National Conference on
"Role of Engineers in Nation Building" organized by VIVA Institute of Technology, Mumbai
(6th and 7th March 2020)
International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

An Analysis of Anomalous Behavior Detection Techniques

Aditya Parab[1], Prajwal Mogaveera[2], Abhishek Nikam[3], Ashwini Save[4]

[1]Department Computer Engineering, Mumbai University, MUMBAI
Email:adityaparab04@gmail.com
[2]Department Computer Engineering, Mumbai University, MUMBAI
Email:prmm98@gmail.com
[3]Department Computer Engineering, Mumbai University, MUMBAI
Email:abhinikam15@gmail.com
[4]Department Computer Engineering, Mumbai University, MUMBAI
Email:ashwinisave@viva-technology.org

***Abstract*—*Anomalous behaviour is any harmful behaviour which is different from the normal behaviour in a particular situation or a place. As anomalous behaviour causes harm to people directly or indirectly, therefore detecting such abnormal behaviour automatically is very crucial for the welfare of society. For instance, normal behaviour in ATM would be to withdraw money and anomalous behaviour might include robberies, fighting etc. which is harmful to the people. Many research have been done on anomalous behaviour detection which were based on IoT, Machine Learning and Deep learning-based techniques such as Multiple Instance Learning, Random Forest Classification and Convolution Neural Network with or without LSTM. This paper analyses various techniques that are used to detect anomalous behaviour.*

Keywords*—*Anomalous Behaviour, Deep Learning, IOT, Machine Learning, Surveillance.

I. INTRODUCTION

Anomalous behaviour is any behaviour that can be held as inconsistent within the community standards. Anomalous behaviour is usually considered as abnormal behaviour when it is atypical or not ordinary, consists of inappropriate or indecent behaviour and results in an undesirable outcome. It also results in impairment in one's individual functioning. Such behaviour is described as deviance which violates the social and ethical norms. Anomalous behaviour can be classified into various categories like arson, assault, burglary, fighting, gunpoint, kidnapping, murder, shooting, rape, etc. Any behaviour which is not normal comes under anomaly. Thus it is crucial to detect such behaviour and classify it accordingly. This can be accomplished either using normal behaviour or then distinguishing it from abnormal behaviour or by directly classifying abnormal behaviour in the above mentioned classes. This paper focuses on various techniques like Multiple instance learning [1], Random Forest classification [4], Gaussian Mixture Model [9], Support Vector Machine [10], CNN [3] [5] [11], CNN with LSTM [6] [7] [12] and IOT based techniques using arduino, temperature sensors [2] and ARM controller [8] to detect human activities which includes normal as well as anomalous behaviour.

II. LITERATURE STUDY

W. Sultani,C. Chen and M. Shah[1] have proposed a model based on MIL i.e Multiple instance learning by treating normal and anomalous videos as bags and short segment in each video as an instance in a bag. Anomaly often occurs only for short time therefore video is divided into multiple temporal video segments in video bags. Features for every 16-frame video clip are computed followed by l2 normalization. To obtain features for a video segment, this system takes an average of all 16-frame clip features within that segment. After extracting features from video segments fully connected neural network is trained by utilizing novel ranking loss function which computes the ranking loss between between the highest scored instances in positive bags and the negative bags. Dataset having 13 different types of anomalies is used. Proposed method provides successful detection of anomalies and able to achieve 75.41% accuracy. It also generates false alarms because of flying insects in front of camera and also failed to identify normal group activities like people watching relay race on street etc.

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

Jacintha .V,J. Nagarajan, K .Thanga[2] have proposed IOT based system for ATM security which have several layers of protection against physical as well as electronic theft. Proposed system is based on embedded arduino for ATM security which takes input from various sensors placed in ATM cells. Various sensors like temperature sensors, GSM modem, vibration sensors, relay, tilt sensors are used to get input data for arduino. When any of the sensor exceeds threshold value alarm sound is decoded and alerts are sent through the mail and GSM modem makes a call to security authority. SQL servers and local disk array are used to store all types of alarms generated by the system. When sensor exceeds the normal value mail is sent, relay turns on, chloroform is switched automatically, allows call through GSM modem etc. System is having acceptable accuracy and do not require continuous human monitoring. System is not that efficient because it does not work on temporal data and may generate false alarms.The future scope can be use of thermal sensors to detect number of persons inside the ATM cell.

A. Khaleghi, M Moin[3] have proposed Deep learning based system for anomaly detection. Architecture of this system has two main phases which are called train network and detection classifier. First phase aims for feature extraction and it consists of five components with deep structure. Second phase is detection phase consists of five deep neural network classifiers and reconstruction network. The main contribution of this paper is the use of deep learning techniques in all phases of anomaly detection.The first step before starting extracting and learning features is to estimate and remove the background. Next step is feature extraction and learning component and output of these phase is detected objects. Third step is motion extraction which performs feature extraction based on moving objects in scene of video patch. Last step is reconstruction network which reconstructs scene. In the detection component, learned features which are generated in the train network are given to a classifier with two classes of normal and abnormal to detect anomaly in video. To evaluate proposed method UCSD dataset is used which is one of the most standard datasets related to the anomaly detection and proposed method shows 15% to 20% increase in accuracy with respect to DOC model proposed in paper[13]. This dataset is related to the pedestrian walkway surveillance camera. Any objects other than people are identified as anomaly, such as bicycle or car but apart from that no other anomaly has been classified by this system.

V. Tripathi1, A. Mittal, D. Gangodkar, V. Kanth[4] have proposed a system for detecting abnormal events at ATM installations. In process of proposed model videos. Firstly video is divided into frames. Preprocessing is performed on every N number of successive frames to combine information of all N frames into one frame. Newly generated frame then contains high amount of useful data and sequence information. After this processing HOG (feature descriptor) is applied to extract useful information and dataset is created. Then this dataset is fed into random forest classifier along with training dataset.Classifier generates model from training dataset and predict most likely class for every testing instance.Researchers have made their own dataset which simulates ATM working with frame size 320 * 240 and 25 fps frame rate.Second and third datasets are CAVIAR and HMDB-51 and got 75.38% accuracy for CAVIAR dataset and 50.84% accuracy for HMDB-51 dataset. Proposed system is restricted to work only for video,aspects like object selection, structural variation, audio based recognition can be focused.

P.Singh and V. Pankajakshan[5] have proposed deep learning based technique for anomaly detection in Surveillance videos. In this paper, system is presented for detecting anomalies using general features that are automatically extracted from video data. Layered convolutional neural network is used for feature extraction and then convolutional Long Short-term Memory stack is used to construct the future motion sequence. After this, a stack of transpose CNN is used to construct the future video sequence from this predicted motion sequence.These steps together capture the spatio-temporal patterns present in the input videos. For anomaly detection, after predicting the output video sequence from an input video sequence, an error is computed between the two, which is thresholded to determine if the input video sequence is anomalous or not. UCSDPed1 and UCSDPed2 datasets are used to obtain experimental results. Proposed technique was able to achieve 74.8% accuracy for UCSDPed1 and 80.2% accuracy for UCSDPed2. A key advantage of the proposed approach is that the feature extraction process does not contain any hand-crafted features. Another advantage is that it does not have any dataset specific parameters.

N. Shree , R. Sah and S. Gowda[6] have proposed a system to detect and notify about real time suspicious activities in indoor scenarios. Proposed framework is designed to detect indoor violence like stabbing, thrashing or any activity involving physical force. A person being attacked by a knife is the main concern of the project. Framework starts in first phase by background

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

subtraction and blob(human individual) detection followed by object identification. If the number of individuals in the scenario is more than one then only program enters in the second phase where edge detection and tracking is done. By processing every block of the frame object detection module returns positive if three conditions are satisfied that are 1. Hand mould and gesture 2. Presence of Sharp object affirmation and 3. Link between the hand and object to meet the appropriate conditions. If scene is insecure then program goes to third phase which is notification. By evaluating the algorithm real time videos it was clear that algorithm works efficiently in bright areas with 73% accuracy, whereas works moderately in less sharpen areas with 67% accuracy when experimented against the real time videos captured from different locations.

R. Ionescu, S. Smeureanu, B. Alex, M. Popescu[7] have proposed a framework that requires no training for abnormal event detection. This approach is completely unsupervised because it cannot build a model in advance and then find derivations in new data. Window sliding algorithm is applied for each window. Then model considers first n frames as normal and last n frames as abnormal but this hypothesis must be true.So for that both motion and appearance features are extracted from the frames and binary classifier is trained with high regularization to distinguish between the labeled frames. Then accuracy is retained from the classifier and this process is repeated with eliminating some of the best features. This process is called unmasking. Abnormal events correspond to high accuracy while normal events correspond to low accuracy.By this method abnormal events are detected in the window. Model has achieved 68% accuracy on UCSD ped1 data set and 82.2% accuracy on UCSD ped2 data set. Empirical results indicated that given approach is gives better performance than the base unsupervised method.

A.Kande, P. Reddy[8] have proposed a methodology to detect abnormal event at ATM system by using image processing based on IOT technologies. A system is built for a structure where objects are moving with respect to fixed background. First foreground extraction technique is used to obtain clear outline of people. Then a fixed size of window is used to record the MHI. MHI stands for Motion History Image. It is a binary image where pixel intensity is a function of recency in motion. Brighter (whiter) the pixels have greater the recency. As an object moves it leaves behind more recent movements and according to the image motion is represented. Once MHI is obtained, features are extracted from it using Hu moments function. Dimensionality reduction is done with the help of principal components analysis (PCA) for improving the efficiency in computation. Furthermore, this system makes use of support vector machine to predict the most likely class and the result is displayed. This methodology uses their own created dataset and got 72% accuracy for single normal, 69.89% accuracy for multiple normal and 70% accuracy for multiple abnormal.

R. Leyva, V. Sanchez and Chang-TsunLi[9] presented an online framework for video anomaly detection. As big data continues to grow exponentially and surveillance videos are one of the main contributors, there was a need of developing automatic video surveillance methods to capture intelligently. In proposed work binary features are generated from data which is used to create dictionaries then Gaussian Mixture model is used to detect abnormal events. Features are computed from two motion sources: the back-ground and temporal gradients. In given model, the temporal gradients and background of frames are calculated. Interest points are detected by using the FAST detector. Binary encoding then generates binary features, which are used to create dictionaries. GMMs are used to model all binary features and those obtained by computing the foreground occupancy. An inference mechanism that uses GMM votes detects abnormal events. UCSD ped1 and UCSD ped2 datasets are used for evaluation and efficiency is shown in terms of Equal Error Rate which is got to be 25.34/21.2 which is much lower than the optimal.

Arpitha K, HonnarajuB[10] have proposed a vision based anomaly detection method for ATMs. Most ATMs are open 24 hours and their zones are spread everywhere in the city. Due to low manual security of ATMs they are more basic danger of being burgled. In the initial stage, video frames are converted into gray scale images and these gray scale images are used for feature extraction. In this paper methodology is explained in two main parts, the first is feature extraction and second classification. Scale Invariant Feature transformation (SIFT) and Gabor filter are used for feature extraction. Texture analysis is done by Gabor filter, which means that it analyses whether there is any specific frequency content in image in particular directions in localized area throughout the point or region of analysis. Dataset used for evaluation by the researchers was created by them. Support

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

vector machine (SVM) is used in recognition and classification stage. SVM classifier, classifies the data into two classes according to its features. Using SVM classifier researchers have obtained low accuracy for complex data.

A. Mathew, J. Mathew, M. Govind and A. Mooppan[11] have presenter transfer learning approach for intrusion detection. IN this paper helmet detection is done by deep convolutional neural networks. ATM visitors who have wore helmets makes it painful to identify the person if an abnormal activity happens, thus helmet detection in ATM were crucial. Deep convolutional network with transfer learning found to be the best way to tackle this detection problem to achieve state of the art performance with minimum computational requirement. Real time processing takes much less time than offline processing so which provides faster results. Google's inception v3 model which is trained on 1.28 million images with 100 classes from Imagenet LSVRC 2014 is used in this paper and this knowledge is transferred and used on ATM surveillance dataset of 4719 images with two classes that are helmet or without helmet. Accuracy of 95.3% was achieved in testing phase but proposed network was found to be harder to train due to vanishing gradient and degradation problems.

X. Cai, F. Hu, L. Ding[12] have proposed deep learning based model to detect abnormal behaviour in examination hall. Because of increase in examinations and people paying more attention to the fairness and order of examination it is necessary to detect abnormal behaviour efficiently. In this paper 3D CNN model is used to detect abnormal behaviour from examination surveillance video. In this model Farneback's algorithm is used to extract optical flow, and then it is transformed into "flow images". 3D CNN model take these images as an input. Proposed CNN model has 2 convolution layers, 2 pooling layers and 2 fully connected layers.if any of the sub-region samples is classified into positive then there is an abnormality in test video clip and that video is stored. Model is evaluated on their own dataset and compared with motion blob[14], template matching[15] and skin+SVM[16]. It is seen that the proposed model achieves superior performance to current methods with accuracy of 89.8%. Accuracy of model can be further increased with good camera angles and quality of test videos.

III. ANALYSIS

The Table given below is a summary of research papers on anomaly detection. It states the different techniques used for anomalous behaviour detection. The accuracy varies as per the system used.

TABLE 1
ANALYSIS TABLE

Sr. No.	Paper Name	Technique Used	Data Set	Accuracy
01.	Real-world Anomaly Detection in Surveillance videos.[1]	Multiple Instance Learning(MIL)	UCF-Crime dataset	75%
02.	An IOT Based ATM Surveillance System. [2]	Arduino and Temperature sensor, GSM modem, vibration sensor, Relay, Tilt sensors	--	Acceptable performance
03.	Improved Anomaly Detection in Surveillance Videos Based on A Deep Learning Method [3]	Convolution Neural Network (CNN)	Public UCSD dataset.	15% to 20% accuracy over DOC model[13]
04.	Real time security framework for detecting abnormal events at ATM	Random forest classification.	CAVIAR, HMDB 51	CAVIAR 75.83%, HMDB-51 50.84%

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

	installations[4]			
05.	A Deep Learning Based Technique for Anomaly Detection in Surveillance Videos[5]	Convolutional Neural Network along with ConvLSTM2D	UCSD Ped1 and UCSD Ped2	74.8% for UCSD Ped1 and 80.2% for UCSD Ped2
06.	Surveillance video based robust detection and notification of real time suspicious activities in indoor scenarios[6]	Convolutional Neural network	Own Real time data set	73% in bright areas and 67% in less sharpen areas
07.	Unmasking the abnormal events in video[7]	Linear classifier	UCSD ped1, UCSD ped2	68% - UCSD ped1 and 82.2% - UCSD ped2
08.	To detect abnormal event at ATM System by using image processing based on IOT technologies[8]	ARM controller based embedded system to process real time data collected using the vibration sensor.	Own dataset created.	72% for Single normal, 69.89% for multiple normal and 70% for multiple abnormal
09.	Fast detection of abnormal events in videos with binary features[9]	Binary Features are generated from data which are used to create dictionaries then Gaussian Mixture Model is used to detect Abnormal events.	UCSD ped1 and UCSD ped2	Shown in terms of Equal Error Rate(EER) 25.34/21.2
10.	Vision Based Anomaly Detection System for ATM[10]	Support Vector Machine	Own dataset created.	Low Accuracy
11.	An Improved Transfer Learning Approach for Intrusion Detection[11]	Transfer Learning with Google's inception model (CNN)	Own dataset created.	95.8%
12.	Detecting Abnormal Behavior in Examination Surveillance Video with 3D Convolutional Neural Networks[12]	Convolutional Neural Networks(CNN)	Own dataset created.	89.8%

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

The various algorithms used for anomaly detection are analyzed in the above table. It includes the IOT, Machine Learning, and Deep Learning based techniques. From the analysis table above it can be seen that CNN gives better result and the accuracy of which can be further increased by LSTM due to temporal processing by LSTM.

IV. CONCLUSION

With the increase in anomalous activities around the world it is very much necessary to detect such behaviours while they are happening. Various Machine Learning, Deep Learning and IOT based techniques are used to classify human behaviour as anomalous or non anomalous among which deep learning approaches such as CNN, CNN with LSTM have proved to be more accurate in classification. In this paper different machine learning, deep learning and IOT based techniques have been analysed and studied. Here, loads of surveillance videos have been used as dataset. From studying papers it is apparent that CNN along with LSTM yields better results and accuracy because of temporal data processing by LSTM.

ACKNOWLEDGEMENTS

We would like to express a deep sense of gratitude towards our mentor Dr. TatwadarshiNagarhalli, Department of Computer Engineering for his constant motivation and valuable suggestions. The work that we have been able to present is because of his timely guidance and encouragement.

REFERENCES

[1] W. Sultani, C. Chen, M. Shah, "Real-world Anomaly Detection in Surveillance Videos", IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2018, pp. 6479-6488.
[2] Jacintha .V, J. Nagarajan, K.Thanga, "An IOT Based ATM Surveillance System", IEEE International Conference on Computational Intelligence and Computing Research, 2017, pp. 978-983.
[3] A. Khaleghi, M Moin, "Improved Anomaly Detection in Surveillance Videos Based on A Deep Learning Method", Artificial Intelligence and Robotics (IRANOPEN), 2018, pp. 73-81.
[4] V. Tripathi, A. Mittal, D. Gangodkar, V. Kanth, "Real time security framework for detecting abnormal events at ATM installations", Springer-Verlag Berlin Heidelberg, 2016, pp 1-11, pp. 1-8.
[5] P.Singh, V. Pankajakshan, "A Deep Learning Based Technique for Anomaly Detection in Surveillance Videos", Twenty Fourth National Conference on Communications (NCC), IEEE, 2018, pp. 1-6.
[6] N. Shree , R. Sah and S. Gowda, "Surveillance video based robust detection and notification of real time suspicious activities in indoor scenarios", DOI : 10.5121/csit.2016.60618, pp. 227-236
[7] R. Ionescu, S. Smeureanu, B. Alex, M. Popescu, "Unmasking the abnormal events in video", arXiv:1705.08182v3 [cs.CV], 2017, pp. 1-9.
[8] Kande A, P B Reddy "To detect abnormal event at ATM system by using image processing based on IOT technologies" International Journal of Engineering & Technology, 7 (3) (2018), pp. 1000-1004.
[9] R Leyva, V Sanchez and C-T Li "Fast Detection of Abnormal Events in videos with binary features" 2018 IEEE, pp. 1318-1322.
[10] Arpitha K, Honnaraju B., "Vision Based Anomaly Detection System for ATM." International Research Journal of Engineering and Technology (IRJET), 2018, pp. 4235-4240.
[11] A. Mathew , J. Mathew, M. Govind, Asif Mooppan, "An Improved Transfer learning Approach for Intrusion Detection.", 7th International Conference on Advances in Computing & Communications, ICACC-2017, pp. 251-257.
[12] X. Cai, F. Hu, L. Ding, "Detecting Abnormal Behavior in Examination Surveillance Video with 3D Convolutional Neural Networks", 6th International Conference on Digital Home, 2016, pp. 20-24
[13] RyotaHinami, Tao Mei, and Shin'ichi Satoh, "Joint Detection and Recounting of Abnormal Events by Learning Deep Generic Knowledge", arXiv:1709.09121v1, 2017
[14] Y. B. Wang, "An intelligent algorithm for detecting cheating behavior at the exam site," Chang Sha: National University of Defense Technology, 2011.
[15] J. Li, "Detection and analysis of abnormal behavior in elec-tronic invigilating," Tai Yuan: Taiyuan University of Technology, 2013.
[16] S. Xiong, "Research of SVM-based abnormal behavior detection in electronic invigilated examination room," Journal of Hubei University of Education, vol. 30, no. 8, pp. 42-46,2013.