SUSPICIOUS ACTIVITY DETECTION BY USING DEEP LEARNING

Dr.P.Satish Reddy[1]|CH.Sangeetha[2]|Dr.M.Muthukumaran[3]|Jadala Akhila[4]

1 & 3Associate Professor, CSE department, Kasireddy Narayanreddy College of Engineering And Research, Hyderabad, TS.

2 Assistant Professor, CSE department, Kasireddy Narayanreddy College of Engineering And Research, Hyderabad, TS.

4 UG SCHOLAR, CSE department, Kasireddy Narayanreddy College of Engineering And Research, Hyderabad, TS.

.

ABSTRACT: The work of observation security is incredibly boring and tiresome. To determine whether the observed exercises are unusual or questionable, a workforce and their continuous evaluation are needed. Here, we will build a framework to automate the process of looking at video reconnaissance. We will regularly examine the video feed in order to identify any odd exercises that seem startling or questionable. There have been advancements in deep learning computations for deep reconnaissance since the earlier encounters. These developments ensure a drastic increase in efficacy and have demonstrated a basic pattern in deep reconnaissance. Burglary distinguishing proof, brutality discovery, and explosion possibility recognition are typical applications of profound observation. We will introduce a spatio-worldly auto-encoder for this endeavor, which relies on a 3D convolutional brain architecture. The decoder then replicates the edges after the encoder portion eliminates the spatial and transient data. By using Euclidean distance between the original and replicated batches to register the recreation disaster, the unexpected occurrences are identified.

KEYWORDS: Surveillance; Deep Learning; Spatio temporal; Euclidean distance; auto-encoder.

I.INTRODUCTION: Currently, the numbers of offensive activities taking place are increasing rapidly. With this rise, it is more important than ever to prevent them and detect them. In public places, surveillance cameras are increasingly being used. A large number of videos are created and stored for a period of time. Constantly keeping track of these surveillance videos is practically hard for authorities to evaluate whether the incidents are suspicious since it requires a large crew and continual

monitoring. As a result, a demand for high-precision automation of this process is emerging. It is also required to specify which frame is being used. And which parts of it contain the unusual activity, as these aids in the quicker determination of whether or not the unusual activity is abnormal or suspicious. This will assist the concerned authorities in determining the root cause of the anomalies while also saving time and effort required to manually searching the recordings. Automated anomaly detection is extremely useful in reducing the amount of data that must be manually processed by focusing attention on a specific portion of the data while ignoring vast amounts of irrelevant data.

The problem of anomaly detection, on the other hand, is open to a wide range of interpretations, and research efforts are dispersed not only in terms of approach, but also in terms of interpretation of the problem, assumptions, and objectives. By evaluating the problem formulations and solution methods used in anomaly detection research as applied to automated surveillance, this review will attempt to bring synergy to these disparate efforts. Anomaly detection is a subset of behaviour classification problems reduced to a two-class or one-class classification problem in automated surveillance. Sensors in an environment collect data representing the behaviour of surveillance targets in the anomaly detection in automated surveillance process, with some behaviours assumed to be anomalous. After that, the raw sensor data is subjected to a feature extraction procedure.

The resulting features are fed into a modeling algorithm, which employs a learning method to determine whether the observed behaviour is normal or abnormal. This project aims to detect and classify levels of high movement in the frame using various Deep Learning models. Videos are divided into segments in this project. In the event of a threat, a detection alert is raised, indicating the suspicious activities at a specific point in time. The videos in this project are divided into two categories: threat (abnormal activities) and safe (normal activities) (normal activities). Abuse, Burglary, Explosion, Shooting, Fighting, Shoplifting, Road Accidents, Arson, Robbery, Stealing, Assault, and Vandalism are among the anomalous activities we recognize. Individuals would be safer as a result of these anomalies.

Figure 1.1: CCTV Camera

Deep learning techniques are used to solve the existing problems, resulting in phenomenal results in the detection and categorization of activities. Two different neural networks were used in this study: CNN and RNN. The CNN is a basic neural network that is primarily used to extract advanced feature maps from recorded data. The complexity of the input is reduced by extracting high-level feature maps. A pre-trained model is chosen because modern object recognition models take into account a large number of parameters and thus require a significant more amount of time to fully train. The approach of transfer learning, would improve this task by first considering the previously learned model for a set of classified inputs, such as Image Net, which can then be re-trained using new weights assigned to various new classes. The RNN receives the output of the CNN as input. The RNN also has the ability to predict the next item in a sequence. As a result, it primarily serves as a forecasting engine.

The motivation for using this neural network in this work is to provide meaning to the captured sequence of actions/movements in the recordings. The primary layer of this network contains an LSTM cell, which is followed by some hidden layers with appropriate activation functions, and the output layer provides the final classification of the video into the 13 groups (12 anomalies and 1 normal). This system's output is used to perform real-time surveillance on various organizations' CCTV cameras in order to avoid and detect any suspicious activity. As a result, the time complexity is greatly reduced. The basic procedure for crime detection using video surveillance is shown in fig. 1. Crime detection in video surveillance is difficult, so data mining method was used to analyze the crime. For preventing the crime, object tracking is important if the interloper handled any weapons, the video surveillance camera is automatically detected. By using this technique, the prevention of crime is the easiest task. Machine learning and deep learning methods are used to identify crime. Detection of an object is also a challenging task, and it plays a major role in crime identification. In object detection, there are

three stages; they are differencing the frame, optical flow, and background subtraction. The background subtraction is

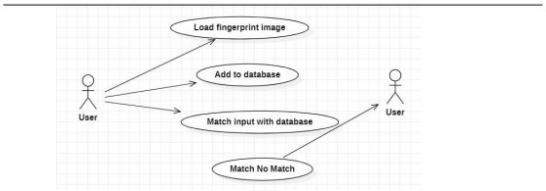

Figure 1.2: Crime Detection using Video Surveillance

II.EXISTING SYSTEM: Clustering is a kind of structure training and is an exploratory data exploratory statics finding process. The Clustering Technique was helped to grouping the data into clusters by using different techniques. It plays a major role in data mining and analysis. Rasoul Kiani et al. presented a paper based on the clustered crime that happened during various years. For improving, outlier detection Genetic Algorithm was used by the Rapid Miner tool. As a result, to determine the effect and quality, the maximized and non maximized parameters were matched. In the past few decades, the spotting and hampering of crime required years of research and inspection. The most widely used K-mode algorithm is a failure clustering method. To address this issue, the fusion of K-modes and Elephant Herding Optimization (EHO) was developed by Farhad et al.. As a result, the proposed model shows purity inaccuracy. The comparison chart of the proposed method and K-Mode algorithm based on their precision and purity. Nowadays, in the field of crime detection, various researches are going on, and there is no advanced technology till now. To control the crimes, CCTV's are commonly used in the surroundings, but still, there is nothing improved in controlling crimes. To address this issue, Umadevi V et al. proposed the Intension Of crime detecting program. It detects the crime in cameras and alerts the organizer to take perspective action. The already trained model VGGNet19 was used in this proposed system to detect the crime intention. An algorithm used to draw the square box over the suspecting images is Fast Regional based Convolutional Neural Network (RCNN and RCNN), and it is well known as Faster RCNN.

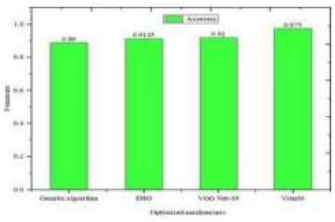

Figure 2.1: Accuracy of Combined optimization mechanisms

III.PROPOSED SYSTEM: The proposed model highlights a detailed specification that is used to detect the suspicious activity.

Archives of crime rate are increasing quickly. As a human it is very hard to keep an eye at every place on earth for preventing these crime activities. Hence, we tend to square measure proposing our model wherever the formula is trained for detecting suspicious activity by deep learning technique. Pre-trained deep convolution neural network, Spatio Temporal Auto Encoder are used for initial classification and a recurrent neural network is used for final detection of suspicious activity. And is performing well with upper accuracy. The flow diagram of the projected model is shown within the below figure.

3.1 Basic flow-chart of proposed design

The Methodology that we used is clearly described in this section. Firstly, live video feed is given to the system, which is obtained from CCTV. The video is then converted into frames with a fixed and small interval of time (say 1 frame per second). These frames are passed to spatio temporal auto encoder, which is based on 3D convolution network. The encoder part extracts 21 the spatial and temporal information, and then the decoder reconstructs the frames. The abnormal events are identified by computing the reconstruction loss using Euclidean distance between original and reconstructed batch.

This section is then utilized to determine the final classification. Collections of these frames are used to classify the live CCTV feed. The singly merged feature map is given as input to 3D-CNN. In this methodology we established an LSTM cell so that the training time becomes small. This 3D-CNN is trained with UCF-Crime dataset. UCF-Crime dataset is taken from Kaggle. UCF-Crime dataset consists of 1900 clips each of with sixty to six hundred seconds in length with variable resolution and is recorded with surveillance cameras that operate in real world. This dataset is intended to detect 13 genuine abnormalities, such as cruelty, imprisonment, fires, attack, crash, robbery, eruption, combat, theft, killing, theft, snatching, and vandalism. At last Soft max layer is used to determine the probilistic classification. Based on this an alarm is raised if suspicious activity is detected.

IV.RESULTS: To simplify the user interaction with the model, a simple web page is developed which provides the direct access of the overview. Whenever the model is run it automatically activates to a window as shown in the figure.

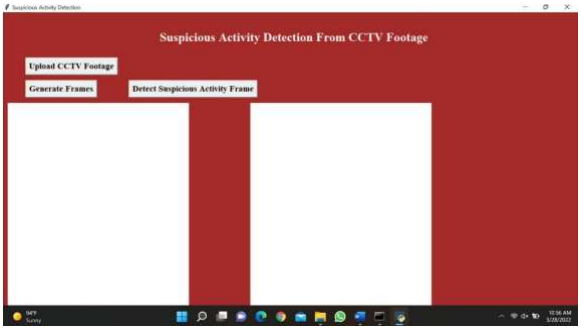

Figure 4.1: Upload CCTV footage

Using upload CCTV footage button the desired video or live video can be uploaded and generate frames button start the model, which the initial step of generating frames can be done.

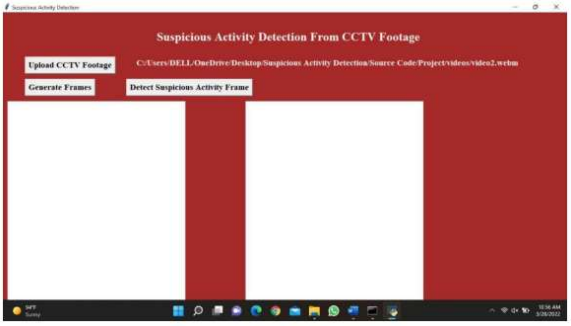

Figure 4.2: Footage uploaded

Now by clicking detect suspicious activity the model starts its execution.

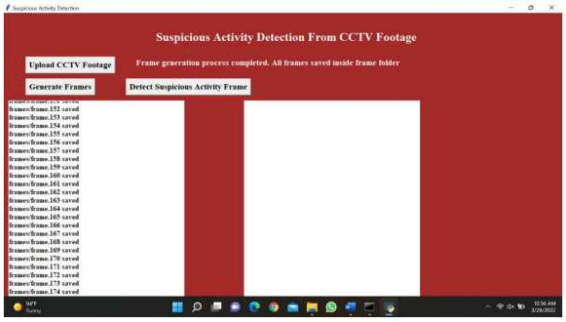

Figure 4.3: Frames generated

Figure 4.4: Suspicious activity frames are detected

The below figure is detected as suspicious activity frame by the model and it can be clearly seen that there is a man with face mask trying to steal.

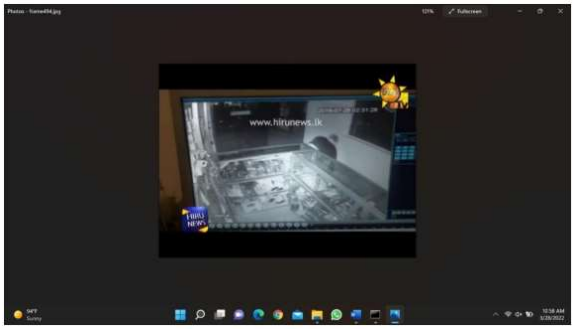

Figure 4.5: Suspicious activity frame

V.CONCLUSION: The detection of suspicious behavior has become increasingly important in recent years due to the daily rise in crime. This experiment has led us to the conclusion that we can use Deep Learning techniques to identify suspicious activity occurring around us. Before putting this research forward, we encountered numerous approaches that did, in fact, result in a highly realistic model. The approaches we encountered are discussed in length and thoroughly examined to determine their

benefits and drawbacks. Since not all activities are identified, this suggested strategy has a lot of room for improvement in the future. Therefore, it may be enhanced such that it can identify any kind of activity from the live CCTV footage that is presented.**REFERENCES:**

[1] Guruh Fajar Shidik, Edi Noersasongko, Adhitya nugraha , Pulung andono, Juanto, and Edi jaya kusuma, "A Systematic Review of Intelligence Video Surveillance: Trends, Techniques, Frameworks, and Datasets" IEEE ACCESS (Volume: 7), Dec 2019.

[2] Ali bou nassif , (Member, IEEE), Manar abu talib , (Senior Member, IEEE), Qassim nasir, and Fatima Mohamad dhakalbab, "Machine Learning for Anomaly Detection: A Systematic Review" IEEE ACCESS (Volume: 9), Jun 2021.

[3] Waqas Sultani , Chen Chen , Mubarak Shah, "Real-world Anomaly De- tection in Surveillance Videos" Cornell university papers, Feb 2019.

[4] Angela A. Sodemann, Matthew P. Ross, and Brett J. Borghetti, "A Re- view of Anomaly Detection in Automated Surveillance" IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) (Volume: 42, Issue: 6), Nov 2012.

[5] Karishma Pawar and Vahida Attar, "Deep learning approaches for video- based anomalous activity detection" World Wide Web CrossMark, Apr 2018.

[6] Maria Valera and Sergio Velastin, "Intelligent distributed surveillance systems" IEEE Xplore, IEE Proceedings - Vision Image and Signal Processing 152(2):192 – 204, Oct 2021.

[7] https://cloud.google.com/tpu/docs/inception-v3-advanced

[8] Christian Szegedy, Vincent Vanhoucke, Sergey Ioffe, Jonathon Shlens, Zbig- niew Wojna, "Rethinking the Inception Architecture for Computer Vision" In Google Research, 2015.

[9] Ming Cheng, Kunjing Cai, Ming Li, "RWF-2000: An Open Large Scale Video Database for Violence Detection", slack, Nov 2019.

[10] W. Sultani, C. Chen, and M. Shah, "Real-world anomaly detection in surveillance videos," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2018, pp. 6479–6488.

[11] Shipra Ojha and Sachin Sakhare. "Image processing techniques for object tracking in video surveillance-A survey". In: International Conference on Pervasive Computing (ICPC). IEEE (2015)