[1] J. V. Arjun
[2] R. Kishore
[3] K. Ajay Adithya
[4] S. Ashwin

Intelligent Surveillance System Leveraging IoT for Enhanced Situational Awareness

Journal of Electrical Systems

Abstract: - Home surveillance systems are still challenging, particularly for patrolling or tracking subjects through CCTV images despite recent developments. Therefore, it is crucial to instantly identify human intruders in real time based on motion and face recognition. The proposed model represents a cost-efficient real-time Intelligent surveillance system for home and small offices using raspberry pi, PIR Sensor, and computer vision. The proposed system detects for motion with PIR sensor in its field of view and starts video capturing once motion is detected and sends it to user via email. HOG Descriptor and SVM Classifier is used to differentiate between human and inhuman objects. Haarcascade filter is implemented to detect intruders jumping over the wall. For Facial recognition, Images are captured or imported to create a database with help of frontal face LBHP filter. This database is used to train a facial recognition model. The trained facial recognition model can recognize authorized and unauthorized person. In our proposed model, the system tracks the detected individuals face in the frame and only focuses on the image content in these facial regions. Then, LBHP filter is used for recognizing detected faces based on the pre-provided face database and differentiate as known or unknown user. The system works satisfactorily in normal lighting conditions with accepted accuracy.

Keywords: IoT, Home Surveillance, Intelligent Systems, motion detection, face recognition, smart systems.

I. INTRODUCTION

The need for intelligent surveillance systems is on the rise as more and more processes are being automated. Nowadays Home Security is a major concern. Existing home security systems although technologically advanced are still ineffective. Burglars have found ways to work around existing security systems and disable them as they tend to know the placements of the sensors, while majority of detection by burglar alarms are false positives and existing systems are also very expensive. While there are a lot of CCTV surveillance systems to detect intruders and they are not able to detect suspicious activities in real time and send out alerts. Fig. 1 presents the general framework of conventional surveillance system. The proposed framework aims to reduce the amount of human intervention significantly. The proposed model developed by us aims to make an easily modifiable home security system at its base while also being affordable. The framework can be implemented in wide range of areas and will improve the overall surveillance of the region of interest.

The proposed work aims to build an IoT based intelligent surveillance system using machine learning algorithm to correctly recognize an unknown human intrusion with the help of python programming and OpenCV library and forward an alert message to an authorized person via SMS or emails. The main objective of our proposed work is to develop a cost-efficient real-time surveillance system for home and small offices using raspberry pi and computer vision.

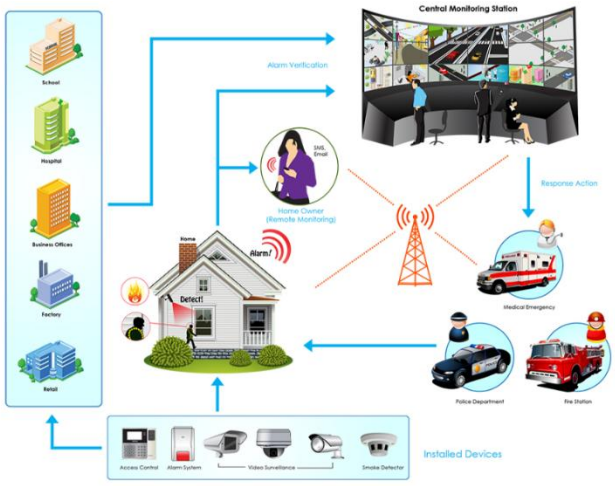

Fig. 1. Framework of conventional surveillance system

[1] Sri Sivasubramaniya Nadar College of Engineering, Chennai, India. Email: arjun18023@ece.ssn.edu.in
[2] Sri Sivasubramaniya Nadar College of Engineering, Chennai, India. Email: kishorer@ssn.edu.in
[3] Sri Sivasubramaniya Nadar College of Engineering, Chennai, India. Email: ajay18012@ece.ssn.edu.in
[4] Sri Sivasubramaniya Nadar College of Engineering, Chennai, India. Email: ashwin18025@ece.ssn.edu.in

The rest of the paper organized as follows: Section 2 addresses the related works, Section 3 describes the proposed architecture, Section 4 presents the experimental results and Section 5 concludes.

II. RELATED WORKS

Recent advancements in IoT-based monitoring systems have shown considerable potential in security and healthcare domains. One study proposed an intelligent Line of Control (LoC) surveillance system utilizing infrared sensors, video analytics, and machine learning to ensure real-time threat detection and data-driven situational awareness at national borders. It highlighted robust integration of wireless communication and edge computing for autonomous, low-latency monitoring in harsh environments [1]. Another work focused on elderly care, developing a wearable fall detection device combining MPU6050 sensors and ESP8266 microcontrollers, capable of real-time motion analysis and remote alerting via Wi-Fi and mobile apps. The system demonstrated practical usability, sensitivity above 85%, and potential for integration with cloud-based health management tools. Both studies emphasize scalability, data reliability, and user safety as core strengths of IoT-based monitoring. These approaches underline the broader applicability of smart sensor networks across diverse domains requiring timely intervention and decision-making [2].

Danish Chowdhry et al [3] presented a home automation system which detected human motion from the video sequence and rejected non-human motion (pets, birds) with HOG Descriptor. The intrusion Detection mainly used the Histogram of Oriented Gradients (HOG) feature descriptors and Support Vector Machine (SVM) classifier to differentiate between human beings and animals to rule out false alarms. Challenges mentioned were the variable poses and appearances of intruders. With the process flow of background subtraction, Hog feature Descriptor, and motion discrimination the false positives were reduced to a great extent and detection speed was also improved. The proposed system was thus 87.2% accurate in detecting and classifying the moving intruder. Errors in the experiments were mostly due to unconstrained illumination.

A. Shahbaz and K. -H. Jo [4] proposed a change detection algorithm GMM+ SuBSENSE with image enhancement to tackle problems due to false negatives in SZM. The proposed algorithm aims to segment out an intruder from the scene. In this paper, Gaussian Mixture Models (GMM), which can be classified as parametric algorithms were used and were concluded to be one of the most efficient and most employed algorithms in the field of change detection. The proposed ISS used a Dual camera (color/IR), to eliminate the problems of camouflage intruder and a decision module is implemented which decreases the number of false positives in three crucial ways. The proposed work overcome the inherent drawback of change detection algorithms posed by the dual-camera sensors (color/IR).

B. Mukhopadhyay et al [5] proposed a model to predict state of motion of an intruder using geophone with STA/LTA algorithm to detect human footfall events. The proposed event extraction technique detected footfall events and extracts portions of the signal that correspond to an event. In Combination with the SVM-RBF classifier and the proposed event extraction technique the presence of an intruder was predicted with an accuracy of 86% and its state of motion with an accuracy of 77%. Ying-Wen Bai et al [6] discussed a model with multiple ultrasonic sensor which works on the basis of Majority Voting Mechanism (MVM) and detect the motion in home surveillance. Ultrasonic sensors were used instead of PIR sensors as the PIR sensor has a high miss rate when the intruder moves slowly. The distance between the receiver circuit and transmitter circuit was 6 meters. Enhancement in sensing probability was observed to increase from 58% to 83% at 6 meters by using 5 sensors. One of the main limitations of this approach was the requirement of a high- performance core which has high power consumption leading to increase in costs.

Kishore R et al [7] presented a framework that identified hidden patterns to make better predictions for automatic control of AC and an intrusion detection system that detected suspicious/unusual activities in real time. The advantage of this proposal was that unlike traditional surveillance systems, it can provide a secure environment by detection of suspicious movements in unusual timings while they are taking place. Background subtraction method was adopted here which helps in analyzing the intruder better. The limiting factor of this proposal is that raises false alarms for non-human images generated from the video.

Arjun D et al [8] proposed a hybrid Wireless Sensor Network (WSN) system architecture. This utilized the integration of five different types of sensors namely: Geophones, Hydrophones, Microphones, Infrared sensors and Camera sensors for effective surveillance and detection of human intrusion in the border regions with early warning capability. PANCHENDRIYA was a new framework with minimum human involvement for solving the problem of unauthorized movement of the human intruders. The paper proposed a new architectural design model for sensing and detection circuits based on the following three scenarios: flat border areas, the border area

with river or pond crossings, and the border area covered by dry leaves. The advantage of this proposal was that it involved few to zero human requirement for surveillance in the border regions.

Sanoob A.H et al [9] proposed a new design for surveillance using smart phone along with the passive infrared (PIR) sensor and the microcontroller unit (MCU) is proposed. The PIR sensor was attached to the smart phone through the MCU to detect motion. In the design discussed, the video is captured only when the motion was detected and the short message services alert is sent to the user straight away. To overcome the memory restrictions of smart phone and to ensure the safe storage of surveillance records, it was uploaded in cloud, and the link is sent to the user through email. The proposed intelligent surveillance system offered cost effective, storage effective, energy efficient, and secured solution as it used the computation and communication capabilities of the smart phone and the storage capabilities of cloud. In this work the authors combined the abilities of both PIR sensor and a smart phone for designing an intelligent surveillance system. The advantage of using smart phone is, requirement of any extra camera module as a good quality camera is available by default. The energy usage is reduced by activating the camera only when the movement detected by the PIR sensor.

C. M. Patil et al [10] mainly focused on multiple human detection and activity recognition. The highlight of the proposed paper included Histogram of Oriented Gradient feature descriptor to extract features. For human activity recognition Support Vector Machine classifier was used. The limitations of this proposal were the GMM and Graph cut methods are more complex and larger amount of calculation and computational power is required. This system failed to detect shadows and reflection of human thereby raising false alarms. In addition, the main limitation of this proposal is that it can't be used for moving objects.

F. Pasqualetti et al [11] presented a surveillance system which considered smart intruders who appear at arbitrary times and locations and are aware of the cameras configuration and move to avoid detection for as long as possible. Distributed Camera Coordination Along an Equal-Waiting Trajectory algorithm is implemented and has come to notice that it continues to function despite hardware failure. Sonali P. Gulve et al [12] proposed a system that intimates about presence of any person in the premises, also providing more security by recording the activity of that person. The proposed system is activated once the authorized user leaves the premises by specifying a password. The proposed system starts working with detection of motion refining to human detection followed by counting the number of intruders present in the premise. It also notifies the neighbors by turning on the alarm and sends a notification about the same to the user through email or SMS.

Manoranjan Paul et al [13] discussed and compared the available techniques for detecting human beings in surveillance videos. The paper also presented characteristics of few benchmark datasets. The proposed system in the paper implemented Background subtraction, Optical flow and Spatio-temporal filtering method. The main challenge in this system is the low-resolution images from the surveillance camera which makes it difficult for the human detection methods to analyze. So, the paper gave a review of available detection techniques and object classification methods and also the characteristics of the benchmark datasets.

Khaled Assaleh et al [14] proposed a face recognition system based on a database called SCface comprised of images taken under different surveillance conditions. The recognition is done using different cameras of different resolutions and imaging sensors. A combination of image filtering, segmentation, frequency domain feature extraction and linear classification was implemented in the proposed work. The proposed framework was also compared with the well-known eigenfaces recognition solution. Experimental results showed that the proposed system yields superior recognition rates compared to those obtained by the standard eigenfaces solution. The paper presented variety of experimental results that demonstrated the advantage of the proposed solution as compared to the standard eigenfaces solution.

J Yotirmaya Ijaradar et al [15] proposed a cost-effective real time face- recognition based surveillance system for home and small offices using raspberry pi and computer vision. The proposed framework tracks the detected individual faces in the frame and only focuses on the image content in the image content in the facial regions. Then a powerful algorithm for recognizing detected faces is used using a pre-provided face database. The models used for face detection and classification are Haar Cascade and Local Binary Pattern Histogram (LBPH) algorithms. The system worked perfectly in normal lighting conditions with acceptable accuracy. Experimental evaluation depicted that the proposed framework can be used in small private home surveillance system. The result of the experimental system was found satisfactory. Although the system's accuracy is more than 70%, it may be improved by incorporating new characteristics.

Kunal Deo et al [16] proposed a Human intrusion detection system which detects for presence of human being using sensors. The disadvantage that the system possessed is that it is based on a star topology network and if the central hub is disabled through any means, it will cause the entire system to collapse. Another disadvantage

of the current system is the usage of a single sensor to detect a human, which although more accurate than an active IR sensor in human detection could still give false positives. A simple solution to overcome this would be to combine a network of sensors to collect enough data to make sure the detected object is a human.

Having understood the advantages and limitations of the literature, the proposed work aims to build an IoT based intelligent surveillance system to correctly recognize an unknown human intrusion and forward an alert message to an authorized person. The main objective of our proposed work is to develop a cost-efficient real-time surveillance that is scalable to variety of applications.

III. PROPOSED SURVEILLANCE SYSTEM

The detailed framework of the proposed system architecture is depicted in Fig. 2 that presents the complete working process of the Surveillance system. The hardware, software modules and workflow which were used in the proposed framework is presented in detail. The proposed system detects for the motion first, and once it detects the motion, the video clip is recorded, and human detection and recognition is performed on the frames from video to differentiate between known and unknown faces using OpenCV libraries. The system also detects the intruders trying to enter the premise by jumping over the wall.

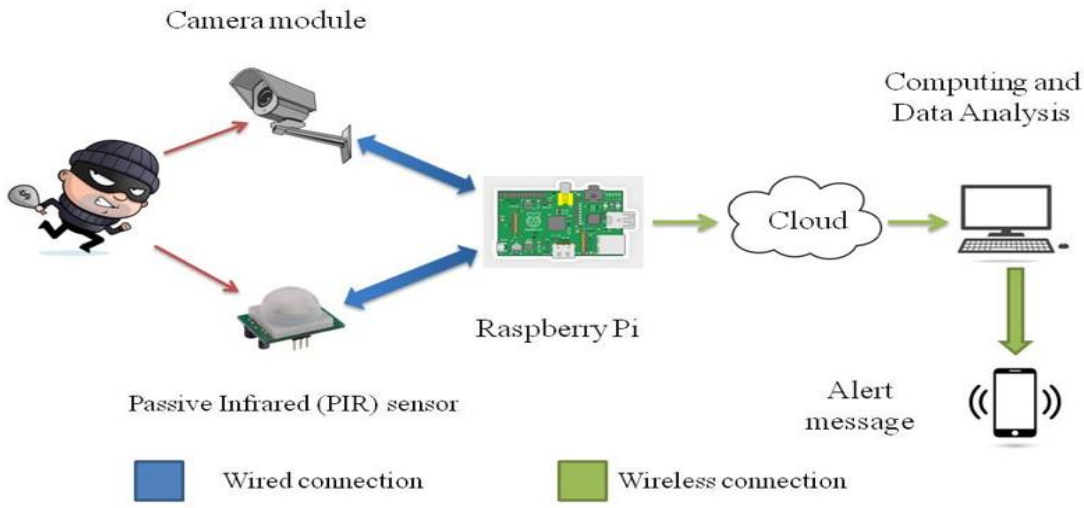

Fig. 2. Proposed Framework

RaspberryPi 4 model B, RaspberryPi 5MP Camera board Module and a PIR Sensor modules were used to design and deploy the above proposed model as mentioned in the architecture. The hardware schematic of interfacing the three modules is depicted in Fig. 3. A camera module is connected to the Raspberry Pi-camera port. PIR Sensor is connected to the Raspberry Pi general Input/Output pins. Pin 2 which supplies +5V is connected to the power pin of PIR Sensor. Ground pin of PIR Sensor is connected to pin 6 of RPI. The data pin is connected to pin 11 which is GPIO 17.

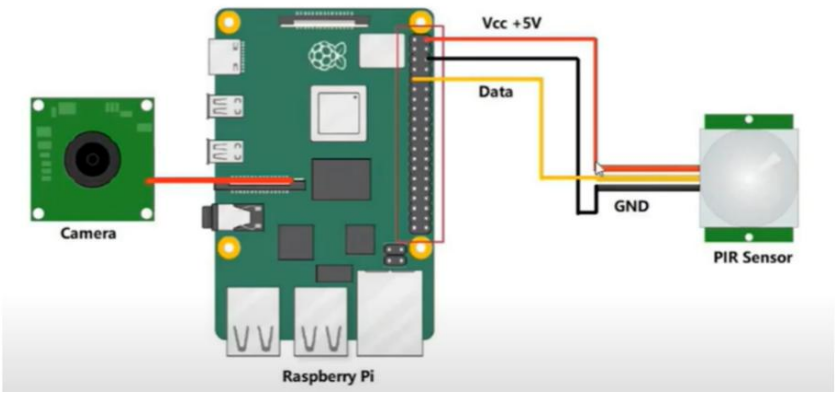

Fig. 3. Hardware Connection Diagram

The workflow of the proposed architecture is depicted in Fig. 4 as a flowchart. Each block represents the process of workflow in the proposed IoT surveillance model. The process is iterative and continues to execute till the program is shutdown. The Implementation of Human detection, Dataset creation and Facial recognition model is also explained further in the following sections.

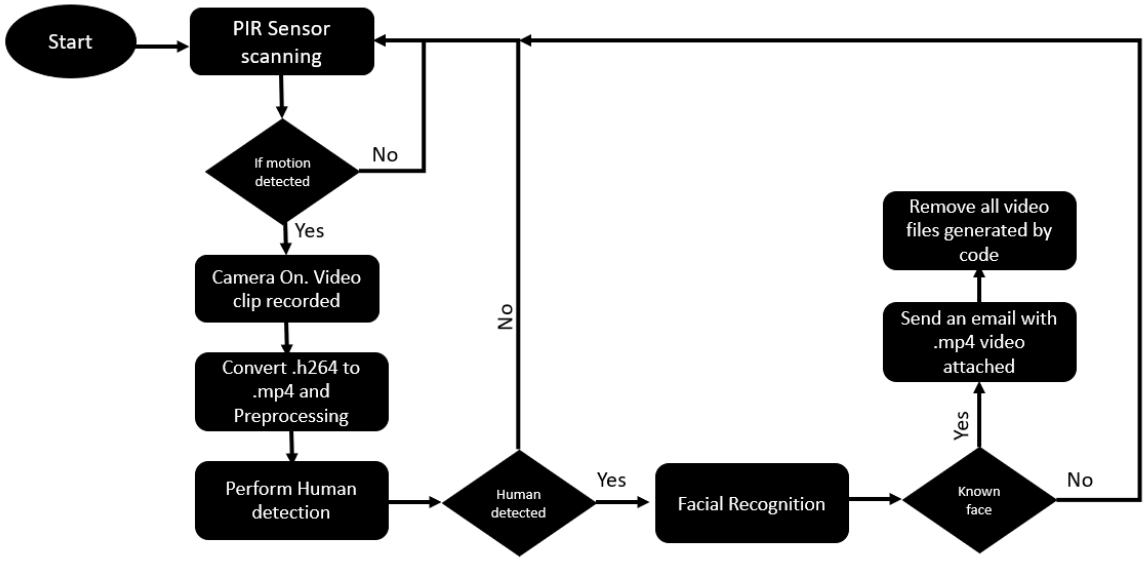

Fig. 4. Proposed Workflow

3.1 Steps in the Proposed Workflow

1. Start the program in a Raspbian OS.
2. Scan the PIR Sensor for motion continuously.
3. If Motion detected in the FOV of PIR Sensor, turn on the camera module and record video for 10 seconds, else go to step 2.
4. Convert the h264 video file to mp4 format using gpac module.
5. Perform human detection on the recorded video clip with the help of OpenCV Haar Cascades library to accurately detect intruders who try to enter the premise by jumping over the walls.
6. Validate the pre-processed frames from the video clip to differentiate between known and unknown person with the facial recognition model.
7. If the face is not recognized by the model, send alert message to the authorized user with the video clip as attachment and go to Step 2.
8. If the face is recognized, continue the process once again by going back to step 2.

We run the surveillance.py program in the terminal after making all the connections as mentioned in the schematic and installing all the required packages. Once the program starts to run, the PIR sensor is switched on to detect the motion. The camera module is not switched on unless a motion is detected by the motion detection sensor. This saves the energy and power consumptions due to camera running continuously. So, if motion is detected by the PIR Sensor, the RPI camera module starts recording a video clip of the intruder for a fixed amount of time. Then the captured video is converted from .h264 to .mp4 format via gpac package. This .mp4 video clip undergoes pre-processing and frames are extracted from the video clip. Human detection is performed on the pre-processed video clip with Haarcascade filter from the OpenCV library. This is done to remove false alarms due to inhuman object motions which can trigger the motion sensor. Human detection with SVM Classifier and HOG Descriptor makes sure only human motion is taken into consideration. With this human detection, the framework developed can detect intruders trying to enter the premise by jumping over the wall. Then Facial Recognition model validates whether the intruder is a known person or not with the help of Local Binary Patterns Histogram (LBPH) algorithm. The facial recognition model is trained with the faces of authorized person from the dataset. If the face detected is Unknown, then a video clip of the intruder is attached to an email and is sent to the authorized person's email which is given in the program. Once the email is sent, the captured video is deleted from the RPI's storage, and the process starts again to detect the motion. Fig. 5 depicts the process of the facial recognition model implemented in the proposed system. Fig. 6 presents the dataset creation flow.

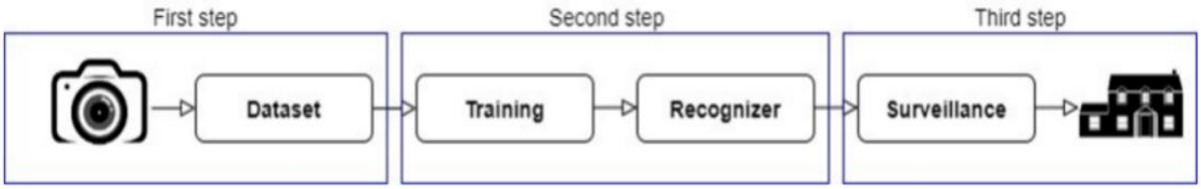

Fig. 5. Basic Flow chart of Facial Recognition model

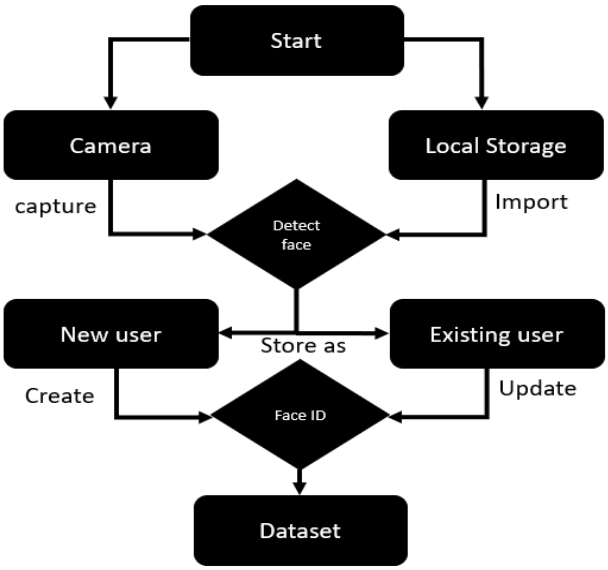

Fig. 6. Dataset Creation flow

Fig. 7 shows how the model trained from the database which we collected differentiates between known and unknown faces and notifies the authorized person. In this way the proposed system detects for unusual activities in a closed premise.

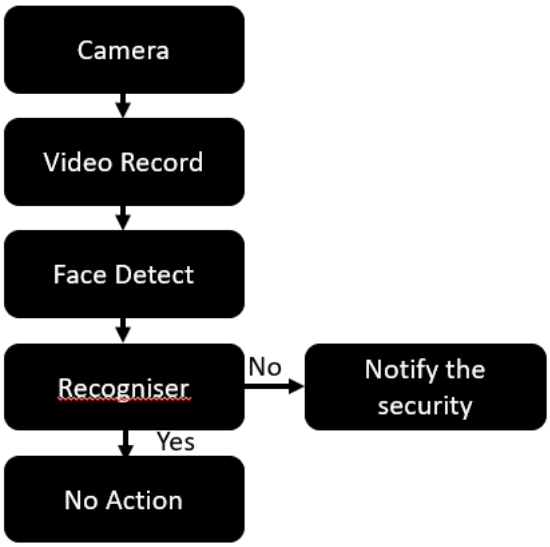

Fig. 7. Operation of facial recognition

Human detection in our proposed model is performed by using the pre-trained classifier known as Haarcascade full body classifier. This classifier is present as a part of the OpenCV Library. The pre-trained model Cascade Classifier is loaded which is trained with several hundred “positive” samples of particular object and arbitrary “negative” images of same size. This can be applied on the ‘gray’ frames extracted from the preprocessed video clip and can detect human body. A bounding box is created around the human body region

with coordinate system on the frames. Haarcascade classifier is used as this method is fast compared to other object detection methods like YOLO, Mask R- CNN, SSD etc. It requires less Computational power and can run even without a GPU. It has some disadvantages as well. Sometimes the bounding boxes flicker in cases when the illumination is less.

IV. Experimental Results and Discussions

The whole system setup constitutes the raspberry pi board interfaced with PIR Sensor and RPI Camera module. Once motion is detected by the PIR Sensor, the camera module starts to capture the video clip of the intruder for 10 seconds. The duration of the recorded video clip can be modified by the user. The captured video was of high quality and was tested under different circumstances. The captured video by the module was in .h264 module. As this video format is not supported to view in most of the devices and require additional software, we have converted the video format from .h264 format to .mp4 format. Observations from recording and converting videos in different cases are listed in the table 1.

Table 1: Observation on recorded video and conversion

Video duration (secs)	5	10	15	20
Frame rate (fps)	30	30	30	30
Quality (pixels)	480	480	480	480
Time taken to convert from .h264 to .mp4 (secs)	8	13	17	22
Size (megabytes)	2.3	5.0	8.2	11.0

The video clip captured and converted fromm.h264 to .mp4 undergoes video preprocessing. Video is converted into separate frames and each frames undergoes noise removal, gray conversion, filtering and binarization. This preprocessing of each frame from video clip is necessary as it is required in human detection and facial recognition models. To detect humans from the preprocessed frames in order to reduce false alarms due to other inhuman motion, we implemented pre-trained SVM (support vector machine) algorithm and HOG (Histogram of gradients) descriptor. These models were already trained using existing datasets like MIT Pedestrian set (509 images for training, 200 images for testing), INRIA Pedestrian set (1805 images for training, 64*128 images for testing). HOG Descriptor uses a detection window of 64px wide x 128 pixel tall. Some of the 64x128 pixel images used in training the model is given below in Fig. 8. The process of human detection is given below in Fig. 9.

Fig. 8. Images used for training HOG Descriptor

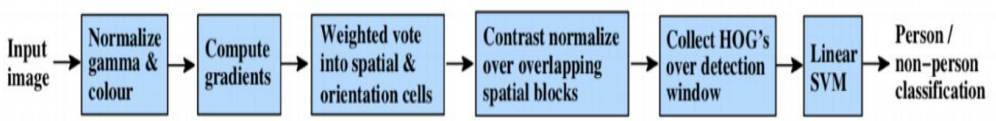

Fig. 9. Human detection process

Frames extracted from the video which is used to test the human detection model in the proposed system is listed in Fig. 10. These images were retrieved from the video clip before preprocessing as frames. These frames are then converted into grayscale images in preprocessing and noise are removed. This will make the process of human detection easier for the pre-trained model.

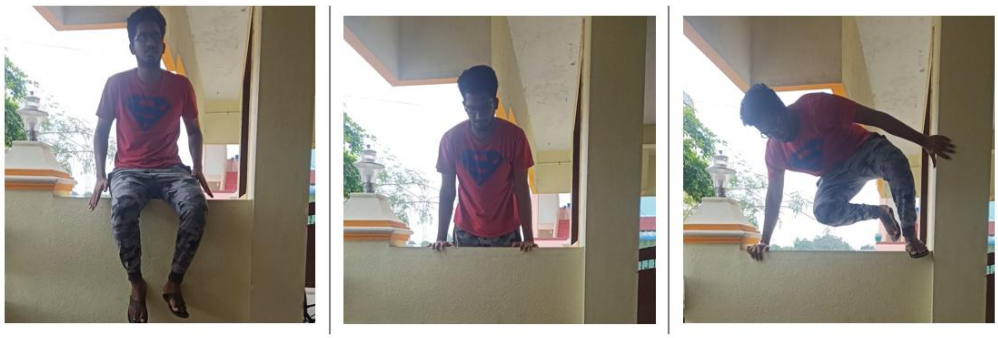

Fig. 10. Frames from video clip to test human detection model

To illustrate this point a large image of size 720×475 is shown in Fig. 11. We have selected a patch of size 100×200 for calculating our HOG feature descriptor. This patch is cropped out of an image and resized to 64×128. This process along with gamma corrections comes under preprocessing. Now we are ready to calculate the HOG descriptor for this image patch.

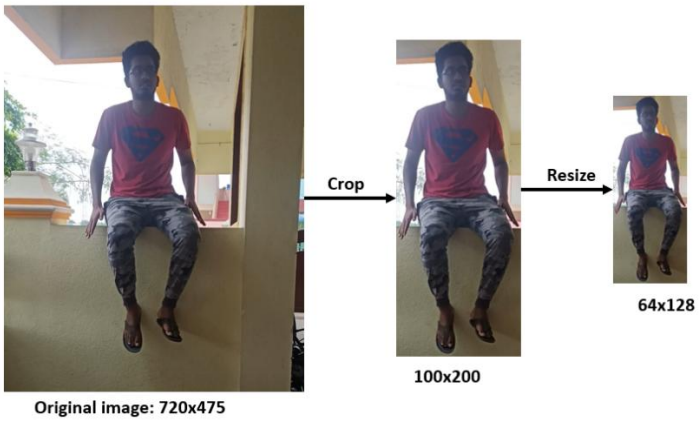

Fig. 11. Preprocessing in human detection

Fig. 12 shows how the gradients are calculated from the frames. Notice, the x-gradient fires on vertical lines and the y-gradient fires on horizontal lines. The magnitude of gradient fires where-ever there is a sharp change in intensity. None of them fire when the region is smooth. I have deliberately left out the image showing the direction of gradient because direction shown as an image does not convey much. Gradients removes unwanted details and highlights the outline of the object in the frames.

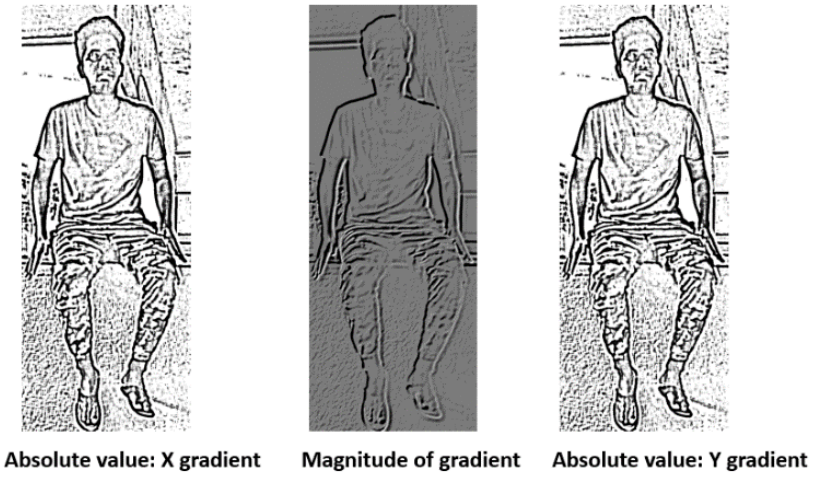

Fig. 12. Image gradient calculation

The 8x8 HOG is depicted in Fig. 13. Center image in Fig. 13 is very informative. It shows the patch of the image overlaid with arrows showing the gradient — the arrow shows the direction of gradient and its length shows the magnitude. On the right, we see the raw numbers representing the gradients in the 8×8 cells with one

minor difference — the angles are between 0 and 180 degrees instead of 0 to 360 degrees. These are called **"unsigned" gradients** because a gradient and it's negative are represented by the same numbers. In other words, a gradient arrow and the one 180 degrees opposite to it are considered the same.

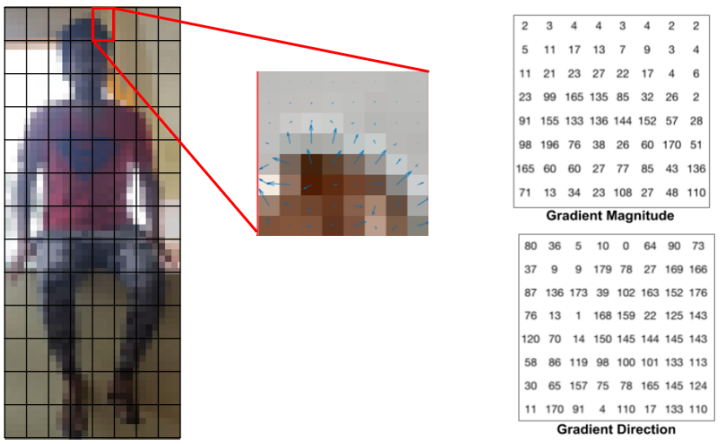

Fig. 13. 8x8 HOG image with Gradient magnitude and directions

In this manner Gradients are calculated and plotted as a histogram. The knowledge from the histogram is used to create bounding boxes around intruders in the preprocessed frames from video clips. Fig. 14 depicts an intruder being detected by the model. The model also doesn't detect inhuman objects like pets, birds etc.

Fig. 14. Intruder jumping over the wall being detected

We observed that the proposed model scans for motion continuously and once it detects motion, the camera starts recording and human detection, face recognition is performed on the video clip to differentiate between authorized and unauthorized person and sends an alert to the user through email with the video attachment.

V. CONCLUSIONS

In this work, we have developed a surveillance system with PIR Sensor, RaspberryPi 4 and a RPI Camera Module. The system was tested in real time to detect any motion in a confined place and to differentiate between authorized and unauthorized person. It was observed that the system works satisfactorily well in detecting motion with the PIR Sensor interfaced with the Raspberry Pi and was able to send warnings to the authorized person immediately with a recorded video clip as an attachment via email. Some False alerts were also sent due to the placement of the PIR Sensor in irregular surfaces. But the number of successful alerts greatly outnumbered the number of false alarms. The model was also able to differentiate between human and inhuman objects satisfactorily in well illuminated environment. The proposed framework was also able to detect intruders entering a confined place by jumping over the wall by creating a bounding box. In absence of illumination, the model made few false detections and was not able to recognize the authorized user accurately. But the number of times

false detections were made was very less compared to the number of times the proposed model detected and recognized the intruder as unauthorized person accurately. In this way, the performance of our model was recorded and analyzed with real time testing.

REFERENCES

[1] T. Petkar, "IoT based Line of Control Monitoring System," 2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS), Prawet, Thailand, 2025, pp. 1940-1945, doi: 10.1109/ICMLAS64557.2025.10967893.

[2] Y. S D, A. Saraswathi M, Ankitha, S. D and P. K. M, "Design and Development of an IoT Based Stability Monitoring System for Remote Data Visualisation and Control for Elderly People," 2025 International Conference on Emerging Systems and Intelligent Computing (ESIC), Bhubaneswar, India, 2025, pp. 537-541, doi: 10.1109/ESIC64052.2025.10962625.

[3] D. Chowdhry, R. Paranjape and P. Laforge, "Smart home automation system for intrusion detection," *2015 IEEE 14th Canadian Workshop on Information Theory (CWIT)*, St. John's, NL, Canada, 2015, pp. 75-78, doi: 10.1109/CWIT.2015. 7255156.

[4] A. Shahbaz and K. -H. Jo, "Improved Change Detector Using Dual-Camera Sensors for Intelligent Surveillance Systems," in IEEE Sensors Journal, vol. 21, no. 10, pp. 11435-11442, 15 May15, 2021, doi: 10.1109/JSEN.2020.3010563.

[5] B. Mukhopadhyay, S. Anchal and S. Kar, "Detection of an Intruder and Prediction of His State of Motion by Using Seismic Sensor," in IEEE Sensors Journal, vol. 18, no. 2, pp. 703-712, 15 Jan.15, 2018, doi: 10.1109/JSEN.2017.2776127.

[6] Y. -W. Bai, L. -S. Shen and Z. -H. Li, "Design and implementation of an embedded home surveillance system by use of multiple ultrasonic sensors," in IEEE Transactions on Consumer Electronics, vol. 56, no. 1, pp. 119-124, February 2010, doi: 10.1109/TCE.2010.5439134.

[7] R. Kishore, U. R. Vigneshwari, N. Prabagarane, K. Savarimuthu and S. Radha, "IoT Based Intelligent Control System for Smart Building," 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT), Sakheer, Bahrain, 2020, pp. 1-6, doi: 10.1109/3ICT51146.2020.9311944.

[8] D. Arjun, P. K. Indukala and K. A. Unnikrishna Menon, "PANCHENDRIYA: A Multi-sensing framework through Wireless Sensor Networks for Advanced Border Surveillance and Human Intruder Detection," 2019 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2019, pp. 295-298, doi: 10.1109/ICCES45898. 2019.9002161.

[9] A. H. Sanoob, J. Roselin and P. Latha, "Smartphone Enabled Intelligent Surveillance System," in IEEE Sensors Journal, vol. 16, no. 5, pp. 1361-1367, March1, 2016, doi: 10.1109/JSEN.2015.2501407.

[10] C. M. Patil, B. Jagadeesh and M. N. Meghana, "An Approach of Understanding Human Activity Recognition and Detection for Video Surveillance using HOG Descriptor and SVM Classifier," 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), Mysore, India, 2017, pp. 481-485, doi: 10.1109/ CTCEEC.2017.8455046.

[11] F. Pasqualetti, F. Zanella, J. R. Peters, M. Spindler, R. Carli and F. Bullo, "Camera Network Coordination for Intruder Detection," in IEEE Transactions on Control Systems Technology, vol. 22, no. 5, pp. 1669-1683, Sept. 2014, doi: 10.1109/ TCST.2013.2290708.

[12] Gulve, S.P., Khoje, S.A., Pardeshi, P. (2017). Implementation of IoT-Based Smart Video Surveillance System. In: Behera, H., Mohapatra, D. (eds) Computational Intelligence in Data Mining. Advances in Intelligent Systems and Computing, vol 556. Springer, Singapore. https://doi.org/10.1007/978-981-10-3874-7_73.

[13] Paul, M., Haque, S.M.E. & Chakraborty, S. Human detection in surveillance videos and its applications - a review. EURASIP J. Adv. Signal Process. 2013, 176 (2013). https://doi.org/10.1186/1687-6180-2013-176.

[14] K. Assaleh, T. Shanableh and K. Abuqaaud, "Face recognition using different surveillance cameras," 2013 1st International Conference on Communications, Signal Processing, and their Applications (ICCSPA), Sharjah, United Arab Emirates, 2013, pp. 1-5, doi: 10.1109/ICCSPA.2013.6487270.

[15] Ijaradar, Jyotirmaya, and Jinjing Xu. 2022. “A Cost-Efficient Real-Time Security Surveillance System Based on Facial Recognition Using Raspberry Pi and OpenCV”. Current Journal of Applied Science and Technology 41 (5):1-12. https://doi.org/10.9734/cjast/2022/v41i531665.

[16] Kunal Deo, Rishi Deedwania, Swati Bairagi . Human Intrusion and Motion Detection System. International Journal of Computer Applications. 176, 28 (Jun 2020), 46-49. DOI=10.5120/ijca2020920315.