International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X
Original Research Paper
www.ijdim.com

AbusoGAN: GAN-Based AI System for Detecting Abuse, Unlawful Activities, and Suspicious Behavior in Surveillance Video Streams for Security Applications

[1]Dr. A. Tirupatiah,[2]Ravuri Hiranmai,[3]Velpuri Pavithra,[4]Shaik Adam Shafi
[1]Associate Professor, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.
[2,3,4]B. Tech Student, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

ABSTRACT

AbusoGAN is a sophisticated surveillance system that applies deep learning techniques to identify abuse, illegal behavior, and unusual activity in video feeds. By integrating Generative Adversarial Networks and Convolutional Neural Networks, it processes security footage and automatically identifies unusual activities. The process includes extracting frames from uploaded videos and processing them using trained AI models to identify unusual activities. A secure web interface is used for user login and provides real-time prediction output. It reduces manual surveillance and improves prediction accuracy, providing a detailed description of activities and video playback for confirmation.

KEY WORDS: Deep Learning, Surveillance System, GAN, CNN, Activity Detection, Computer Vision, Abnormal Behavior Detection.

INTRODUCTION

Surveillance systems are an important component of the current security in public areas, schools, transportation hubs, and smart cities. They generate massive video data that needs to be constantly monitored to identify abnormal behavior. In the past, it was done by human observers, but this is time-consuming and prone to missing out on important details. With the increasing number of cameras, manual monitoring of the system is not feasible. Therefore, intelligent automated surveillance systems using Artificial Intelligence and Deep Learning techniques are becoming essential for real-time monitoring and threat detection. These systems improve accuracy, reduce human effort, and enable faster responses to suspicious activities and emergency situations. The development of artificial intelligence and computer vision has enabled the automation of surveillance systems, allowing for the accurate identification of

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X
www.ijdim.com
Original Research Paper

GANs that identifies abuse, illegal behavior, and suspicious activity in video streams. The system analyzes video frames using deep learning models and provides automated outputs.

LITERATURE REVIEW

Recent breakthroughs in artificial intelligence and computer vision have enabled the development of automated surveillance systems. These systems can process video streams without human supervision. In the past, traditional image processing and manually designed features were employed.

However, these approaches were difficult to scale and less accurate. Deep learning has enabled the use of Convolutional Neural Networks (CNNs) to enhance image and video classification through the automatic learning of valuable features. Generative Adversarial Networks (GANs) have also assisted in the detection of unusual events by learning typical and unusual data patterns. Some research has combined CNNs with approaches that learn from time to demonstrate the ability to identify activities in video streams.

RELATED WORK

There have been a few research on automatic anomaly detection of surveillance videos employing deep

learning. CNNs are widely applied for action recognition since they extract good features. GANs assist in the detection of abnormal patterns by learning the typical appearance of data. Weakly supervised and unsupervised approaches have been adopted to reduce the dependence on labeled data. Some research applies recurrent networks to capture time in video analysis. Despite the progress, most of the current systems are only applicable to particular datasets or controlled settings. This indicates the requirement for scalable and feasible surveillance solutions such as AbusoGAN.

EXISTING SYSTEM

Conventional surveillance systems rely on human observers to monitor the screens. The security personnel monitor the screens continuously to identify any suspicious behavior, but this makes them lethargic and less responsive.

Some conventional systems rely on simple motion detection, which simply detects the motion but does not interpret it. They fail to detect complex events such as violence and theft. It is inefficient to monitor multiple camera feeds simultaneously. This makes the system less accurate and less responsive to incidents. This highlights the need for intelligent AI-based surveillance systems.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X
www.ijdim.com
Original Research Paper

PROPOSED SYSTEM

The proposed AbusoGAN system is an AI-based surveillance system that automatically detects abuse and suspicious events in video recordings. The system processes security videos via a safe web interface and applies computer vision to analyze the videos. The system pre-processes video frames and analyzes them using a deep learning model assisted by GAN. The generative network enhances the learning of features and improves the model's ability to detect anomalies. A CNN classifier determines the activity being performed and predicts the outcome. The system provides activity names, descriptions, and recommendations. Video playback is enabled to confirm the accuracy of the results.

SYSTEM ARCHITECTURE

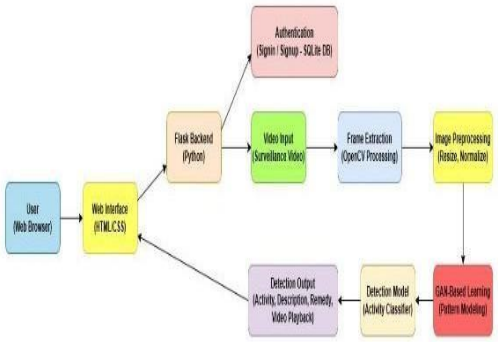


Fig 1: System Architecture

METHODOLOGY

The process involves a straightforward and step-by-step workflow. The process begins when a video is uploaded via the web interface. The video is then processed frame by frame for analysis. The frames are preprocessed to normalize, resize, and rearrange them according to what the deep learning model requires. The trained model examines each frame to identify abnormal or suspicious activity. GAN-assisted learning enables the model to identify features more easily, making it simpler to distinguish between normal and abnormal activities. A CNN-based classifier is then used to predict and classify the activities. The output is presented on a web page with labels, descriptions, and valuable insights of the activities. The optimized preprocessing and fast inference ensure that the performance is consistent and detection is fast.

RESULTS AND DISCUSION

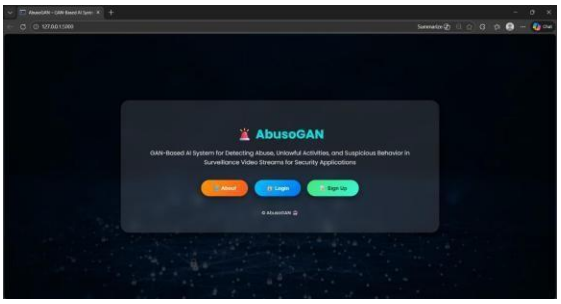
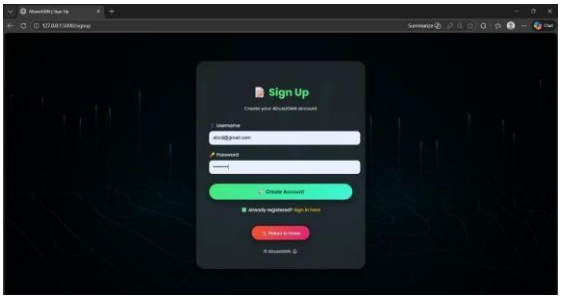


Fig.2: Home Page

The homepage presents a clean and visually appealing interface displaying the project title and description. It includes About, Sign In, and Sign Up buttons for easy navigation.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X
www.ijdim.com
Original Research Paper



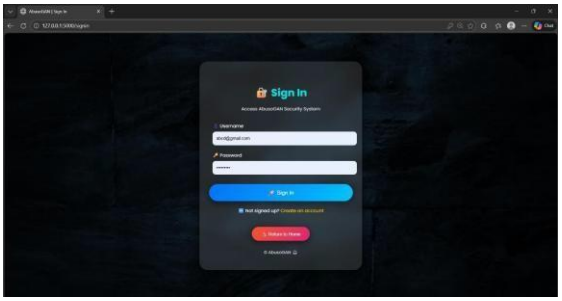


Fig.3: Sign In & Sign Up Pages

The Sign Up and Sign In pages provide a secure authentication interface for user registration and login. Users can create a new account or enter valid credentials to access the AbusoGAN system.

Fig.4: Video Upload Page

The video upload page provides a simple interface for submitting surveillance videos for analysis. Users can choose a video file and start the detection process using the Analyze Video button.

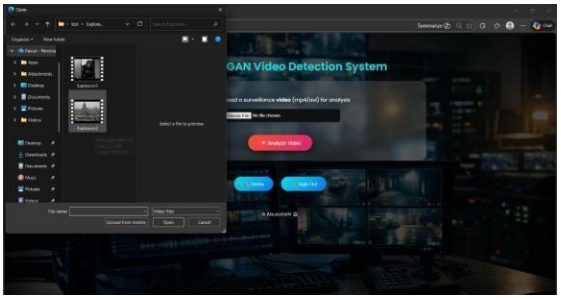
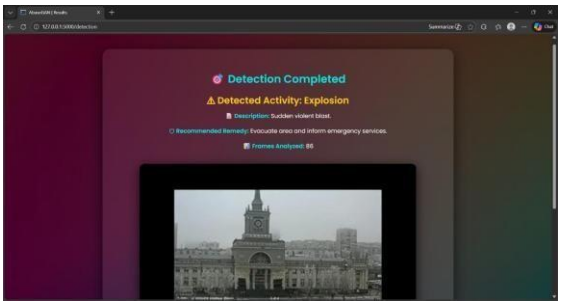


Fig.5: File Selection Dialog

The file selection dialog allows users to browse and choose a surveillance video from local storage. The selected file is displayed before initiating the detection process.



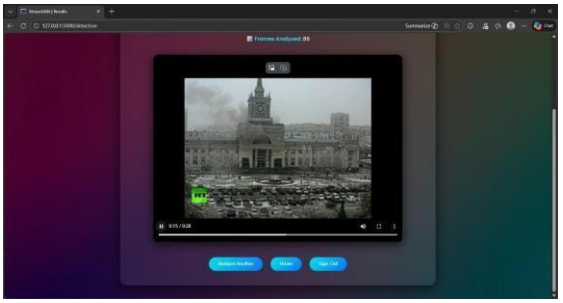


Fig.6: Detection Result Page

The detection result page shows the predicted activity with description and remedy. It also includes video playback for result verification.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X
www.ijdim.com
Original Research Paper

CONCLUSION AND FUTURE ENHANCEMENTS

Conclusion

ABUSOGAN effectively uses GAN-based deep learning to detect abuse, unlawful activities, and suspicious behavior in real-time surveillance. It identifies anomalies by learning normal patterns, reduces manual monitoring, and improves security response with accurate, automated alerts. The system is scalable and suitable for modern surveillance applications.

Future Enhancements

Future improvements include training with larger datasets for better accuracy, adding audio analysis for multimodal detection, and using edge computing for low-latency performance. Integration with IoT systems, explainable AI, and privacy-preserving techniques can further enhance reliability and ethical deployment.

REFERENCES

1. Harini, P. (2019). GESTURE CONTROLLED GLOVES FOR GAMING AND POWER POINT PRESENTATION CONTROL. *GESTURE*, *6*(12).
2. Krizhevsky, A., Sutskever, I., & Hinton,
3. G. E. (2012). ImageNet Classification with Deep Convolutional Neural Networks. *Advances in Neural Information Processing Systems*, 25, 1097–1105.
4. Simonyan, K., & Zisserman, A. (2015). Very Deep Convolutional Networks for Large-Scale Image Recognition. *International Conference on Learning Representations*.
5. He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep Residual Learning for Image Recognition. *IEEE Conference on Computer Vision and Pattern Recognition*, 770–778.
6. Sultani, W., Chen, C., & Shah, M. (2018). Real-World Anomaly Detection in Surveillance Videos. *IEEE Conference on Computer Vision and Pattern Recognition*, 6479–6488.
7. Hasan, M., Choi, J., Neumann, J., Roy-Chowdhury, A. K., & Davis, L. (2016). Learning Temporal Regularity in Video Sequences. *IEEE Conference on Computer Vision and Pattern Recognition*, 733–742.
8. Ravanbakhsh, M., Nabi, M., Mousavi, H., Sangineto, E., & Sebe, N. (2017). Abnormal Event Detection in Videos Using Generative Adversarial Nets. *IEEE International Conference on Image Processing*, 1577–1581.
9. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly Detection: A Survey. *ACM Computing Surveys*, 41(3), 1–58.
10. Tran, D., Bourdev, L., Fergus, R., Torresani, L., & Paluri, M. (2015). Learning Spatiotemporal Features with 3D Convolutional Networks. *IEEE International Conference on Computer Vision*, 4489–4497.
11. Ionescu, R. T., Smeureanu, S., Alexe, B., & Popescu, M. (2019). Detecting Abnormal Events in Video Using Narrowed Normality Clusters. *IEEE Winter Conference on Applications of Computer*

Vision, 1951–1960.

12. Medel, J. R., & Savakis, A. (2016). Anomaly Detection in Video Using Predictive Convolutional LSTM Networks.
13. Zhu, Y., Newsam, S., & Zheng, L. (2020). Video Anomaly Detection Using Deep Learning: A Survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*.
14. Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You Only Look Once: Unified, Real-Time Object Detection. *IEEE Conference on Computer Vision and Pattern Recognition*, 779–788.
15. Liu, W., Anguelov, D., Erhan, D., Szegedy, C., Reed, S., Fu, C. Y., & Berg, A. C. (2016). SSD: Single Shot MultiBox Detector. *European Conference on Computer Vision*, 21–37.
16. Sabokrou, M., Fathy, M., Hoseini, M., & Klette, R. (2017). Deep-Anomaly: Fully Convolutional Neural Network for Fast Anomaly Detection in Crowded Scenes. *Computer Vision and Image Understanding*, 172, 88–97.
17. Doshi, K., & Yilmaz, Y. (2020). Continual Learning for Anomaly Detection in Surveillance Videos. *IEEE International Conference on Image Processing*.
18. UCF-Crime Dataset. (2018). Large-Scale Anomaly Detection Dataset for Surveillance Videos. University of Central Florida.
19. Paszke, A., Gross, S., Massa, F., et al. (2019). PyTorch: An Imperative Style, High-Performance Deep Learning Library. *Advances in Neural Information Processing Systems*, 32.
20. Bradski, G. (2000). The OpenCV Library.
21. *Dr. Dobb's Journal of Software Tools*.
22. Bishop, C. M. (2006). Pattern Recognition and Machine Learning. Springer.