Anomaly Detection in Surveillance Videos

Akash Pal[1], Pappu Bishwas[2], Vanisha Rai[3], Mohammad Usama Ashraf[4], and Mohammad Ahmed Al-Ghaili[5]
[1]School of Computer Engineering, KIIT Deemed to be University, Bhubaneswar 751024, India
Email: {2106006, 2106287, 2106289, 2106317, 2106310}@kiit.ac.in

Artificial Intelligence (AI) related anomaly detection is becoming more and more common in surveillance systems. The task of sorting through huge volumes of video footage in order to spot anomalous behaviors within a scene is a challenge for this technology. The core principle is to acquire an in-depth understanding of common behavioral patterns. To do this, AI algorithms examine recent videos while considering variables like object movement, crowd dynamics, and activity frequency. Security staffs receive notifications when there are deviations from this provided baseline, such as someone spending a lot of time in a prohibited area, things moving at unusual speeds, or unexpected crowds. Compared to traditional surveillance techniques, anomaly detection has several advantages. It reduces human monitoring of the responsibility by automatically identifying suspicious events, which might have been missed in an endless stream of video feeds. This increases productivity and enables faster responses in security-related scenarios. Anomaly detection can also be adapted for certain contexts. For example, a traffic camera system might concentrate on identifying anomalous vehicle behavior or accidents, whereas a bank surveillance system might prioritize detecting abandoned objects. However, there are still difficulties. Algorithms for anomaly detection must be adaptable to variables such as changing lighting, camera angles, and scene obstacles. Moreover, the concept of ”normal” can be flexible and may need to be adjusted by humans. Nevertheless, anomaly detection in surveillance cameras is a potent AI tool that might greatly improve safety and security protocols.

I. Introduction

In this technology era, security has been the top priority for all, so new technologies are being introduced to keep track of the increasing threats and to provide a safe environment to the public. Surveillance cameras are one of the common technologies that have been widely used. Surveillance cameras are being mostly used in public areas to ensure the safety of the public by detecting unusual activities such as fraud, dangerous items, and other abnormal events. According to Amazon Web Services (AWS), anomaly detection is the process of examining certain data points and detecting abnormal events that seem suspicious as they deviate from the established pattern of behavior [1]. The surveillance cameras can be used to detect early anomaly behaviors such as fighting, the presence of prohibited items, and behaviors that are against the predetermined rules. Therefore, an intelligent computer vision algorithm for anomaly detection in surveillance videos can be implemented to reduce time and to detect the abnormalities early [2]. The need for more security can be fulfilled by increasing surveillance and taking preventative steps that reduce possible impact from threats. This strategy focuses on enhancing the surveillance capacity [5], by implementing more cameras, security personnel, or other monitoring systems, a wider range of information about potential threats can be gathered. More insights from surveillance data can be extracted using new technologies like facial recognition or AI-powered analytics, which may help detect suspicious activities. Due to the increased surveillance cameras, individual privacy can be a concern, thus a balance between security needs and protecting personal information is important. With the era of massive data collection and imperfect measurement systems [6], the real world is full of anomalous and unforeseen events, so it is difficult to list all the anomalous things that could happen. Data errors may result from measurement systems that are prone to biases, errors, or inaccuracies. These flaws can make it difficult for anomaly detection systems to accurately identify between normal and abnormal behavior by hiding genuine anomalies or introducing fake anomalies. As a result, anomaly detection systems must possess enough knowledge to identify anomalous activity on their own, without the need for manual supervision. Without depending on predefined requirements or thresholds, these systems should be able to learn from data, adjust to changing environments, and identify anomalies in real-time or near real-time. To continuously enhance their detection skills, autonomous anomaly detection systems need to integrate a variety of knowledge sources, such as domain expertise, historical data, feedback mechanisms, and contextual information. The system will then be able to distinguish meaningful anomalies from noise or anomalies caused by known sources due to this integration. To develop autonomous anomaly detection systems, machine learning and artificial intelligence plays a crucial role. These techniques enable the system to analyze complex patterns in data, identify anomalies, and make informed decisions autonomously based on learned patterns and feedback. Surveillance cameras are becoming the common security technology that can detect anomalous activity and improve public safety. But the most important factor to their efficiency is our capacity to sort through the massive amounts of data they gather, which may contain a lot of inaccurate information because measurement methods are imperfect. Anomaly detection systems must advance through strict guidelines and ongoing human supervision to solve this. They need to develop the intelligence to learn and adapt on their own, which can be done using artificial intelligence (AI) and machine learning. A new problem arises through this increased dependence on monitoring technologies: striking a balance between security and personal privacy. As we strive to create safer communities, these advances should be applied with proper consideration for protecting individual rights to build safer communities. Essentially, the key to successfully integrating modern surveillance technology is figuring out how to make use of its security advantages while protecting personal privacy. Therefore, the common use of surveillance technologies, such cameras, makes it possible to identify unusual behaviors and events, assisting in risk prevention and maintaining public safety. However, the effectiveness of surveillance hinges on the ability to identify anomalies from huge data collection and inaccurate measuring techniques. Without human intervention, anomaly detection systems must develop to recognize abnormalities on their own. To do this, they must use machine learning and artificial intelligence (AI) approaches to integrate various knowledge sources and adapt to changing settings. This emphasizes the significance of moral issues in the use of surveillance technologies and demands establishing a balance between security requirements and individual privacy concerns. In conclusion, communities can become safer through the integration of modern technologies and careful implementation approaches that protect private rights while enhancing security measures.

II. Basic Concepts

A. Anomaly Detection

In real world scenarios, data is often high-dimensional (having a lot of features) which might make the anomaly detection more challenging because it may be difficult for traditional methods to properly record the complex interactions between variables [3]. The MGFN: Magnitude-Contrastive Glance-and-Focus Network for Weakly-Supervised Video Anomaly Detection analyzes the entire video to understand the overall flow, then it focuses on areas to identify anomalies and a unique method (Feature Amplification Mechanism) improves the way MGFN analyses the footage in order to spot anomalies more accurately and uses several tools to achieve feature extraction, examining details and learning from normal vs. abnormal patterns [4]. In a weakly supervised learning approach, the surveillance videos are treated as bags and video segments as instances within these bags, using video-level labels for training, then a deep learning model is trained to rank video segments, and sparsity and smoothness constraints are introduced in the ranking loss function to improve the localization of anomalies during training so that the system can automatically detect and localize anomalies in surveillance footage with minimal supervision [2]. Normal vs Anomalous Activity: • Normal Activity: This is related to the ordinary behaviors and situations that are seen through the camera. It may involve pedestrians, vehicles passing by, or behaviors that are common in that area (such as patrons using an ATM). • Anomalous Activity: These are events that differ significantly from the accepted guidelines of typical behavior. Lingering, fighting, leaving things unattended, and messing with equipment that may be prohibited. The Anomaly Detection Process: 1. Data Acquisition and Preprocessing: The surveillance camera collects video. To handle issues like noise, changes in lighting, or camera angle adjustments, this raw data may require preprocessing. 2. Learning Normal Activity: Machine learning algorithms are frequently used by anomaly detection systems. A lot of the video data used to train these algorithms only shows common events. The system establishes a baseline for what is considered ”normal” in the specific environment with the support of the training process. 3. Real-time Anomaly Detection: After training, the system keeps analyzing raw footage taken by the camera. It makes a comparison between the learnt model of normal behavior and the observed activity patterns. An anomaly warning may be triggered by significant differences from the normal trends. Anomaly Detection Types: Object Detection and Tracking Anomalies: The goal of object detection and tracking anomalies is to spot odd behavior in objects. Examples include unattended items left behind, objects traveling in the incorrect direction, and loitering (objects standing still for a long time). Activity Detection Anomalies: This analyses the movements and conversations taking place in the scene. Examples include fighting, individuals speeding exceptionally quickly, and unplanned crowd gatherings. Challenges in Anomaly Detection: • Normal vs. Anomalous Recognition: The parameters of normality can change based on the surroundings. Thus, it is critical to establish precise thresholds for anomaly detection. • False Alarms: At times, regular activity patterns are mistaken for abnormalities by anomaly detection systems, leading to false positives. To prevent burdening security staff with pointless notifications, it is important to reduce false alarms. • Data Variations: The way the system detects a scene can be influenced by differences in the lighting, weather, and camera angle. For the system to manage these changes, thus, it must be robust.

III. Requirement Gathering

A. Project Planning

The following are the mentioned steps taken to effectively develop the system to detect the anomaly activities in surveillance videos: • Requirement Gathering: Specify the problem statement and security concerns as well as the anomaly types (like loitering, and object abandonment). Gather the required information from the existing projects and analyze the scenarios where it would be mostly used. Determine the performance expectations (accuracy, false alarm rate, latency) for the project. • Determination of Anomaly Detection Techniques: Supervised/Unsupervised Learning: select whether to use an unsupervised approach, where a model learns normal behavior and detects anomalies, or use a supervised approach, where it trains with labeled anomalous events. Deep Learning Algorithm: consider which deep learning techniques like Convolutional Neural Networks (CNNs), Autoencoders, or Recurrent Neural Networks (RNNs) to use for anomaly detection. • Resource Identification: Specify the type of video data needed (resolution, frame rate, lighting conditions) considering the various requirements such as storage capacity and data transfer needs. Determine the computing resources (such as GPUs) with enough processing power for video analysis and training models. Explore various software tools for data preprocessing, and specify the machine learning libraries and frameworks for anomaly detection model development. • Timeline Estimation: Develop a detailed project timeline for the project to be completed on time and produce an efficient system. Assign each task to the expertise in the team. • Risk Assessment: Identify the possible risks like data quality, model overfitting, deployment obstacles, and privacy concerns. Create measures to reduce them. • Communication Plan: Conduct regular team meetings to track the progress of the project and discuss challenges. Document the necessary information regarding the project.

B. Project Analysis

• Feasibility: determine whether the project is technically feasible. The accuracy of the study on having access to a large video dataset that captures both typical and unusual activity and captures the footage from the specific environment. • Benefits: Security: the system will detect the anomalous behavior automatically providing a secured environment. Security incidents can be handled more quickly with the real-time anomaly alerts. Future security strategies can be derived from the patterns and trends in criminal activity that are indicated by the analysis of discovered anomalies. • Challenges: Poor video quality and limited training data will affect the performance of anomaly detection. Unusual environmental conditions or unseen anomaly may cause difficulties to the model. It is important to minimize false alarms that waste resources while maintaining the accuracy of anomaly detection. Regulations related to data storage and video surveillance have to consider data privacy into consideration.

C. System Design

1) Design Constraints: Software Environment: • Python is used as the primary language for its availability of various computing libraries. • Libraries include: o Scikit-learn: used for data preprocessing and machine learning algorithms. o Pandas: for data manipulation and analysis. o TensorFlow/PyTorch: used for deep learning frameworks for model development and deployment. o OpenCV: for computer vision tasks (video processing and object detection). Hardware Environment: • High computational requirements including GPUs for intensive tasks is required for efficient results.

2) System Architecture: The anomaly detection will consist of the following modules: • Data Collection: collects video data from surveillance cameras in real-time or from recorded video archives. • Data Preprocessing: the data collected is then preprocessed to reduce noise, resizing frames to standard size and normalize the pixel values. • Feature Extraction: from the preprocessed video data, extract the meaningful features that represent normal activity patterns. • Anomaly Detection Model Development: develop and train the model to identify the abnormalities from the normal activity patterns. • Model Evaluation: the performance of the trained model is assessed using metrics like accuracy, precision, recall and F1 score. • Model Deployment: the model is then integrated into the surveillance system infrastructure.

IV. Implementation

A. Methodology

The following are the steps to detect the anomalies in surveillance videos: • Data Collection: gather the diverse dataset of surveillance videos with labeled anomalies to train and validate the model taking privacy and ethical regulations into consideration.

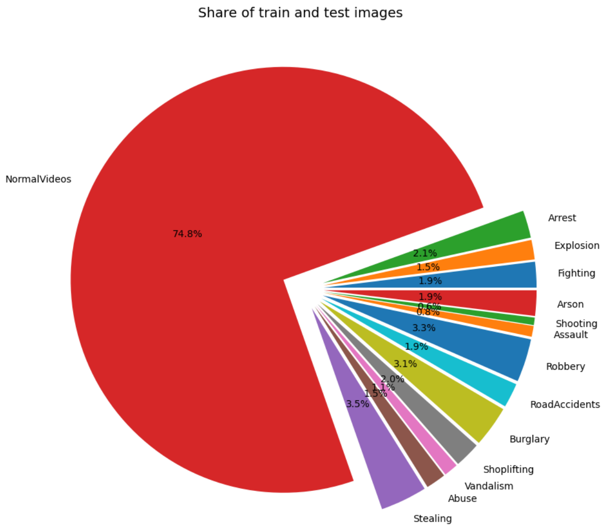


Fig. 1. Different types of UCF crime dataset

• Data Preprocessing: convert the surveillance videos into the required format for noise reduction, frame extraction, and resizing. From the videos, extract labels or annotations that indicate the existence of abnormalities at timestamps. • Feature Engineering: determine and extract key features from the video frames that can help in identifying between normal and unusual behavior. When dealing with high-dimensional feature areas, Principal Component Analysis (PCA) and t-Distributed Stochastic Neighbor Embedding (t-SNE) techniques can be used to minimize dimensionality while maintaining significant information. • Data Splitting: this involves dividing the surveillance video data into two main sets: 1. Training data: The anomaly detection model gets its ”training” from this greater fraction of the data. Through analysis of this data, the model discovers patterns of normal activity in the video footage. 2. Testing data: The model has smaller fraction of the data. The testing set is used to evaluate the model after it has been trained on the training set of data.

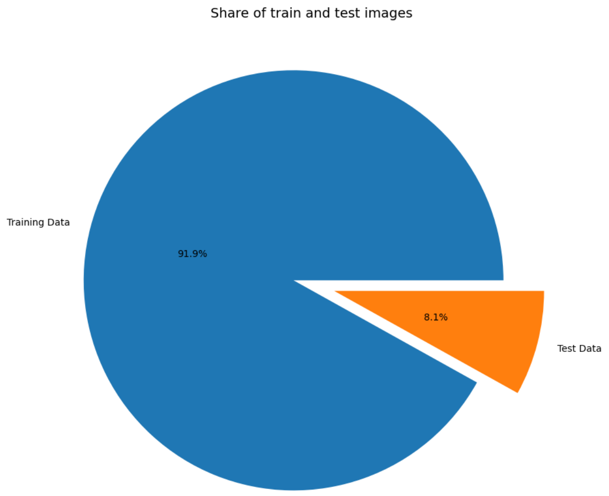


Fig. 2. Portion of training and testing UCF crime dataset

• Model Selection: to detect anomalies in video data, choose the suitable machine learning algorithms. Also, select models that can record sequential patterns and temporal dependencies. • Model Training: to train the model, divide the labeled dataset into sets for validation and training, and optimize the model for performance metrics like AUC, accuracy, precision, recall, or F1-score. • Model Evaluation: assess the performance of the trained model using the proper evaluation metrics. To enhance the performance, iterate on the model architecture, features, and hyperparameters according to the evaluation outcomes. • Model Deployment: integrate the final trained model into the surveillance system infrastructure. • Document and Reporting: maintain thorough documentation of the methodology, including data collection, preprocessing, model architecture and evaluation outcomes. Also create reports that include a summary of the methodology, findings, and recommendations for future use.

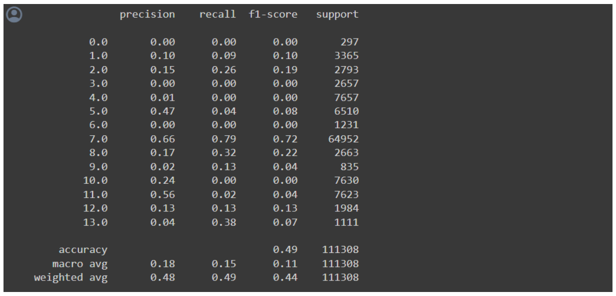
B. *Testing*

TABLE I
TEST CASES OF ANOMALY DETECTION IN SURVEILLANCE VIDEOS

Test ID	Test Case Name	Test Condition	System Behavior	Expected Result
T01	Anomalous Activity	Loitering for a longer period, tailgating and tampering	System should detect these behaviors and raise an alert	The system should accurately detect loitering, tailgating, and tampering and send out the proper notification.
T02	Testing Procedure	System evaluation, metrics calculation and ground truth data preparation (test on two or more videos with normal and anomaly activities)	The system should undergo evaluation metrics calculation and utilize ground truth data	This test case guarantees that ground truth data (manually labeled video data) is ready for performance evaluation and that the system is assessed using the proper metrics.
T03	Evaluation and Refinement	Analyze the result based on metrics calculations.	If TPR is high and FPR is low, then the system is ideal. If the TPR is low, then the training data or the anomaly detection algorithm should be refined. If the FPR is high, the system will be overly sensitive and create false alarms.	The objective of this test case is to evaluate the functioning of the system with the metrics determined in T02. A high True Positive Rate (TPR), which indicates that the system successfully detects most abnormalities, and a low False Positive Rate (FPR), which indicates that there are few false alarms, are the desired results.

C. *Result Analysis OR Screenshots*

The result below shows the performance of a classification model on a test dataset. Here, the rows and the columns represent the actual classes and the predicted classes respectively. Each cell of the matrix shows the number of instances in a class. Here, the model performed well at classifying class 7 with a precision of 0.66 and a recall of 0.79. It performed poorly at classifying classes 0, 3, 4, 5, 10, 11 and 13 with a precision of 0.00 or close to it.



```
              precision    recall  f1-score   support

         0.0       0.00      0.00      0.00       297
         1.0       0.10      0.09      0.10      3365
         2.0       0.15      0.26      0.19      2793
         3.0       0.00      0.00      0.00      2657
         4.0       0.01      0.00      0.00      7657
         5.0       0.47      0.04      0.08      6510
         6.0       0.00      0.00      0.00      1231
         7.0       0.66      0.79      0.72     64952
         8.0       0.17      0.32      0.22      2663
         9.0       0.02      0.13      0.04       835
        10.0       0.24      0.00      0.00      7630
        11.0       0.56      0.02      0.04      7623
        12.0       0.13      0.13      0.13      1984
        13.0       0.04      0.38      0.07      1111

    accuracy                           0.49    111308
   macro avg       0.18      0.15      0.11    111308
weighted avg       0.48      0.49      0.44    111308
```

Fig. 3. Result Analysis of the model

The graph below shows that the model performs well at classifying explosions and shoplifting whereas performs poorly at classifying road accidents and robbery.

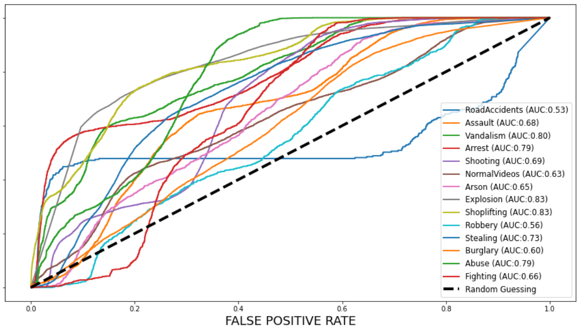


Fig. 4. ROC Curve of the UCF Crime Datasets

TABLE II
AUC PERCENTAGE OF DIFFERENT TRANSFER LEARNING MODEL

Model	**AUC Percentage**
VGG16	78.12
MobileNetV2	79.35
Resnet50	81.98
DenseNet121	83.45

Therefore, our proposed model is DenseNet121 transfer learning model that provides the highest accuracy rate of AUC 83.45

D. *Quality Assurance*

The quality of the anomaly detection in surveillance cameras can be ensured through a multi-step process. For the training data to accurately represent the real-world situation, it must be diverse and well-labeled. Cleaning up data and filling in the blanks are also important. When selecting the metrics to assess the performance of the model, factors like maintaining a balance between detecting all abnormalities (recall) and preventing false alarms (accuracy) should be considered. Before deployment, real-world testing and false alarm analysis are crucial to find application problems and improve the system. ALso, consider privacy issues, scalability to manage big camera networks, and integration with current security systems. These quality assurance procedures will help create a dependable anomaly detection system for security cameras.

V. STANDARDS ADOPTED

A. *Design Standards*

• IEEE Standards • ISO/IEC 27001 [Information Security]: This protects the safe handling and maintaining possible private security video. • Standardized machine learning libraries: Use widely used libraries for consistent function calls and readable code, such as Scikit-learn or TensorFlow.

B. Coding Standard

• Clear and concise comment: for future reference, document any assumptions, algorithms and decision points in the code to provide clear understanding. • Code understandability: for improved readability and reusability, divide complicated tasks into smaller functions. • Adaptability: to reduce false alarms, design systems with the ability to learn from and adjust to changing lighting conditions and settings.

C. Testing Standards

• Functional Testing: Verify that the key features such as motion tracking, object detection and anomaly alerting act as expected in several kinds of situations. • Non-Functional Testing: Performance testing: evaluate response times and processing power to find anomalies. Testing for security: verify that the system is protected from tampering or illegal access that could lead to false alerts or compromise video data. Scalability testing: determines how well the system manages more camera feeds or higher-resolution video to provide future flexibility. • Usability Testing: Ensure that the user interface is simple and easy to use so that the security staff can effectively handle the system and monitor alerts. Assess how well the system reduces false alarms caused by activity patterns, shadows or camera shake. • Test Data: Provide a variety of datasets that include normal and unusual events from real-world surveillance footage. To evaluate detection accuracy, create targeted test cases that represent scenarios such as loitering, fighting, or trespassing.

VI. Conclusion and Future Scope

A. Conclusion

Anomaly detection in surveillance video serves as an effective means for improving public safety and security. The identification of anomalous events can be done automatically, reducing security staff in need for constant supervision. However, there would still be challenges, thus it is crucial to maintain a balance between low false alarms from regular tasks or changes in the environment and provide accurate anomaly detection. The issues about the privacy consequences of massive data storage and video surveillance should also be considered, thus it is essential to implement confidentiality or strong data security procedures and provide clear regulations and transparent practices to maintain public trust and responsible use of the technology. Therefore, real-time processing requires effective algorithms to reduce latency and offer rapid responses to security concerns. Despite these challenges, through active research and continuous improvements in machine learning and processing power, an even more reliable system for community safety could be created by anomaly detection in surveillance cameras and can evolve from being passive tools for observation into proactive shields of public safety.

B. Future Scope

The field in anomaly detection in surveillance videos has the potential for enormous growth in the future. The use of integration capability is one potential approach where merging anomaly detection with other video analysis methods such as object recognition and activity analysis can go beyond basic event detection. For example, a system that not only alerts users when someone enters a restricted area but also reports suspicious activity such as hanging around a secure exit. With an integrated strategy, security professionals could be able to target their interventions more effectively and have a much clearer understanding of potential security issues. Future developments in interpretable machine learning are promising. Security professionals can gain valuable insights about why an event is marked as abnormal by increasing the transparency of these models. This deeper understanding may result in better decision-making and increased trust in the system. Anomaly detection in surveillance videos has the ability to completely change security procedures by overcoming these obstacles and using these developments, it is possible to evolve surveillance cameras into intelligent protectors that actively watch over the communities.

VII. References

[1] ”What is Anomaly Detection?” Amazon Web Services (AWS), [Online]. Available: https://aws.amazon.com/what-is/anomaly-detection/: :text=Anomaly

[2] W. Sultani, C. Chen and M. Shah, ”Real-world Anomaly Detection in Surveillance Videos,” CVPR, 2018.

[3] S. Thudumu, P. Branch, J. Jin and J. J. Singh, ”A comprehensive survey of anomaly detection techniques for high dimensional big data.,” Journal of Big Data, vol. 7, no. 42, 2020.

[4] Y. Chen, Z. Liu, B. Zhang, W. Fok, X. Qi and Y.-C. Wu, ”MGFN : Magnitude-Contrastive Glance-and-Focus Network for Weakly-Supervised Video Anomaly Detection,” PaperwithCode, p. 10, 28 11 2022.

[5] C. Brax, ”Anomaly Detection in the Survelliance Domain,” Diva Portal, 2011.

[6] R. Foorthuis, ”On the nature and types of anomalies: a review of deviations in data,” Int J Data Sci Anal, vol. 12, pp. 297-331, 4 August 2021.