IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 1, January 2023

DOI: 10.17148/IJARCCE.2023.12111

# VIDEO ANOMALY DETECTION BY DEEP LEARNING

**Ankur Raj[1], Bhargav Potdar[2], Saniya Upendra[3], Mr. Baliram Gayal[4]**

RMD Sinhgad School of Engineering Warje, Pune, India[1-3]

Assistant Professor, E&TC Department, RMDSSOE, Pune[4]

**Overview:** The video surveillance system market has become popular and used in public places such as shopping malls, hospitals, banks, streets, educational institutions, municipal governments, smart cities, etc. to improve the security of public life and assets . Timely and accurate detection of video anomalies is almost always the primary goal of any security application. A video anomaly, such as anomalous activity or anomalous entity, is defined as an anomaly or irregular pattern present in the video that does not correspond to the normal trained pattern. Unusual activities such as brawls, riots, traffic violations, mass panics, and unusual entities such as weapons and misplaced luggage in sensitive locations should be automatically detected in time. However, it is difficult to detect video anomalies due to the ambiguity of anomalies, various environmental conditions, the complex nature of human behavior, and the lack of suitable datasets. This article focuses on the evolution of anomaly detection, followed by an overview of the various methods developed to detect anomalies in intelligent video surveillance. Additionally, it leverages the last decade of anomaly detection research. The following is a systematic taxonomy of anomaly detection methods. Since the concept of anomalies is contextual, anomaly detection identifies different objects of interest and published datasets. Since anomaly detection is a time-sensitive application of computer vision, we explore anomaly detection using edge devices and approaches designed explicitly for it. We also explore the confluence of edge computing and anomaly detection for real-time, intelligent surveillance applications. It also discusses the challenges and opportunities of anomaly detection.

**Keywords:** Detection, Anomaly, Normal-abnormal, Neural-Network

## I. INTRODUCTION

Anomaly detection has been an important topic of research for centuries. Many different methods have been developed and used to detect anomalies in various applications. However, video anomaly detection is a complex but very important topic in anomaly detection that needs to be addressed. Our approach here is to solve the problems related to video anomaly detection and build a robust video anomaly detection system. Surveillance cameras are being used more and more in public places. Increase public safety on roads, intersections, banks, shopping malls, and more. However, law enforcement's surveillance capabilities have not kept pace. The result is a marked underutilization of surveillance cameras and a dysfunctional ratio of cameras to human surveillance. An important task in video surveillance is the detection of unusual events such as traffic accidents, crimes, or illegal activities. In general, anomalous events are rare compared to normal activity. Therefore, there is an urgent need to develop intelligent computer vision algorithms that automatically detect video anomalies in order to reduce effort and time wastage. The goal of a practical anomaly detection system is to provide timely notification of activity that deviates from normal patterns and identify the timeframes in which anomalies occur. Anomaly detection can therefore be viewed as a coarse-grained level of video understanding that excludes anomalies from normal patterns. Once an anomaly is detected, it can be further classified into one specific activity using classification techniques. A small step towards anomaly detection is the development of algorithms to detect specific anomalous events. B. Violence detector [30] and traffic accident detector [23, 35]. However, it is clear that such a solution cannot be generalized to detect other anomalous events. As such, it is of limited usefulness in practice.

Real-world anomalies are complex and diverse. It is difficult to list all possible anomalous events. Anomaly detection algorithms should therefore not rely on prior information about events. In other words, anomaly detection should be done with minimal supervision. Video anomaly detection is an essential task in computer vision and is used in many important applications such as video surveillance, scene understanding, activity detection, and road traffic analysis. Frame-level video anomaly detection aims to identify frames where events or behaviors that differ from expectations or regulations exist for a given video clip. Another problem actually arises from the data imbalance between normal and abnormal samples. Anomalous events are rare and unpredictable in real-world scenarios. Collecting and labeling anomalous videos is difficult, time-consuming and labor-intensive.

  

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 1, January 2023

DOI: 10.17148/IJARCCE.2023.12111

## II . TARGET

Another problem actually arises from the data imbalance between normal and abnormal samples. Anomalous events are rare and unpredictable in real-world scenarios. Collecting and labeling anomalous videos is difficult, time-consuming and labor-intensive. Priority for using contextual anomaly detection techniques is determined by the importance of the contextual anomaly in the region of interest. The availability of categorical attributes is another important aspect. In some cases, it makes sense to use a context-aware technique, as the context can be easily identified. Otherwise, you cannot give the impression that a particular method is hard to use. As a result, the use of surveillance cameras is clearly underused, making the ratio of cameras to human surveillance impractical. An important task in video surveillance is the detection of unusual events such as traffic accidents, crimes, or illegal activities. In general, anomalous events are rare compared to normal activity.

## III. METHODOLOGY

As a result, the use of surveillance cameras is clearly flawed and the ratio of cameras to human surveillance is unrealistic. An important task in video surveillance is the detection of unusual events such as traffic accidents, crimes, or illegal activities. In general, anomalous events are rare compared to normal activity.

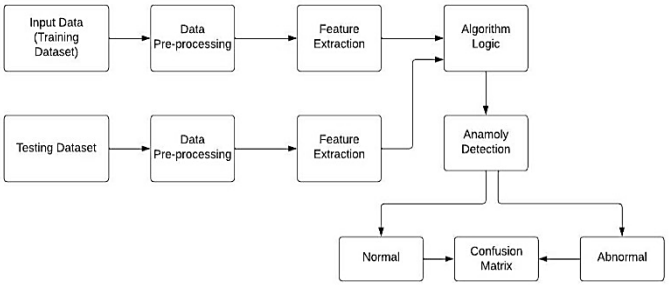


FIG. 1 METHODOLOGY

Video classification is not as trivial as individual frame classification. Context should be captured from a series of frames, not just one frame. Given an image of a patient in a hospital bed, most image classification algorithms will correctly classify this as either "patient" or "human". However, looking at subsequent frames, we can see the difference between a patient having a seizure and simply resting. Not only the sequence of events, but also the timeframe in which the events occur is important for detecting anomalies. These are subtle parameters that can distinguish a peaceful gathering of people from an angry mob. This led to the adoption of a methodology capable of extracting spatiotemporal features. The proposed methodology can be divided into four phases:

- Frame extraction
- Feature extraction
- LSTM training
- Classification

## IV. LITERATURE SURVEY

[1] In this Paper “Anomaly Detection With Particle Filtering for Online Video Surveillance” by Ata-Ur-Rehman 1, Sameema tariq2, Haroon Farooq 1, Abdul jaleel3, and Syed Muhammad wasif4 With increasing security threats, many online and offline frames for detecting anomalies in video sequences work is proposed. However, existing online anomaly detection techniques are either computationally intensive or lack the required accuracy. In this work, we propose a novel particle filter-based online anomaly detection framework that detects video frames containing anomalous activity based on the posterior probability of the activity in the video sequence. The proposed method also detects abnormal regions within abnormal video frames. We propose new prediction and measurement models for accurately detecting anomalous video frames and anomalous regions within video frames. A new predictive model for particle prediction and a probabilistic model for assigning weights to these particles are proposed. These models effectively use a variable-size cell structure that creates variable-sized subregions of the scene within the video frame. In addition, we efficiently extract and use information in the form of size, motion, and position features from video images. The proposed framework is tested on UCSD and LIVE datasets and compared with existing state-of-the-art algorithms in the literature.

DOI: 10.17148/IJARCCE.2023.12111

[2] Authors of this article, Anomaly Detection with Particle Filtering for Online Video Surveillance: Ata-Ur-Rehman 1, Sameema Tariq2, Haroon Farooq 1, Abdul jaleel3, and Syed Muhammad wasif4 As security threats grow, many online and offline frameworks have been proposed to detect anomalies in video sequences. However, existing online anomaly detection techniques are either computationally intensive or lack the required accuracy. In this work, we propose a novel particle filter-based online anomaly detection framework that detects video frames containing anomalous activity based on the posterior probability of the activity in the video sequence. The proposed method also detects abnormal regions within abnormal video frames. We propose new prediction and measurement models for accurately detecting anomalous video frames and anomalous regions within video frames. A new predictive model for particle prediction and a probabilistic model for assigning weights to these particles are proposed. These models effectively use a variable-size cell structure that creates variable-sized subregions of the scene within the video frame. In addition, we efficiently extract and use information in the form of size, motion, and position features from video images. The proposed framework is tested on UCSD and LIVE datasets and compared with existing state-of-the-art algorithms in the literature. The cloud system uses the Structural Similarity AES algorithm. The main purpose of the similarity index is to check image quality such as brightness, contrast, structure, and measure the similarity between two images. We use encryption methods to store large amounts of data efficiently and avoid duplication of text and images.

[3] Authors of this article "Self-reasoning framework for anomaly detection using video-level labels": Muhammad Zaighham Zaheer, Arif Mahmood, Hochul Shin, Seung-Ik Lee Detecting Anomalous Events in Surveillance Video is a challenging and practical study of issues in the image and video processing community. Obtaining video-level annotations is considerably faster and cheaper when compared to image-level annotations of anomalous events, but such high-level labels can contain significant noise. More specifically, a video flagged as anomalous may actually contain only a short anomaly, but the rest of the video frames may be normal. In the current work, we propose a weakly supervised anomaly detection framework trained in a self-intentional manner based on deep neural networks using only video-level labels. To perform self-reflection-based training, we use binary His clustering of spatio-temporal video features to generate pseudo-labels. This helps reduce the noise present in labels for anomalous videos. The proposed formulation encourages both the main network and clustering to complement each other to achieve the goal of more accurate anomaly detection. The proposed framework was evaluated against publicly available real-world anomaly detection datasets such as UCF-crime, Shanghai Tech and UCSD Ped2. Experiments demonstrate the superiority of the proposed framework over current state-of-the-art methods.

[4] In this article, "Anomaly Detection in Surveillance Video" Author: Dr. Annala M.R. Computer Science and Engineering RV College of Engineering, Malika Makker Computer Science and Engineering RV College of Engineering, Aakanksha Ashok Computer Science and Engineering RV College of Engineering Today it is desirable to monitor all public or private areas to ensure a high level of security. Because the surveillance is done 24/7, the data collected in the process is huge and it takes a lot of manual work for him to sift through the recorded video every second. This white paper presents a system that can detect anomalous behavior and warn users about the nature of the anomalous behavior. Due to the myriad of anomalies, it was necessary to narrow down the classification of anomalies. There are certain anomalies such as explosions, traffic accidents, assaults, and shootings that are commonly seen and have a significant impact on public safety. To narrow down the variations, the system specifies frames for explosions, traffic accidents, shootings, fights, and even their appearance. The model was trained on videos belonging to these classes. The dataset used is the UCF Crime dataset. Learning patterns from videos requires learning both spatial and temporal features. A convolutional neural network (CNN) extracts spatial features and a long short-term memory (LSTM) network learns the

## V. CONCLUSIONS

Detecting video anomalies is a fascinating but challenging task. The proposed model uses a deep learning CNN model for accurate and efficient anomaly detection. The fact that we have used CNNs over other deep learning algorithms gives us more variety than others, such as their performance on multidimensional and representative abstract data that can be extracted from raw data, and the different variations of training strategies offered. Because it has its advantages. The efficiency of the model is analyzed and improved using various algorithms to calculate the performance based on the various performance parameters considered. This area of research is new and will see a tremendous amount of progress in the near future. This proposed model is only an effort in the area of anomaly detection.

## REFRENCES

[1]. [1] B. Nassif, M.A. Talib, Q. Nasir und F. M. Dakalbab, "Machine Learning for Anomaly Detection: A Systematic Review," IEEE Access, vol. 9, pp. 78658-78700, 2021, doi: 10.1109/ACCESS.2021.3083060.

[2]. [2] Ata-Ur-Rehman、S. Tariq、H. Farooq、A. Jaleel und S. M. Wasif, “Anomaly Detection by Particle Filtering for Online Video Surveillance,” IEEE Access, vol. 9, pp. 19457-19468, 2021, doi: 10.1109/ACCESS.2021.3054040.

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 1, January 2023

DOI: 10.17148/IJARCCE.2023.12111

[3]. [3] M.Z. Zaheer, A. Mahmood, H. Shin und S.-I. Lee, "Self-Inference Framework for Anomaly Detection Using Video-Level Labels," IEEE Signal Processing Letters, vol. 27, pp. 1705–1709, 2020, doi:10.1109/LSP.2020.3025688.

[4]. [4] A.M.R., M. Makker, Ashok, "Anomaly Detection in Surveillance Video", 2019 26th International Conference on High Performance Computing, Data and Analysis Workshop (HiPCW), 2019, pp. 93-98, doi:10.1109/HiPCW.2019.00031.

[5]. [5] X. Wang et al., “Robust Unsupervised Video Anomaly Detection with Multipath Frame Prediction,” IEEE Transactions on Neural Networks and Learning Systems, vol. 33, Nr. 6, pp. 2301-2312, June 2022, doi: 10.1109/TNNLS.2021:3083152.

[6]. [6] J. Wren, F. Xia, Y. Liu and I. Lee, "Deep Video Anomaly Detection: Opportunities and Challenges," 2021 International Conference on Data Mining Workshops (ICDMW), 2021, pp. 959–966, doi: 10.1109/ICDMW53433.2021.00125.