JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

SUSPICIOUS ACTIVITY RECOGNITION USING YOLO ALGORITHM

[1]GURRAMKONDA KAVYA, [2]G.UMAMAHESWAR REDDY
[1]M.Tech Student, Department of Electronics and Communication Engineering, S.V.University, Tirupati, A.P.India
[2]Professor, Department of Electronics and Communication Engineering, S.V.University, Tirupati, A.P. India

Abstract: In our daily life, we see a lot of crimes and theft taking place which is not known properly. Suspicious Activity is predicting the body part of a person from video. In this work the entail detecting suspicious human Activity from camera and sending warning to authorized personby using Yolo Algorithm. A system that utilizes the You Only Look Once (YOLO) algorithm to recognize and identify suspicious activities. The system aims to enhance security measures by automatically generating SMS alerts to mobile devices once suspicious activities are detected. The proposed system uses deep learning to analyze video that captured by cameras and immediately send the alert message with image to the authorized person. Using visual surveillance, human activities can be monitored in public areas such as bus stations, railway stations, airports, banks, shopping malls, school and colleges, parking lots, roads, etc. to prevent terrorism, accidents and illegal parking, vandalism, fighting, crime and other suspicious activities. It is very tough to watch public places continuously, it is required to monitor the human activities from camera and categorize that usual and unusual activities and can generate an alert and send the image notification to authorized person.

IndexTerms– SMS Alerts, YOLO Object,Suspicious Activity Recognition, Computer Vision, Pre-Processing etc.

1. INTRODUCTION

In recent years, computer vision has emerged as a powerful tool for analyzing and interpreting visual data. One important application of computer vision is the recognition of suspicious activities in various settings, such as public spaces, transportation hubs, and security-sensitive areas. The ability to automatically identify suspicious behavior can greatly enhance surveillance systems and improve public safety.

To tackle this challenge, researchers and engineers have developed numerous techniques and algorithms, and among them, one popular approach is the You Only Look Once (YOLO) object detection framework. YOLO is renowned for its real-time processing capabilities and high accuracy, making it an excellent choice for detecting objects and activities in video streams.

The core principle of YOLO is to divide the image into a grid and predict bounding boxes and class probabilities for each grid cell simultaneously. This unique approach allows YOLO to achieve remarkable speed without compromising accuracy. By leveraging YOLO's capabilities, we can efficiently detect and recognize objects relevant to suspicious activities in real-time.The recognition of suspicious activities using YOLO object detection involves multiple stages. First, a training phase is required to teach the model to recognize specific objects and activities associated with suspicious behavior. This typically involves collecting and annotating a dataset that includes examples of both normal and suspicious activities. The model is then trained using these labeled examples, allowing it to learn patterns and features that distinguish suspicious actions.Once the model is trained, it can be deployed in a real-world surveillance system. The system continuously analyzes video streams, applying YOLO object detection to identify objects and activities of interest. It examines various factors such as unusual object movements, interactions between objects, and the presence of specific objects associated with suspicious behavior. The model's ability to detect these indicators can provide early warnings and assist security personnel in taking appropriate actions swiftly.

The benefits of utilizing YOLO object detection for suspicious activity recognition are numerous. Its real-time processing capabilities enable prompt detection and response, minimizing the potential risks associated with suspicious behavior. Additionally, YOLO's high accuracy reduces false positives, ensuring that security personnel can focus on genuine threats, thereby increasing overall efficiency.In conclusion, the combination of computer vision and YOLO object detection offers a promising solution for recognizing suspicious activities in various settings. By harnessing the power of deep learning and real-time analysis, this approach can contribute to enhancing public safety and security. As advancements in computer vision continue, we can expect further refinements and applications of YOLO-based systems, ultimately creating safer environments for individuals and communities.

The organizational framework of this study divides the research work in the different sections. The Literature survey is presented in section 2. Further, in section 3 shown Existing Method is discussed and in section 4 shown in proposed Method, In section 5Results and discussion of work is shown. Conclusion and future work are presented by last sections 6.

2. LITERATURE SURVEY

Suspicious activity recognition is a critical task in video surveillance systems for ensuring public safety and preventing potential threats. Computer vision techniques, combined with deep learning models, have shown promising results in detecting and analyzing suspicious activities in real-time. One such widely used approach is the integration of the You Only Look Once (YOLO) object detection algorithm with computer vision techniques. In this literature survey, we explore the existing research and advancements in suspicious activity recognition using YOLO object detection.

This paper presents YOLOv3, an improved version of the YOLO object detection algorithm. It introduces a series of architectural enhancements and achieves superior performance in terms of accuracy and speed.[1]

This Paper proposes the concept of "Scribbler," a framework that utilizes YOLO-based object detection to recognize and synthesize images based on sketch and color inputs. It demonstrates the potential application of YOLO in various computer vision tasks, including suspicious activity recognition.[2].

This Paper proposes an overview of various techniques and approaches used for suspicious activity recognition in video surveillance. It covers both traditional methods and deep learning-based approaches, including those that leverage YOLO object detection. The paper discusses challenges, datasets, and evaluation metrics in this domain.[3].

This paper presents an automated system for detecting suspicious activities in surveillance videos using the YOLO object detection algorithm. It discusses the system architecture, dataset preparation, and experimental results, demonstrating the effectiveness of YOLO for real-time suspicious activity recognition.[4].

This paper proposes a suspicious human activity recognition method that combines YOLO with deep learning techniques. It focuses on recognizing abnormal behavior in crowded scenes and evaluates the performance using benchmark datasets. The study highlights the effectiveness of the YOLO-based approach for real-world surveillance scenarios. [5].

This paper presents the use of YOLO for human activity recognition, including suspicious activities. It explores the potential of YOLO as a tool for real-time surveillance and discusses the integration of YOLO.[6]

3. EXISTING METHOD

Object Detection is the process of finding and recognizing real-world object instances such as car, bike, TV, flowers, and humans out of an images or videos. An object detection technique lets you understand the details of an image or a video as it allows for the recognition, localization, and detection of multiple objects within an image.It is usually utilized in applications like image retrieval, security, surveillance, and advanced driver assistance systems (ADAS).Object Detection is done through many ways:

- Feature Based Object Detection
- Viola Jones Object Detection
- SVM Classifications with HOG Features
- Deep Learning Object Detection

Object detection from a video in video surveillance applications is the major task these days. Object detection technique is used to identify required objects in video sequences and to cluster pixels of these objects.

The detection of an object in video sequence plays a major role in several applications specifically as video surveillance applications.

Object detection in a video stream can be done by processes like pre-processing, segmentation, foreground and background extraction, feature extraction.Humans can easily detect and identify objects present in an image. The human visual system is fast and accurate and can perform complex tasks like identifying multiple objects with little conscious thought. With the availability of large amounts of data, faster GPUs, and better algorithms, we can now easily train computers to detect and classify multiple objects within an image with high accuracy.

4. PROPOSED METHOD

Suspicious Activity Recognition using YOLO (You Only Look Once) object detection is a system that aims to detect and identify potentially suspicious activities in real-time using computer vision techniques.

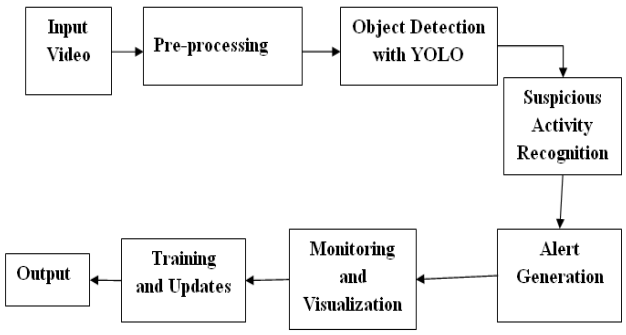

Fig.1: Proposed block diagram

Figure 1 shows the proposed system block diagram. The system typically consists of the following components:

1. Video Input: The system takes video streams as input from surveillance cameras or other sources. These video streams can be captured in real-time or pre-recorded.
2. Pre-processing: The video frames are preprocessed to enhance their quality and prepare them for object detection. Common preprocessing steps may include resizing, normalization, and noise reduction.

3. Object Detection with YOLO: The YOLO algorithm is employed to detect and localize objects in the video frames. YOLO divides the image into a grid and predicts bounding boxes and class probabilities for objects within each grid cell. It can detect multiple objects simultaneously with high accuracy and efficiency.
4. Suspicious Activity Recognition: Once objects are detected, the system applies specific rules or algorithms to determine whether the observed activities are suspicious. These rules can be based on predefined criteria, such as abnormal behavior, specific poses, or interactions between objects and individuals.
5. Alert Generation: If a suspicious activity is identified, the system generates an alert or notification. This alert can be in the form of an alarm, a message to security personnel, or an integration with other security systems.
6. Monitoring and Visualization: The system provides a monitoring interface where security personnel can view the video stream in real-time and observe detected objects and suspicious activities. Visualization tools, such as bounding boxes around objects or trajectory tracking, may be used to aid in monitoring.
7. Training and Updates: The system can be trained using labeled data to improve its accuracy and ability to recognize suspicious activities. As new suspicious activities emerge or the system encounters false positives/negatives, the training process can be repeated to fine-tune the model.
8. Integration with Security Systems: The system can be integrated with other security systems, such as access control or alarm systems, to enhance overall security measures. For example, upon detecting a suspicious activity, the system may trigger a lockdown procedure or activate additional surveillance cameras for further investigation.

Overall, Suspicious Activity Recognition using Computer Vision with YOLO enables automated monitoring and detection of potentially suspicious activities, improving the effectiveness and efficiency of security systems in various domains, including public spaces, airports, banks, and other critical infrastructure.

Implementation of Yolo Algorithm

To implement suspicious activity recognition using computer vision and YOLO object detection, you can follow these general steps:

1. **Dataset Collection**: Collect a dataset that includes images or videos of suspicious activities. This dataset should cover a range of activities you want to detect.
2. **Annotation**: Annotate the collected dataset by labeling the objects and activities of interest. For example, mark the regions of interest (bounding boxes) around people performing suspicious activities.
3. **YOLO Model Training**: Train a YOLO (You Only Look Once) object detection model using the annotated dataset. YOLO is known for its real-time object detection capabilities.
   - Set up a training environment with the required dependencies, such as TensorFlow, Keras, or Darknet (YOLO's original framework).
   - Prepare the dataset in the required format for YOLO training, typically in the format of YOLO's labeled bounding box format (YOLO darknet format).
   - Configure the YOLO model architecture according to your requirements, such as the number of classes and the desired backbone network (e.g., YOLOv3 or YOLOv4).
   - Start the training process using the annotated dataset and adjust hyperparameters like learning rate, batch size, and number of training epochs.
   - Monitor the training process, evaluate the model's performance on a validation set, and save the best-performing model.
4. **Model Testing**: Once the YOLO model is trained, you can test it on new images or videos to detect suspicious activities.
   - Preprocess the test images or frames from the videos by resizing or normalizing them to fit the input size of the trained YOLO model.
   - Pass the preprocessed images or frames through the YOLO model to obtain bounding box predictions and class labels for detected objects.
   - Apply post-processing techniques to filter out false positives and refine the detection results if needed.
   - Use the detection results to identify and recognize suspicious activities based on the labeled classes.
5. **Thresholding and Alert Generation**: Determine suitable thresholds for recognizing suspicious activities based on the confidence scores or other metrics provided by the YOLO model. You can define thresholds for individual classes or a combination of classes.
   - Analyze the detection outputs, such as the bounding boxes and class labels, to identify specific patterns or combinations of objects that constitute suspicious activities.
   - Apply appropriate decision rules or heuristics to determine when a detected combination of objects should be classified as a suspicious activity.
   - Generate alerts or take further actions when a suspicious activity is detected, such as triggering alarms, sending notifications, or saving evidence.
6. **Iterative Refinement**: Evaluate the performance of your system, including the detection accuracy

and false positive/negative rates. Iterate on the model training and testing steps, adjusting hyperparameters, collecting more data, or refining the annotation process to improve the overall performance.

5. RESULTS AND DISCUSSIONS

In this project in a disclosed room or secure room if any motion occurred it automatically detect the object and identify the object and send the information to the authorized person

STEP 1: Detecting Motion And Capturing The Image

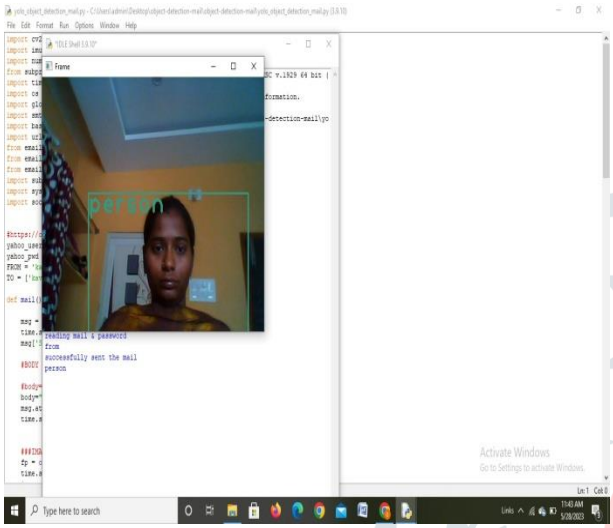

Fig.2: It detects the motion in a secured room

Fig 2 shows Firstly if any motion occurs it capture the image and also identify the moment that happen it may be person or any object and before taking any further step it sends the information

STEP 2: Sending Notification of image to authorized person

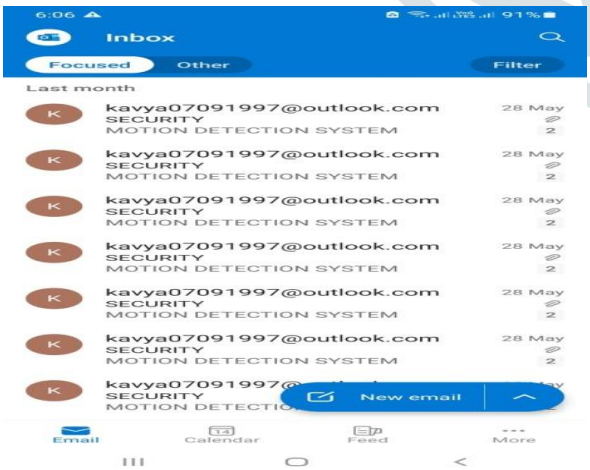

Fig.3: sends the notification

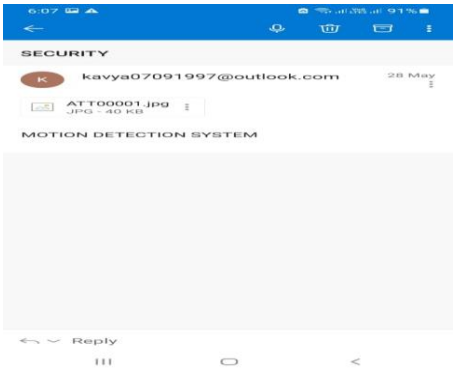

Fig.4:Alert the person after receiving the notification

Figure 3 and 4 shows when the Detecting Person as a Suspicious Activity and when the Detecting Closing Camera as a Suspicious Activity.

STEP3: Received notification alert after detecting motion

Fig.5: Detecting Closing Camera as a Suspicious Activity

STEP 4: Detecting multiple images

Fig.6: Detecting Suspicious Activity Detection for multiple images

STEP 5: Detecting fire arm

Fig.7: Detecting Suspicious Activity Detection for Firearm

The firearm Detection shown in fig.7 that model identifies the presence of firearms and knives. Upon weapon identification, the system triggers alarms and notifies security personnel and authorities about the incident.

6. CONCLUSION

One of the key advantages of this system is its ability to send SMS alerts to mobile devices when suspicious activity is detected. This feature allows for immediate notification to security personnel or relevant authorities, enabling swift response and intervention. By leveraging mobile communication, the system ensures that the right people are informed promptly, regardless of their location, enabling them to take appropriate action to address the situation.

Overall, the YOLO algorithm for suspicious activity recognition represents a significant advancement in security systems. It offers the potential to enhance public safety, protect valuable assets, and prevent potential threats in real-time. However, it is important to note that while this technology can be a valuable tool, it should be used responsibly and ethically, with appropriate safeguards in place to protect individual privacy and prevent misuse.

FUTURE SCOPE

The future scope for suspicious activity recognition using computer vision and sending SMS alerts to mobile devices using the YOLO (You Only Look Once) algorithm is promising. Here are some potential advancements and opportunities in this field:

1. Computer vision algorithms can benefit from the integration of multiple modalities, such as combining visual data with audio or sensor data. By incorporating audio analysis or other sensor inputs, the system can improve its ability to detect and classify suspicious activities accurately.
2. In addition to sending SMS alerts, future systems could integrate with other communication channels, such as email, push notifications, or voice calls. This would enable a more comprehensive and customizable alerting mechanism based on the preferences of the users or security personnel.

REFERENCES

[1]. Redmon, J., &Farhadi, A. (2018). YOLOv3: An Incremental Improvement. arXiv preprint arXiv:1804.02767.

[2]. Sangkloy, P., Lu, J., Fang, C., Yu, F., & Hays, J. (2017). Scribbler: Controlling Deep Image Synthesis with Sketch and Color. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 6223-6232).

[3]. Mohammadi, M., &Razzazi, F. (2020). A Survey on Suspicious Activity Recognition Techniques in Video Surveillance. Journal of AI and Data Mining, 8(2), 169-189.

[4]. Roy, N., & Islam, M. M. (2020). Automated Detection of Suspicious Activity in Surveillance Video Using YOLO Object Detection. In 2020 International Conference on Computer, Communication, Chemical, Material and Electronic Engineering (IC4ME2) (pp. 1-6).

[5]. Li, L., Guo, J., Ma, H., & Huang, F. (2018). Suspicious Human Activity Recognition Based on YOLO and Deep Learning. In 2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA) (pp. 2346-2350).

[6]. Madhow, A., Rao, R., &Venkatesh, S. (2019). Human Activity Recognition Using YOLO. In 2019 IEEE International Conference on Consumer Electronics (ICCE) (pp. 1-6).

[7]. A Review on Object Detection in Video Processing, International Journal of u- and e- Service, Science and Technology, Vol. 5, No. 4, December, 2012, Kauleshwar Prasad, RichaSharmaand, DeepikaWadhwani, BIT, Durg, India.

[8]. Suspicious Human Activity Detection from Surveillance Videos, (IJIDCS) International Journal on Internet and Distributed Computing Systems, Vol: 2 No: 2, 2012, Gowsikhaa D, Manjunath, Abirami S, Department of information science and technology, Anna University, Chennai, Tamilnadu.

[9]. M. Fahad Khan, Hafiz Adnan Habib, “Video Analytics for Quantitative Employee Performance Evaluation”, Canadian Journal on Image Processing & Computer Vision Vol. 1, No. 1, pp. 9-15, February 2010.

[10]. Benjamin Maurin, Osama Masoud and Nikos Apanikolopoulos, “Camera Surveillance of Crowded Traffic Scenes”, IEEE Computer Society Press Vol. 22,No. 4, pp.16-44, 2010.

[11]. Gwang Goo K Lee, Hwan Ka, Byeoung Su Kim, WhoiYul Kim, Ja Young Yoon and Jae Jun Kim, ”Analysis of crowded scenes in Surveillance Videos”, Canadian Journal on Image Processing & Computer Vision Vol. 1, No. 1, pp.52-75, 2010.

[12]. Paul Viola and Michael J. Jones, “Robust Real-Time Face Detection”, International Journal of Computer Vision Vol. 57, No. 2, pp. 137–154, 2004.

[13]. Suspicious Human Activity Recognition for Video Surveillance System, 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Ahmad Salihu Ben-Musa, Sanjay Kumar Singh, PrateekAgrawal,

Department of Computer Science and Engineering, Lovely Professional University, Punjab, India.

[14]. Face Detection using SURF Cascade, Jianguo Li, Tao Wang, Yimin Zhang, Intel Labs China.