www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 10, October 2023, pp : 169-172

e-ISSN : 2583-1062

Impact Factor : 5.725

AUTOMATIC THREAT RECOGNITION USING SURVEILLANCE CAMERA

Arun Prasath. S[1], Alex. J[2], Guru Ganesh. S[3], Dr. T. Vijay Anand[4], Mr. K. Subramanian[5]

[1,2,3,4,5]Department of ECE, National Engineering College, India.

ABSTRACT

The government has stated that SMART cities are crucial for the prosperity of our country. Cities that are SMART change social norms. cleanliness, traffic control, surveillance, monitoring and identifying human activity, contemporary infrastructure, and upgrading public amenities. CCTV camera installation in homes and workspaces is now typical in order to monitor human activity. Camera recordings needed to be stored on hard drives, and viewing the pictures was necessary to detect movement. Overall, it is an inactive strategy. Event detections are found after the event has already happened and had an impact. Event detection is essential for understanding the situation dynamically and taking effective action. These security cams cannot be consistently watched over by humans. It requires the workforce and their constant attention to determine whether the documented actions are anomalous or suspicious. As a result, this flaw is fueling demand for this operation's highly precise automation. Additionally, in order to determine whether the strange behavior is suspicious or atypical more quickly, it is essential to pinpoint which frames and segments of the recording contain the odd activity. The suggested project uses 80:20 of the specified input data for training and testing, respectively. The test findings are as follows: Validation precision of 99.96% and Validation cost of 2.7%.

1. INTRODUCTION

In order to ensure people's security, public spaces like shopping malls, streets, banks, etc. are progressively being outfitted with CCTVs. Because of this difficulty, a very accurate computerization of this system is now necessary. Since it is nearly impossible for people to constantly monitor these security cameras. To determine whether the recorded activities are aberrant or suspicious demands the workforce and their constant attention. Consequently, this shortcoming is driving demand for highly accurate automation of this operation. Additionally, it is necessary to show which frames and sections of the tape include the unexpected behavior in order to make a quicker determination of whether or not it is unusual or suspicious. It is nearly hard for people to continuously monitor these security cameras. For workers to determine if the recorded behaviors are aberrant or suspicious, they must pay close attention at all times. This disadvantage makes it necessary to automate this operation with great precision. Furthermore, it is necessary to show which frames and sections of the video include the unexpected behavior in order to make a quicker determination of whether or not it is unusual or suspicious. the danger is dynamically identified.

2. LITERATURE REVIEW

Title of the paper	Author	Inference
Real-Time Anomaly Recognition Through CCTV Using Neural Network"	Virender Singha, Swati Singha,	This study offers a method for identifying deviations from the standard in actual CCTV footage. It might not be possible to identify anomalies in these recordings using only the usual data. Therefore, both normal and anomalous videos have been taken into consideration in order to manage the complexity of these realistic anomalies, which has increased the model's accuracy.
"Deep Automatic Threat Recognition: Considerations for Airport X-Ray Baggage Screening"	Kevin J Liang	Here, they looked into the application of cutting-edge methods for the difficult job of threat detection in bags at airport security checkpoints. First, we gathered a large quantity of data by manually putting together numerous bags and bins to represent typical traffic. These hid a broad range of dangers. Each bag was scanned to create X-ray images, and both scan perspectives were annotated. Then, using the data that had been gathered, we trained a number of contemporary object recognition algorithms, investigating various settings and engineering them for

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 10, October 2023, pp : 169-172

e-ISSN : 2583-1062

Impact Factor : 5.725

		the task at hand.
"A CNN-RNN Combined Structure for Real-World Violence Detectionin Surveillance Cameras"	Soheil Vosta, Kin Choong yow	Here, they looked into the application of cutting-edge methods for the difficult job of threat detection in bags at airport security checkpoints. First, we gathered a large quantity of data by manually putting together numerous bags and bins to represent typical traffic. These hid a broad range of dangers. Each bag was scanned to create X-ray images, and both scan perspectives were annotated. Then, using the data that had been gathered, we trained a number of contemporary object recognition algorithms, investigating various settings and engineering them for the task at hand.

3. METHODS

Input Video datasets are converted into image frames using a Python script, then given as input. Pre-processing The "label-img" program was used to annotate the images after the datasets were retrieved as frames. The selected region of the photos will be encoded, and the encodings and attributes will be saved in an XML file. With no context information stored and only the object credentials, we used a polygon entity to identify objects. TRAINING The data that have been encoded above are given to the transfer learning model as inputs. The supplied data will be trained, and during real-time detection, a file called an engine will be generated and run**.** The Vott, A Microsoft-Approved Open-Source Tool, Is Used To Educate The Data. Retrained Records From The Vott Have Been Used. Transfer Learning Is The Process Of Retraining And Distributing Pre-Existing Datasets From A Network. Used Model For This Undertaking, The Mobile Net Ssd (Single Shot Detector Architecture) Model Has Been Selected. The Pytorch Framework Is Used Here To Train For Data Labeling Because It Is A Lightweight Model. Improve Reliability And Epoche: In This Structure, Only The Lowest Layer Is Dynamic; The Layers Above It Are Locked. Epochs: The Number Of Epochs Indicates How Many Times Our Dataset Has Been Processed. After A Predetermined Number Of Epochs, It Enters A Stage Of Absorption, And Training Is Complete At This Point After A Predetermined Amount Of Time. 250 total groups will be created if there are 1000 total datasets and a back size of 4. The number of batches into which the datasets are split is indicated by the back size. Since there are more groups when the back size level is raised, accuracy rises because it won't matter if one or two photos among the rest aren't accurate. There aren't many different back measurements either. DEPLOYMENT: We will have a Pytorch model after training, but it won't be very helpful when used with OpenCV. and cannot provide the necessary precision. We first translate it into the Onnx format and then into the Tensor Arc engine in order to execute it. Operating it has the benefit of optimizing the process because it is dependent on the device and is being executed in engine format. and it performs in line with the characteristics of the equipment. such that accuracy is not sacrificed and frames don't lag

4. METHODOLOGY

Recurrent and convolutional neural networks are combined in the design of the anomaly detection system. The first neural network, convolutional, was used to acquire the high-level feature maps of the images. The input of the second neural network will be simpler as a consequence. We are utilizing the inceptionV3 pre-trained algorithm from Google. This model uses transfer learning, a common object identification approach. This has a number of traits, and it might take a while to completely train. Transfer learning streamlines a lot of this work by using a model that has already been learned. Before being retrained for new classes, the model is trained for the weights of current classes, such as ImageNet. To deduce meaning from the sequence of behaviors seen in a specific frame, the second neural network is used as a recurrent neural network. Using this methodology, the components of videos will be classified as either secure or dangerous.

Data Analysis

We create our own Video datasets using a Python script, which are then converted into picture frames. The ruined photos were then taken out before selecting which ones to annotate. The images were then annotated using the "label-IMG" and "vott" Applications. With the encodings and attributes for the Selected area of the photos, an XML file will be generated and saved. We used a polygon entity and the Pascal VOC format for object recognition in order to remove the backdrop information and only save the object credentials.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 10, October 2023, pp : 169-172

e-ISSN : 2583-1062

Impact Factor : 5.725

5. RESULTS AND DISCUSSIONS

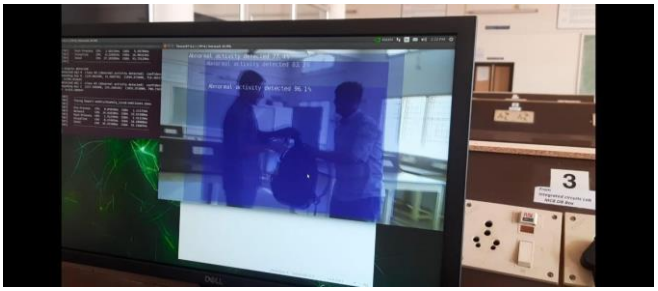

Fig.1. Real-Time Detection

The real-time event detection of our model is depicted in the above image. A person attempting to steal a person's bag is identified as an anomaly. 96.1% of the time, abnormal activity is accurately identified.

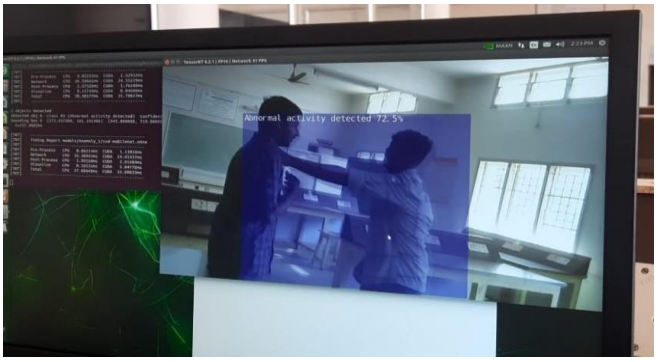

Fig.2. Real-Time Detection

The real-time event detection of our model is depicted in the above image. The detection of an anomaly is two people battling. The detection of abnormal behavior is accurate to within 72.5%.

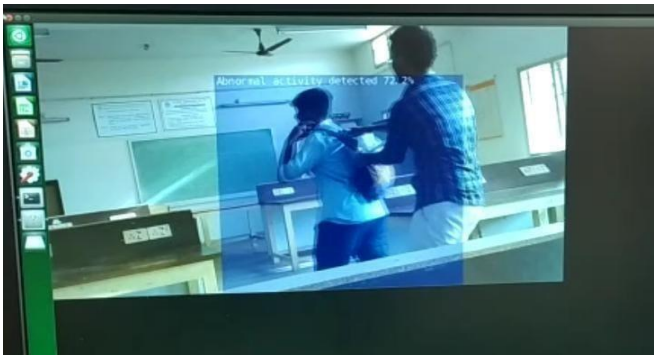

Fig.3

The Real-Time Event Detection of Our Model is Displayed in the Above Figure. An individual attempting to steal someone's bag is identified as an anomaly. 72.2% of the abnormal activity is accurately identified.

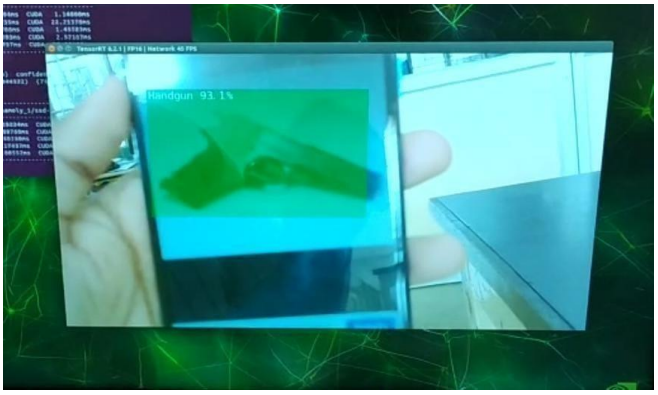

Fig.4. Real-Time Detection

The Real-Time Event Detection of Our Model is Displayed in the Above Figure. A handgun model image has been discovered. 93.1% of the abnormal activity was accurately identified.

6. CONCLUSION

The first challenging task for an anomaly detection system is to locate high-quality datasets. The second difficult element is selecting the appropriate model for it. The model's real-time execution and dynamic anomaly detection are the most difficult aspects. In this project, a 99.6% accuracy rate was achieved. Real-Time Detection has a minor accuracy issue when detecting anomalies and objects like guns, but the rate of false positive detection is very high. In the future, a more economical and effective strategy can be used to handle the problem. In industrial settings, there are certain places or offices that need foolproof security to deter intrusions. These types of sensors are used to monitor human activity. It can identify people, track their behavior, and record the times these events took place for security reasons as well as training with familiar faces. As a result, it can also be used as an audit device and for incident log monitoring. This might be useful in resolving problems if there is a difference.

7. REFERENCES

[1] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM computing surveys (CSUR), 41(3), 1-58.

[2] Sultani, W., Chen, C., & Shah, M. (2018). Real-world anomaly detection in surveillance videos. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 6479-6488).

[3] Sodemann, A. A., Ross, M. P., & Borghetti, B. J. (2012). A review of anomaly detection in automated surveillance. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 42(6), 1257-1272.

[4] Pranav, M., & Zhenggang, L. (2020). A day on campus-an anomaly detection dataset for events in a single camera. In Proceedings of the Asian Conference on Computer Vision.

[5] Song, X., Wu, M., Jermaine, C., & Ranka, S. (2007). Conditional anomaly detection. IEEE Transactions on Knowledge and Data Engineering, 19(5), 631-645. 26

[6] Yagan, M., Yilmaz, E. A., & Özkan, H. (2022, May). Anomaly Detection in Surveillance Videos Using Regression With Recurrent Neural Networks. In 2022 30th Signal Processing and Communications Applications Conference (SIU) (pp. 1-4). IEEE.

[7] Jain, A., & Garg, G. (2020, August). Gun detection with model and type recognition using haar cascade classifier. In 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 419- 423). IEEE.

[8] Lim, J., Al Jobayer, M. I., Baskaran, V. M., Lim, J. M., Wong, K., & See, J.(2019, November). Gun detection in surveillance videos using deep neural networks. In 2019 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC) (pp. 1998-2002). IEEE.

[9] Bushra, S. N., Shobana, G., Maheswari, K. U., & Subramanian, N. (2022, April). Smart Video Surveillance Based Weapon Identification Using Yolov5. In 2022 International Conference on Electronic Systems and Intelligent Computing (ICESIC) (pp. 351-357). IEEE.

[10] Mithal, A., & Baser, M. (2020, November). Automatic Threat Detection in Baggage Security Imagery using Deep Learning Models. In 2020 IEEE 15th International Conference on Industrial and Information Systems (ICIIS) (pp. 180-185). IEEE.

[11] Sultani, W., Chen, C., & Shah, M. (2018). Real-world anomaly detection in surveillance videos. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 6479-6488).

[12] Xu, S., & Hung, K. (2020, April). Development of an ai-based system for automatic detection and recognition of weapons in surveillance videos. In 2020 27 IEEE 10th Symposium on Computer Applications & Industrial Electronics (ISCAIE) (pp. 48-52). IEEE.

[13] Liang, K. J. (2020). Deep Automatic Threat Recognition: Considerations for Airport X-Ray Baggage Screening (Doctoral dissertation, Duke University).