BRENCH SUSPECT

Benedict Vinusha. V
Department of Artificial Intelligence and Data Science
R.M.K. Engineering College
Kavaraipettai – 601206. India.
bene20108.ad@rmkec.ac.in

Indhuja. V
Department of Artificial Intelligence and Data Science
R.M.K. Engineering College
Kavaraipettai – 601206. India.
indh20114.ad@rmkec.ac.in

Varshitha Reddy M
Department of Artificial Intelligence and Data Science
R.M.K. Engineering College
Kavaraipettai – 601206. India.
meda20121.ad@rmkec.ac.in

Nikhitha N
Department of Artificial Intelligence and Data Science
R.M.K. Engineering College
Kavaraipettai – 601206. India.
naga20123.ad@rmkec.ac.in

Mrs. R. Priyanka Pramila
Department of Artificial Intelligence and Data Science
R.M.K. Engineering College
Kavaraipettai – 601206. India.
rpp.ad@rmkec.ac.in

Abstract-The massive rise in criminal activity in urban and suburban regions and suspicious behavior in public places pose a considerable risk to peoples safety and social order so it is vital to minimize those activities previously monitoring of these activities was done manually by humans is a very strenuous task but now behavior recognition understanding and classifying the incredulous activity is possible with the help of artificial intelligence and deep learning concepts the main idea of the LRCN model is to combine CNNs and LSTMs to learn visual features from video frames and to transfer a sequence of image embeddings into class labels probabilities and sentences as a result this model has the benefit of both convolutional and recurrent neural networks this model uses the LRCN model with Keras and TensorFlow in python to categorize the events this model collects frames from the videos and compares them to trained models accessibility and high functionality make the model practically feasible in solving an ample number of cases with limited resources.

Keywords : Keras, Tensorflow, Long Term Recurrent Neural Network(LRCN), Neural Networks

I. INTRODUCTION

A.Problem Statement

Many innocent people got affected due to criminal activities that have threatened our daily lives and property. The way to prevent these kinds of events became a hot topic of great concern worldwide. Constant and manual monitoring of data by humans to judge if the activities are abnormal or not is a near-impossible task as it requires a workforce and their constant attention. Suspicious activity detection is an effective way to prevent or minimize these suspicious activities. So, This creates a need to automate the same. So our project is to classify human activity from CCTV footage using the LRCN model with Keras and TensorFlow in Python.

B.Objective

Our system objective is to identify suspicious and normal activities from the data. It is not easy for humans to determine the incredulous events manually. It is very time consuming and excruciating. Therefore, it is necessary to keep an eye out for activities to see if any need close examination. You should also look for early warning signs of attack severity and scope as you continue to filter, sort, and correlate events to see if you have enough evidence to take action, like tracking an incident formally or opening a formal investigation.Here, LRCN model is used suits for large-scale visualization. This method immediately converts a variable-length input to a map as output. They can simulate complicated temporal dynamics. A sizable video dataset serves as

the performance's context. Because of these actions, abnormal events can be minimized to some extent, leading to society's benefit.

C.Scope

This model will be favorable everywhere as it is a basic security measure. In today's world, CCTV surveillance is the most basic & impactful security feature premises can have. It. Bune is an academic campus with more than 100 CCTV in multiple buildings like Hostels, Classes, Canteen, Sports area, Auditorium, etc. Manual monitoring of all the events on the CCTV camera is impossible. Even if the event had already happened, searching manually for the same event in the recorded video wastes a lot of time. Our model would identify unusual activities from running CCTV streams on the basis of peculiar gestures and body movements and physical movements. So, this model will be beneficial to these situations, reducing human time and effort.

D.Highlights

- Identify abnormal activities and differentiate them based on various types of suspicious behaviors.
- This approach uses the LRCN model and combines the advantages of both convolutional and recurrent Neural networks.
- Greater accuracy.

II. LITERATURE SURVEY

In their approach [1], the authors proposed employing CNN for feature extraction and a discriminative deep belief network for action classification to identify suspicious behavior in surveillance video. Human activities are detected using the background subtraction method, seven-frame selection. The CNN receives 33 feature maps as input and outputs 128D features as a single vector. DDBN is the output format. Output is in DDBN form. Suspicious Human Activity Recognition from CCTV with the LRCN model [2] is a proposed system of the LRCN model with 4 CNN layers followed by an LSTM layer. The limitation of this system is the complexity of the model increased. The author's proposed work [3] on Unusual activity detection for video surveillance detects humans carrying or abandoning an object and segments the objects from humans tracked. The limitation of the system is poor accuracy. Suspicious Activity Detection from Videos using YOLOv3 [4] proposed system the processing time is concerned for one image detection, YOLOv3 outperforms Faster R-CNN. The drawback of the system is current feature extraction method gives accurate results if and only if a controlled environment is present. Eamthanakal et al. [5] used the background subtraction method for computation. The median filter removes noise. The system used an image processing technique to analyze a traffic condition. It detects how many objects or cars are on the road. Ahmad Salihu et al. [6] Suspicious Human Activity Recognition for Video Surveillance System Sanjay Kumar Singh, Ben-Musa, and Prateek Agrawal used SURF (Speed Up Robust Features) to extract points and detect features. This method has low accuracy when the rotation angle is too great and a high dimension of feature descriptor. Rachana Gugale and Abhiruchi Shendkar et al. [7] proposed a system for detecting human suspicious activities using deep learning and CNNs (convolutional neural networks), and they compared the systems' accuracies. When more training data is required, it is challenging to infer patterns from various spatial situations. It has regularly been employed for time-series data processing, prediction, and classification, the Deep Convolutional Framework for Abnormal Behavior Detection in a Smart Surveillance System by Kwang-Eunko and Kwee-Bo-sim uses LSTM (Long Short Term Memory). A technique for detecting suspicious activities utilizing YOLO3 and crowd density analysis [8] by Shriya Akella, Priyanka, and Vinit Agrharkar. This technique provides thorough information on population density and behavior and facilitates large-scale detection suitable for crowded places. However, it has a high localization error and recall. J.A. Freer and B.J. Beggs proposed a system [9] for automatic intrusion detection. Its construction makes use of digital processing and object identification techniques. Images are processed to obtain information that computers can understand. The density and contrast of the image's pixels can be changed as desired. It costs a lot and takes more time. The authors proposed system [10] improves the recognition rate for suspicious objects. The system's importance lies in its ability to enhance the performance of AI-based W-band incredulous object identification systems for moving people. Miwa Takai et al. [11] method pinpoints the detecting point of suspicious activity and finds the degree of risk of suspicious activity so that the observer can lessen the

physician and mental burden in monitoring. Basha et al. [13] used the CNN-DBNN algorithm for detecting suspicious human activity and acquired for detecting human activity and acquired accuracy of 90%. The foundation subtraction method is to identify the human population after seven cases are selected, each of which found a larger boundary box for it. Nipunjita Bordoloi and Anjan Kumar Talukdar et al. [14] proposed a system for Suspicious Activity detection Using YOLO3 covers the entire image. Though it is quick and precise, the accuracy of the feature extraction requires additional training time. Satyajit Loganathan and Gayashan Kariyawasam et al. [15] Suspicious Activity Detection in Surveillance Footage recommended deep neural network models with computer vision. In surveillance footage, this model may spot probable gun-related crimes and cases of abandoned luggage. The main issue is that it only focuses on those two actions, not all suspicious behaviors.

III. RELATED WORK

Suspicious Activity detection using LRCN Model

Suspicious activity detection model was constructed by using the LRCN model based on Keras and Tensorflow library in python. LRCN model incorporates both CNN and LSTM for better understanding and classification of data, especially videos for image and video description. This technique includes the following steps:

- Gathering visual data.
- Using CNN to extract visual features
- Sequential learning with LSTM
- Making predictions.

So, the LRCN model follows the above steps to state predictions on suspicious activities.

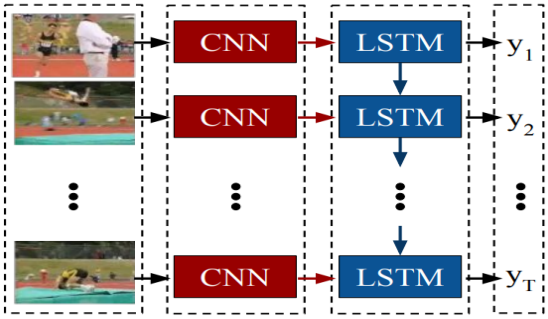

Fig 1. Combination of CNN and LSTM

A. Taking Visual Input

At first videos, Activity or an image is taken as input for visualizing and captioning them.

B. Extracting Visual Features through CNN

CNN helps by creating an interactive visualization that shows the similarity between the features of two images at any given layer of a network. The procedure is as follows.

- The video is separated into different frames.
- Perform a forward pass on each image to extract the features at the desired network layer
- Create an invisible grid overlay on each image where the number of cells is equal to the dimension of the extracted features
- Select a grid square from img1 and calculate the similarity of that feature to all possible feature locations in img2

C.Sequential learning using LSTM

A predictive modeling problem known as sequence classification involves a sequence of inputs that spans either space or time. The task is to predict a category from the stream useful for viable predictions.

D.Algorithm

A class of models known as LRCN is deep both temporally and spatially. It employs an LSTM (decoder) to produce natural language strings and a ConvNet (encoder) to encode deep spatial state vectors.

- At each timestep, ConvNet is unbiased and time-invariant.
- It provides concurrent training across all input timesteps.
- It is unaffected by batch processing.

Modeling of sequential data with mutable lengths is possible with LSTM. LRCN architecture takes a sequence of T inputs and generates a stream of T outputs.

Long Short-Term Memory Network(LSTM) is an advanced RNN, a sequential network, that allows information to hold out. It can solve the RNNs' vanishing gradient issue. Persistent memory implemented using an RNN, recurrent neural network.

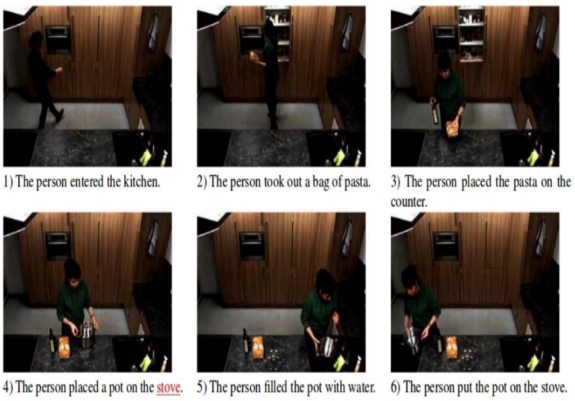

Fig 2. Video Captioning

LRCN for video captioning:

Sequential Input < X1, X2, X3,...,Xt > (A inputs)

Sequential Output {Y1, Y2, Y3,…,Yt' } (A' outputs)

An "encoder-decoder" strategy adopts varying input and output.

The function of an encoder is to map the input sequence to a fixed-length vector.

The role of the decoder is to produce successive outputs of any length by unrolling this vector. In this approach, input and output timesteps A+ A' take the entire system into account.

Using the MAP of a CRF, a semantic representation of the video is obtained. Encoder-decoder LSTM architecture is used to transform it into a phrase.

A comparison is made between LSTM and an SMT-based method for video description.

Simpler decoder architecture achieves better performance than BLEU-4 scores.

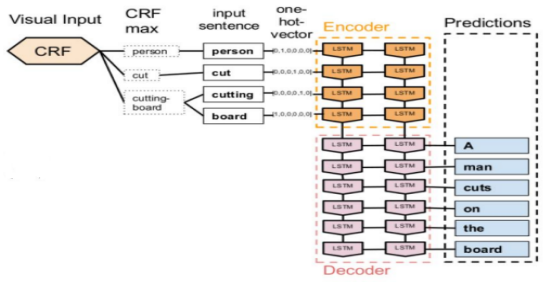

Fig 3: Working

MODEL DEVELOPMENT:

In the real world, there are many uses for human behavior recognition, such as clever video monitoring and the study of consumer behavior. Video surveillance has numerous applications, especially in indoor and outdoor situations. An essential component of security is the surveillance process. Security cameras are currently necessary due to the demand for safety and security. The recommended system will use CCTV footage to monitor people's behavior on campus and provides a friendly warning when anything unusual occurs. Recognizing human activity is one of the core aspects of intelligent video monitoring. In our model, The varying-length visual input is processed by the LRCN using a CNN. In addition, their outputs are served into the LSTM, a stack of recurrent sequence models in the picture. The final result of the sequence models is a variable-length prediction. The LRCN becomes a suitable model for addressing these tasks when dealing with time-varying inputs and outputs, such as activity recognition, image captioning, and video description. The picture below displays task-specific LRCN model instantiations for each task. The model accurately detects the crime committed sequence from the complete footage and shows it as the outcome.

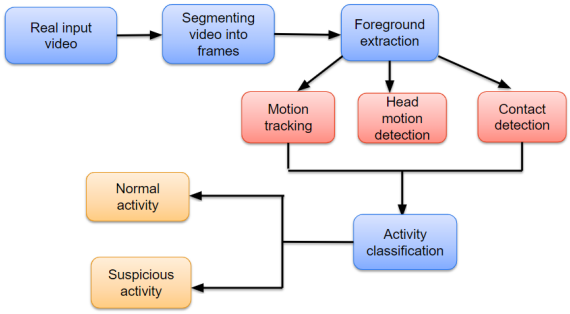

Fig 4: Architecture

IV. FUTURE WORKS

According to our findings, future work on this project involves evaluating various designs and comparing them to increase the speed of forecasts for weapons. To allow for future studies on how to improve the detection of guns in real-time, Due to concerns about time and resource constraints, we were only able to advance the research to the point mentioned in this report. To improve real-time detections, it could also be a good idea to explore the addition of components other than surveillance film. Since the method used in this study for detecting abandoned luggage does not address issues such as item detection in unexpected changes of brightness, more research can be done on this subject to progress the area.

V. CONCLUSION

We have discussed the various methods for foreground object extraction, tracking, feature extraction, and classification related to fire detection, violence detection, theft detection, falling detection, accidents, illegal parking detection, and abandoned object detection. To decrease false object detection, various researchers put out unique ways with noise removal, light handling, and occlusion handling techniques in previous decades. Numerous research projects have been made to develop a real-time intelligent surveillance system, but the processing speed of the video frames is not adequate. No mechanism has developed that has 100% detection accuracy and 0% false detection rate for movies with complex backdrops. The following suspicious activity detection tasks need considerable attention: Theft detection and abandoned object detection. The majority of the work has been done to identify abandoned objects in surveillance footage shot by stationary cameras

.

VI. REFERENCES

[1] Alert Age on Location of Dubious Action Utilizing Move Learning (eleventh global gathering on figuring, correspondence, and Systems administration Technologies(ICCCNT) At Kharagpur, India.

[2] Profound Gaining Approach for Dubious Movement Recognition from reconnaissance video(C.V Amrutha, C.Jyotsna,j.Amudha.

[3] Crime action Discovery Utilizing machine learning(Ravinarayana B, Shakhin M, Shetty Pooja, Shreya Shetty, Yashodha Amberg)

[4] Illicit Movement Recognition in Enormous Scope Dim and Hazy Web Social Networks(Dhara Shah, T.G. Harrison, Christopher B. Freas, David Maimon, Robert W. Harrison)

[5] Inspection of dubious human movement in the publicly supported regions caught in reconnaissance cameras(P.Bhaya Divya, S.Shalini, R.Deepa, Baddeli Sravya Reddy).

[6] Unusual movement discovery for video observation by Rajat Singh, Pravesh Vishwakarma, Anupam Agrawal, M.D Tiwari.

[7] suspiciousness Movement Recognition in reconnaissance video utilizing segregation profound conviction network by Elizabeth Scalia, aby abahai t.

[8] Secure reconnaissance Structure for IoT framework utilizing probabilistic picture encryption by khan Muhammad, Rafik hamza.

[9] Crowd thickness examination and dubious movement recognition (2020 global gathering for advancement in innovation).

[10] A novel calculation to anticipate and identify dubious ways of behaving of individuals in open regions for observation cameras. (2017 global meeting on wise economical frameworks)

[11] Human dubious movement recognition utilizing outfit AI techniques(2022 shrewd technologies(CONIT), global gathering on).

[12]Recognition of dubious human exercises involving KLT and Kalam Channel for ATM Reconnaissance Framework. (2021 worldwide gathering on (ICIPTM)

[13] Study on video Surveillance System for object detection and tracking(3rd International Conference on “Computing for sustainable global development.

[14]Smart CCTV surveillance System for intrusion detection(International Conference on electronics and electrical circuits 2020)

[15]suspicious activity detection in surveillance video using a discriminative deep belief network(international journal of control theory and applications).