Sustainable Abnormal Events Detection and Tracking in Surveillance System

Apurva Khandekar1*, Vikas Meneni1, Haseeb Uddin1, Bhusa Nikhil1, M Tejeshwar1, and Ramy Riad Al-Fatlawy2

1Department of Computer Science and Engineering, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, Telangana, India.
2The Islamic university, Najaf, Iraq

Abstract. With the proliferation of surveillance cameras, managing and analyzing vast amounts of video data have become challenging. This paper introduces a sustainable automated approach to detect abnormal events in surveillance footage. Leveraging Convolutional Neural Networks (CNNs) and deep learning techniques, our system identifies unusual activities by analyzing video frames. By automating this process, we reduce the burden of manual monitoring and enable timely responses to security threats. This sustainable solution has broad applications in public safety, security, and crime prevention.

1 Introduction

1.1 Background and Context of the Research

In recent times, concerns about security have grown due to increased anti-social activities. Many organizations have installed CCTV cameras for monitoring people and their actions. In a developed country with a population of 64 million, each person is recorded by cameras about 30 times daily. This results in a massive amount of video data, where just one image at a standard resolution and frame rate can generate 20 gigabytes of data daily. Monitoring all this data manually is nearly impossible as it requires a large workforce and constant attention. Therefore, there's a need to sustainably automate this process.

1.2 Significance of Detecting Abnormal Events in Surveillance Systems

Surveillance systems are vital for public safety and security. However, they face a significant challenge in identifying and tracking abnormal events within the vast amount of video data. This research aims to provide a sustainable solution using advanced computer vision techniques to detect and track abnormal events in real-time. Deep learning algorithms are employed to analyze video streams from surveillance cameras, enabling automatic identification and tracking of events that

* Corresponding author : khandekarapurva@gmail.com
don't conform to normal patterns.

1.3 Problem Statement and Motivation

The core problem lies in managing the ever-growing repository of surveillance footage. Manual review by humans is impractical and time-consuming. Moreover, it's essential to pinpoint the exact frame and area within the footage where unusual activity occurs. This helps identify abnormal events within the extensive surveillance data. To address these challenges, this research proposes converting video streams into individual frames and analyzing them in detail.

Machine learning and deep learning algorithms are used to sustainably automate this process.

1.4 Research Objectives and Scope

The primary aim of this research is to sustainably create an automated system for detecting and tracking abnormal events in surveillance video data. This sustainable system incorporates computer vision techniques, deep learning algorithms, and anomaly detection methods to achieve real-time event identification. The research also involves designing and implementing a sustainable machine learning model, specifically a Convolutional Neural Network (CNN) using the Tensor Flow Python module. This sustainable model automates the detection of suspicious behavior. Additionally, the research explores the practical and sustainable use of this system, including video uploads, frame extraction, and the sustainable classification of frames as 'suspicious' or 'normal.'

2 Literature Review

Surveillance systems have emerged as vital tools in upholding public safety and security. The widespread deployment of Closed-Circuit Television (CCTV) cameras by organizations has enabled the meticulous monitoring of individuals and their interactions[1]. In densely populated regions, such as developed countries with millions of residents, these cameras record the activities of each person approximately 30 times daily. This relentless surveillance generates massive volumes of video data. For instance, even a single image captured at a resolution of 704x576 pixels and a frame rate of 25 frames per second (fps) yields an astonishing 20 gigabytes of data per day. The traditional method of human manual monitoring to detect abnormal events has become impractical due to the sheer data volume, necessitating the imperative to automate this process.

2.1 Prior Research on Detecting and Tracking Abnormal Events

The realm of surveillance and the identification of abnormal events have been subjects of ongoing research. The primary goal has been to develop automated techniques for recognizing unusual activities. Various strategies have been explored in previous studies, ranging from the application of computer vision methods to the utilization of machine learning algorithms.[2][3] These endeavors aim to enhance both the efficiency and accuracy of abnormal event detection, as human-based monitoring is both resource-intensive and error-prone.
2.2 Current Approaches and Algorithms in Video Analysis

A wealth of methodologies and algorithms has been employed for video analysis, particularly within the context of surveillance systems\[4]\[5]. The field extensively relies on computer vision and machine learning techniques to process and interpret video data. Deep learning algorithms, including Convolutional Neural Networks (CNNs), have risen to prominence due to their proficiency in extracting intricate patterns and features from video frames, rendering them well-suited for identifying abnormal events. Additionally, the fusion of anomaly detection algorithms with object tracking algorithms has demonstrated considerable potential in precisely pinpointing and tracing abnormal events in video streams.

2.3 Challenges and Constraints in Modern Surveillance Systems:

Despite remarkable progress, contemporary surveillance systems confront several challenges and limitations\[6]\[7]. Coping with the staggering volume of video data necessitates robust automated mechanisms for event detection and tracking. Striking a balance between precision and computational efficiency remains a formidable task, especially in real-time applications. Furthermore, addressing privacy concerns and ensuring the ethical use of surveillance systems presents complex ethical dilemmas. Machine Learning techniques used for classification of images and attacks in [8][9][10]. The practical implementation of automated surveillance solutions, such as the integration of machine learning models, entails tackling technical hurdles related to data preprocessing, model training, and seamless real-time application.

This literature review furnishes an overview of surveillance systems, underscores the significance of detecting abnormal events, encapsulates the findings of prior research endeavours, encapsulates the contemporary techniques and algorithms for video analysis, and deliberates the challenges and constraints that beset modern surveillance systems.

Fig. 1. System Architecture

1. System design transitions from a user-oriented document to programming or database personnel, outlining the approach to creating a new system in logical and physical stages.
2. Database table design involves analyzing system functions, defining field roles, and avoiding unnecessary fields to optimize storage.

3. Software design principles include modularity, partitioning, low coupling, high cohesion, and shared use to enhance system efficiency.

4. Input design links the information system with the user, focusing on data preparation specifications, controlling input, and ensuring security and ease of use.

5. Output design ensures quality output that meets user requirements, communicates processed information, and aids user decision-making.

6. Efficient and intelligent output design involves an organized approach, selecting methods for presenting information, and creating formats to achieve specific objectives.

7. The design of computer output must be user-friendly and effectively convey information about past activities, current status, projections, events, opportunities, problems, or trigger actions.

8. Input design considers data arrangement, coding, dialog guidance, input validation, and error-handling steps to streamline the input process.

9. Software design principles focus on creating a hierarchy of modules, minimizing module dependencies, ensuring single-function modules, and avoiding duplication.

10. Overall, system design encompasses logical and physical development stages, efficient database and software design, user-friendly input and output interfaces, and adherence to design principles for optimal system functionality.

4 Methodology

This methodology outlines the systematic approach for collecting, preparing, and analysing surveillance data, employing computer vision and deep learning techniques, and focusing on the detection and classification of abnormal events.

1. Data Collection and Preparation.
The initial step involves the collection of data related to surveillance videos. This encompasses obtaining video Footages from various sources.

2. Data Pre-processing:
Data pre-processing is essential, involving tasks like cleaning, noise reduction, and ensuring data consistency. This stage ensures that the data is ready for analysis.

3. Acquiring Video Data:
The next phase is the acquisition of video footage from a range of surveillance cameras. It's crucial to ensure diversity in the dataset, representing various real-world scenarios.

4. Data Management:
To efficiently manage the data, a structure database or storage system is established.
This system is designed to keep the data well-organized and easily accessible.

5. Data Integrity:
Data management protocols are implemented to guarantee data integrity. These protocols help maintain the quality and reliability of the collected data.

6. Utilizing Computer Vision Techniques:
Computer vision methodologies are employed to analyse the surveillance videos. These techniques include object recognition, tracking, and feature extraction.

7. Leveraging Convolutional Neural Networks (CNNs):
Convolutional Neural Networks (CNNs) are a critical component of the methodology. They are used to extract features from video frames and are trained to recognize patterns in the surveillance data.

8. Exploring Deep Learning Algorithms:
Various deep learning algorithms are explored to enhance event detection. Deep learning is chosen for its ability to handle complex visual data effectively.

9. Anomaly Detection and Object Tracking:
Anomaly detection algorithms are integrated to identify unusual events within the video data. Object tracking algorithms are used to monitor the movement of objects.

10. Model Development:
Building a comprehensive training dataset that contains labelled instances of both normal and abnormal events. This dataset is crucial for model development.

11. Model Creation:
Developing machine learning models, with a particular focus on Convolutional Neural Networks (CNNs). Tensor Flow and Python are utilized for model creation.

5 Equation based algorithm

Event Detection = Apply Trained Models (Develop Machine Learning Models (Create Training Dataset (Preprocess (Collect Data (Various Sources)))), Extract Frames (Preprocess (Collect Data (Various Sources))))

Collect Data (Various Sources): Collects data from various sources (e.g., surveillance cameras).

Preprocess: Preprocesses the collected data, which may include tasks such as cleaning, noise reduction, and normalization.

Create Training Dataset: Generates a training dataset from the preprocessed data, typically involving labeling instances of normal and abnormal events.

Develop Machine Learning Models: Trains machine learning models using the training dataset to learn patterns and features indicative of different events.
Extract Frames: Extracts frames from the preprocessed data, possibly for further analysis or feature extraction. Apply Trained Models: Applies the trained learning models to the extracted frames to detect events based on learned patterns and features.

6 Experimental Results

To initiate the project execution, simply double-click on the 'run.bat' file located in the project folder. Upon doing so, you will encounter the following interface:

Project Interface:

Click on the 'Upload CCTV Footage' button to select and upload the desired video for analysis. In this example, we are using a normal video. Once the video is uploaded, proceed by clicking the 'Generate Frames' button. This action will trigger the extraction of individual frames from the video.

As the frame extraction process unfolds, a console window will display the progress. You will observe that the extracted frames are being saved in the 'frames' folder, each frame labelled with a unique frame number.

![Fig. 2. Uploading video](image)

Once the frame extraction is complete, the 'frames' folder will contain all the extracted images from the uploaded video.

![Fig. 3. Frame Extraction process](image)

Now, to initiate the monitoring of frames for suspicious activity, click on the 'Detect
Suspicious Activity Frame' button. The console window will exhibit the process of analysing each frame for any signs of suspicious activity.

**Fig. 4.** Extracted Frames

In the event that no suspicious activity is detected, the interface will reflect this status.

**Fig. 5.** No Suspicious Activity detected

**Fig. 6.** Suspicious Activity detected
To further illustrate the process, we will upload another video named 'Video2' and follow the same procedure. After uploading and extracting frames, you will notice that suspicious activity has been identified in frame '117.jpg.' These frames containing suspicious activity are listed in the details screen.

By selecting any of the frames from the 'frames' folder, you can view the corresponding image. This allows for a closer examination of the suspicious activity.

Fig. 7. Frame Examination

Fig. 8. Detailed Information

7 Performance of Proposed Approach

Fig. 9. Performance of proposed approach
8 Conclusion

To recapitulate, this study has addressed the pressing issue of detecting and tracking abnormal events within surveillance systems. The increasing prevalence of anti-social activities highlights the urgent need for bolstered security measures. In developed nations with widespread CCTV deployment, an overwhelming deluge of video data is generated daily, rendering manual surveillance impractical. This research has effectively harnessed advanced computer vision and deep learning techniques to craft a system capable of autonomously identifying and tracking abnormal events in real-time. The analysis underscores the system's prowess in accurately pinpointing a broad spectrum of abnormal activities, encompassing suspicious behaviour, unauthorized access, and potential security threats.

8.1 Contributions of the Research:

The contributions of this investigation are of significant import. The devised solution not only alleviates the daunting challenge of parsing copious surveillance data but also expedites the detection of abnormal events. By capitalizing on machine learning and deep learning algorithms, the system elevates the efficiency and efficacy of surveillancesystems, serving as a testament to the potential of automation in upholding public safety and security. Furthermore, the incorporation of object tracking algorithms enhances the precision of event monitoring, further augmenting its worth in the domain of surveillance technology.

8.2 Future Avenues for Research:

As the landscape of surveillance technology continues to evolve, future research endeavours should chart courses to refine and enhance the detection and tracking of abnormal events. This may encompass the development of more sophisticated machine learning models adept at handling a diverse array of surveillance scenarios. Ethical considerations pertaining to surveillance technology also merit thoughtful exploration, with future research aimed at striking a balance between privacy concerns and the imperative of public safety. Additionally, the scalability of the proposed solution opens doors to its application across various domains, extending beyond security to areas like traffic management and environmental monitoring. In summation, this study has introduced a promising solution for the identification and tracking of abnormal events within surveillance systems. Through the adept utilization of machine learning and computer vision, this system emerges as a significant contributor to the realm of public safety and security, offering potential ramifications that extend well into the future.

References