving humans can refer to an unauthorized act in case of removal of nuclear material or unauthorized motion at restricted area or unauthorized access of persons. The detection time calculated from the first sensing time of intrusion presence and alarm rising to alarm assessing. As shown in Fig. 4, it shows the operation timeline for a physical protection system that presents the detection and response times for an adversary at the nuclear facility. The top line shows the time sequence of the opportunities of intrusion attack along the adversary's path to detect the presence of threat through the physical protection system. The proposed system meets the physical protection requirements recommended in the nuclear regulatory guidelines, and can be used as an unmanned surveillance system.
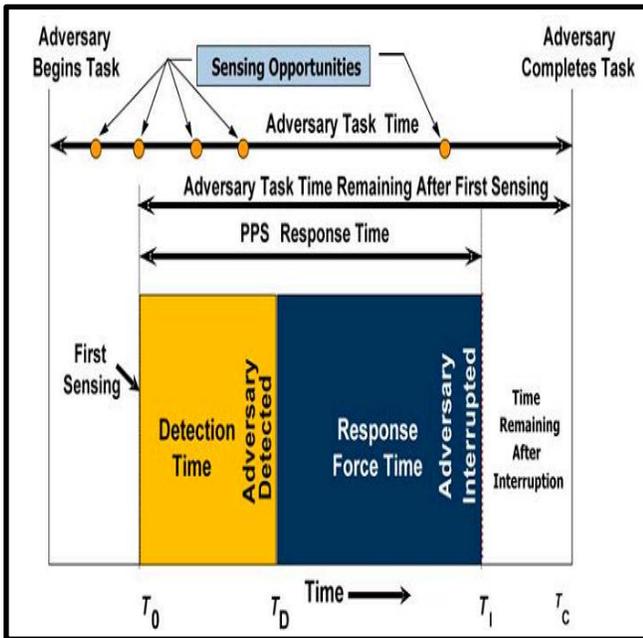
The Physical Protection System (PPS) response time is represented by the time duration from the first successful sensing of an adversary presence at T_0 to the interruption time at T_I. From T_0 to T_D is represented the time duration of acceptable detected motion at the controlled area in nuclear facility. The first sensing time is occurred early enough to permit the successful detection and interruption of intrusion before completing the attack scenarios at T_C [17]. The detected motion of humans is monitored with the time series data through using a private channel in IoT environment. If the occupation time of detected motion exceeds T_D, it can refer to the presence of threat from intrusion or risk on the insider workers from radiation exposure. Then, the proposed system can launch the alarm notifications for taking the suitable decision.

3-3- Human face detection and recognition technique

Face recognition module is implemented through three main steps as shown in Fig.5. The first one includes face detection and representation to model a face regarding the successive algorithms such as Haar-like features. The face image is rotated and scaled to get the same position according to the stored images at system database [18]. The second step is used to extract the face features for matching the detected face with the stored images. The third step is called classification; it gives the face images which have the highest matching features among the stored images comparing with the detected input image. Many methods can be used to recognize the face from a digital image. Local Binary Patterns Histogram (LBPH) method is one of the most useful techniques in face recognition procedures [19]. It divides a picture into a number of small regions and extracts the features from each one. These features are coded into binary patterns. Then, it can combine the calculated features from small regions to a single feature histogram for representing the face image.

Fig. 4: The detection and response time for adversary with the physical protection system [17].
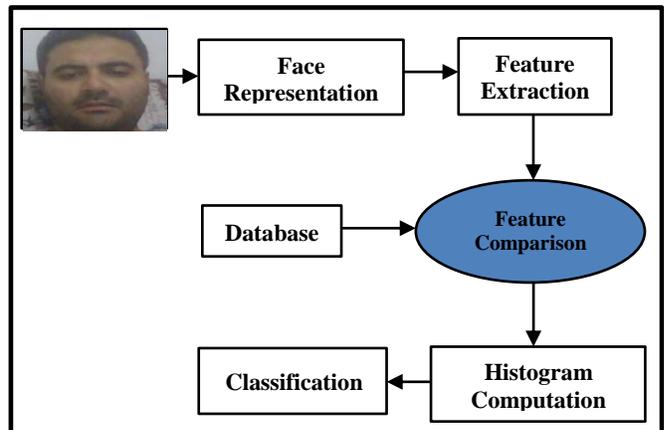
Fig.5: the general steps for identification and recognition procedure [13]

OpenCV is one of the most popular and usage computer vision techniques to recognize the faces from streaming real-time videos or video files. It depends on three methods for face recognition: Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), and Local Binary Patterns Histograms (LBPH). Local Binary Patterns Histogram (LBPH) method with Haar-like features is very suitable for real-time applications because of the efficient and robust results. It has high speed with progressive performance especially at different variations such as brightness, scaling, and rotation of face images. Also, it gives the highest accuracy with less execution time.

Local Binary Pattern (LBP) can be used for describing the texture and shape of a digital image. It divides an image into small areas to extract the face features. The LBP code is calculated for every pixel at the image. It is defined as an orders set of binary comparisons of pixels intensities between the center pixels and its surrounding pixels. The pixels of an image are labeled by taking the threshold for the neighborhood with the center value and providing the result as a binary number. The LBP operator is going to compare the center value with its P neighbor values on the circle with radius R. Then, it assigns neighbor value as 1 if the center value is bigger than the neighbor, assigns 0 on the contrary.

As shown in Fig. 6, P = 8 and R = 1 which means that 3×3 check is considered. The LBP operator supplies 8 bits as a binary number and transforms it into a decimal between 0 and 255 as a result for each center pixel. The following notation is used to describe the LBP operator [13]:

$$LBP(x_c, y_c) = \sum_{n=0}^{8} \text{Sin}(i_n - i_c)2^n \qquad (2)$$

Where (x, y) is the coordinate of center pixel such as 3x3 checks. i_c represents the value of center pixel to the value of eight surrounding pixels.
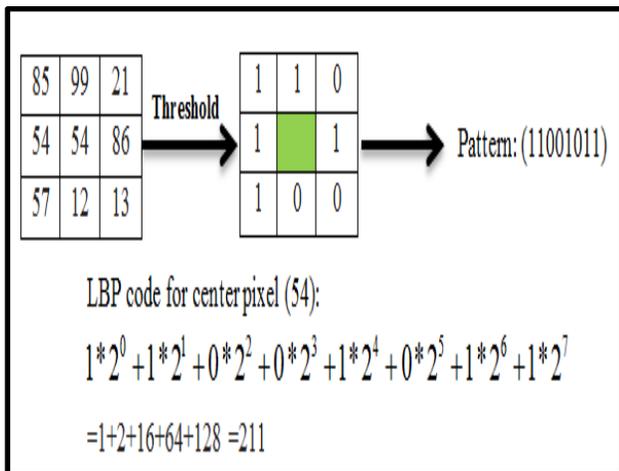
Fig. 6: Example of LBPH code

Then, the histograms of LBP operators are calculated to get the local features over the image portions. The feature vector can be constructed from the concatenate histograms for the divided parts of a whole image. Every bin in a histogram can describe a pattern and the hesitancy of its appearance at each portion. This histogram involves information about the distribution of local micro patterns including the edges, spots, and flat regions over the whole image. The face is described on three different levels of locality. It can be used to detect the matching of comparing images by calculating their histograms distances. The histogram of the labels can be used as a texture descriptor. The histogram of the picture LBP (x, y) can be described as follows:

$$LBPH(i) = \sum_{x,y} I\{i, LBP(x, y)\}, i = 0, ... n-1 \qquad (3)$$

Where i can denote the number of labels that produced by the LBP operator [20]. The detected face image is compared with the stored images to obtain the matching features through the histogram matching methods. For the face image, the highest matching level can refer to the output of image classification process. There are many techniques for the images classification including, Support Vector Machines (SVM), Gaussian Mixture Model (GMM), K-Nearest Neighbors (KNN) [21].

KNN technique gives the simplest way among the entire machine learning techniques for classifying objects from the closest neighbor at the training dataset in the feature environment. After the LBPH feature vector is extorted, the K-Nearest Neighbor (KNN) classifier is executed for the face recognition process through the histogram matching scenario. According to two face images, Chi-square statistic can use to measure the similarity of two images histogram. It assures if the two face images are concerning to the same human or not. The weighted Chi-square can be defined as following [16]:

$$d_{x^2}(G, E) = \sum_{i=1}^{B} \frac{(G_i - E_i)^2}{G_i + E_i} \qquad (4)$$

B is defined as the number of bins in the image histogram. G and E are the comparing normalized histograms for the detected face image and a stored one at the training dataset. i refers to the bin number in histogram which corresponding to one local region. The histogram features can describe the feature vectors of two face images for comparing their characteristics. The KNN classifier can recognize the faces from a measured distance between features via Chi-square equation [22] as it is very suitable for the face recognition systems. The features are classified regard to its closest neighbor in the dataset. In KNN, the whole dataset is divided into many portions and KNN is applied to each one separately to introduce high accurate and efficient results [23]. But, in PCA and LDA methods, the whole training dataset is processed which meaning the introducing of less accurate results.

Input:

   Vs = real-time video stream

   I1,I2 = a pair of consecutives frames

   Tth = the threshold size

   Ts = the object appeared in Tth

   Td = the detected moving object

   Toc = the threshold time for object occupation

Output:

   Lo = label to the detected object

   Pud = updated mqtt message to the ThingSpeak channel

   Ri = Reacts ThingHTTP action to invite Twilio API to send SMS notifications

```
1: While frame I in Vs do
2:      For each pixel position in frame I do
3:             Compute DI (x, y) by Eq. (1)
4:          If DI(x, y) > Tth then
5:             Td ← The detected moving object
6:          End If
7:      End For
8:      For each element in Td do
9:             Find label Lo for Td
10:            Lo ← Training Dataset (Faces)
11:         If ( Lo = = known face in Faces & Ts < Tex) then
12:            Permission granted
13:            Pud ← MQTT message to ThingSpeak channel
14:         Else
15:             Permission blocked
16:             Ri ← ThingHTTP action to invite Twilio API
17:             Publish notifications to SMS phone number
                 and E-mail account
18:         End If
19:     End For
20: End
```

Algorithm 1 shows the pseudo-code for object detection and recognition mechanism with using the channels of ThingSpeak platform. At the start, the input video streams divided into frames and each one processed through the background subtraction method to extract the moving regions. If the bounding box around the detected object converges in the training dataset (Faces). The mechanism will call the label for that detected object. In addition, if the object belongs to the dataset, the system will publish MQTT message to ThingSpeak channels and grant permission. Nevertheless, if the detected object belongs to the unknown faces, the system feeds MQTT messages with notifications in form of SMS messages, twitter, and e-mail notifications.

4- Experimental Results and Discussion

4-1- Human face detection and recognition evaluation

By using IoT platforms, operators can monitor and control the hardware devices of any IoT application. ThingSpeak considers one of the most usage IoT platforms. It provides an analytics service that permits collecting, analyzing and visualizing the live data streams in a cloud environment. It visualizes the streaming posted data from the IoT devices. Also, it allows performing a real-time data analysis and processing. As shown in Fig.7, it shows the architecture of integrating faces recognition and occupation time's detection modules with ThingSpeak platform and the system tracking interfaces. It introduces the proposal system for detecting the unknown faces and occupation times of moving humans with real time data processing. Twilio is a web based open Application Programming Interface (API) which provides the building blocks of adding text and multimedia messages to the IoT applications [24]. ThingView represents the graphical interface for ThingSpeak channels at the smart mobile phone applications [25].
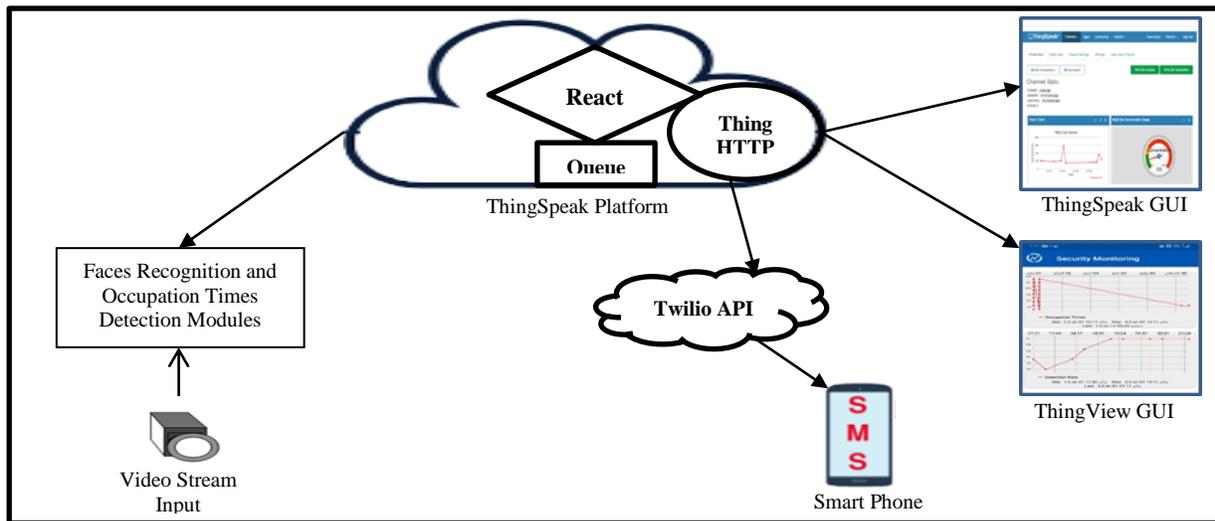
Fig.7: Architecture of monitoring data system with IoT

The monitoring system consists of camera, computer, and smart mobile phone with internet access. It has many advantages including simple implementation, low cost, and suitable for real time applications. The results of moving object\human detection and recognition are concluded as shown in Fig 8, 9. Fig. 8 shows two statuses during absence and detection of motion at any monitoring area for example (control room). The first status refers to unoccupied condition which no motion is detected. But, the second status refers to occupied condition which the presence of motion is detected. Also, it shows the date and time of any motion detected with recording availability for the historian usage.

Fig.8: Detection of any movements at a monitoring area

The proposed system has dataset for the authorized persons in different views for their faces. Each face has 20 images in the different views and the total number of faces is 10. So, the total number for the collected images at the training dataset is 200 images. The dataset can extend at any time with the new authorized faces. The system acts the same performance for detecting all the faces at the dataset. Also, it can show the detected known and unknown faces at the dashboard of ThingSpeak.

Fig. 9 shows a detection scenario for different faces at the monitoring area. Known faces come from the matching features of a detected face with any of the face images at a training dataset. Detection of known face can grant permission for accessing the system or area. But, the permission is blocked through the unknown face detection [26, 27]. If the occupation time exceeds the preset threshold value or the system detects an unknown face, ThingSpeak "React" initializes the application "ThingHTTP" to import (twilio API) to transmit SMS alerts.
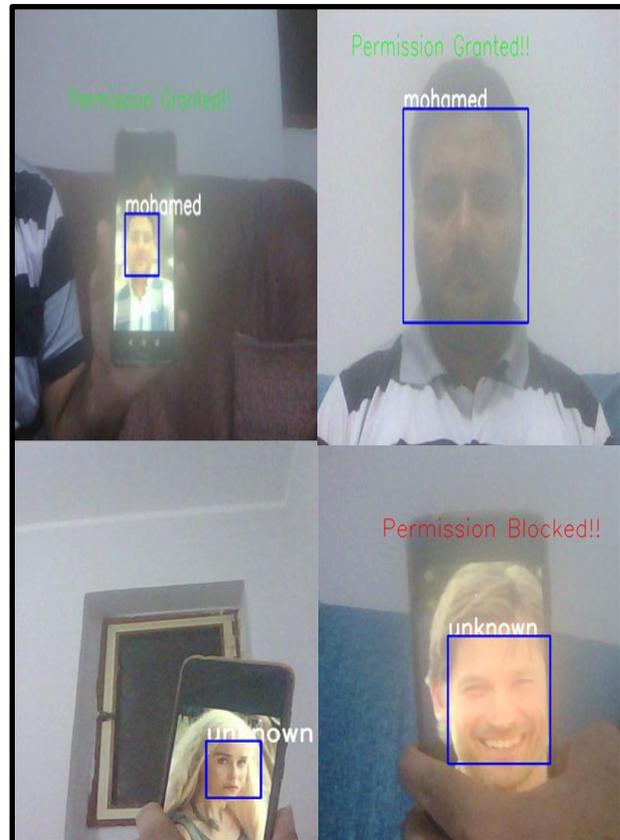
Fig.9: Detection and recognition of different faces with permission access control

Biometric face recognition systems have suffered from series attacks mainly the presentation attack. The systems are vulnerable to attacks by different sources of the faces identification such as photographs, photo display at any electronic device, photo print, and 3D faces reconstruction. The proposed system used local binary pattern technique as a simplest anti-spoofing technique of texture image analysis which threshold the image pixels according to their neighbors. But, it has a weak performance against the various series attack. At the same time, it presents better performance when combining with other techniques. A comprehensive study for all the presentation attack detection methods is discussed for the face recognition systems in [28, 29].

One of these solutions use a light field camera to reveal the presentation attack [30]. Another one presented a comparison of the last works considering cross database presentation attack detection. It used an optical flow based approach to outperform the state-of-the-art results in most experiment settings. Also, it considers the required capture time to obtain a confident presentation attack detection decision [31]. The system can add an essential condition to give an authorization for the known faces and overcome the problem of presentation attack. This condition can be the result of moving object detection module which assures the motion of detected contours around the faces with any solution of attack mitigation like eye blink detection.

IoT platforms provide a continuous and real-time remote monitoring especially at the emergencies or in critical situations with the historian reports to the authorized operators. ThingSpeak is one of the most popular and practical usage IoT platforms. It allows integrating the programmable hardware with the cloud dashboards and analytical tools [32]. Also, it provides the simple integration with other application programming interfaces (APIs) to launch the corresponding alerts during exceeding the threshold levels. In the proposed system, ThingSpeak monitors the behavior of humans based on faces recognition and their motion time series data analysis at the facility. It detects the number of known and unknown faces with the occupation time series at the secure corresponding channels.

The face recognition system can use to implement a human-computer interaction regime for the computerized systems. The faces detection and recognition programming modules integrate with ThingSpeak platform to provide the recognition information. The recognition statuses can be monitored and tracked through a dedicated dashboard at any computer or mobile phone. The results prove the high performance of detection and recognition even with low resolution cameras or virtual images and video streams.

4-2- ThingSpeak based data analysis

If the object (human) is detected, then the system would recognize the faces and show their status at ThingSpeak dashboard as IoT environment. Once the face was detected successfully and compared with the stored images at a system dataset. Then, the system sends its status (known or unknown) to a secure private channel of ThingSpeak through the programmable modules. The monitoring data is visualized through authenticated and secured channel for the end-user. The graphs provide the status of any detected face and their occupation time at the monitoring area. The channel enables to receive the detection data with updates every 5 seconds for implementing real-time system.

As shown in Fig. 10, it shows the number of detected faces and their status variation at the private channel of ThingSpeak. The channel can feed the operation center with all the monitoring data in files with CSV format for the historian purposes. Whenever the status of a detected face is changed to unknown, the system can launch alarm notifications to the operation center. The collected information is gathered and uploaded through internet for monitoring at ThingSpeak dashboard and ThingView mobile application. The occupation time of moving object can be detected and uploaded from the programming modules of motion detection to the ThingSpeak channel.
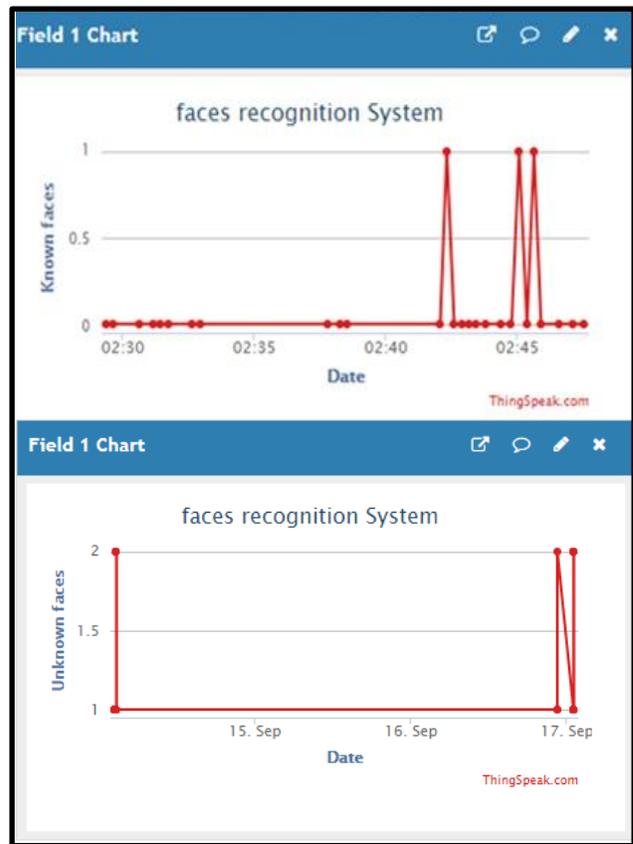
Fig.10: Known and unknown Faces recognition information at ThingSpeak dashboard

As shown in Fig. 11, it shows the occupation of moving object at different times even if it takes very simple time for high accurate detection. Whenever the occupation time exceeds a stored threshold value, the system can launch alarm notifications to the operation center. The proposed system is suitable for physical systems protection and human-computer interaction. It can authenticate the faces of humans to detect the intruders with unwanted behaviors. Also, it can operate with fixed cameras at any dedicated monitoring area. These modules can provide accurate results even through unclear video streams captured from low resolution cameras.
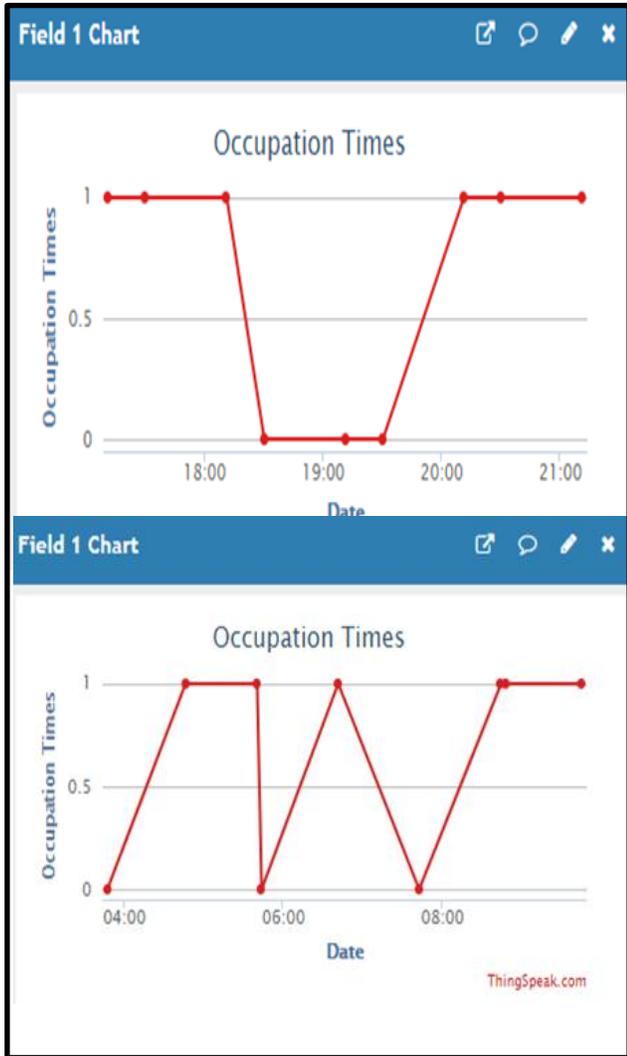
Fig.11: Occupation Times of moving object at ThingSpeak dashboard

4-3- System notifications based data analysis

As shown in Fig. 12, it shows the results of faces detection and recognition modules with the occupation times at ThingView mobile application. It allows tracking the monitoring information at a smart mobile phone as showing on the ThingSpeak platform. The channel was configured with a private API key to provide secure real-time data for monitoring at the graphical user interfaces. After the system had detected an unknown faces at the dedicated monitoring area. The operation center can be notified with alarming messages through the IoT environment. These notifications are received whenever detecting an intruder face and exceeding the occupation times of human motion. It is created via integration of ThingHTTP and React applications with Twilio and Twitter APIs.
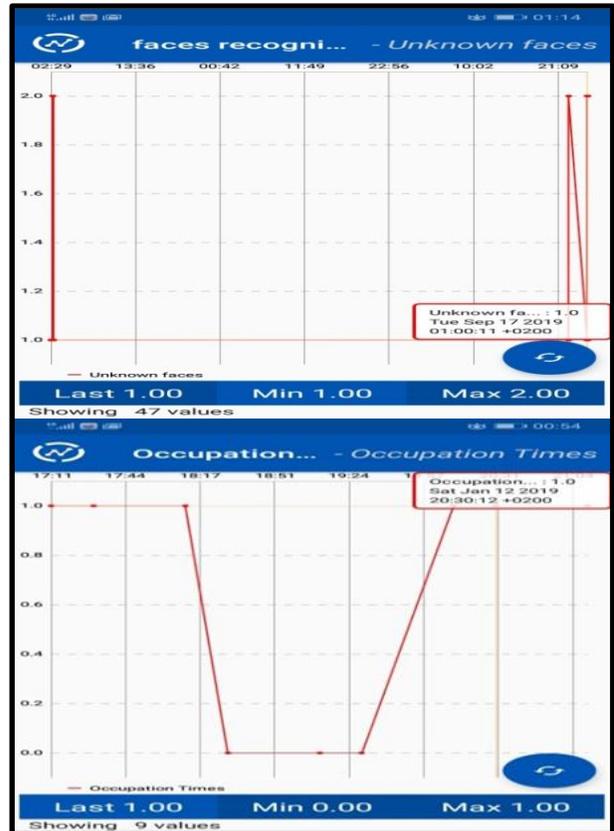
Fig.12: Faces recognition and occupation Times at ThingView mobile application

Also, Fig. 13 shows the received notifications through SMS from twilio API at the mobile phone. The operation center is received the SMS messages whenever the unknown faces are detected and the occupation time are exceeded a threshold value.
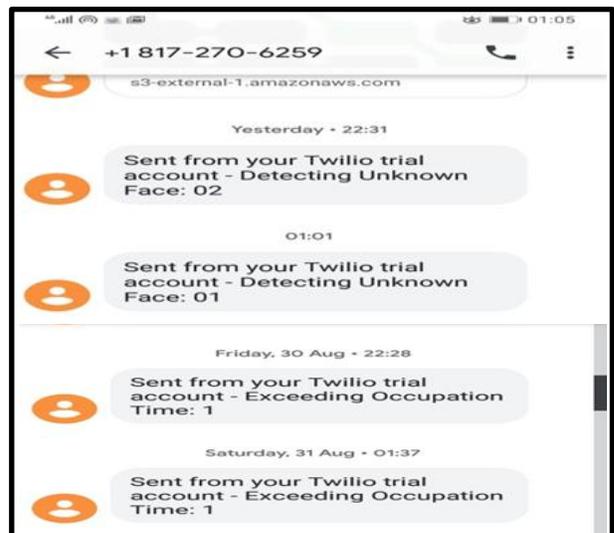
Fig.13: SMS notifications for detecting unknown faces and exceeding occupation time threshold

E-mail accounts can use to notify the operator about the detected face images through an attached file. As shown in Fig. 14, the system can launch an e-mail notification to a stored e-mail account with the latest detected face image. It considers as a real time system to detect and recognize the face images through e-mail notifications and showing their status with the occupation times at ThingSpeak dashboards. Currently, the alarming scenarios can depend on redundant ways including SMS, twitter, e-mail, and ThingView notifications.
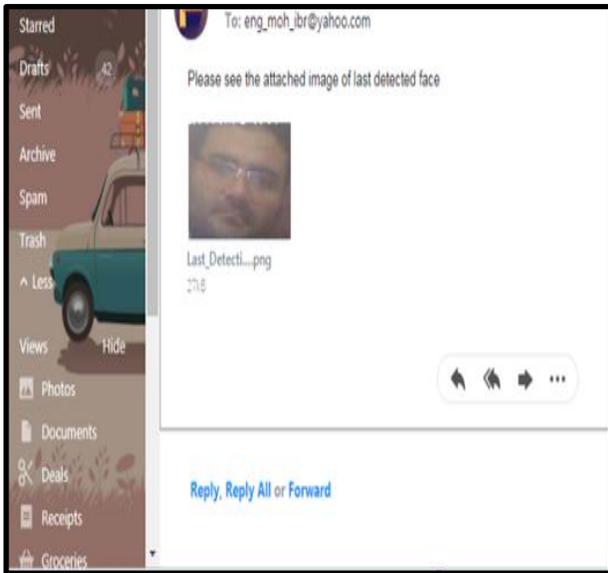
Fig.14: E- mail notification received with the latest detected face image

4-4- Execution time and complexity

The execution time has an essential role for enhancing the performance of monitoring systems regarding the real-time services. As shown in fig. 15, it shows a simple comparison between the required times for launching alert in our proposed system with the others to validate the performance.
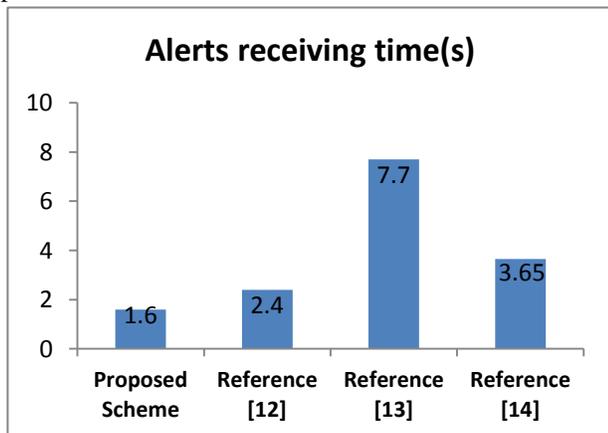
Fig.15: Comparison of Alerts receiving time at different methodologies

5- Conclusion and Future Work

In this paper, the computer vision algorithms are integrated with internet of things technologies to implement a real-time system for human detection and recognition. It provides the effective features for physical systems protection through the human and activity recognition. It depends on the usage of background subtraction and LBPH extraction techniques for human motion detection and his face recognition. The system integrates the robustness and efficient algorithms in real time scenarios. It presents a persuasive performance to protect the facility assets against any sabotage for improving the security regime. The monitoring data is tracked through the ThingSpeak channels to display in a computer based dashboard and mobile application. The system produces accurate results even with some weak points such as low resolution cameras and low internet streaming. Also, it allows alerting the operators via SMS, and e-mail notifications to take the suitable actions

The current study can extend through using the different machine learning algorithms. It will improve the human classification and recognition accuracy with an efficient data analysis algorithm for the anomaly activities detection. In addition, we will use the embedded systems including Arduino, Raspberry Pi, and the other electronic kits to improve the accuracy of human activity recognition with large datasets to coverage a wide area of the security applications. We will test the performance of our system regarding the serious security attacks.

REFERENCES

[1] S. H. Kim, and S. C. Lim, "Intelligent intrusion detection system featuring a virtual fence, active intruder detection, classification, tracking, and action recognition", Annals of Nuclear Energy, Vol.112, 2018, pp. 845-855.

[2] S. Chen, and K. Demachi, "Proposal of an insider sabotage detection method for nuclear security using deep learning", International Journal of Nuclear Science and Technology, Taylor and Francis, Vol. 56, No. 7, 2019, pp. 599-607.

[3] N. A. Othman, and I. Aydin, "A New IoT Combined Body Detection of People by Using Computer Vision for Security Application", in 2017 9th International Conference on Computational Intelligence and Communication Networks, IEEE, 2017, pp. 108-112.

[4] S. Y. Chiu, C. C. Chiu, and S. S. D. Xu, "A Background Subtraction Algorithm in Complex Environments Based on Category Entropy Analysis", Applied Sciences, Vol. 8, No. 6, 2018, pp. 1-21.

[5] R. K. Kodali, and V. S. K. Gorantla, "Restful Motion Detection and Notification using IoT", in International Conference on Computer Communication and Informatics, IEEE, 2018, pp.1-5.

[6] J. Im, S. Kim, and D. Kim, "IoT Mashup as a Service: Cloud-based Mashup Service for the Internet of Things", in 2013 IEEE International Conference on Services Computing, IEEE, 2013, pp. 462- 469.

[7] https://www.thingspeak.com

[8] M. Muniraj, A. R. Qureshi, D. Vijayakumar, A. R. Viswanathan, and N. Bharathi, "Geo tagged Internet of Things (IoT) device for Radiation Monitoring", in International Conference on Advances in Computing, Communications and Informatics, IEEE, 2017, pp.431-436.

[9] D. Miki, S. ABE, S. Chen, and K. Demachi, "Robust human motion recognition from wide-angle images for video surveillance in nuclear power plants", Mechanical Engineering Journal, 2020.

[10] K. Sabanci, E. Yigit, D. Üstün, A. Toktaş, and Y. Celik, " Thingspeak Based Monitoring IoT System for Counting People in A Library", in 2018 International Conference on Artificial Intelligence and Data Processing, IEEE, Vol. 56, No. 7, 2018, pp. 1-6.

[11] R. Madeira, and L. Nunes, "A Machine Learning Approach for Indirect Human Presence Detection Using IOT Devices", The 7 th international conference on digital information management, IEEE, 2016.

[12] F. Mehmood, I. Ullah, S. Ahmad, D. Kim, " Object detection mechanism based on deep learning algorithm using embedded IoT devices for smart home appliances control in CoT ", Journal of Ambient Intelligence and Humanized Computing, Springer, 2019.

[13] N. B. Harum, M. F. Ali, N. A. Zakaria, and S. Anawar, "Smart Surveillance System using Background Subtraction Technique in IoT Application", International Journal of Advanced Computer Science and Applications, Vol. 9, No. 12, 2018, pp. 122-128.

[14] H. Belhani, L. Guezouli, "Automatic Detection of Moving Objects in Video Surveillance", in: 2016 Global Summit on computer & Information Technology (GSCIT). IEEE, 2016, pp.70-75.

[15] N. A. Othman, and I. Aydin, "A Face Recognition Method in the Internet of Things for Security Applications in Smart Homes and Cities", in 2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG), IEEE, 2018, pp. 20–24.

[16] M. Upala, and W. K. Wong, "IoT Solution for Smart Library Using Facial Recognition", in IOP Conference Series: Materials Science and Engineering, 2019, pp. 1–12.

[17] International Atomic Energy Agency, "Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)", IAEA Nuclear Security Series No. 27-G, Vienna, 2018.

[18] T. Ahonen, A. Hadid, and M Pietikainen, "Face Description with Local Binary Patterns: Application to Face Recognition", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 28, No. 12, 2006, pp. 2037–2041.

[19] F. Deeba, A. Ahmed, F. A. Dharejo, H. Memon, and A. Ghaffar, "LBPH-based Enhanced Real-Time Face Recognition", International Journal of Advanced Computer Science and Applications, Vol. 10, No. 5, 2019, pp. 274-280.

[20] A. Ahmed, J. Guo, F. Ali, F. Deeba, and A. Ahmed, "LBPH Based Improved Face Recognition at Low Resolution", in International Conference on Artificial Intelligence and Big Data, IEEE, 2018, pp. 144-147.

[21] J. E. Bibault, P. Giraud, and A. Burgun, "Big Data and machine learning in radiation oncology: State of the art and future prospects", Cancer letters, Vol.382, No. 1, 2016, pp. 110-117.

[22] A. Kumar , P. S. Kumar , and R. Agarwal, "A Face Recognition Method in the IoT for Security Appliances in Smart Homes, offices and Cities", in 3rd International Conference on Computing Methodologies and Communication (ICCMC), IEEE, 2019, pp. 964–968.

[23] Z. Deng, X. Zhu, D. Cheng, M. Zong, and S. Zhang, "Efficient KNN classification algorithm for big data", Neurocomputing, Vol. 195, 2016, pp. 143-148.

[24] J. Kumar, S. Kumar, A. Kumar, B. Behera, "Real-Time Monitoring Security System integrated with Raspberry Pi and e-mail communication link", in 2019 9th International Conference on Cloud Computing, Data Science & Engineering (confluence), IEEE, 2019, pp. 79-84.

[25] www.twilio.com

[26] S. Pawar, V. Kithani, S. Ahuja, and S. Sahu, "Smart Home Security using IoT and Face Recognition", in 2018 fourth International Conference on Computing Communication Control and Automation (ICCUBEA),IEEE, 2018, pp. 1–6.

[27] S. Mehra, A. Khatri, P. Tanwar, and V. Khatri, "Intelligent Embedded Security control system for Maternity ward based on IoT and Face recognition", in 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), IEEE, 2018, pp. 49–53.

[28] R. Ramachandra and C. Busch, "Presentation Attack Detection Methods for Face Recognition Systems: A Comprehensive Survey," ACM Computing Surveys, Vol. 50, No. 1, 2017, pp.1-37.

[29] C. Murthy, M. Hashmi, N. Bokde, and Z. Geem, " Investigations of Object Detection in Images/Videos Using Various Deep Learning Techniques and Embedded Platforms-A Comprehensive Review", Applied sciences , 2020, pp1-46.

[30] R. Raghavendra, K. Raja, C. Busch, "Presentation Attack Detection for Face Recognition using Light Field Camera", IEEE Transactions on Image Processing , Vol. 24 , No. 3 , 2015, pp. 1-16.

[31] N. Damer, and K. Dimitrov, "Practical View on Face Presentation Attack Detection", in: BMVC, 2016, pp.1-11.

[32] K. Sree, G. Rao, " IoT Based Low Cost and Ageing Healthcare Monitoring System", International Journal of Engineering and Advanced Technology, Vol. 9, No.6, 2020.

[33] J. Comor, "Production of radionuclides by cyclotrons", Private Communication, Cairo, Egypt, 2019, pp. 282–325.