International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 21 No. 3 (1) 2025

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, No. 3(1), 2025

Research Paper

ANOMALYNET: AN ANOMALY DETECTION NETWORK FOR VIDEO SURVEILLANCE

[1] S. Komali,[2] A. Chathrika,[3] P. Manish ,[4] T.K. Nithin,[5] T. Priyanka
[1234] Students, [5] Assistant Professor
Department Of Computer Science and Design
Teegala Krishna Reddy Engineering College, Meerpet, Balapur, Hyderabad-500097

ABSTRACT

Sparse coding based anomaly detection has shown promising performance, of which the keys are feature learning, sparse representation, and dictionary learning. In this work, we propose a new neural network for anomaly detection (termed AnomalyNet) by deeply achieving feature learning, sparse representation and dictionary learning in three joint neural processing blocks. Specifically, to learn better features, we design a motion fusion block accompanied by a feature transfer block to enjoy the advantages of eliminating noisy background, capturing motion and alleviating data deficiency. Furthermore, to address some disadvantages (e.g., nonadaptive updating) of existing sparse coding optimizers and embrace the merits of neural network (e.g., parallel computing), we design a novel recurrent neural network to learn sparse representation and dictionary by proposing an adaptive iterative hard- thresholding algorithm (adaptive ISTA) and reformulating the adaptive ISTA as a new long short term memory (LSTM).

Received: 10-7-2025 Accepted: 18-8-2025 Published: 25-8-2025

I. INTRODUCTION

With the increasing demand for security, surveillance cameras have been widely deployed as the infrastructure for video analysis. One major challenge faced by surveillance video analysis is detecting abnormal events (see Figure 1 for an intuitive illustration), which requires exhausting human efforts. Fortunately, such a labor-intensive task can be recast as an anomaly detection problem [1], [2], [3] which aims to identify unexpected events or patterns. Anomaly detection differs from the traditional classification problem in the following aspects: 1) It is very difficult to list all possible negative (anomaly) samples. 2) It is a daunting task to collect sufficient negative samples due to the rarity. To achieve anomaly detection, one of the most popular methods is using the videos of normal events as training data to learn a model, and then detecting the abnormal events which would do not conform the learned model. Following the aforementioned strategy, sparse coding has successfully applied to anomaly detection [4], [5], which consists of dictionary learning and sparse representation. To be specific, sparse coding based anomaly detection (SCAD) first learns a dictionary from a training data set that only consists of normal events and then discovers the abnormal events that cannot be exactly reconstructed by a few of atoms of the learned dictionary. In other words, SCAS assumes that an abnormal event always leads to a large reconstruction error since it does not appear in the training data. Furthermore, extensive studies [5], [6], [7] have proved that well-established features could remarkably improve the performance of anomaly detection, namely, feature learning and sparse coding have lay onto the heart of SCAD. During past decades, a variety of features have been widely used in SCAD. For example, histogram of oriented gradients (HOG) [8], 3D spatiotemporal gradient [9], and the histogram of oriented flows (HOF) [10] have been extensively used in [6], [11], [12], [13]. The

major disadvantage of these works is that the used features are handcrafted while data-driven ones are more favourable since the latter could lead to better performance. To enjoy the representative capacity of neural networks, some recent works tried to marriage deep learning and anomaly detection.

MOTIVATION

In an increasingly security-conscious world, video surveillance has become a critical tool for monitoring public and private spaces. However, the sheer volume of video data generated makes it impractical for human operators to manually monitor and identify unusual or suspicious activities in real-time. This challenge highlights the urgent need for intelligent systems that can automatically detect anomalies with high accuracy and efficiency.

ANOMALYNET is motivated by the goal of enhancing the effectiveness of surveillance systems through the integration of deep learning techniques for automatic anomaly detection. By leveraging the power of neural networks, this project aims to create a robust and scalable solution that can learn complex patterns in video streams and identify deviations that may indicate threats, accidents, or abnormal behavior—without the need for manual intervention.

The core motivation behind ANOMALYNET is to contribute to the development of safer environments by enabling proactive responses to potential incidents, minimizing human error, and reducing the burden on security personnel. The project seeks to bridge the gap between traditional surveillance and intelligent, real-time anomaly detection, ultimately paving the way for smarter and more secure spaces.

PROBLEM STATEMENT

Video surveillance systems are widely used for ensuring security in public and private spaces, but they often rely on human operators to monitor multiple video feeds simultaneously. This manual approach is not only time-consuming but also prone to human error due to fatigue, distraction, or information overload. As a result, critical incidents or suspicious activities can go unnoticed, reducing the overall effectiveness of the surveillance system. Traditional surveillance lacks the capability to intelligently and automatically detect anomalies in real-time. Therefore, there is a pressing need for an automated, intelligent solution that can accurately and efficiently identify abnormal events or behaviours in video streams.

SCOPE and OBJECTIEVE

The objective of this project is to develop ANOMALYNET, a deep learning-based anomaly detection network designed specifically for video surveillance systems. The goal is to create an intelligent model capable of automatically identifying abnormal or suspicious activities in real-time, without the need for continuous human supervision. By learning normal behavioural patterns from video data, the system will be able to detect and flag deviations that may indicate potential threats, accidents, or unusual events. This will significantly enhance the effectiveness, accuracy, and responsiveness of surveillance systems, reduce human workload, and contribute to creating safer environments through smart, automated monitoring.

II. LITERATURE SURVEY

This work mainly involves anomaly detection oriented feature learning, sparse coding (i.e., sparse representation and dictionary learning), and RNN-based optimizers (i.e., LISTA and its variants). In this section, we briefly introduce these three topics one-by-one. Most existing works combine handcrafted features and spatial temporal information to represent videos for anomaly detection, such as histogram of oriented gradients (HOG) [27], 3D spatiotemporal gradient [28], histogram of oriented tracklets (HOT) [29], and histogram of optical flows [30]. The major disadvantage of these methods is that hand-crafted feature based methods cannot give a desirable performance in complex real-world situations. To embrace the data-driven feature learning [31], [32], recent attention has shifted from feature engineering to deep neural net- works.

For example, [33] proposes a two-stream network wherein one stream extracts either appearance or motion. However, the method ignores the connection between appearance and motion, thus breaking the spatiotemporal connection. [3], [34] propose using 3D-CNN to model normal video patterns by partitioning inputs into multiple video cubes. The major challenge is training a 3D-CNN since it involves much more parameters than traditional CNNs.

[14] recently proposes ConvLSTM-AE by incorporating convolutional filters into an LSTM to process sequential data in a self-supervised way. However, due to the limitation of architecture, it can only learn features from the local scope and cannot utilize the pre-trained models from other tasks. More recently, more and more researches focus on either of the fully convolutional neural networks (FCNs) [35] and generative adversarial networks (GANs) [36], [37], [38],[39].

EXISTING SYSTEM:

- **Manual Monitoring**: Human operators monitor surveillance footage, which is time- consuming and prone to errors.
- **Traditional Methods**: Utilize handcrafted features (e.g., HOG, 3D gradients) and rule- based algorithms but suffer from limited accuracy and scalability.
- **Deep Learning Models**: Previous models, like ConvLSTM and 3D-CNNs, handle motion and appearance separately, breaking the spatiotemporal connection and requiring large datasets for training.

DRAWBACKS:

- High False Alarm Rate
- Lack of Real-Time Processing
- Limited Generalization
- Scalability Issues
- Difficulty in Anomaly Definition
- Need for Large Labelled Datasets
- Privacy Concerns

PROPOSED SYSTEM:

The proposed system, AnomalyNet, is a deep learning framework for detecting anomalies in video surveillance. It focuses on:

- **Motion Fusion Block**: Compresses video frames into a single dynamic image, capturing both spatial and temporal motion information.
- **Feature Transfer Block**: Extracts spatiotemporal features using a pre-trained ResNet- 50 model for transfer learning.
- **Optimization Block (SC2Net)**: Utilizes an LSTM-based sparse coding network (SLSTM) to efficiently detect anomalies by learning sparse representations and dictionary updates.

III. MODULE DESCRIPTION

The ANOMALYNET project is divided into multiple interdependent modules that collectively enable real-time anomaly detection in video surveillance systems. Each module plays a crucial role in processing video input, detecting irregular activities, and generating alerts. Below is the description of the main modules:

1. Video Input Module

This module captures real-time video streams from surveillance cameras or pre-recorded video files. It handles video decoding, frame extraction, and frame resizing to ensure uniform input for further processing. It may support various formats and integrate with IP cameras or CCTV systems.

2. Preprocessing Module

This module prepares raw video frames for the anomaly detection model. Preprocessing may include operations such as grayscale conversion, noise reduction, normalization, background subtraction, and resizing. These steps enhance the quality and consistency of input data fed to the model.

3. Feature Extraction Module

In this module, visual features are extracted from the preprocessed frames using deep learning models, primarily Convolutional Neural Networks (CNNs). These features represent the spatial structure of the scene, allowing the model to learn patterns of normal and abnormal activities.

4. Temporal Analysis Module

Using Recurrent Neural Networks (RNNs) or Long Short-Term Memory (LSTM) networks, this module analyzes the temporal sequence of frames to detect unusual behavior over time. It helps in identifying patterns that are only detectable when considering movement across several frames, such as loitering or sudden crowd formation.

5. Anomaly Detection Module

This is the core module that classifies incoming video sequences as normal or anomalous. It uses the features and temporal data to compute anomaly scores. If the score crosses a predefined threshold, it flags the segment as suspicious. The model is trained on normal activity data to distinguish unexpected or rare events.

6. Alert and Notification Module

When an anomaly is detected, this module triggers real-time alerts through visual signals, sounds, or notifications via email, SMS, or mobile apps. This ensures immediate action can be taken by security personnel.

7. Data Storage and Logging Module

All video data, detection results, and logs are stored in a secure and structured manner for future reference, auditing, or retraining purposes. This module ensures data integrity and supports analytics and performance evaluation.

8. User Interface Module

A user-friendly interface allows operators to monitor live feeds, review anomalies, adjust system settings, and visualize model performance. It enhances usability and makes the system accessible to non-technical users.

Each module in ANOMALYNET is built with scalability, efficiency, and accuracy in mind, ensuring a robust and intelligent surveillance solution that can be deployed in a variety of environments.

IV. SYSTEM DESIGN

SYSTEM ARCHITECTURE

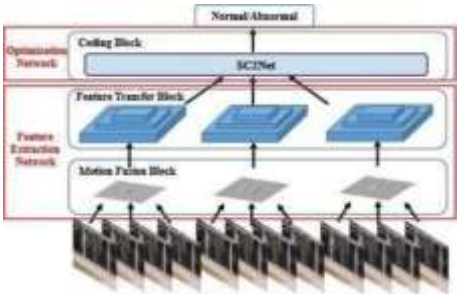

Fig. System Architecture

V. OUTPUT SCREENS

Fig: To Open Jupyter notebook

Fig: To Check the Code

Fig: Code

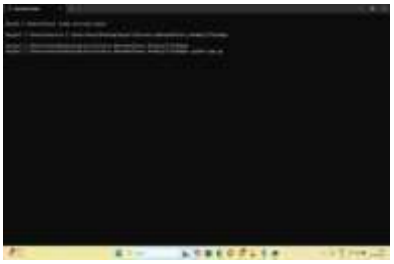

Fig: FlaskApp for Execution

Fig.: For output Press on link holding CTRL

Fig : Choose the Video file for the Output.

Fig: Choose the video file

Fig. :Output Is shown.

VI. CONCLUSION

ANOMALYNET: An Anomaly Detection Network for Video Surveillance offers a highly effective and technologically advanced solution to modern security challenges. With the rapid growth of surveillance systems in critical environments, the need for intelligent and automated anomaly detection has never been greater. By leveraging powerful machine learning techniques, such as Convolutional Neural Networks (CNNs) for spatial feature extraction and Recurrent Neural Networks (RNNs) or Long Short-Term Memory (LSTM) networks for temporal analysis, ANOMALYNET is designed to detect a wide range of anomalies in video feeds in real-time, significantly improving the accuracy, efficiency, and responsiveness of security operations. The system is technically feasible due to the availability of advanced technologies, including GPUs for processing and cloud infrastructure for scalability.

REFERENCE

1. B Kundan, Sangaralingam P. Combining Machine Learning and Deep Learning in the Retinopathy Diagnostic Algorithm for Enhanced Detection of DR and DME. J Neonatal Surg [Internet]. 2025Apr.2 [cited2025Apr.9];14(5):128-40.Availablefrom: https://www.jneonatalsurg.com/index.php/jns/article/view/2914
2. C. Lu, J. Shi, and J. Jia, “Abnormal event detection at 150 fps in matlab,”in Proceedings of the IEEE international conference on computer vision, 2013, pp. 2720–2727.
3. M. Sabokrou, M. Fathy, M. Hoseini, and R. Klette, “Real-time anomaly detection and localization in crowded scenes,” in The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops, June 2015.
4. M. Hasan, J. Choi, J. Neumann, A. K. Roy-Chowdhury, and L. S. Davis, “Learning temporal regularity in video sequences,” in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016, pp. 733–742.
5. B. Zhao, L. Fei-Fei, and E. P. Xing, “Online detection of unusual events in videos via dynamic sparse coding,” in Computer Vision and Pattern Recognition (CVPR), 2011 IEEE Conference on. IEEE, 2011, pp. 3313–3320.
6. W. Luo, W. Liu, and S. Gao, “A revisit of sparse coding based anomalydetection in stacked rnn framework,” in The IEEE

International Conference on Computer Vision (ICCV), Oct 2017.
7. S. Wu, B. E. Moore, and M. Shah, "Chaotic invariants of lagrangian particle trajectories for anomaly detection in crowded scenes," in Computer Vision and Pattern Recognition (CVPR), 2010 IEEE Conference on. IEEE, 2010, pp. 2054–2060.
8. V. Mahadevan, W. Li, V. Bhalodia, and N. Vasconcelos, "Anomaly detection in crowded scenes," in Computer Vision and Pattern Recognition (CVPR), 2010 IEEE Conference on. IEEE, 2010, pp. 1975– 1981.
9. N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," in Computer Vision and Pattern Recognition, 2005. CVPR 2005. IEEE Computer Society Conference on, vol. 1. IEEE, 2005, pp. 886–893.
10. L. Kratz and K. Nishino, "Anomaly detection in extremely crowded scenes using spatio-temporal motion pattern models," in Computer Vision and Pattern Recognition, 2009. CVPR 2009. IEEE Conference on. IEEE, 2009, pp. 1446–1453.
11. N. Dalal, B. Triggs, and C. Schmid, "Human detection using oriented histograms of flow and appearance," in European conference on computer vision. Springer, 2006, pp. 428–441.
12. F. Jiang, J. Yuan, S. A. Tsaftaris, and A. K. Katsaggelos, "Anomalous video event detection using spatiotemporal context," Computer Vision and Image Understanding, vol. 115, no. 3, pp. 323–333, 2011.
13. D. Zhang, D. Gatica-Perez, S. Bengio, and I. McCowan, "Semi-supervised adapted hmms for unusual event detection," in Computer Vision and Pattern Recognition, 2005. CVPR 2005. IEEE Computer Society Conference on, vol. 1. IEEE, 2005, pp. 611–618.
14. J. Kim and K. Grauman, "Observe locally, infer globally: a space-time mrf for detecting abnormal activities with incremental updates,"in Computer Vision and Pattern Recognition, 2009. CVPR 2009. IEEE Conference on. IEEE, 2009, pp. 2921–2928.
15. J. R. Medel and A. Savakis, "Anomaly detection in video using predictive convolutional long short-term memory networks," arXiv preprint arXiv:1612.00390, 2016.
16. Y. S. Chong and Y. H. Tay, "Abnormal event detection in videos using spatiotemporal autoencoder," in International Symposium on Neural Networks. Springer, 2017, pp. 189–196.