Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

DEEP LEARNING APPROACH FOR SUSPICIOUS ACTIVITY DETECTION FROM SURVEILLANCE VIDEO

P.GAYATRI[1],V.MADHAN GOPAL[2]
S.G.V.SAMPATH[3], P.PREETHI[4]
G.MOULI SAI CHANDAR [5]

1. Assistant Professor 2. Engineering student, 3.Engineering student
4. Engineering student, 5. Engineering student
DEPARTMENT OF COMPUTER SCIENCE, SANKETIKA VIDYA PARISHAD ENGINEERING COLLEGE Visakhapatnam, India

ABSTRACT
Security has recently received the highest priority due to the rise in anti-social activities that have occurred. CCTVs have been placed by numerous organizations to continuously monitor individuals and their interactions. Every person in a developed nation with 64 million people is photographed 30 times a day. An enormous amount of video data is created and kept for a specific amount of time. A picture with a resolution of 704x576 and 25 frames per second will produce about 20GB every day. It is nearly hard for humans to continuously monitor data to determine whether events are anomalous because it takes a workforce and their undivided attention. This means that the same has to be automated. To help with the quicker determination that the odd activity is abnormal, it is also necessary to indicate which frame and what portion of it contains the unexpected activity. In order to accomplish this, video is divided into frames, and each processed frame's people and activities are examined. Algorithms and techniques for machine learning and deep learning assist us widely in making possible

Keywords:-CCTV, OpenCV, CNN, Anomaly, Activity
.

1 INTRODUCTION

Identification of an individual is greatly aided by their facial features and behavioral patterns. One important source for these identifications is visual information. Such visual data is available through surveillance videos, which can be seen live or recorded for later use. Even in the realm of video analytics, the recent trend toward "automation" has an impact. Numerous applications, including motion detection, person identification, aberrant activity recognition, vehicle counting, people counting in crowded areas, and human activity prediction, can be made with video analytics. Within this field, In technical terms, face recognition and gait recognition are the two characteristics that are used to identify a person. Face recognition is the more flexible of these two methods for automatic human identification from security footage. Face recognition technology can be used to anticipate a person's head orientation, which helps predict their behavior. In several applications, such as identity verification, motion detection with facial recognition, and presence/absence detection at a certain location and time, motion recognition combined with facial recognition is highly helpful.A system that successfully detects and recognizes suspicious conduct among students in an examination hall is also created by utilizing human interactions, such as delicate eye contact, head motion detection, hand gesture identification, and estimating. This research presents a face recognition algorithm for the detection of questionable human activity. Research and security are the two primary areas in which video processing is employed. This kind of technology keeps an eye on live videos using clever algorithms. Time and computational complexity are two important considerations in real-time system design. For time-sensitive applications like bank robbery detection, patient monitoring systems, identifying and reporting suspicious activity at train stations, etc., the system that employs an algorithm with a relatively lower time complexity, using less hardware resources, and producing good results will be more beneficial.Exam hall manual monitoring via invigilators and manual exam hall monitoring via surveillance films are carried out globally. Manpower-wise, keeping an eye on a test hall is a really difficult chore. Errors can occur when manually monitoring exam rooms while under human supervision. When such a system is put into place as a "automatic suspicious activity detection system," it will assist in both identifying and reducing suspicious activity. Furthermore, there will be a significantly lower chance of inaccuracy. This method will be beneficial for educational institutions as a surveillance tool.This paper describes a technology that analyzes real-time recordings and uses them to assess human activity in an exam room. This technology helps classify a person's activity and determine whether or not it is suspicious. The devised system detects unusual head movements and forbids copying. It also indicates when a student moves or changes positions with another student. Lastly, by detecting student contact, the technology stops students from sharing potentially damning information with one another. As a result of our research, a system that can intelligently analyze live video from test rooms involving students and categorize their behavior as suspicious or not has been developed. This study suggests an

intelligent algorithm that can keep an eye on and evaluate students' actions in a testing environment.and can alert the educational institute's administration on account of any malpractices/suspicious activities. The Suspicious Human Activity Detection system aims to identify the students who indulge in malpractices/suspicious activities during the course of an examination. The system automatically detects suspicious activities and alerts administration.

2. LITERATURE SURVEY AND RELATED WORK

2.1. Suspicious Activity Detection in Surveillance Footage

Authors: Satyajit Loganathan, Gayashan Kariyawasam.

Abstract: Concerning the potential risk that suspicious activity poses to people, it is an issue. Given the rise in illicit activity in suburban and national settings, it is imperative to assess these locations in order to reduce recurrence of such incidents. In the past, surveillance was carried out manually by people, which was a taxing process because suspicious activity wasn't commonplace.

.

2.2. Suspicious Activity Detection from Videos using YOLOv3

Authors: Nipunjita Bordoloi; Anjan Kumar Talukdar; Kandarpa Kumar Sharma

Abstract: A self-acting method of analyzing video sequences and intelligently selecting which actions to include in the film is human activity detection for video systems. It's one of the fields of artificial intelligence and computer vision that is expanding. The practice of identifying undesired human behavior in locations and circumstances is known as suspicious activity detection. To do this, video is divided into frames, and the activities of people are analyzed from the repurposed frames.

2.3. Detection of Suspicious Activity and Estimate of Risk from Human Behavior shot by Surveillance Camera

Authors: Miwa Takai

Abstract: These days, surveillance camera systems are the most popular security systems since they can monitor large areas from a distance utilizing a webcam connected to a video observer over a network. Additionally, low-cost, mass-produced digital goods like hard drives and web cameras are available. Furthermore, the performance gain of these digital products increases quickly. The current surveillance camera system displays dynamic photos captured simultaneously by many Web cams in certain oversight locations. Additionally, the system wears out the viewer's body and mind because of the massive amount of dynamic visuals that are updated on a regular basis. A significant issue with this technique is that it has a viewer-slips over crime predictor.

Author: **Crowd consistence Anal**.

Abstract: Not only is this crucial for people's comfort, but it is also critical for their safety. This research demonstrates that it is possible to understand a video clip and evaluate a behavior as normal or suspicious, especially in densely populated places. The YOLOv3 algorithm is used by the suggested system to detect objects. The features are first calculated from the picture. The classifier then generates a forecast based on the properties that were identified. The technique uses an object detection to determine whether to classify a frame as normal or suspicious. The number of people in a frame is used to assess crowd density, while suspicious things like firearms, knives, and separated bags are used to identify suspicion in a frame.

3 Implementation Study

The technique known as Advance Motion Detection (AMD) was employed to find an illegal entry into a prohibited location. Using background subtraction, the item was identified in the first step, and it was then retrieved from frame sequences. The identification of suspicious activity was the second stage. The system's advantage was that the algorithm's low computing complexity allowed it to process videos in real time. However, the system's storage capacity was constrained. Nevertheless, it might be used in conjunction with a cutting-edge method of video capture in monitoring zones.

.

3.1 PROPOSED Methodology AND ALGORITHM

When any suspicious activity takes place, the suggested system will monitor student activity on campus using CCTV footage and notify the appropriate authorities.

The architecture is divided into several stages, including pre-processing, feature extraction, classification, prediction, and video

recording.

The system classifies the videos into three classes.

1)Students using Mobile phone inside the campus- Suspicious class.

2)Students fighting or fainting in campus-Suspicious class.

3)Walking, running- Normal class.

4 METHODOLOGIES

4.1 Data Validation/ Cleaning/Preparing Process

Importing the library packages with loading given dataset. To analyzing the variable identification by data shape, data type and evaluating the missing values, duplicate values. A validation dataset is a sample of data held back from training your model that is used to give an estimate of model skill while tuning models and procedures that you can use to make the best use of validation and test datasets when evaluating your models. Data cleaning / preparing by rename the given dataset and drop the column etc.to analyze the uni-variate, bi-variate and multi-variate process. The steps and techniques for data cleaningwill vary from dataset to dataset. The primary goal of data cleaning is to detect and remove errors and anomalies to increase the value of data in analytics and decision making.

4.2 Exploration data analysis of visualization

Data visualization is an important skill in applied statistics and machine learning. Statistics does indeed focus on quantitative descriptions and estimations of data. Data visualization provides an important suite of tools for gaining a qualitative understanding. This can be helpful when exploring and getting to know a dataset and can help with identifying patterns, corrupt data, outliers, and much more. With a little domain knowledge, data visualizations can be used to express and demonstrate keyrelationships in plots and charts that are more visceral and stakeholders than measures of association orsignificanceEven before predictive models are prepared on training data, outliers can result in misleading representations and in turn misleading interpretations of collected data. Outliers can skew the summary distribution of attribute values in descriptive statistics like mean and standard deviation and in plots such as histograms and scatter plots, compressing the body of the data. Finally, outliers can representexamples of data instances that are relevant to the problem such as anomalies in the case of fraud detection and computer security.It couldn't fit the model on the training data and can't say that the model will work accurately for the real data. For this, we must assure that our model got the correct patterns from the data, and it is not getting up too much noise. Cross-validation is a technique in which we train our model using the subset of the data-set and then evaluate using the complementary subset of the data-set.

The three steps involved in cross-validation are as follows:

- Reserve some portion of sample data-set.
- Using the rest data-set train the model.
- Test the model using the reserve portion of the data-set.

4.3 Advantages of train/test split

- This runs K times faster than Leave One Out cross-validation because K-fold cross-validationrepeats the train/test split K-times.
- Simpler to examine the detailed results of the testing process.
- Advantages of cross-validation:
- More accurate estimate of out-of-sample accuracy.
- More "efficient" use of data as every observation is used for both training and testing.

4.4 Data Pre-processing

Pre-processing refers to the transformations applied to our data before feeding it to the algorithm. Data Preprocessing is a technique that is used to convert the raw data into a clean data set. In other words, whenever the data is

gathered from different sources it is collected in raw format which is not feasible forthe analysis. To achieving better results from the applied model in Machine Learning method of the data has to be in a proper manner.Some specified Machine Learning model needs information in a specified format; for example, Random Forest algorithm does not support null values. Therefore, to execute random forest algorithmnull values have to be managed from the original raw data set. And another aspect is that data set should be formatted in such a way that more than one Machine Learning and Deep Learning algorithms are executed in given dataset.

4.5 CNN Algorithm

Building a suspicious activity detection algorithm involves several steps. Here's a generalized step-by-step guide for creating one using Convolutional Neural Networks (CNNs):

1. Define the Problem: Clearly define what constitutes "suspicious activity" in your context. This could include actions like trespassing, stealing, or violence in surveillance videos.

2. Data Collection: Gather a large dataset of videos containing both normal and suspicious activities. Label each video or frame with the corresponding category (normal or suspicious).

3. Data Preprocessing:

- Extract relevant frames from the videos.
- Resize the frames to a standard size.
- Normalize the pixel values (typically between 0 and 1).
- Augment the data if necessary to increase the diversity of the dataset (e.g., rotation, flipping, adding noise).

4. Split the Data: Divide the dataset into training, validation, and testing sets. The training set is used to train the model, the validation set is used to tune hyperparameters and prevent overfitting, and the testing set is used to evaluate the final model's performance.

5. Model Architecture Design:

- Design a CNN architecture suitable for the task. Start with popular architectures like VGG, ResNet, or Inception, and customize them according to your dataset and problem.
- Add layers such as convolutional layers, pooling layers, and fully connected layers.
- Utilize techniques like dropout and batch normalization to improve generalization and training stability.

6. Model Training:

- Initialize the model's weights.
- Define a loss function suitable for binary classification (e.g., binary cross-entropy).
- Choose an optimizer (e.g., Adam, RMSprop).
- Train the model on the training data while monitoring its performance on the validation set.
- Adjust hyperparameters (e.g., learning rate) based on validation performance.

7. Model Evaluation:

- Evaluate the trained model on the test set to assess its performance.
- Metrics like accuracy, precision, recall, and F1-score are commonly used for classification tasks.
- Analyze any misclassifications to identify patterns or areas for improvement.

8. Fine-tuning and Optimization:

- Fine-tune the model architecture and hyperparameters based on the evaluation results.
- Experiment with different network architectures, optimization algorithms, and data augmentation techniques to improve performance.

9. Deployment:

- Once satisfied with the model's performance, deploy it in a real-world setting.
- Integrate the model into the surveillance system to analyze live video feeds for suspicious activities.

10. Monitoring and Maintenance:

- Continuously monitor the model's performance in the deployed environment.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

- Retrain the model periodically with new data to adapt to evolving scenarios and maintain effectiveness.

5 RESULTS AND DISCUSSION

Fig1 : Double click on 'run.bat' file from project folder to start project execution. We will get below screen.

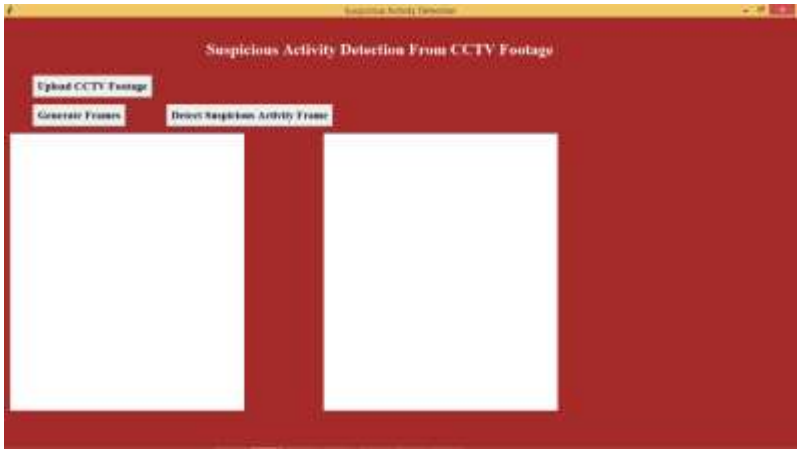

Fig 2: Click on 'Upload CCTV Footage' button to upload video.

Fig 3: In above screen I am uploading one normal video. After uploading video click on 'Generate Frames' button to generate frame.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

Fig 4: In above
black screen we can see extracted frames are saving inside ‘frames’ folder frame no. Now we see frames folder below which has images from video

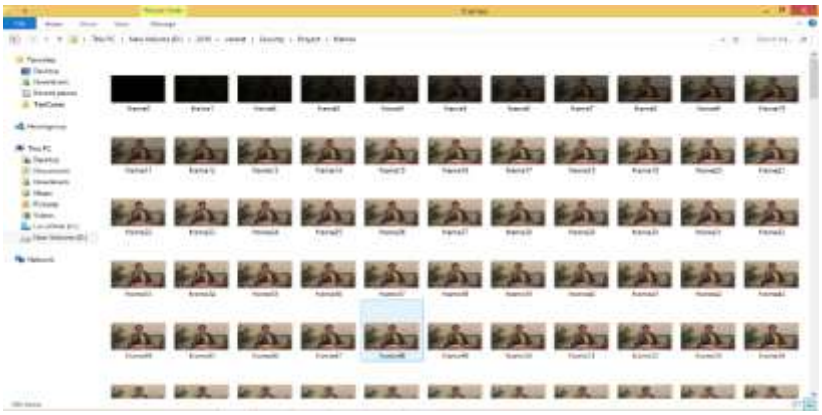

Fig 5: In above folder screen we can see all images from video extracted. After frame extraction will get below screen.

Fig 6: Now click on ‘Detect Suspicious Activity Frame’ button to start monitoring frames for suspicious activity**.**

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

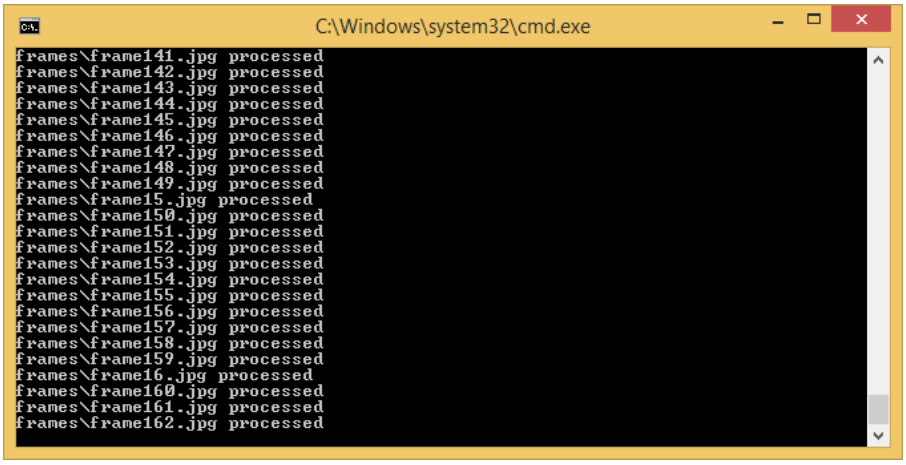

Fig 7: In above black console window, we can see processing of each frame to detect suspicious activity.

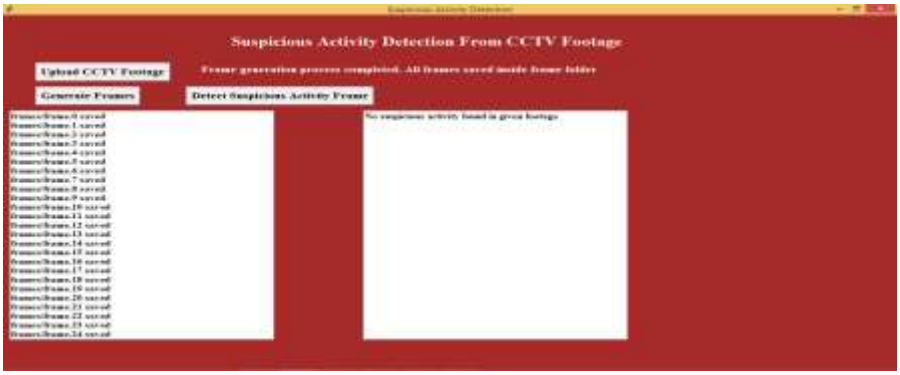

Fig 8: In above screen we can see frames scanned and no suspicious activity found. Now we will upload another video and check status.

Fig 9: In above screen I am uploading 'Video2' and then extract frames.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

Fig 10: In above screen for uploaded video, we can see suspicious activity found at farme117.jpg. After scanning all images, we will get below details screen. Now in below screen we can see frame117.jpg image from frames folder**.**

Fig 11: In above screen frame117 showing one image of a person with face covering. Similarly, we can see all frames details in below screen which has such activities

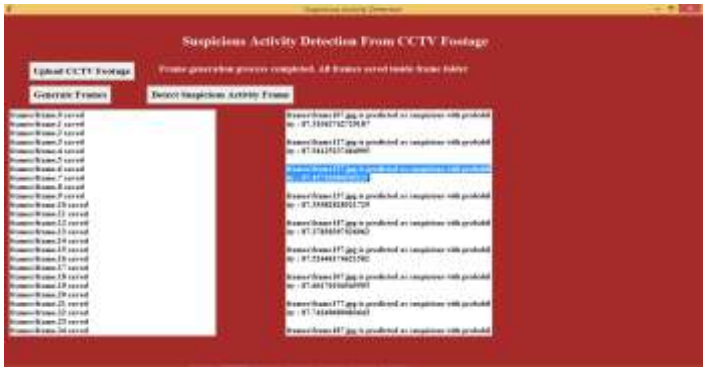

Fig 12: In above screen in right text area, we can see details of all frames which has such activities.

Note: you too can upload your own videos and check but your videos must have person covering their faces or doing shop lifting robbers videos. Your videos must be like similar one which I used in this project

6.CONCLUSION AND FUTURE SCOPE

6.1 Almost everyone in the modern world understands the value of CCTV footage, but in the majority of cases, these recordings are used for investigative purposes following a crime or occurrence. One advantage of the suggested model is that it deters crime before it occurs. The CCTV footage captured in real time is being monitored and examined. The analysis's conclusion is a directive to the appropriate authority to take appropriate action should the conclusion suggest that an undesirable incidence will occur. Thus, we can put an end to this.

.

6.2 FUTURE SCOPE

Nowadays, practically everyone is aware of the value of CCTV footage; yet, in the majority of cases, these recordings are employed for investigative purposes following a crime or occurrence. Preventing crime before it occurs is one of the benefits of the suggested model. We are tracking and analyzing the live CCTV feed. If the analysis's outcome shows that an undesirable incidence is likely to occur, the relevant authority is instructed to take appropriate action. Thus, this can be put an end to.

.

7 REFERENCES

[1] P.Bhagya Divya, S.Shalini, R.Deepa, Baddeli Sravya Reddy,"Inspection of suspicious human activity in the crowdsourced areas captured in surveillance cameras",International Research Journal of Engineering and Technology (IRJET), December 2017.

[2] Jitendra Musale,Akshata Gavhane, Liyakat Shaikh, Pournima Hagwane, Snehalata Tadge, "Suspicious Movement Detection and Tracking of Human Behavior and Object with Fire Detection using A Closed Circuit TV (CCTV) cameras ", International Journal for Research in Applied Science & Engineering Technology (IJRASET) Volume 5 Issue XII December 2017.

[3] U.M.Kamthe,C.G.Patil "Suspicious Activity Recognition in Video Surveillance System", Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), 2018.

[4] Zahraa Kain, Abir Youness, Ismail El Sayad, Samih Abdul-Nabi, Hussein Kassem, " Detecting Abnormal Events in University Areas ", International conference on Computer and Application,2018.

[5] Tian Wanga, Meina Qia, Yingjun Deng, Yi Zhouc, Huan Wangd, Qi Lyua, Hichem Snoussie, "Abnormal event detection based on analysis of movement information of video sequence" ,Article-Optik,vol152,January-2018.

[6] Elizabeth Scaria, Aby Abahai T and Elizabeth Isaac, "Suspicious Activity Detection in Surveillance Video using Discriminative Deep Belief Netwok", International Journal of Control Theory and Applications Volume 10, Number 29 -2017.

[7] Dinesh Jackson Samuel R,Fenil E, Gunasekaran Manogaran, Vivekananda G.N, Thanjaivadivel T , Jeeva S , Ahilan A, "Real time violence detection framework for football stadium comprising of big data analysis and deep learning through bidirectional LSTM",The International Journal of Computer and Telecommunications Networking,2019.

[8] Kwang-Eun Ko, Kwee-Bo Sim "Deep convolutional framework for abnormal behavior detection in a smart surveillance system. "Engineering Applications of Artificial Intelligence ,67 (2018).

[9] Yuke Li "A Deep Spatiotemporal Perspective for Understanding Crowd Behavior", IEEE Transactions on multimedia, Vol. 20, NO. 12, December 2018