International Conference on Neural Nexus and Synergy:Innovation in Emerging Technologies
Vol. 1. (2024).PP.191-198. SNIST

SUSPICIOUS ACTIVITY DETECTION

[1]Kanchanapally Keerthi, [2]Kadari Sreeya,[3]Racharla Abhinaya,[4]Budidha Malathi

[1,2,3,4] Department of CSE, Sreenidhi Institute of Science and Technology,

ABSTRACT: Providing observation security is a very boring and time-consuming job. Determining if the captured workouts are unusual or questionable necessitates a labor force and their constant consideration. Here, we will build a system to automate the task of analyzing video reconnaissance. We will continually monitor the video stream in order to identify any unusual workouts, such as those that seem shocking or questionable. There have been advancements in profound learning computations for profound reconnaissance since the prior interactions. These advancements have demonstrated a basic pattern in in-depth reconnaissance and ensure a significant increase in efficacy. Profound observation is typically used for burglary evidence differentiation, cruelty detection, and explosion potential identification.

We will introduce a spatio worldly autoencoder for this project, which relies on a 3D convolution.

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

I.INTRODUCTION: At this moment, there are a lot more offensive actions occurring more frequently. Detecting and preventing them is now more crucial than ever due to their increase. Security cameras are being used in public spaces more and more. Video files are produced in bulk and kept on file for a while. Since continuous monitoring and a huge crew are needed, it is virtually difficult for authorities to maintain track of these surveillance footage and determine whether the instances are suspicious. High-precision automation of this process is therefore becoming more and more in demand. Identifying the frame being used is also necessary. Additionally, pinpoint the areas that have the odd activity as this helps determine the strange activity's cause more quickly.

On the other hand, there is much room for interpretation when it comes to the anomaly detection problem, and there is a wide range of approaches, assumptions, and goals among the research efforts. This review aims to bring these various efforts together by analyzing the issue formulations and solution techniques employed in anomaly detection research as applied to automated surveillance. In automated surveillance, anomaly detection is a subset of behavior classification issues that are condensed into two- or one-class classification issues. An environment's sensors gather information on the actions of surveillance targets with the purpose of automatically detecting anomalies in surveillance processes, with certain actions presumed to be abnormal. Following that, a feature extraction process is used to the unprocessed sensor data.

The final features are fed into a modeling system that uses a learning technique to identify if the behavior being seen is typical or deviant. The goal of this research is to use multiple Deep Learning models to identify and categorize high movement levels in the frame. This project uses segments to organize videos. When there is a threat, a detection alert is triggered, revealing the questionable activity over a particular period. Two categories—threat (abnormal behaviors) and safe (regular activities)—are used to group the movies in this research. Among the unusual behaviors we identify are abuse, burglary, explosion, shooting, fighting, shoplifting, car accidents, arson, robbery, theft, assault, and vandalism. People would feel safer because of these abnormalities.

Figure 1.1: CCTV Camera

The study employed two distinct neural networks, CNN and RNN. CNN is a basic neural network that is primarily used to extract advanced feature maps from recorded data. By extracting high-level feature maps, the complexity of the input is reduced. A pretrained model is chosen because modern object recognition models take into account a large number of parameters and thus require a significant amount of time to fully train. Deep learning techniques are used to solve the existing problems, leading to phenomenal results in the detection and categorization of activities. By initially taking into account the previously taught model for a set of categorized inputs, such as Image Net, the transfer learning technique would enhance this job. The model may then be retrained using fresh weights given to various new classes. The CNN's output is sent into the RNN as input. The following item in a sequence may also be predicted by the RNN. It functions essentially as a forecasting engine as a result.

The purpose of this study is to provide meaning to the recorded sequence of motions and activities by utilizing a neural network. An LSTM cell is present in the network's primary layer. A few hidden layers with suitable activation functions come next, and the output layer offers the final categorization of the video into the 13 categories (12 anomalies and 1 normal). The output of this system is utilized to monitor CCTV cameras in different companies in real-time to look for and identify any suspicious activities. The temporal complexity is therefore significantly decreased.Figure 1 depicts the fundamental process for employing video surveillance to detect criminal activity. Since it is challenging to discover crimes using video surveillance, the crime was analyzed using a data mining approach. Object tracking plays a critical role in crime prevention since it immediately detects any weapons handled by the intruder and activates the security camera. The easiest goal is to prevent crime by employing this strategy. Crime is identified using deep learning and machine learning techniques. Identifying objects is a difficult activity that is essential to the investigation of crimes. There are three steps in object detection: background removal, optical flow, and frame differentiation.

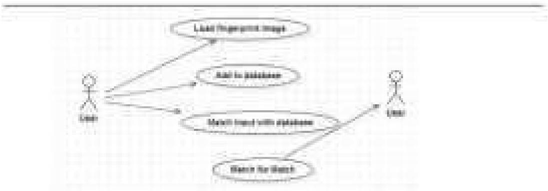


Figure 1.2: Crime Detection using Video Surveillance

The moving front portion is removed from the original environment by using the background subtraction technique. The final step in the crime detection procedure is facial utterance identification, which recognizes the criminal's face from pictures or videos. The analysis of the offender takes longer, but the offense is accurately detected. The process of face detection involves matching a person's face, either by itself or in a crowd. The suggested technique used video monitoring to identify the crime. The survey was based on video surveillance utilized for criminal detection, and this article will discuss the various literature studies of the researchers. It provides a comprehensive explanation of crime detection and the challenges that law enforcement agencies encounter.

II.EXISTING SYSTEM: Clustering is an exploratory data exploratory statics discovery procedure and a type of structure training. By employing several strategies, the Clustering Technique assisted in organizing the data into clusters. In data mining and analysis, it is crucial. A study based on clustered crimes that occurred across a range of years was given by

Rasoul Kiani et al. The Rapid Miner tool employed the Genetic Algorithm for outlier detection in order to improve.

As a consequence, the maximized and nonmaximized parameters were matched to ascertain the effect and quality. In the last several decades, it took years of investigation and examination to identify and impede criminality. A failure clustering technique is the K-mode algorithm that is most frequently employed. To solve this problem, the combination of K-modes and Consequently, the suggested model has purity error. The precision and purity comparison chart between the K-Mode algorithm and the suggested technique. There is currently no cuttingedge technology in the subject of crime detection, however several studies are being conducted in this area. CCTVs are frequently deployed in the neighborhood to reduce crime, yet crime control remains unchanged. Umadevi V. et al. suggested the Intention Of crime detection software as a solution to this problem. When a crime is detected by cameras, it notifies the organizer to take appropriate action. This suggested solution employed the previously trained VGGNet19 model to identify the purpose of the crime.One method that is commonly referred to as Faster RCNN is Fast Regional based Convolutional Neural Network (RCNN and RCNN), which is used to create the square box over the suspicious pictures.

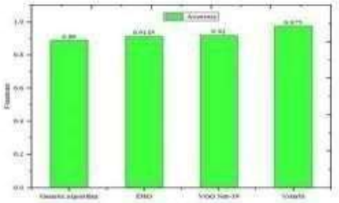
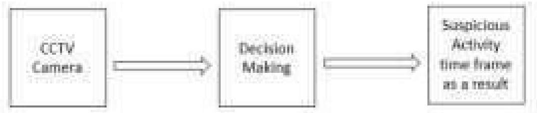


Figure 2.1: Accuracy of Combined optimization mechanisms

The suggested VGG19 is therefore more accurate in identifying the purpose of a crime. Additionally, as a result of the layer increase, the VGG-19 connects and the rate of accuracy improvement decreases. Many scholars have proposed the data mining method—which uses a variety of algorithms—for identifying crimes during the past few decades. They employ ANNs and Forest Decision Trees (DTs) for categorization. Reem Razzaq Abdul Hussein et al. created two additional couplings in order to get around this.

The Viterbi and Baum Welch algorithms were integrated in two steps: first to estimate the crime scene; and second, to detect the crime. This solution presented integrated the DT and Viterbi algorithms. It takes less time and provides precise forecasts as a consequence. A hybrid deep learning algorithm and neural networks are used in a solution for video flow file identification that was proposed by Sharmila Chackravarthy et al. This technique is employed to examine the offender swirl and reduce workloads. The outcome demonstrates that it is effective and appropriate for identifying crimes.

III.PROPOSED SYSTEM: A thorough specification that is utilized to identify suspicious activities is highlighted in the suggested model. The crime rate is rapidly rising, according to archives. It is quite difficult for humans to monitor every location on Earth in order to stop these criminal actions. Therefore, we often propose our approach in cases where the deep learning technique has been used to train the formula for identifying suspicious activities. A recurrent neural network is employed for the final identification of suspicious behavior, while a pre-trained deep convolution neural network and Spatio Temporal Auto Encoder are utilized for the initial categorization. and is operating at a high level of precision. The predicted model's flow diagram may be seen in the image below.



3.1 Basic flow-chart of proposed design

This section provides a detailed description of the methodology that we employed. First, A live video feed that is received from CCTV is sent into the system. Next, the video is divided into frames at a predetermined, brief interval of time (let's say one frame per second). The spatiotemporal auto encoder, which is based on a 3D convolution network, receives these frames. The decoder then reconstructs the frames after the encoder portion collects the temporal and spatial information. By calculating the reconstruction loss using the Euclidean distance between the original and rebuilt batch, the aberrant events are found. The final categorization is then determined using this section. The live CCTV stream is classified using sets of these frames. The 3D-CNN receives the single merged feature map as input. To reduce the training time, we built an LSTM cell in this manner. The UCF-Crime dataset is used to train this 3D-CNN. The UCF-Crime dataset may be found on Kaggle. The 1900 films in the UCFCrime dataset, each lasting between sixty and six hundred seconds and having a different resolution, were captured by realworld security cameras. The goal of this dataset is to identify 13 real-world anomalies, including assaults, robberies, snatchings, vandalism, attacks, crashes, robberies, eruptions, and thefts that result in death.

Lastly, the probilistic categorization is determined using the Soft Max layer. In light of this, if any suspicious behavior is found, an alarm is triggered.

IV.RESULTS: A straightforward web page that offers immediate access to the overview has been designed in order to streamline user engagement with the model. The model automatically opens in the window seen in the picture whenever it is executed.

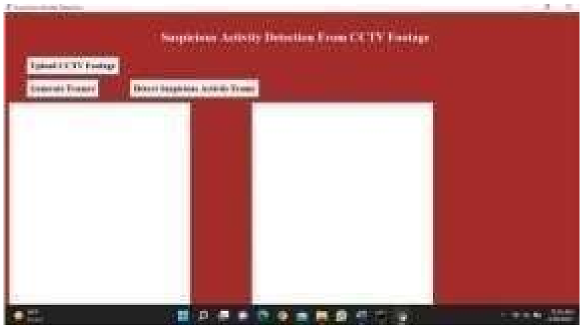

Suspicious Activity Detection From CCTV Footage
Upload CCTV Footage
Generate Frames
Detect Suspicious Activity Frames

Figure 4.1: Upload CCTV footage

The appropriate video or live video may be supplied using the upload CCTV footage button. The model can then be started, completing the first phase of producing frames.

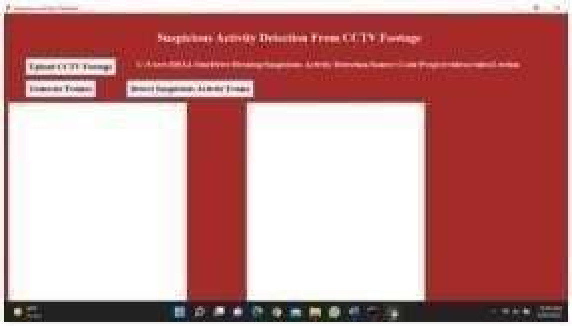

Suspicious Activity Detection From CCTV Footage
Upload CCTV Footage
Generate Frames
Detect Suspicious Activity Frames

Figure 4.2: Footage uploaded

Detect suspicious behavior now initiates the model's execution.

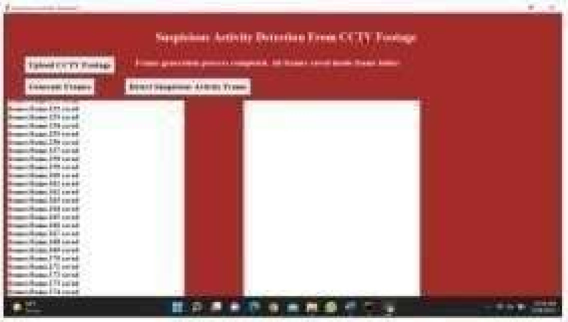

Suspicious Activity Detection From CCTV Footage
Upload CCTV Footage
Generate Frames
Detect Suspicious Activity Frames

Figure 4.3: Frames generated

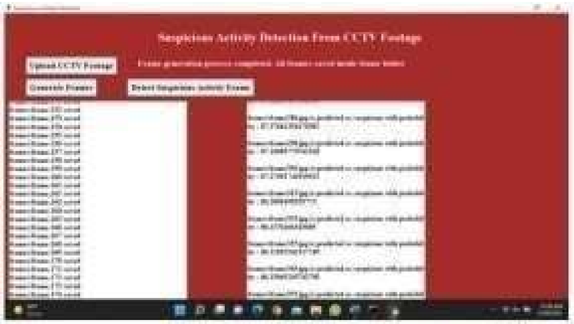

Suspicious Activity Detection From CCTV Footage
Upload CCTV Footage
Generate Frames
Detect Suspicious Activity Frames

Figure 4.4: Suspicious activity frames are detected

The model has identified the following figure as a suspicious activity frame. It is evident that a guy wearing a face mask is attempting to steal.

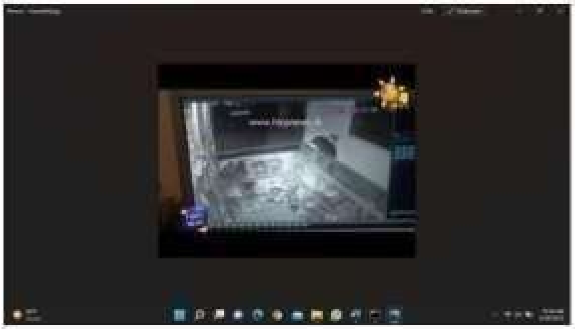


Figure 4.5: Suspicious activity frame

V.CONCLUSION: With the number of crimes rising daily in recent years, suspicious activity detection has become increasingly important. This experiment has shown us that we can use Deep Learning algorithms to identify suspicious activity occurring around us. Numerous approaches that we encountered before to submitting this project have in fact resulted in a highly accurate model. The approaches that we encountered are discussed in great detail and their benefits and drawbacks are extensively examined. Since not all types of behaviors are recognized, there will be more developments in this suggested strategy in the future. In order to detect all kinds of actions from supplied live CCTV footage, it may be enhanced.

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/inc ep tionv3-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, "Realworld 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)