ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AI ENABLED SYSTEM WITH REAL TIME MONITORING OF PUBLIC SURVEILLANCE VIDEOS FOR ABNORMALITY DETECTION AND NOTIFICATION

PRATHAP ABBAREDDY[1] DR. SK. YAKOOB[2] RAMU KUCHIPUDI[3] BHUJANGA REDDY BHAVANAM[4]

[1]Software Engineer
[2]Associate Professor &HOD, Dept. of CSE, Sai Spurthi Institute of Technology B.Gangaram,Sathupally, Khammam-507303 ,Telangana,
[3]Associate Professor, Chaitanya Bharathi Institute of Technology, Department of Information Technology, Gandipet, Hyderabad, Telangana -500075
[4]Asst.Professor computer science and engineering, Geethanjali college of engineering and technology

Email :prathap.abbareddy@gmail.com [2]yakoobcs2004@gmail.com [3] kramupro@gmail.com [4] [4]bhujangareddy.cse@gcet.edu.in

ABSTRACT

Public surveillance videos are increasingly playing key role in identification of certain incidents and people who misbehave or perform illegal activities. Monitoring surveillance videos manually to detect abnormalities is time consuming and it may lead to delay in getting required information. With the usage of Artificial Intelligence (AI) video analytics in real time can help in acquiring such information on time so as to make well informed decisions. Particularly deep learning is great help in learning from incidents and detect anomalous behaviours. In this study, we suggested an autonomous system for anomaly detection from surveillance films, based on deep learning. For anomaly detection, an improved Convolutional Neural Network (CNN) model is employed. We presented a method that utilizes the upgraded CNN model for its functionality, called Learning based Video Anomaly Detection (LbVAD). To lower the prediction process's error rate, a loss function is defined. For our empirical investigation, we gathered data from many benchmark datasets, including UMN, UCSD, Ped1, and Ped2. The suggested approach works better than the current models, according to the results of our experiments.

Keywords: *Machine Learning, Deep Learning, Artificial Intelligence, Video Abnormality Detection*

1. INTRODUCTION

In the contemporary era, there have been increasing incidents in public places pertaining to human misbehaviour, traffic accidents, fire accidents and so on. When such mishaps occur, it is very important to establish evidence of events. Towards this end, public surveillance videos play crucial role as they stream video content continuously. However, it is very important to analyse the videos and identify incidents that look abnormal [1]. Towards this end traditional approach of human observation of videos is very time consuming and leads to delay in making decisions. Artificial Intelligence-enabled techniques were developed to solve this issue. Particularly deep learning models are widely used for image processing. Models like CNN are found to be more suitable for dealing with image content [2]. Automatic detection of video abnormalities and notification to concerned authorities is very important for public video surveillance to be very useful. Towards this end, many researchers contributed in developing learning based approaches. Moin et al. [4] opined that surveillance cameras' data analysed for effective anomaly detection using deep learning techniques, enhancing accuracy and isolation for pre-training. Nawaratne et al. [9] proposed deep learning for evolving anomalies in real-time surveillance. Active learning updates anomalies, addressing dynamic challenges. Gamarra et al. [14] shown improved performance using a new IVADC-FDRL model that was suggested for anomaly detection and classification in surveillance footage. Attar et al. [17] showed

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

promise for various domains such as health care and self-driving cars, but challenges remain for real-time anomaly detection and parallel deep learning architectures. Vu et al. [22] presented a multi-channel system for supervised finding anomalies in CCTV footage, outperforming existing methods. Next steps include developing an end-to-end model and investigating new datasets. Asad et al. [26] suggested a two-stage design for anomaly identification in surveillance videos, emphasizing spatiotemporal features and utilizing deep learning. Hussein et al. [30] investigated on the importance of human behaviour recognition that has led to increased focus on anomaly detection. From the review of literature, It is discovered that a deep learning-based framework is required in order to enhance the detection procedure. The following are our contributions to this publication.

1. Our deep learning-based framework was suggested for automatically detecting abnormalities from surveillance videos.
2. An enhanced Convolutional Neural Network (CNN) model is used for detecting abnormalities.
3. We put out a learning-based system that Video Anomaly Detection (LbVAD) which exploits the enhanced CNN model for its functionality.
4. A program is designed to assess LbVAD algorithm and compare its performance with existing models.

This is the format for the rest of the paper. Section 2 examines the research on a number of methods available based on deep learning. Section 3 presents our methodology for video anomaly detection. The study's findings are shown in Section 4. In addition to providing room for further research, Section 5 wraps up our study and offers insightful observations.

2. RELATED WORK

This section examines the research done on existing video abnormality detection methods. Nayak et al. [1] observed that video surveillance widely used in public places for safety. Challenges in anomaly detection due to varied factors and lack of research. Aberkane et al. [2] explored deep learning combined with reinforcement learning that detects anomalies in surveillance videos, addressing computational cost for improved efficiency. Kiran et al. [3] investigated surveillance videos that lack annotations, necessitating unsupervised anomaly detection. Categories include models that are generative, spatiotemporal predictive, and reconstruction-based. Moin et al. [4] opined that surveillance cameras' data analysed for effective anomaly detection using deep learning techniques, enhancing accuracy and isolation for pre-training. Amin et al. [5] studied EADN model that addresses surveillance complexity with CNN and LSTM for precise anomaly detection in surveillance data analysis. Shah et al. [6] proposed deep learning model detects anomalies, outperforming existing methods on challenging real-world datasets. Rezaee et al. [7] proposed automated detection of crowd anomalies that aids in effective security. Methods involve crowd analysis, tracking, and deep learning. Mohan et al. [8] found that public places increasingly utilize video surveillance for security. Anomaly detection combines PCANet and CNN for accurate recognition and location.

Nawaratne et al. [9] proposed deep learning for evolving anomalies in real-time surveillance. Active learning updates anomalies, addressing dynamic challenges. Singh et al. [10] proposes a DNN-based method for identifying anomalies in CCTV footage, performing comparably with simpler complexity. Chriki et al. [11] introduced deep characteristics and manually developed algorithms for anomaly identification in UAV-based surveillance operations. Doshi et al. [12] proposed online anomaly detection using transfer and continual learning, enhancing surveillance capabilities for dynamic scenarios. Shao et al. [13] invented a powerful deep learning framework that detects anomalies in videos and offers answers, demonstrating comparable performance. Gamarra et al. [14] presented a brand-new IVADC-FDRL model for the identification and categorization of anomalies in surveillance footage, demonstrating superior performance. Amudha et al. [15] observed that it might be difficult to identify anomalies in video surveillance because dynamic environments. The proposed deep learning model efficiently predicts anomalies, surpassing others. Shen et al [16] proposed Spatial-Temporal Fusion Features (STFF) in a Fast Sparse Coding Network (FSCN) improves video abnormality identification. The FSCN efficiently generates sparse coefficients, surpassing traditional methods. Attar et al. [17] showed promise for various domains such as health care and self-driving cars, but challenges remain for real-time anomaly detection and parallel deep learning architectures. Yu et al. [18] proposed human-machine cooperative approach for video anomaly

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

detection incorporates expert feedback, improving anomaly classification. Experiment results show competitive performance, warranting further research for computational efficiency improvement.

Table 1: Shows Summary Of Important Literature Findings

References	Methods	Dataset	Advantages	Limitations
[2]	DL and DRL	UCF10 and HMDB51	High accuracy	Computational cost is more
[4]	DL	UCSD	Reduces training time	Anomaly localization needs to be done.
[5]	DL	UCSDPet1 and UCSDPet2	High accuracy	Attention based DL is to be explored.
[9]	DL	UCSD Pedestrian and CUHK Avenue	Can handle high dimensional data with better performance.	False negatives are to be reduced.
[11]	CNN	MDVD	Good and acceptable detection	More diversified datasets are to be used
[12]	CNN and LSTM	CUHK avenue, UCSD	Learning efficiency leading to better accuracy	To be evaluated with more challenging scenarios
[14]	DL and DRL	Test004 and test007	Higher accuracy	More abnormal activities are to be achieved.
[18]	DL	UCSD and CUHKAvenue	Improved detection accuracy	Computational cost is to be reduced.
[22]	GAN	Avenue, Ped1	Improved PSNR in the detection results	To be evaluated in diversified dataset
[26]	CNN variants	Ped1, Ped2, CUHK	Modeling characterization improved	Needs improvement in terms of segmentation and tracking.

Mansour et al. [20] introduced IVADC-FDRL, a sophisticated approach for identifying and classifying anomalies in surveillance footage. The prototype leverages Faster R-CNN and DQL for accurate detection, demonstrating superior performance on the UCSD dataset. Boudihir et al. [21] introduced a Deep Q Learning Network to identify and pinpoint irregularities in security footage. Experimental results demonstrate superior performance. Future work aims to minimize computational costs. Vu et al. [22] presented a multi-channel system for guiding identification of anomalies in surveillance footage outperforming existing methods. Future work involves exploring to build a complete model and adding fresh datasets. Lian et al. [23] offered a TSC framework for identifying anomalies, optimizing parameters and using data-dependent similarity measurements for improved performance. Furthermore, it introduces a comprehensive dataset to support the proposed approach. Nabi et al. [24] suggested an anomaly detection technique based on GANs for crowded scenes, outperforming existing approaches in various evaluation tasks. Future work will explore alternative motion representation methods for improved performance. Lopes et al. [25] proposed approach combines various features for anomaly scoring, validated by public dataset experiments. Further research is needed. Asad et al. [26] suggested a two-stage architecture for anomaly identification in surveillance videos, emphasizing spatiotemporal features and utilizing deep learning.

Yuan et al. [27] introduced an innovative autoencoder architecture to capture appearance and motion regularities separately. Enhanced by a variance attention module and deep K-means clusters, the method showcases superior performance on various datasets. Hoang et al. [28] found that deep learning is essential for anomaly detection in video surveillance and human behaviour recognition. Various methods,

Journal of Theoretical and Applied Information Technology
15th May 2024. Vol.102. No 9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

including reconstruction-based and classification techniques, have significantly advanced the field. Benchmark databases assist in addressing challenges related to robust feature extraction in dynamic environments. Lee et al. [29] explored anomaly detection that remains an attractive area for study because of its complexities and limited normal data availability. Recent methods are surveyed, considering network architectures and datasets from 2015 to 2018. Hussein et al. [30] investigated on the importance of human behaviour recognition that has led to increased focus on anomaly detection. This comprehensive review discusses DL methods, architectures, datasets, and performance metrics in video AD. Applications and challenges are also highlighted for future research. Table 1 shows summary of important literature findings. From the review of research, a deep learning-based framework is shown to be necessary, that could improve detection process.

3. METHODOLOGY

This section presents our methodology for identifying anomalies in videos using supervised learning. During training, the proposed method, shown in, starts by dividing up security film into a preset number of parts. These sections provide examples in a bag. We train the anomaly detection model using both positive (anomalous) and negative (normal) bags using the proposed deep MIL ranking loss. The following optimization expressed in Eq. 1 is used to train the classifier in conventional supervised support vector machine classification tasks where the labels for everything, both good and bad samples are known.

$$\min_{w} \frac{1}{k} \sum_{i=1}^{k} \overbrace{max\left(0, 1 - y_i(\mathrm{w}.\emptyset(\mathrm{x}) - \mathrm{b})\right)} + \frac{1}{2} \| w \|^2 \quad (1)$$

The hinge loss is represented by y_i, the label of each sample is denoted by w, the classifier to be learnt is represented by \(x), which indicates the features extracted from a video clip or an image patch. A bias is represented by b. Good and negative example annotations are required in order to train a robust classifier. It is imperative that each video segment have temporal annotations for a classifier in the context of supervised anomaly detection. Time-consuming and hard work, however, goes into getting temporal annotations for videos.

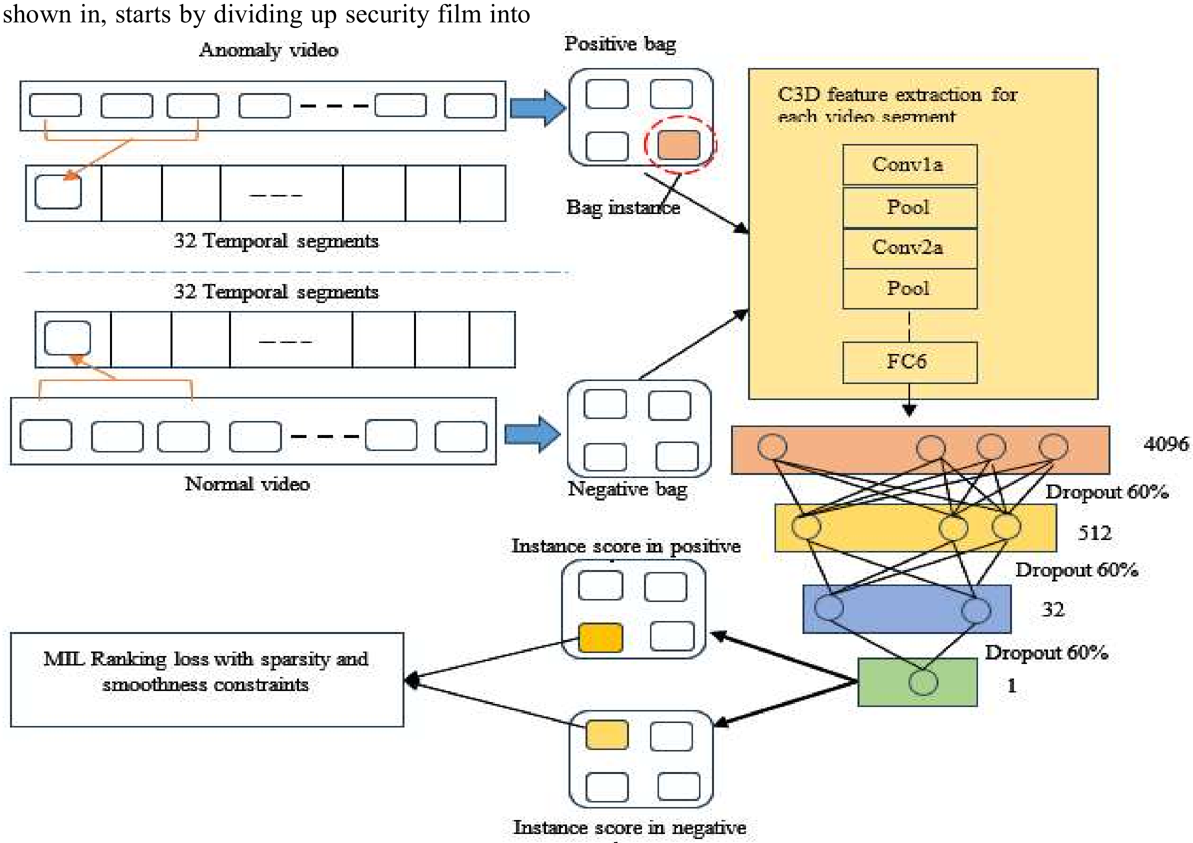

Figure 1: Overview of the proposed methodology

Journal of Theoretical and Applied Information Technology
15th May 2024. Vol.102. No 9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The requirement of possessing these precise temporal annotations is loosened by MIL. The exact time positions such unusual occurrences in films is not known in MIL. Rather, all that is required are video-level labels showing the existence of an abnormality throughout the whole film. Videos with anomalies are classified as positive; those with none at all are classified as negative. Next, A positive bag B_a is used to symbolize a good video, in wherein discrete time intervals make up individual occurrences, $(p^1, p^2, \ldots \ldots p^m)$ where m denotes how many occurrences there are in the bag. We presume that the abnormality is present in at least one of these cases. Similar to this, we describe the negative video as a negative bag, B_n, whose temporal segments create negative instances $(n^1, n^2, \ldots \ldots n^m)$ Not a single occurrence in the negative bag has an abnormality. Given the uncertainty surrounding the precise details (i.e., instance-level label) the goal function may be optimized with respect to the highest scoring instance inside each bag, as demonstrated by the positive examples [31]. It is expressed as in Eq. 2.

$$\min_w \frac{1}{z}\sum_{j=1}^{z} max\left(0, 1 - Y_{B_j}\left(\max_{\mathrm{i}\in B_j}(\mathrm{w}.\emptyset(\mathrm{x_i})) - \mathrm{b}\right)\right) + \frac{1}{2}\parallel w \parallel^2, \quad (2)$$

where Y_{B_j} indicates he label at the bag level; z is the total number of bags; the remaining variables are equivalent to those found in Eq. 1. Aberrant behaviour is difficult to accurately describe since it is very subjective and differs widely from person to person. [32]. Moreover, the process of giving 1/0 labels to anomalies is not clear-cut. Additionally, rather than being a classification challenge, anomaly detection is usually handled as a low probability pattern identification issue since there aren't enough instances of anomalies [33]. In our proposed technique, we structure anomaly identification as a regression issue. The goal is to obtain greater points for anomalies in the video portions that don't seem right for the typical portions. The simplest method would be to implement a ranking loss that encourages atypical video sequences to receive higher scores than conventional segments, as indicated in Eq. 3.

$$\mathrm{f}(v_a) > \mathrm{f}(v_n), \quad (3)$$

where v_a and v_n depict both typical and aberrant video fragments, $\mathrm{f}(v_a)$ and $\mathrm{f}(v_n)$ indicate the corresponding expected anomaly scores, which are between 0 and 1. When training, if the segment-level annotations are known, then the previously specified ranking algorithm should perform well. However, using Eq. 3 is not viable when annotations at the video segment level are not present. Instead, we propose an objective function for multiple instance ranking, which is expressed in Eq. 4.

$$\max_{\mathrm{i}\in B_a} \mathrm{f}(v_a^i) > \max_{\mathrm{i}\in B_n} \mathrm{f}(v_n^i), \quad (4)$$

where each bag's maximum is applied to every video section. Rather of applying ranking to every bag instance, we only apply ranking to the two examples in both the positive and negative bags that, respectively, have the greatest anomaly scores. The real positive instance, or the section that has the highest anomaly score in the positive bag is probably the anomalous one. Though it appears most like an abnormal segment, which is really a regular occurrence, is the segment in the negative bag with the greatest anomaly score. This negative situation is considered a hard occurrence in anomaly detection that might result in a false warning. The goal of applying Eq. 4 is to increase the difference between the positive and negative examples' anomaly scores. Thus, the hinge-loss formulation gives us the ranking loss expressed in Eq. 5.

$$\iota(B_a, B_n) = \max(0,\ 1 - \max_{\mathrm{i}\in B_a} \mathrm{f}(v_a^i) + \max_{\mathrm{i}\in B_n} \mathrm{f}(v_n^i)). \quad (5)$$

The fact that the aforementioned loss overlooks the aberrant video's underlying temporal structure is one of its limitations. Initially, anomalies in real-world situations often last for a brief period of time. In this instance, there could just be a few portions that have the anomaly, as indicated by the sparse scores of the instances (segments) in the anomalous bag. Second, the anomaly score need to transition smoothly across video parts because the video is divided into pieces. Thus, by enforce temporal smoothness between anomaly scores of temporally adjacent video segments in order to minimize the difference in scores for surrounding video segments. The loss function is transformed by adding the smoothness and sparsity restrictions on the instance scores as expressed in Eq. 6.

$$\iota(B_a, B_n) = \max(0,\ 1 - \max_{\mathrm{i}\in B_a} \mathrm{f}(v_a^i) + \max_{\mathrm{i}\in B_n} \mathrm{f}(v_n^i)) + \lambda_1 \overbrace{\sum_i^{(n-1)}(\mathrm{f}(v_a^i) - \mathrm{f}(v_a^{i+1}))^2} + \lambda_2 \overbrace{\sum_i^n \mathrm{f}(v_a^i)} \quad (6)$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

where stands for the sparsity term and denotes the temporal smoothness term. In this MIL ranking loss, the error is back-propagated from the highest scored video portions in both positive and negative bags. After training on a large number of positive and negative bags, we expect the network to learn a generalized model to predict high scores for anomalous areas in positive bags. Lastly, the expression gives us the entire goal function that we have in Eq. 7

$$\mathcal{L}(w) = \iota(B_a, B_n) + \lambda_3 \parallel w \parallel_F \tag{7}$$

W stands for model weights in this instance. Every video is divided into an equal quantity of discrete temporal segments, which are then utilized as bag instances. We extract the 3D convolution features given each section of the movie [36]. We employ this feature representation because it is computationally efficient and clearly able to capture appearance and motion dynamics in the context of video action detection.

Algorithm: Learning based Video Anomaly Detection (LbVAD)
Input: Our training dataset of videos D, test video v
Output: Anomaly detection results R and performance statistics P

1. Begin
2. Configure enhanced CNN model m
3. Compile the model m
4. F←ExtractFeatuers(v)
5. (pbags, nbags)←Divide(F)
6. Train m with D
7. Save the model m
8. R←DetectAbnormalities(m, pbags, nbags)
9. P←Evaluation(R, ground truth)
10. Display R
11. Display P
12. End

Algorithm 1: Learning based Video Anomaly Detection (LbVAD)

Our suggested method is dubbed Learning based Video Anomaly Detection (LbVAD) which exploits the enhanced CNN model for its functionality. A loss function is defined to reduce error rate in the prediction process. We collected dataset from different benchmark datasets such as UMN, UCSD, Ped1 and Ped2 for empirical study. Our algorithm is based on enhanced CNN. The given training data is used by the model to learn and gain knowledge. The given test video is subjected to feature extraction and dividing the features into positive and negative bags. These are further given to learned model to perform abnormality detection.

4. EXPERIMENTAL RESULTS

This segment showcases experimental results of our methodology. Python 7 and libraries like Keras and Tensorflow are used for developing an improved CNN model used as part of the proposed framework. A loss function is defined to reduce error rate in the prediction process. We collected dataset from several benchmark datasets, including Ped1 and Ped2, UMN, UCSD, and others, for empirical research.

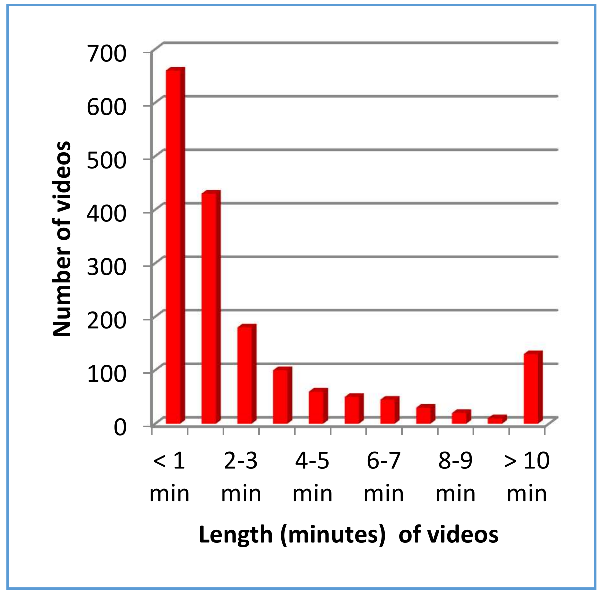

Figure 2: Dataset Dynamics In Terms Number Of Videos And The Length

As presented in Figure 2, the dataset we collected has been distributed into videos of different lengths.

Abuse	Arson	Accident	Vandalism	Arrest	Assault	Burglary
						

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Normal	Explosion	Robbery	Stealing	Fighting	Shooting	Shoplifting

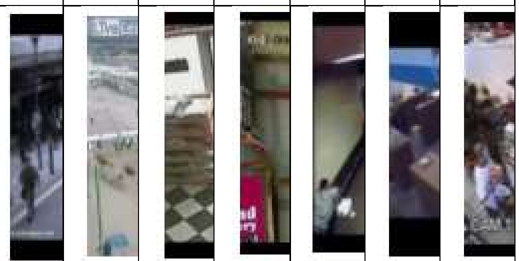

Figure 3: Abnormality Detection Results Of Experiments

As presented in Figure 3, different abnormal activities are detected by the very accurate system that has been suggested. Performance statistics are obtained by comparing the predictions with the ground truth.

Table 2: Performance Comparison

Method	AUC
Binary classifier method	75.45
Method in [34]	80.60
Method [35]	85.51
Proposed method	92.79

As shown in Table 2, the suggested method's performance is expressed in terms of AUC and contrasted with that of the current approaches.

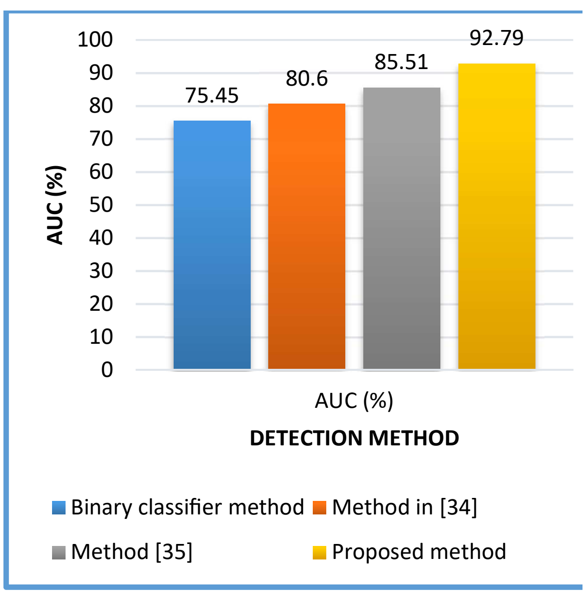

Figure 4: Performance Comparison Among Detection Models

As presented in Figure 4, the proposed method for automatic detection of video anomalies is measured in terms of AUC. Higher in AUC indicates better performance. It has been noted that the suggested approach showed highest performance due to its efficient internal processing and loss function. The baseline binary classifier showed 75.45% ACU, the method in [34] 80.60%, the method in [35] 85.51% while the proposed method exhibited 92.79% AUC. Based on the findings, it can be concluded that the suggested technique provides a reliable means of automatically identifying anomalies in public surveillance footage.

5. CONCLUSION AND FUTURE WORK

Our proposal in this study was to use deep learning to framework for automatically detecting abnormalities from surveillance videos. For anomaly detection, an improved Convolutional Neural Network (CNN) model is employed. In our proposed technique, anomaly identification is formulated as a regression issue. The aim is to get higher anomaly scores for the anomalous than for the normal video parts. Applying a ranking loss that encourages high scores for aberrant video sections relative to typical segments would be the easiest approach. We presented a method that utilizes the upgraded CNN model for its functionality, called Learning based Video Anomaly Detection (LbVAD). To lower the prediction process's error rate, a loss function is defined. Ped1 and Ped2, UMN, UCSD, and other benchmark datasets are utilized in empirical research. According on the outcomes of our experiments, the suggested algorithm performs better than current models with 92.79% accuracy. Our goal is to enhance our framework in the future by including deep learning models based on the Generative Adversarial Network (GAN) architecture.

REFERENCES

[1] Nayak Rashmiranjan, Pati Umesh Chandra and Das Santos Kumar. (2021). A comprehensive review on deep learning-based methods for video anomaly detection. Image and Vision Computing, 106, pp.1–69. doi:10.1016/j.imavis.2020.104078

[2] Aberkane Sabrina and Elarbi Mohamed. (2019). Deep Reinforcement Learning for Real-world Anomaly Detection in Surveillance Videos, IEEE, pp.1–5. doi:10.1109/ISPA48434.2019.8966795

[3] Kiran B, Thomas Dilip and Parakkal Ranjith. (2018). An Overview of Deep Learning Based Methods for Unsupervised and Semi-Supervised Anomaly Detection in Videos. Journal of Imaging, 4(2), pp.1–25. doi:10.3390/jimaging4020036

[4] Khaleghi Ali and Moin Mohammad Shahram. (2018). Improved anomaly detection in surveillance videos based on a deep learning method, IEEE, pp.73–81. doi:10.1109/RIOS.2018.8406634

[5] Sareer Ul Amin, Mohib Ullah, Muhammad Sajjad and Faouzi Alaya Cheikh. (2022). EADN An Efficient Deep Learning Model for Anomaly Detection in Videos. MDPI, pp.1-15.

[6] Sultani Waqas, Chen Chen and Shah Mubarak. (2018). Real-World Anomaly Detection in Surveillance Videos, pp.6479–6488. doi:10.1109/CVPR.2018.00678

[7] Khosro Rezaee, Sara Mohammad Rezakhani, Mohammad R. Khosravi and Mohammad Kazem Moghimi. (2021). A survey on deep learning-based real-time crowd anomaly detection for secure distributed video surveillance. Personal and Ubiquitous Computing, pp.1–17. doi:10.1007/s00779-021-01586-5

[8] Mohan Aiswarya, Choksi Meghavi and Zaveri Mukesh A. (2019). Anomaly and Activity Recognition Using Machine Learning Approach for Video Based Surveillance, IEEE, pp.1–6. doi:10.1109/ICCCNT45670.2019.8944396

[9] Rashmika Nawaratne, Damminda Alahakoon and Xinghuo YuDaswin De Silva. (2019). Spatiotemporal Anomaly Detection using Deep Learning for Real-time Video Surveillance. IEEE, pp.1-10.

[10] Prakhar Singh and Vinod Pankajakshan. (2018). A Deep Learning Based Technique for Anomaly Detection in Surveillance Videos. National Conference on Communications (NCC), pp.1-6. doi:10.1109/NCC.2018.8599969

[11] Chriki Amira, Touati Haifa, Snoussi Hichem and Kamoun Farouk. (2020). Deep learning and handcrafted features for one-class anomaly detection in UAV video. Multimedia Tools and Applications, pp.1–22. doi:10.1007/s11042-020-09774-w

[12] Doshi Keval and Yilmaz Yasin (2020). Continual Learning for Anomaly Detection in Surveillance Videos. IEEE, pp.1025–1034. doi:10.1109/CVPRW50498.2020.00135

[13] Chongke Wu, Sicong Shao, Cihan Tunc, Pratik Satam and Salim Hariri. (2022). An explainable and efficient deep learning framework for video anomaly detection. Springer, pp.2715–2737.

[14] Romany F. Mansour, José Escorcia-Gutierrez, Margarita Gamarra, Jair A. Villanueva and Nallig Leal. (2021). Intelligent video anomaly detection and classification using faster RCNN with deep reinforcement learning model. Image and Vision Computing, pp.1–9. doi:10.1016/j.imavis.2021.104229

[15] Kavikuil K. and Amudha J. (2018). Leveraging Deep Learning for Anomaly Detection in Video Surveillance. First International Conference on Artificial Intelligence and Cognitive Computing, pp.239–247. doi:10.1007/978-981-13-1580-0_23

[16] Wu Peng, Liu Jing, Li Mingming, Sun Yujia and Shen Fang. (2020). Fast Sparse Coding Networks for Anomaly Detection in Videos. Pattern Recognition, pp.1–50. doi:10.1016/j.patcog.2020.107515

[17] Pawar Karishma and Attar Vahida. (2018). Deep learning approaches for video-based anomalous activity detection. World Wide Web, pp.1–. doi:10.1007/s11280-018-0582-1

[18] Fan Yang, Zhiwen Yu, Liming Chen, Jiaxi Gu, Qingyang Li and Bin Guo. (2021). Human-Machine Cooperative Video Anomaly Detection . Proceedings of the ACM on Human-Computer Interaction, pp.1–18. doi:10.1145/3434183

[19] Mohan Aiswarya, Choksi Meghavi and Zaveri Mukesh A (2019). Anomaly and Activity Recognition Using Machine Learning Approach for Video Based Surveillance, IEEE, pp.1–6. doi:10.1109/ICCCNT45670.2019.8944396

[20] Romany F. Mansour, José Escorcia-Gutierrez, Margarita Gamarra, Jair A. Villanueva and Nallig Leal. (2021). Intelligent video anomaly detection and classification using faster RCNN with deep reinforcement learning model. Image and Vision Computing, pp.1–9. doi:10.1016/j.imavis.2021.104229

[21] Aberkane Sabrina and Elarbi Mohamed. (2019). Deep Reinforcement Learning for

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Real-world Anomaly Detection in Surveillance Videos, pp.1–5. doi:10.1109/ISPA48434.2019.8966795

[22] Tuan-Hung Vu, Jacques Boonaert, Sebastien Ambellouis and Abdelmalik Taleb-Ahmed. (2021). Multi-Channel Generative Framework and Supervised Learning for Anomaly Detection in Surveillance Videos. Sensors, pp.1–16. doi:10.3390/s21093179

[23] Weixin Luo, Wen Liu, Dongze Lian, Jinhui Tang, Lixin Duan, Xi Peng and Shen. (2019). Video Anomaly Detection with Sparse Coding Inspired Deep Neural Networks. IEEE, pp.1-15.

[24] Ravanbakhsh Mahdyar, Nabi Moin, Sangineto Enver, Marcenaro Lucio, Regazzoni Carlo and Sebe Nicu. (2017). Abnormal event detection in videos using generative adversarial nets. , IEEE, pp.1577–1581. doi:10.1109/ICIP.2017.8296547

[25] Ribeiro Manassés, Lazzaretti André Eugênio and Lopes Heitor Silvério (2017). A study of deep convolutional auto-encoders for anomaly detection in videos. Pattern Recognition Letters, pp.1–13. doi:10.1016/j.patrec.2017.07.016

[26]. Mujtaba Asad, He Jiang, Jie Yang, Enmei Tu and Aftab Ahmad Malik. (2021). Multi-Stream 3D latent feature clustering for abnormality detection in videos . Applied Intelligence. doi:10.1007/s10489-021-02356-9

[27] Chang Y., Tu Z., Xie W., Luo B., Zhang S., Sui H., and Yuan J. (2022). Video anomaly detection with spatio-temporal dissociation. Pattern Recognition, 122, pp.1-12 doi:10.1016/j.patcog.2021.108213

[28] Huu-Thanh Duong, Viet-Tuan Le and Vinh Truong Hoang. (2023). Deep Learning-Based Anomaly Detection in Video Surveillance A Survey. MDPI, pp.1-25.

[29] Zaheer M. Zaigham, Lee Jin Ha, Lee Seung-Ik and Seo Beom-Su. (2019). A Brief Survey on Contemporary Methods for Anomaly Detection in Videos, IEEE, pp.472–473. doi:10.1109/ICTC46691.2019.8939930

[30] Sabah Abdulazeez Jebur, Khalid A. Hussein, Haider Kadhim Hoomod and Laith. (2023). Review on Deep Learning Approaches for Anomaly Event Detection in Video Surveillance. MDPI, pp.1-22.

[31] S.Andrews, I. Tsochantaridis, and T. Hofmann. Support vector machines for multiple-instance learning. In NIPS, pages 577–584, Cambridge, MA, USA, 2002. MIT Press.

[32] V. Chandola, A. Banerjee, and V. Kumar. Anomaly detection: A survey. ACM Comput. Surv., 2009.

[33] X. Cui, Q. Liu, M. Gao, and D. N. Metaxas. Abnormal detection using interaction energy potentials. In CVPR, 2011.

[34] M. Hasan, J. Choi, J. Neumann, A. K. Roy-Chowdhury, and L. S. Davis. Learning temporal regularity in video sequences. In CVPR, June 2016.

[35] C. Lu, J. Shi, and J. Jia. Abnormal event detection at 150 fps in matlab. In ICCV, 2013.

[36] D. Tran, L. Bourdev, R. Fergus, L. Torresani, and M. Paluri. Learning spatiotemporal features with 3d convolutional networks. In ICCV, 2015.