International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 07 | July - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

SUSPICIOUS ACTIVITY RECOGNITION

Shreyas K[1], Seema Nagaraj[2]

[1]*Student, Department of MCA, Bangalore Institute of Technology, Karnataka, India*

[2]*Professor, Department of MCA, Bangalore Institute of Technology, Karnataka, India*

ABSTRACT

In the current security-focused environment, the necessity for advanced surveillance systems capable of detecting suspicious activities is more critical than ever. This project introduces an innovative approach for recognizing such activities using deep learning algorithms on video data. Utilizing the DCSASS Dataset, which includes videos across thirteen distinct classes of suspicious activities such as abuse, arson, assault, and robbery, we developed a hybrid architecture integrating ResNet50 and I3D to manage the temporal and spatial complexities inherent in video data. Our model achieved significant accuracy during training, with approximately 85% accuracy on a validation set. Enhancements included data augmentation, fine-tuning hyperparameters, and ensemble techniques, prioritizing model interpretability through class activation mapping. This project aims to provide a robust, reliable solution for autonomous surveillance systems, reducing reliance on error-prone human monitoring and enhancing real-time security measures.

Keywords Deep Learning, Surveillance Systems, Suspicious Activity Detection, Video, Data Analysis, ResNet50

1. INTRODUCTION

The proliferation of surveillance systems has become ubiquitous, driven by the growing need for security in both public and private spaces. Traditional surveillance methods, heavily reliant on human monitoring, are resource-intensive and prone to errors. Deep learning, inspired by the structure and function of the human brain, has emerged as a powerful tool for analyzing complex data such as images, audio, and video. Our project focuses on developing an advanced surveillance system using deep learning algorithms to recognize suspicious activities, addressing challenges like temporal dynamics, spatial relationships, and semantic understanding. By leveraging the DCSASS Dataset, our system, integrating ResNet50 and I3D architectures, captures both spatial and temporal features, ensuring high accuracy in activity recognition.

2. PROBLEM STATEMENT

The development of efficient surveillance systems capable of automatically recognizing and classifying suspicious activities in video data is critical. Traditional surveillance methods relying on manual monitoring are labor-intensive, prone to human error, and lack scalability. This project aims to design and implement an automated surveillance system leveraging deep learning algorithms to detect and classify suspicious activities in real-time. The system addresses challenges associated with video data, such as temporal dynamics and spatial relationships, using a hybrid architecture combining ResNet50 and I3D. The goal is to enhance situational awareness and enable prompt responses to potential threats.

3. LITERATURE SURVEY

Suspicious Activity Detection Using Deep Learning in Secure Assisted Living IoT Environments - Alexei et al. (2020) developed a method integrating deep learning with IoT to enhance real-time surveillance capabilities[1]. **Hybrid Deep Learning Models for Trustworthy Suspicious Activity Detection** - Amrutha et al. (2020) proposed hybrid models combining CNNs, GRUs, and ConvLSTM networks for high accuracy in activity detection[2]. **A Novel Approach for Suspicious Activity Detection** - Ling et al. (2020) utilized an attention-based convolutional neural network for improved classification accuracy[3]. **EASAD: Efficient and Accurate Suspicious Activity Detection** - Kashika and Venkatapur (2022) introduced a framework integrating enhanced SqueezeNet and U-Net

segmentation for efficient detection[4]. **Detection of Suspicious Human Activities Using Neural Networks** - Kumar et al. (2020) used neural networks and k-means clustering for feature extraction, enhancing real-time detection accuracy[5].

4. EXISTING SYSTEM

Traditional surveillance systems heavily depend on human monitoring, which is resource-intensive and prone to errors. These systems typically involve security personnel observing multiple screens, looking for any unusual activities or behaviours. This approach is not only labour-intensive but also suffers from human limitations, such as fatigue and inattentiveness, which can lead to missed incidents or delayed responses. Additionally, existing automated surveillance systems often rely on predefined rules or heuristics to detect suspicious activities. These systems can identify specific, well-defined actions but struggle with more complex or evolving behaviours. They lack the flexibility to adapt to new types of threats and are often limited by their reliance on static models that do not learn from new data. The combination of manual monitoring and rule-based automation results in a surveillance framework that is neither scalable nor sufficiently adaptable to handle the dynamic nature of real-world environments effectively.

5. PROPOSED SYSTEM

The proposed system leverages advanced deep learning algorithms to create an automated surveillance system efficient of recognizing and classifying suspicious activities in real-time. By utilizing a hybrid architecture that combines elements from ResNet50 and I3D, the system can adeptly capture both spatial and temporal features from video data. This deep learning-based approach allows the model to learn complex patterns indicative of suspicious behaviour, making it more adaptable and accurate than traditional methods. The system is trained on the DCSASS Dataset, which includes a broad spectrum of suspicious activities, ensuring comprehensive coverage and robust performance. Different techniques for improving performance, like data augmentation, hyperparameter tuning, and ensemble learning, are employed to optimize the model's precision and dependability. The proposed system also emphasizes model interpretability, using methods such as class activation mapping to provide insights into the decision-making process. By integrating these advanced techniques, the proposed system aims to provide a scalable, efficient, and highly accurate solution for enhancing surveillance capabilities across diverse environments, significantly improving security measures and situational awareness.

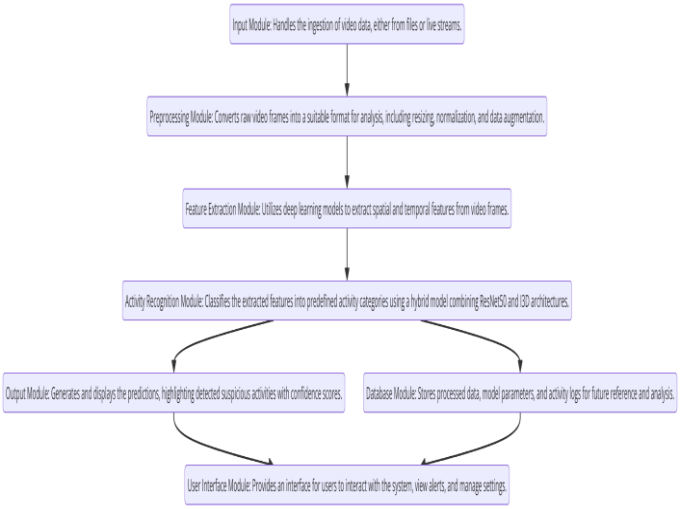

Fig 1- System Architecture

6. METHODOLOGY

1. **Dataset Acquisition and Annotation**: Procure and annotate a comprehensive dataset with video clips depicting various suspicious activities.
2. **Model Architecture Design**: Develop a hybrid deep learning architecture combining ResNet50 and I3D to capture spatial and temporal features.
3. **Model Training and Evaluation**: Train the model using the annotated dataset, optimizing parameters to maximize accuracy. Evaluate performance using metrics like accuracy, precision, recall, and F1-score.
4. **Performance Enhancement**: Explore techniques such as data augmentation, hyperparameter tuning, and ensemble learning to improve model performance.
5. **Real-world Deployment**: Demonstrate the system's effectiveness in real-world scenarios, evaluating its robustness under different conditions.

7. RESULT AND DISCUSSION

The developed model achieved an accuracy of approximately 85% on the validation set. Enhancements through data augmentation, hyperparameter tuning, and ensemble learning further improved performance. The system effectively captures both spatial and temporal features, ensuring reliable activity recognition in diverse environments. The use of class activation mapping provided insights into the decision-making process, enhancing model interpretability. Future work will focus on expanding the dataset, exploring advanced model architectures, and improving real-time processing capabilities.

Fig 2- Project Output

8. CONCLUSION

The Suspicious Activity Detection System has been carefully crafted and implemented to enhance security measures through the automated detection and classification of suspicious activities in video surveillance feeds. Utilizing state-of-the-art deep learning techniques, the system offers a robust and scalable solution capable of operating in real-time on a local server. Throughout the project, we have achieved significant milestones, including the successful deployment of a hybrid deep learning model, comprehensive system integration, and extensive testing to ensure functionality, performance, and reliability.

9. REFERENCES

1. **Amrutha CV, Jyotsna C, Amudha J. "Deep learning approach for suspicious activity detection from surveillance video." IEEE Xplore, 2020.**
2. **Idrees H, Zamir AR, Jiang YG, et al. "The THUMOS challenge on action recognition for videos 'in the wild'." Computer Vision and Image Understanding, 2017.**
3. **Kashika PH, Venkatapur RB. "Automatic tracking of objects using improvised Yolov3 algorithm and alarm human activities in case of anomalies." International Journal of Information Technology, 2022.**
4. **Kumar IP, Gopal VH, Ramasubbareddy S, et al. "Dominant color palette extraction by k-means clustering algorithm and reconstruction of image." Data Engineering and Communication Technology, Springer, 2020.**
5. **Ling H, Wu J, Huang J, Chen J, Li P. "Attention-based convolutional neural network for deep face recognition." Multimedia Tools and Applications, 2020.**