International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 9, No. 6 (Nov-2020)
http://dx.doi.org/10.12785/ijcds/0906022

An Intelligent Camera Surveillance System with Effective Notification Features

Fatimah Khodadin[1] and Sameerchand Pudaruth[1]

[1]Department of Information and Communication Technologies, University of Mauritius, Mauritius

Received 13 Apr. 2020, Revised 3 Jun 2020, Accepted 6 Jul 2020, Published 1 Nov. 2020

Abstract: The focal point of this work is to develop an intelligent camera surveillance system which englobes the key functionalities of existing surveillance systems. Other than regular functionalities such as motion detection, object detection, face recognition and counting people, it also integrates a novel and advanced object displacement detection feature to provide more security by determining if an object has been displaced by an intruder. When people are detected, a counting module displays the number of persons present in the surveillance area. A face recognition module distinguishes between authorised and unauthorised users. This biometric functionality reduces false alarms which makes the system more robust. An object detection module detects certain valuable objects such as handbags, laptops and smartphones. Also, images and short video recordings are stored on the cloud. Furthermore, the system introduces innovative real-time notification approaches for surveillance systems such as WhatsApp messages and phone calls, in addition to SMS and emails. Thus, this system is reliable and meets the aim of a modern intelligent surveillance system by combining multiple approaches to detect intrusions and to inform users effectively.

Keywords: Object Displacement Detection, Motion Detection, Face Recognition, Object Detection, Effective Notifications

1. Introduction

Today, the world is facing a multitude of issues pertaining to the security of people and their assets. Crimes capture the headlines on an almost daily basis. In 2019, the Office for National Statistics (ONS) recorded an 11% increase in the number of thefts in England and Wales [23]. Also, in Mauritius, there was a proliferation of criminal cases from 98,235 in 2017 to 99,652 in 2018 [34]. These law offences have appalling consequences on society and necessitate urgent solutions. Proper monitoring is a fundamental part of surveillance systems, and in this process, technology plays a vital role. Closed-Circuit Television (CCTV) is among the first camera surveillance systems introduced [5]. Its primary function is to record all the movements in an area, and it is still serving its purpose. Criminals are reluctant to intrude in personal and office premises equipped with CCTV surveillance systems since the recordings help in identifying them [9].

Many countries have already implemented camera surveillance systems. According to the Carnegie Endowment for International Peace (CEIP), 43% out of 176 countries monitor activities using surveillance systems. China is one of the most monitored countries where up to 626 million CCTV cameras operate to provide a secure environment [8]. In many other cases, surveillance cameras facilitate the process of identifying criminals such as in the London nail bombings attack in 1999 [19]. Moreover, criminals in high profile cases such as the Boston Marathon bombing in April 2013 and the Charlie Hebdo attack in January 2015 were caught on CCTV [7]. In 2016, two individuals attempted to rob a bank in Southern Brazil, and they were caught by a surveillance camera even though they were covered with outfits made of aluminum foil to prevent the sensor alarm to sound [10].

Surveillance systems have also proved to be an essential tool in a myriad of ways during the Covid-19 pandemic. Firstly, some countries are using modern cameras to ensure that the lockdown is respected. For example, in Moscow, around 100,000 cameras with facial recognition features have been used to ensure that people under quarantine stay off the streets [6]. Also, in Mauritius, CCTV cameras of the Safe City Project are used to deter citizens' movements during the quarantine period [13]. Another major challenge faced by people all around the world is the security of their businesses. The imposed lockdown created an unsafe environment as thieves broke-into business premises. In Israel, several shoplifters were caught on CCTV cameras. Video recordings were then used to identify the shoplifters [33]. Therefore, camera surveillance systems are nowadays more imperative.

E-mails: fatimah.khodadin@umail.uom.ac.mu, s.pudaruth@uom.ac.mu

However, over time people questioned the effectiveness of the originally introduced systems because of the myriad of crimes that still occur. Therefore, this work introduces the Intelligent Camera Surveillance System (ICSS) using an Internet Protocol (IP) camera to ensure more effective and efficient remote monitoring. It consists of an unmanned motion detection functionality and an object displacement detection functionality to detect any intrusion. These allow the system to monitor the level of motion and determine if a valuable object has been moved or stolen by an intruder, respectively. In order to make these functionalities robust, face recognition features have been added. Before triggering the object displacement and motion detection functionalities, the face recognition function determines if there are only intruders in the monitored area, that is, there are no authorised users. Hence, decreasing the number of false alarms. Footages are recorded daily and are used afterwards to identify trespassers. In addition, valuables such as handbags, laptops and smartphones are located, hence providing more visual information when viewing video footages. Following these events, the system uploads images and videos on a server. It also communicates instantly with the user. An email and a WhatsApp message, with a captured image and a video link, are sent to the user informing him/her about any intrusion. Moreover, an short message service (SMS) along with a video link is sent and a call to the user is initiated.

This paper proceeds as follows. An overview of the related works of surveillance systems is provided in section 2. The design and implementation of this system are discussed in section 3 and experimental results are provided in section 4. We conclude the paper in section 5.

2. Literature Review

Related works on surveillance systems which have certain common functionalities to our Intelligent Camera Surveillance System (ICSS) are reviewed in this section. The aim is to highlight the different functionalities implemented in existing systems and the limitations of those systems. As outlined by Shahad et al., it is crucial for intelligent surveillance systems to understand and predict events such as burglary and robbery in a monitored area. Hence, a system based on the Complex Event Processing (CEP) approach was developed to follow previous event patterns and detect anomalous activities [28]. A similar system was designed by Shao et al. using big data for security event detection. A database was set up for storing information about unusual events and warnings from cameras. The pre-alarming functionality is based on analyzing historical data in order to differentiate between normal and abnormal behaviors [29]. However, these systems are limited to only anticipating intrusion detection.

Constant monitoring is a long and arduous task for operators as they need to view each camera stream. Apart from being inefficient, it is also costly, especially when nowadays the number of monitored areas is increasing exponentially globally. The rationale behind automating camera surveillance systems is to reduce the workload on security officers. An approach adopted by automated surveillance systems is motion detection or tracking. Younsi et al. carried out a research on human motion detection in surveillance systems using techniques such as Particle Filter methods along with texture, intensity, special and motion velocity. A model is created for each person in each frame and after observing models from the succeeding frames, similarity distances between those frames are calculated to track intruders. However, the system cannot operate in complex situations [36]. A system designed by Alshammari and Rawat have used techniques such as trajectory analysis and pattern matching to track motion [3]. In addition, background elimination and image histogram are used to detect movements. The person is extracted from the background and subsequently, his/her location is determined by generating the frame histogram. Two cameras are used for tracking, however, only one intruder can be tracked at a time [18].

In addition to motion detection, it is important for a modern surveillance system to carry out object or people detection. Nguyen et al. introduced a surveillance system to detect people in a monitored area. Optical flow and a sampling method extract persons from video frames. Subsequently, a fuzzy classifier is used to classify the extracted template as a person. Nonetheless, the system cannot handle occlusions [22]. The Haar cascade method is adopted by an AI-based surveillance application to detect people in the surveillance area. The classifier was trained for several images to extract facial features from video frames. However, Haar cascade is not accurate in certain environments [1].

Another system using two algorithms namely Haar cascade and face re-identification was designed by Zhang et al. It consists of Edge Computing Nodes (ECNs) which receive video recordings from the cameras and process them for detecting people. After analyzing the data from all the ECNs, the controller responds to a user query such as locating a person. One drawback of the system is that a static background is required [39]. Furthermore, Wang et al. implemented a system in which the Convolutional Neural Network (CNN) algorithm is used for object detection in video frames. Frames are split into images which are analyzed by a CNN training chip to extract relevant features from them. The features are then classified accordingly to detect persons or objects [35]. However, CNN is a slow algorithm compared to other detection algorithms such as YOLO [25][26][27], SPPnet [14], Faster R-CNN [22] and SSD [20].

Face recognition can be used to reduce the number of false alarms since it determines if an owner or an intruder is present. Pudaruth et al. designed an intrusion alert system using face recognition whereby Eigen face recognition was used to differentiate between owners and intruders. The face recognition module compares the detected face to images stored in the database [24]. However, only emails were used to notify the users. Another system which uses Eigen faces was developed by Zhang et al., to locate specific individuals in videos. Each face is projected onto the face space to reconstruct occluded faces. One limitation of the Eigen face method is that it does not cater for extreme variations in expression and pose [38]. Furthermore, Zafar et al. used Bayesian convolutional networks to perform face recognition in their surveillance system whereby two face databases were used to train and test the model. This method showed an improvement of 3% when compared to conventional machine learning approaches [37]. Kaundanya et al. have used the Local Binary Pattern (LBP) approach for classification. Video frames were converted into binary images to obtain LBP histograms. These are eventually compared to a database for recognition. However, binary data can be easily altered if noise is present in the original video frames [17].

With traditional surveillance systems, owners or security officers need to ceaselessly keep a watch on activities in the surveillance area to detect an event. Also, video footages are usually reviewed after intrusions have taken place. In order to overcome these constraints, real-time notifications are used in such systems. Albano et al. implemented a distributed surveillance system allowing devices to connect to the system. In order to monitor an area, the system periodically sends images to the user and this is inefficient [2]. Conversely, Kana et al. designed a system in which an email is sent to the user when an anomalous behavior is detected [16]. However, a user might not always check his/her email and might miss notifications.

In another system, Cloud to Device Messaging (C2DM) is used to notify users when a foreign object is detected in the monitored location. The system is economical as almost everyone has a mobile phone and no additional hardware is required [11]. However, the messaging service developed by Google is no longer available [12]. In some systems, the Global System for Mobile communication (GSM) network is used as a notification platform in their surveillance system. In case of an event, a text message is sent to the user using a GSM modem [30][31]. Nevertheless, it might not always be convenient to read text messages compared to calls which can be answered almost all the time. A basic surveillance system developed by Mutlak et al. implements the call feature. One major component of the system is the mobile phone and a calling circuit. The circuit triggers the keypad of the mobile phone, which in turns calls the owner [21].

In spite of all the functionalities provided by existing systems, crime rates in most cities are still very high. Therefore, innovative and more effective approaches have to be considered when implementing surveillance systems. A major improvement can be made by using different types of communication platforms for successfully notifying users about any suspicious activities that are taking place in the areas being monitored. Therefore, many different and modern approaches for alerting users are considered in this work. The ability to identify whether a specific object has been displaced is a new feature that has been added in order to provide more security. The key features of previous works have been unified into a single surveillance system.

3. Methodology

This section describes the design and implementation of the functionalities of our proposed surveillance system. Figure 1 shows the operations of the Intelligent Camera Surveillance System ICSS, from the moment the frames are captured until the notifications are received by the user.

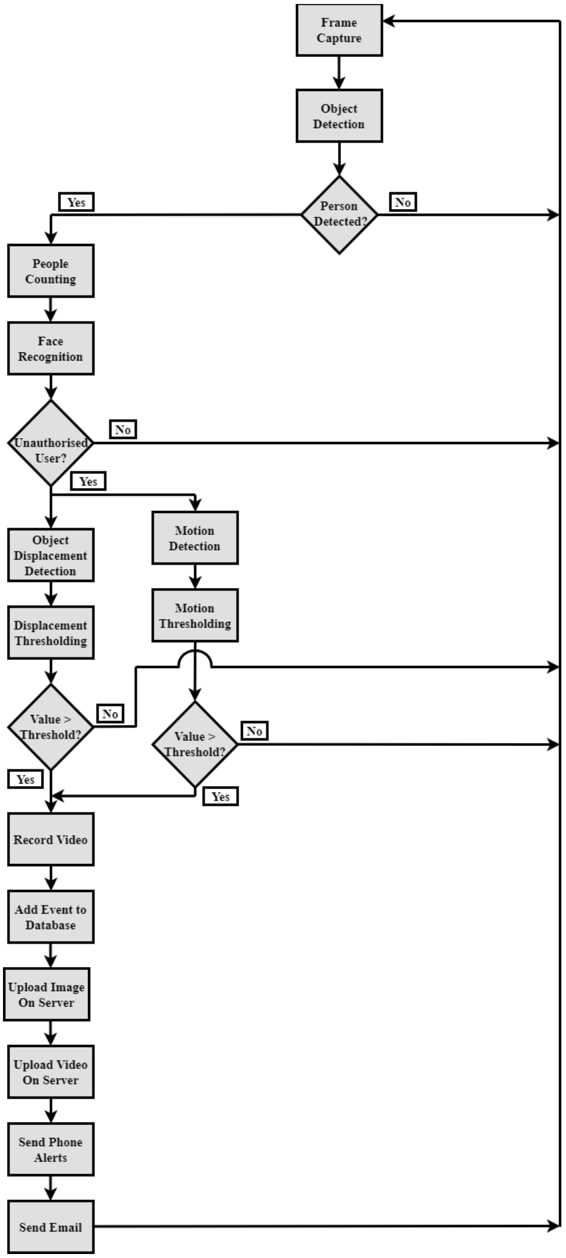


Figure 1. System flowchart

A full HD Cloud IP camera connects to WI-FI and generates frames at a resolution of 1280 x 720 pixels. Each frame received by the system is then written to a video file and this allows the users to view daily video footages. This frame is then processed by the different modules of the system. The frame is first processed for object detection using the YOLO algorithm [26] whereby individuals and objects are detected. Features are extracted from the frame and classified accordingly. Objects that can be detected are mobile phones, handbags, monitors and laptops. This functionality also determines the presence of an individual in the surveillance area and provides more visual information when viewing the footages since objects are labelled on video frames. Prior to setting the system, owners of the system are enrolled as authorised users by providing their respective photos. The authorised users' facial features are extracted and are subsequently stored.

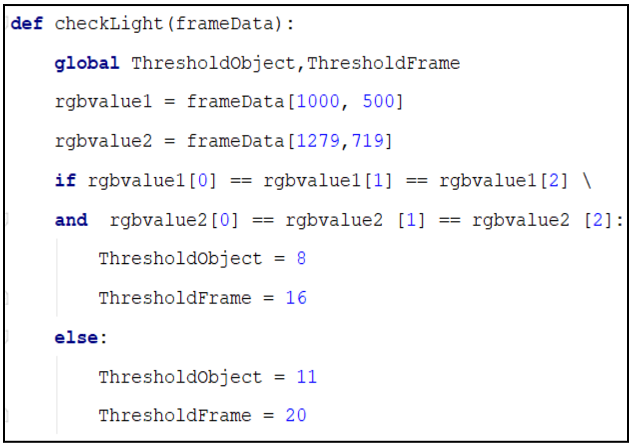
If a person is present in the surveillance area, the counting module and face recognition module are triggered. The system keeps count of the number of people present in the monitored area at each instant and the face recognition module determines whether the person is an authorised user or not. A pre-trained landmark detector of the Dlib toolkit consisting of a combination of HoG and facial landmarks is used for face recognition. The individual's facial features are extracted and compared to the stored features in order to determine if he/she is a registered user of ICSS.

If only unauthorised persons are present, the motion detection and object displacement modules are executed. Subsequently, another short video is recorded for the detected event and event information such as event name, timestamp and people count, are added to a database for log purpose. The short video recording and an image are uploaded to a server which can be accessed by users for viewing media files. Ultimately, all users are notified via email and phone notifications. However, if a user is present with unauthorised users, no further processing is carried out on the frame. The motion detection, object displacement and notifications functionalities are further detailed below.

A. Motion Detection

The level of activity in the monitored area is computed by the pixel difference between a previous frame and the current frame being processed. If the motion level value is greater than the threshold value, an abnormal activity can be inferred. The code snippets in Figure 2 and 3 below show the implementation of the motion detection functionality.

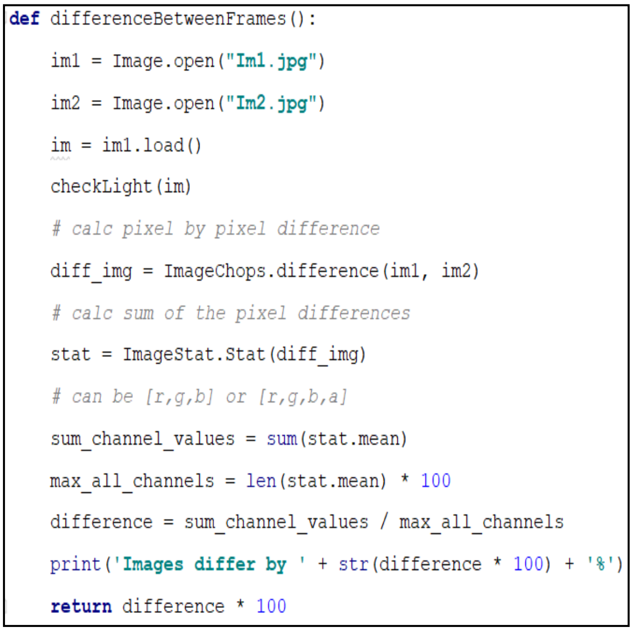
Prior to calculating the level of motion, the mode in which the camera is operating is determined. The function *checkLight* ensures that a proper threshold is set for the day mode and the night mode. The night mode generates greyscale images whereby the three RGB colour values are equal. Two random pixels at position (1000, 500) and (1279, 719) are used to determine the camera mode. Their RGB values are computed and compared to set a threshold according to the camera mode.



```
def checkLight(frameData):
    global ThresholdObject,ThresholdFrame
    rgbvalue1 = frameData[1000, 500]
    rgbvalue2 = frameData[1279,719]
    if rgbvalue1[0] == rgbvalue1[1] == rgbvalue1[2] \
    and  rgbvalue2[0] == rgbvalue2 [1] == rgbvalue2 [2]:
        ThresholdObject = 8
        ThresholdFrame = 16
    else:
        ThresholdObject = 11
        ThresholdFrame = 20
```

Figure 2. Code for setting the threshold for camera modes

Each group of two successive frames are stored as *im1.jpg* and *im2.jpg*. *im2.jpg* is compared with the reference frame, *im1.jpg*. The frame difference of the two images is then computed using *differenceBetweenFrames* method. The absolute value of the pixel-by-pixel difference is saved as *diff_img* image. *Stat.mean* is an array of the average pixel values in the three colour channels of *diff_img* and *sum_channel_values* is the sum of mean pixels of its color bands. With colour images, *max_all_channels* has a value of 300. The overall pixel difference is calculated by the ratio of *sum_channel_values* and *max_all_channels*. Frames having a pixel difference above a certain threshold are processed further.



```
def differenceBetweenFrames():
    im1 = Image.open("Im1.jpg")
    im2 = Image.open("Im2.jpg")
    im = im1.load()
    checkLight(im)
    # calc pixel by pixel difference
    diff_img = ImageChops.difference(im1, im2)
    # calc sum of the pixel differences
    stat = ImageStat.Stat(diff_img)
    # can be [r,g,b] or [r,g,b,a]
    sum_channel_values = sum(stat.mean)
    max_all_channels = len(stat.mean) * 100
    difference = sum_channel_values / max_all_channels
    print('Images differ by ' + str(difference * 100) + '%')
    return difference * 100
```

Figure 3. Code implementation for motion detection

The motion difference value is recorded with some usual movements to determine the threshold value. Figure 4 shows the different values obtained for approximately one minute in daylight.

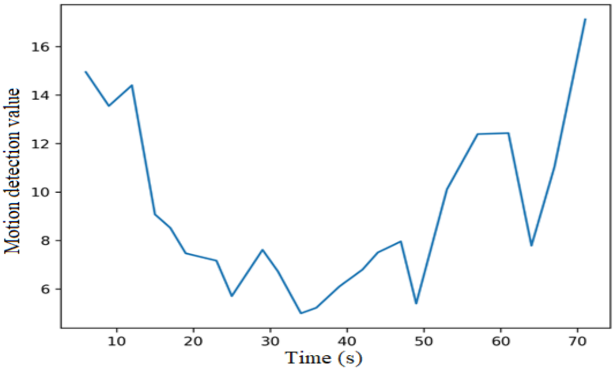


Figure 4. Daylight motion variation

However, at night, the values vary since pixel characteristics are different from color frames. Figure 5 shows the motion values for approximately one minute in night vision.

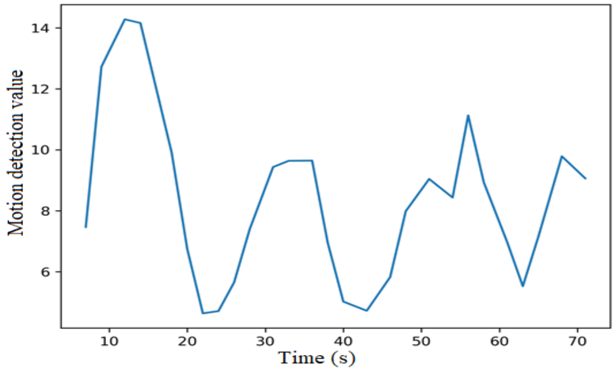


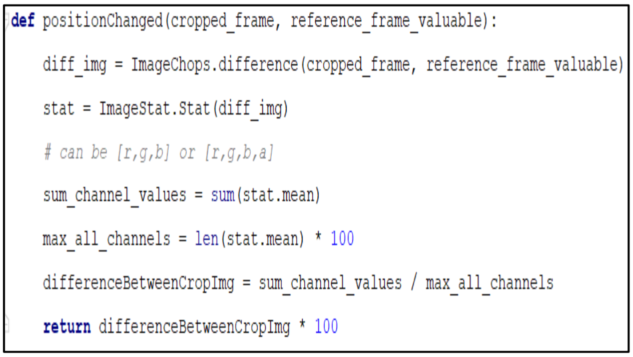
Figure 5. Night mode motion variation

After analysing the variation of the motion values and considering the environment conditions, threshold values, 20 and 16, were set for daylight and night modes, respectively.

B. *Object Displacement Detection*

The object displacement module can detect the displacement of any object specified by the user and this functionality performs well irrespective of the object size or its distance from the camera. A reference image of the object in the monitored location is initially provided when setting up the system. The location coordinates of the object in the reference image are recorded. For each frame processed, the area enclosed by these coordinates is monitored. By comparing each frame cropped at that specific area and the reference image, the displacement of the object is measured using pixel difference. If the pixel difference value is above its defined threshold, it is assumed that the object has been displaced.

Figure 6 shows the code snippet for the object displacement module. The parameter *cropped-frame* is the current frame cropped at specific coordinates and *reference-frame-valuable* is the reference image. The pixel difference between the two images is then calculated to determine if the object has been displaced.



```
def positionChanged(cropped_frame, reference_frame_valuable):
    diff_img = ImageChops.difference(cropped_frame, reference_frame_valuable)
    stat = ImageStat.Stat(diff_img)
    # can be [r,g,b] or [r,g,b,a]
    sum_channel_values = sum(stat.mean)
    max_all_channels = len(stat.mean) * 100
    differenceBetweenCropImg = sum_channel_values / max_all_channels
    return differenceBetweenCropImg * 100
```

Figure 6. Code for object displacement detection

An experiment has been conducted in the area where the object is at its fixed position for around one minute to obtain a suitable threshold. The values are recorded with the camera facing an object. Figure 7 shows the pixel difference values variation when the object is in its fixed position in daylight. In night mode, the values in Figure 8 have been obtained.

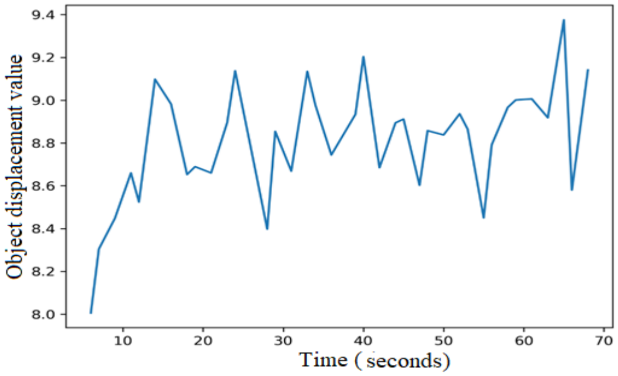


Figure 7. Object displacement value variation in daylight

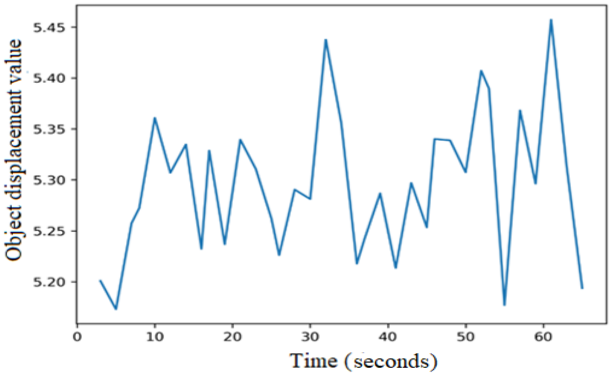


Figure 8. Object displacement value variation in night mode

After analyzing the variation of the difference value and considering the environment condition, the daylight and night vision thresholds were set at 11 and 8, respectively.

C. *User Notifications*

If a specific object is displaced from its usual position in the frame or a high motion level (above the set threshold) is detected, the system notifies all the registered users via platforms such as email, SMS (Short Message Service), phone calls and WhatsApp. In order to send phone notifications for this security application, a Twilio account was set up to obtain a Twilio number. The authorised users must provide their personal phone numbers to the system for receiving phone calls and SMS. Moreover, for enabling WhatsApp messaging services, a Twilio Sandbox had to be configured for the system. The users must connect the Sandbox using their phone number to receive messages from the system. A text message, an image as attachment and a video link are sent via WhatsApp messages and emails. A text message and a video link are also sent via SMS to the user. Furthermore, the system calls the user and a voice message is played to inform him/her about any intrusions.

4. TESTING, EVALUATION AND DISCUSSION

A. *Functionality Evaluation*

The ICSS (Intelligence Camera Surveillance System) application was tested under various scenarios. The IP camera allows remote monitoring and is responsible for the capture of frames (or video). It captures twenty (20) frames per second which are sufficient enough so as not to miss an event. Figure 9 shows a video frame consisting of the timestamp (date and time information) and the number of persons detected in the frame.

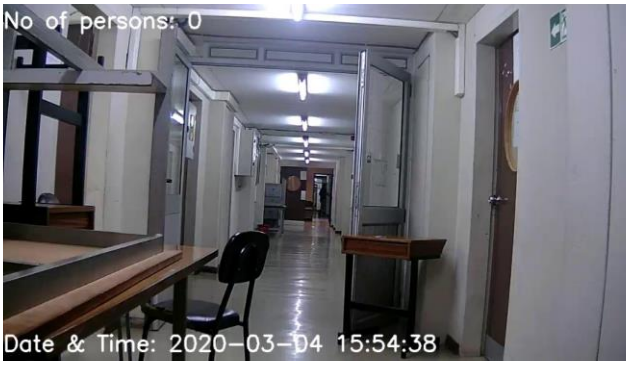
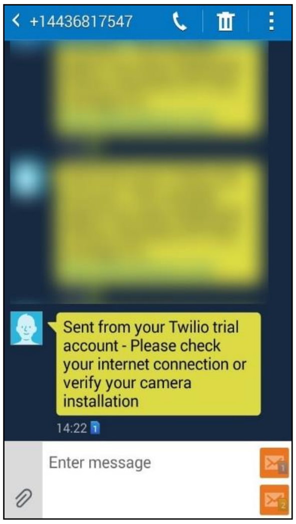


Figure 9. Video frame capture

The owner is informed about any camera malfunction by SMS and email. Figure 10 and Figure 11 show an SMS informing the user about the system malfunction. The message, "Please check your internet connection or verify your camera installation", is sent to the user via SMS. The SMS is a text message with a timestamp (date and time information) and receiver's details. Figure 12 shows the same alert message sent via an email. It is to be noted that the SMS and email are sent simultaneously to the registered users. The date and time in Figure 11 and Figure 12 are identical. There can be one or more registered (authorised) users in the system.

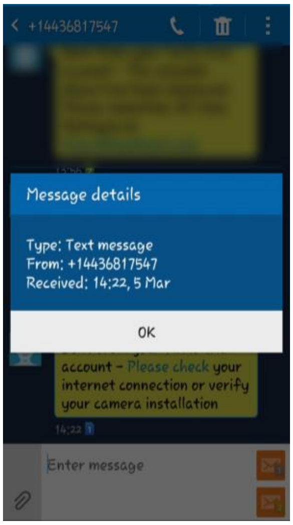

+14436817547

Sent from your Twilio trial account - Please check your internet connection or verify your camera installation

14:22

Enter message

Figure 10. SMS sent to user


+14436817547

Message details

Type: Text message
From: +14436817547
Received: 14:22, 5 Mar

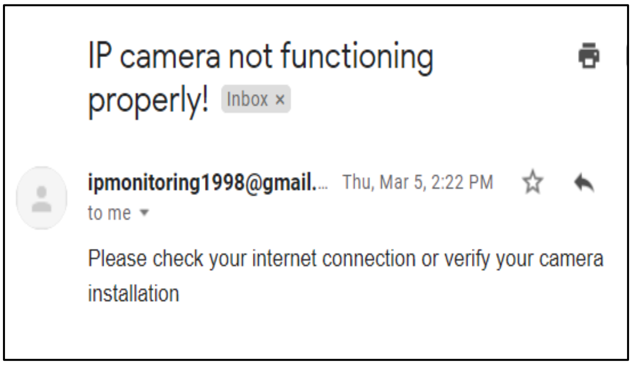
OK

account - Please check your internet connection or verify your camera installation

14:22

Enter message

Figure 11. SMS details


IP camera not functioning properly! Inbox ×

ipmonitoring1998@gmail... Thu, Mar 5, 2:22 PM

to me

Please check your internet connection or verify your camera installation

Figure 12. Email sent to user

In both daylight and night vision, the system successfully detects individuals as well as the four objects namely, handbags, laptops, smartphones and monitors. Figures 13 and 14 show detected people with occlusions in the monitored area. It can be noted that the individuals have different postures and are at varying distances from the camera. Four persons have been detected in Figure 13. As shown in Figure 14, occlusions are also handled quite robustly by the system.

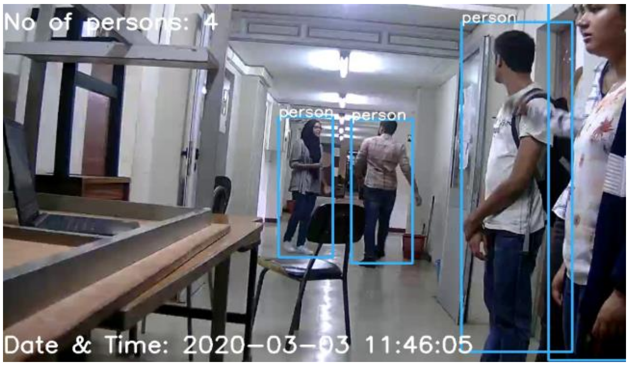


Figure 13. Person detection in daylight

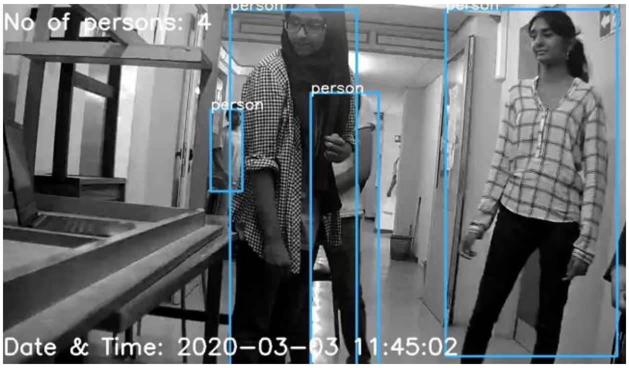


Figure 14. Person detection in night vision

Figure 15 depicts a handbag detected by the system during the day while Figure 16 shows the same handbag, which is successfully identified even in the dark. A label and a bounding box are drawn around the object to outline it in the frame. The date and time information are also included at the bottom of the frame as done earlier.

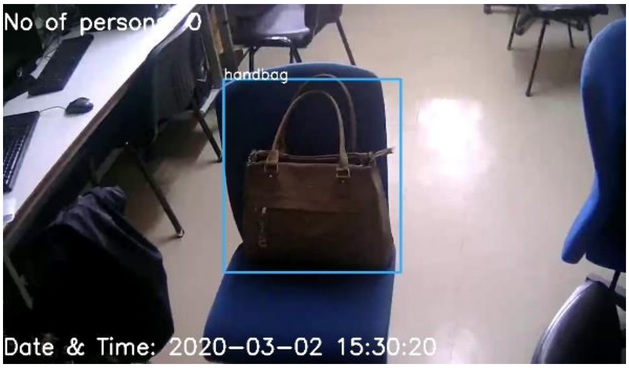


Figure 15. Object detection in daylight

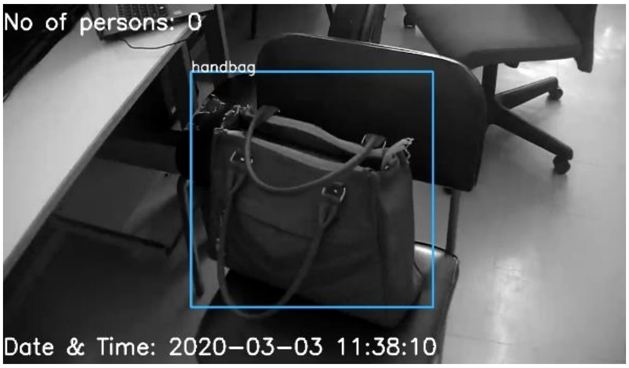


Figure 16. Object detection in night vision

Figure 17 and 18 depict how the object recognition module operates in both daylight and night modes. Faces in each video frame are enclosed in bounding boxes. If the person is known to the system, his/her name is displayed otherwise an unknown tag is displayed.

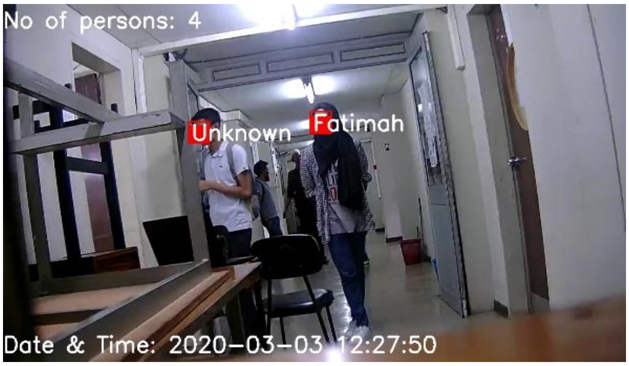


Figure 17. Recognition in daylight

If only unauthorised users are present, the motion detection and object displacement methods are executed. After detecting a high level of activity in the surveillance area, a record is added to the database, the system successfully sends notifications to the user via email, WhatsApp and SMS.

The user also receives the phone call and locally saved images as well as videos are uploaded on the server. When the object is moved from its defined position, a record is added to the database, and the ICSS system sends all the notifications to the user within a very short amount of time, as mentioned previously. Also, the locally saved images and videos are uploaded on a server, for maximum security.

It is noted that for both motion detection event and object displacement event, the same notification platforms are used with modified messages. Furthermore, it has been noted that the notifications are usually sent with a maximum delay of 20 seconds in normal network conditions.

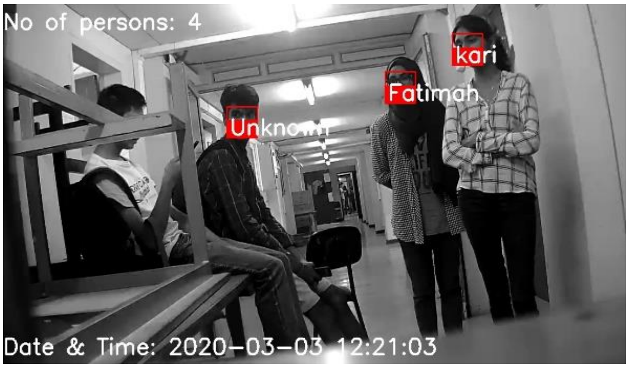
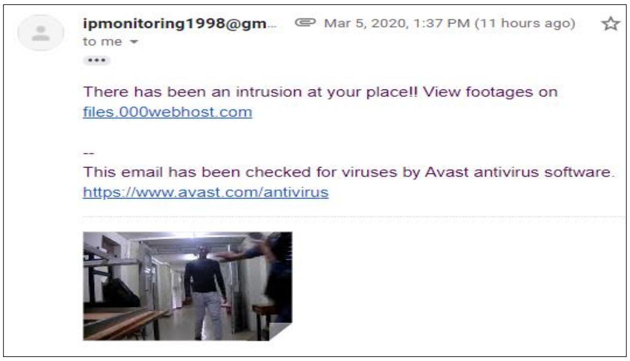


Figure 18. Recognition in night mode

Figure 19 shows a sample of the email sent to the user when a high motion value has been recorded. An image attachment and the video link are provided in the email. The user can then view video footages and images on the link as shown in Figure 20.



ipmonitoring1998@gm... Mar 5, 2020, 1:37 PM (11 hours ago)

to me

There has been an intrusion at your place!! View footages on files.000webhost.com

--

This email has been checked for viruses by Avast antivirus software.
https://www.avast.com/antivirus

Figure 19. Alert via email

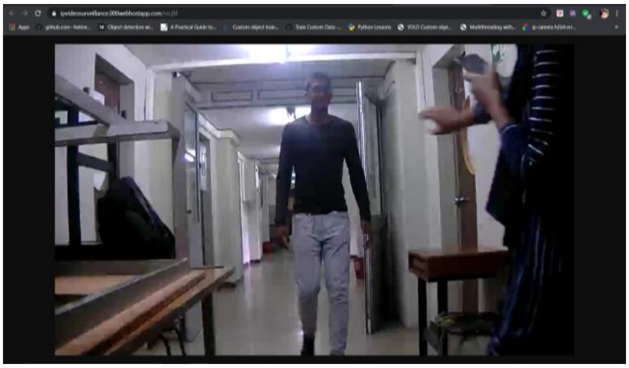
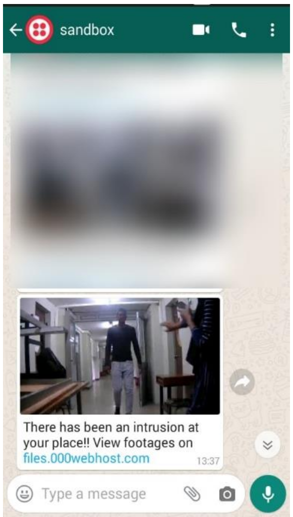


Figure 20. Viewing photo online

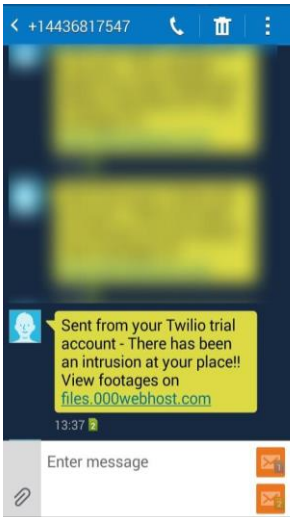
Figure 21 shows the WhatsApp message with an image attachment and a video link allowing users to easily view the images which have been received. Figure 22 illustrates a screenshot of the SMS with the video link received by the user. The message, “There has been an intrusion at your place.” is sent to the user in case the system detects an unknown person and the movement thresholds are met. Furthermore, all the video files are uploaded to a single directory on the web server. Thus, only this static link has to be sent to the user each time.



sandbox

There has been an intrusion at your place!! View footages on files.000webhost.com 13:37

Type a message



+14436817547

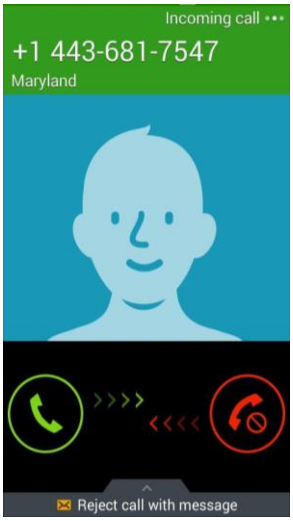
Sent from your Twilio trial account - There has been an intrusion at your place!! View footages on files.000webhost.com

13:37

Enter message

Figure 21. WhatsApp message sent Figure 22.SMS informing user

Figure 23 and Figure 24 show the call received by the user. It is noted that the time at which all the notifications are received is 13:37.

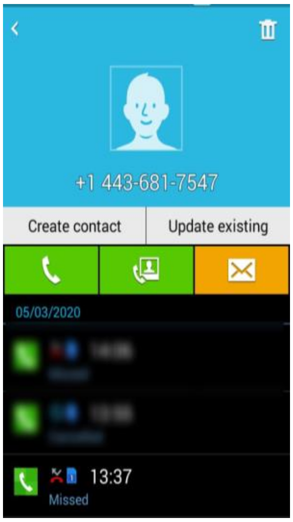


Incoming call

+1 443-681-7547

Maryland

Reject call with message



+1 443-681-7547

Create contact | Update existing

05/03/2020

13:37

Missed

Figure 23. Call to user Figure 24. Exact calling time

Bandwidth is an important factor which contributes to the proper functioning of ICSS. Videos and images are uploaded each time during unusual activities and a certain amount of bandwidth is consumed. Ten uploaded videos have been used in the average calculation of bandwidth. The video size and duration has been used in the bandwidth calculation. Table 1 below shows the bandwidth for each video and it is calculated as follows:

- Converting the video size in bits = video size in bytes x 8 bits

- Calculating the number of bits per second = video size in bits / video duration in seconds
- Converting bits per second to Megabits per seconds = No. of bits per second / 1,000,000

TABLE I. VIDEO DETAILS

Video Size (Bytes)	Video Duration (Seconds)	Bandwidth (Mbps)
3,192,240	3	8.51264
3,177,176	3	8.47247
3,119,904	3	8.31974
3,219,460	3	8.58522
3,285,766	3	8.76204
3,162,856	3	8.43428
3,170,032	3	8.45342
3,256,300	3	8.68347
2,921,518	3	7.79071
3,116,406	3	8.31042

It can be deduced that an average bandwidth of approximately 8 Mbps is required for the system to work properly.

B. System Comparison

This subsection compares the ICSS to recent existing systems having similar functionalities. The objective is to demonstrate how ICSS surpasses these systems in terms of functionalities implemented.

Al-Yamani et al. implemented an event-driven surveillance system using sensors along with a camera and an object classifier. The presence of an intruder is first detected using an IR sensor and then, a target detector module determines his/her geographic position in the area. This allows the camera to rotate in the direction of the intruder and the camera captures images. Subsequently, the image is analyzed for human face detection and as long as faces are detected, video recordings are stored [4]. This system successfully determines the presence of intruders in an area. Also, it captures the target's face even if the latter is moving in different directions. However, the use of sensors might be expensive, and no notification feature has been implemented to inform users about an event. Furthermore, video recordings are stored locally which is vulnerable to data loss. Contrarily, ICSS uses computer vision techniques instead of sensors to detect persons in an area. Moreover, ICSS notifies users about security events implying that our system efficiently monitors an area. Also, video recordings are uploaded on a server as backup.

Jyothi and Vardhan designed a real-time security surveillance system using the Raspberry pi. In addition to thermal sensors used, a pi-camera was integrated into the system. The latter detects moving objects in the monitored area to infer the occurrence of an event. If motion is detected, an alarm connected to the system is triggered and an SMS is sent using a GSM modem. Moreover, photos and recorded videos are stored on the cloud. Another feature of this system is that the camera movement can be controlled by the user. This provides more field of view in the monitoring area. This work addresses the issue of alerting users when an event occurs [15]. However, there might be false alarms since the system cannot determine if the motion is caused by the owner or an intruder. ICSS provides better surveillance by implementing four real-time notification platforms to ensure that the owner is alerted. Moreover, ICSS can successfully identify owners hence, reducing false alarms. Compared to this system, ICSS detects objects and individuals in each video frame to view footages more easily.

Singh et al. introduced an FPGA-based surveillance system integrating motion detection, object detection and alarm notification features. A camera sends video feeds and a Camera Interface module processes the video frame for pixel data extraction. A motion detection module is then triggered and specific regions in the frames are extracted. Motion detection is then carried out on those regions. Ultimately, if there is motion, an alarm is generated for security officers. The system can also track moving intruders by using the extracted information such as the location coordinates, and subsequently, motion history information is generated. The authors state that their work meets the requirements of surveillance systems [32]. However, our proposed ICSS system surpasses this system in many aspects. Instead of extracting pixel information for real-time motion detection, our system uses a simple and fast technique known as pixel difference. Moreover, ICSS provides visual information of detected objects and individuals in the footages. This approach is much faster than generating motion history on each frame to track motion. Besides, only an alarm is triggered to alert the users but, ICSS implements more effective notification features namely, emails, SMS, WhatsApp messages and phone calls. Also, it does not cater for false alert issues compared to ICSS which implements techniques such as face recognition.

The ICSS system implements a combination of functionalities from existing systems in order to successfully monitor an area. Additionally, some innovative functionalities embedded in this system are object displacement detection and various simultaneous notification features. Thus, ICSS can be considered as an upgrade to existing surveillance systems.

5. CONCLUSION

Soaring crime rates have led to the deduction that existing monitoring systems are not fully effective. Therefore, an intelligent IP camera system has been developed in this work which successfully integrates fundamental functionalities from several surveillance systems. Frames are captured at regular intervals so as not to miss any event. The surveillance system accurately detects objects as well as the presence of people in the surveillance area. The number of persons in the area is also calculated. In case an intruder is present, the system verifies if any valuable object has been moved from its regular location. The level of activity in the area is also measured. Subsequently, the user is notified about any unusual activities. A striking feature of our system is the real-time notifications via WhatsApp messages and voice calls. Emails and SMS are also sent to users to inform them about any security breaches. The ICSS system can operate in both daylight and night modes. The IP camera surveillance system demarks itself from existing systems via the implementation of an object displacement detection feature and the use of a plethora of real-time notification features such as WhatsApp messages, SMS, emails and phone calls. Thus, our proposed system meets the goals of an ideal surveillance system.

References

[1] E. Alajrami, H. Tabash, Y. Singer, M.T. El Astal, "On using AI-based human identification in improving surveillance system efficiency". Proceedings of the International Conference on Promising Electronic Technologies (ICPET), pp. 91–95, Oct 2019.

[2] P. Albano et al. "A secure and distributed video surveillance system based on portable devices". Journal of Ambient Intelligence and Humanized Computing, Vol. 5, No. 2, pp. 205–213, April 2013.

[3] A. Alshammari and D.B. Rawat, "Intelligent multi-camera video surveillance system for smart city applications". Proceedings of the 9th Annual Computing and Communication Workshop and Conference (CCWC), USA, pp. 317–323, January 2019.

[4] N. Al-Yamani, S. Qaisar, A. Alhazmi, S. Mohammad and A. Subasi, "An event driven surveillance system," Proceedings of the 5th International Conference on Electronic Devices, Systems and Applications (ICEDSA), Dubai, vol. 6, pp. 1–4, December 2016.

[5] B.A Atya, S.R. Abdul Monem. and J.A.H. Abdul Mohssen, "Design and implementation of secure building monitoring system using programmable wireless mobile camera". International Journal of Computer Network and Information Security, Vol. 9, pp. 29, March 2017.

[6] France 24, 2020. 100,000 cameras: Moscow uses facial recognition to enforce quarantine. Available from: https://www.france24.com/en/20200324-100-000-cameras-moscow-uses-facial-recognition-to-enforce-quarantine [Accessed 28 Mar. 2020].

[7] BBC News, 2019. The end of the CCTV era?. Available from: https://www.bbc.com/news/magazine-30793614 [Accessed on 28 Sept. 2019].

[8] P. Bischoff, "Surveillance camera statistics: which city has the most CCTV cameras?". Available from: https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/#China_leads_the_world_in_CCTV_surveillance [Accessed 21 Feb. 2020].

[9] K.R. Blevins, J.B. Kuhns, and S. Lee, "Understanding decisions to burglarize from the offender's perspective". Available from: https://airef.org/wp-content/uploads/2018/10/BurglarSurveyStudyFinalReport.pdf [Accessed 01 Sept. 2019].

[10] CNN, 2019. Robbers in tin foil suits try to beat bank alarm sensor as camera watches. Available from: https://edition.cnn.com/2016/04/11/americas/brazil-heist-aluminum-foil-disguises/index.html [Accessed on 11 Oct. 2019].

[11] L. Chen, S. Chen, Y.Q. He, J.G Wei, and J.W Dang, "IP camera based network video surveillance mobile security system". Applied Mechanics and Materials, Vol. 411, pp. 1505–1509, Sept. 2013.

[12] Cloud to Device Messaging, 2020. Available from: https://developers.google.com/android/c2dm [Accessed on 28 May 2020].

[13] Government Information Service, 2020. Covid-19: police issue more than 8 000 fines to lockdown rule breakers. Available from: http://www.govmu.org/English/News/Pages/Covid-19-Police-issue-more-than-8-000-fines-to-lockdown-rule-breakers.aspx [Accessed on 28 May 2020].

[14] K. He, X. Zhang, S. Ren and J. Sun, "Spatial pyramid pooling in deep convolutional networks for visual recognition". IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 37, pp. 1904–1916, January 2015.

[15] S.N Jyothi and K.V Vardhan, "Design and implementation of real-time security surveillance system using IoT". Proceedings of the International Conference on Communication and Electronics Systems (ICCES), India, pp. 1–5, October 2016.

[16] S. Kana, G. Prabhu, C. Apoorva and A. Apporva, "Smart surveillance vigilant detection and notification system". Asian Journal For Convergence In Technology, Vol. 4, November 2018.

[17] C. Kaundanya, O. Pathak, A. Nalawade and S. Parode, "Smart surveillance system using raspberry pi and face recognition. database". International Journal of Advanced Research in Computer and Communication Engineering, Vol. 6, April 2017.

[18] J.S Kim, D.H Yeom, Y.H Joo and J.B Park, "Intelligent unmanned anti-theft system using network camera". International Journal of Control, Automation and Systems, Vol. 8, pp. 967–974, Oct 2010.

[19] BBC News, 2019. London nail bombings remembered 20 years on. Available from: https://www.bbc.com/news/uk-england-london-47216594 [Accessed on 10 Oct. 2019].

[20] W. Liu et al., "Ssd: Single shot multibox detector". European conference on computer vision, Amsterdam, pp. 21–37, Oct. 2016.

[21] A.H Mutlak, S.Q Mahdi and O.N.M Salim, "Design and implementation of modern security system based on mobile phone". Journal of Engineering and Sustainable Development, Vol. 16, pp. 314–329.

[22] C.C Nguyen et al., "Towards real-time smile detection based on faster region convolutional neural network". Proceedings of the 1st International Conference on Multimedia Analysis and Pattern Recognition (MAPR), Vietnam, pp. 1–6, April 2018.

[23] Office for National Statistics, 2019. Crime in England and Wales: Year ending March 2019. Available from: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2019 [Accessed on 12 Sept. 2019].

[24] S. Pudaruth, F. Indiwarsingh and N. Bhugun, "A unified intrusion alert system using motion detection and face recognition". Proceedings of 2nd International Conference on Machine Learning and Computer Science (IMLCS), Malaysia, pp. 17–20, Aug. 2013.

[25] J. Redmon and A. Farhadi, "YOLO9000: better, faster, stronger". Proceedings of the IEEE conference on computer vision and pattern recognition, Hawaii, pp. 7263–7271, 2017.

[26] J. Redmon and A. Farhadi, "Yolov3: An incremental improvement". Available from: https://arxiv.org/abs/1804.02767.

[27] J. Redmon, S. Divvala, R. Girshick and A. Farhadi, "You only look once: unified, real-time object detection". Proceedings of the IEEE conference on computer vision and pattern recognition, USA, pp. 779–788, June 2016.

[28] R.A Shahad, M.F Ibrahim, E.L.K Xian, A. Hussain and M.H.M Saad, "Suspicious loitering detection from annotated cctv feed using CEP based approach". Journal of Engineering [Jurnal Kejuruteraan], Vol. 30, pp. 83–91, January 2018.

[29] Z. Shao, J. Cai and Z. Wang, "Smart monitoring cameras driven intelligent processing to big surveillance video data". IEEE Transactions on Big Data, Vol. 4, pp.105–116, Dec. 2017.

[30] S.M. Sheikh, M.K. Neiso and F. Ellouze, "Design and implementation of a raspberrypi based home security and fire safety system". Computer Science & Information Technology (CS & IT), Vol. 3, pp.13, June 2019.

[31] R. Shete and M. Sabale, "Video surveillance using raspberry pi architecture". Proceedings of the International Conference on Computing, Communication, Electrical Electronics, Devices and Signal Processing, India, 2015.

[32] S. Singh, S. Saurav, R. Saini, A.S. Mandal S. and Chaudhury, "FPGA-based smart camera system for real-time automated video surveillance". Proceedings of the International Symposium on VLSI Design and Test. pp. 533–544, June 2017.

[33] The Times of Israel, 2020. Supermarkets see more shoplifters amid outbreak; most are regular customers. Available from: https://www.timesofisrael.com/supermarkets-say-shoplifting-up-since-virus-outbreak/ [Accessed on 28 May 2020].

[34] Supreme Court, 2019. Annual report of the judiciary 2018. Available from: https://supremecourt.govmu.org/ [1 May 2020].

[35] R. Wang et al., "A video surveillance system based on permissioned blockchains and edge computing". Proceedings of the International Conference on Big Data and Smart Computing (BigComp), Japan, pp. 1–6, February 2019.

[36] M. Younsi, M. Diaf and P. Siarry, "Automatic multiple moving humans detection and tracking in image sequences taken from a stationary thermal infrared camera". Expert Systems with Applications, p.113–171, May 2020.

[37] U. Zafar et al., "Face recognition with Bayesian convolutional networks for robust surveillance systems". EURASIP Journal on Image and Video Processing, Vol. 1, p.10, December 2019.

[38] D.X Zhang, P. An and H.X Zhang, "Application of robust face recognition in video surveillance systems". Optoelectronics Letters, Vol. 14, pp.152–155, March 2018.

[39] T. Zhang, A. Chowdhery, P.V. Bahl, K. Jamieson and S. Banerjee, "The design and implementation of a wireless video surveillance system". Proceedings of the 21st Intern. Conference on Mobile Computing and Networking. France, pp. 426–438, Sept. 2015.

Fatimah Khodadin is currently a final year student studying BSc (Hons) Computer Science at the Department of Information and Communication Technologies, Faculty of Information, Communication and Digital Technologies, University of Mauritius. Beginning her career as a software developer intern at PwC Mauritius, she refined her programming skills by developing various Web Technology applications and worked on different platforms such as Java, JavaScript/ NodeJS, Go, Scala, Perl, PHP, Python, VBScript. Her current research interests are Computer Vision, AI, Database Management Systems, Mobile Applications and Web Technologies. After graduation, she intends to embark on an MSc in Applied Artificial Intelligence & Data Analytics to further her expertise in the AI field.

Sameerchand Pudaruth is a Senior Lecturer and Head of the ICT Department at the University of Mauritius. He is a founding member of the IEEE Mauritius Subsection and the current Vice-Chair of the IEEE Mauritius Section. He is also a member of ACM. His research interests are AI, Machine Learning, Data Science, Machine Translation, Computer Vision, Blockchain and IT Law. He has written more than 60+ papers for national & international journals and conferences. He has been in the organising committee of many successful international conferences such as Africon 2013, IST Africa 2014, Africon 2015, ICCCS 2015, BigData 2015, DIPECC 2015, Africhi 2016, Emergitech 2016, Nextcomp 2017 & 2019, ISCMI 2017, 2018 & 2019, Mauritian Academic Conference 2018, icABCD 2018, 2019 & 2020 and Mauricon ICONIC 2018 & 2020. He has also written a book entitled, 'Python in One Week'.