REAL-TIME ANOMALY DETECTION IN CCTV USING MACHINE LEARNING

1Mr.Jajjara Bhargav, 2Doppalapudi Satya Sai, 3Patti Venkat Gopiram, 4Kakunuri Gopaiah, 5RANGISETTI SAI SUJITHA, 6Anitha

1Assistant Professor, 23456Students

DEPT OF CSIT

CHALAPATHI INSTITUTE OF ENGINEERING & TECHNOLOGY

ABSTRACT

The increasing demand for intelligent surveillance systems has led to the development of automated solutions capable of detecting abnormal activities in real time. Traditional CCTV monitoring systems rely heavily on human operators, making them inefficient, time-consuming, and prone to errors due to fatigue and limited attention span. This research proposes a Real-Time Anomaly Detection System in CCTV using Machine Learning and Computer Vision techniques to overcome the limitations of manual monitoring. The system is designed to automatically analyze video streams, identify unusual activities, and generate alerts without human intervention.

The proposed system captures live video footage from CCTV cameras and processes it into frames using OpenCV. These frames are analyzed using machine learning algorithms that compare real-time activity with predefined normal behavior patterns. Any deviation from normal behavior is classified as an anomaly. The system is capable of detecting various abnormal events such as unauthorized entry, suspicious movements, theft, and violent activities. Upon detection, an alert notification is generated and stored along with timestamp details in a SQLite database. A web-based dashboard developed using Flask allows users to monitor alerts and system performance efficiently.

The system architecture includes modules such as video capture, frame processing, feature extraction, anomaly detection, alert generation, and database management. The integration of these modules ensures real-time performance and high detection accuracy. Experimental results demonstrate that the system achieves significant accuracy while maintaining a low false alarm rate and fast processing speed.

The proposed system reduces the burden on human operators and enhances surveillance efficiency in public places such as airports, banks, railway stations, and shopping malls. It provides a scalable and cost-effective solution for modern security challenges. Future enhancements may include deep learning-based models, cloud deployment, and integration with IoT devices for improved performance. Overall, this research contributes to the advancement of intelligent surveillance systems by providing a robust and automated anomaly detection framework.

1. INTRODUCTION

In recent years, surveillance systems have become an essential component of public safety and security infrastructure. The widespread deployment of CCTV cameras in areas such as airports, railway stations, banks, and commercial complexes has significantly increased the volume of video data generated daily. However, manual monitoring of these video feeds is highly inefficient and prone to

human error, leading to missed detection of critical events [1]. This has created a need for automated surveillance systems capable of analyzing video data in real time.

Machine Learning and Computer Vision have emerged as powerful technologies for analyzing visual data and identifying patterns. These techniques enable systems to automatically detect anomalies in video streams by learning from historical data [2]. An anomaly is defined as any deviation from normal behavior, such as unusual movements, unauthorized access, or suspicious activities. Detecting such anomalies in real time is crucial for preventing crimes and ensuring public safety [3].

Traditional surveillance systems are limited to recording and storing video footage without providing real-time insights. Security personnel are required to continuously monitor multiple screens, which is not only exhausting but also ineffective [4]. Studies have shown that human operators tend to miss significant events when monitoring multiple video feeds simultaneously [5]. Therefore, integrating intelligent algorithms into surveillance systems can significantly improve detection accuracy and efficiency.

The use of Computer Vision techniques such as frame extraction, object detection, and motion analysis has enabled automated video analysis [6]. OpenCV, a widely used computer vision library, provides tools for processing video frames and extracting meaningful features [7]. These features can be fed into machine learning models to classify activities as normal or abnormal.

Various machine learning approaches, including supervised and unsupervised learning, have been applied to anomaly detection problems. Supervised methods require labeled datasets, while unsupervised methods identify anomalies based on deviations from learned patterns [8]. In surveillance systems, unsupervised learning is often preferred due to the difficulty of labeling large datasets [9].

Real-time processing is a critical requirement for surveillance applications. The system must analyze video frames quickly and generate alerts without delay [10]. This requires efficient algorithms and optimized system architecture. Lightweight frameworks such as Flask enable the development of web-based dashboards for monitoring system outputs [11].

The proposed system aims to address these challenges by developing a real-time anomaly detection system using machine learning. The system integrates video processing, anomaly detection, and alert mechanisms into a unified platform. It provides an efficient solution for modern surveillance needs by reducing manual effort and improving detection accuracy [12–15].

2. LITERATURE SURVEY

Anomaly detection in video surveillance has been widely studied in recent years, with researchers focusing on improving accuracy, efficiency, and scalability. Early approaches relied on rule-based systems that detected anomalies based on predefined thresholds. However, these methods were limited in their ability to handle complex scenarios [16].

With the advancement of machine learning, data-driven approaches have gained popularity. Researchers have explored various algorithms such as Support Vector Machines (SVM), k-Nearest Neighbors (k-NN), and clustering techniques for anomaly detection [17]. These methods analyze patterns in data and identify deviations from normal behavior. However, their performance depends heavily on feature selection and data quality.

Deep learning techniques have further improved anomaly detection capabilities by enabling automatic feature extraction. Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have been widely used for analyzing video data [18]. CNNs are effective for spatial feature extraction, while RNNs capture temporal dependencies in video sequences.

Another important area of research is real-time video processing. Efficient frame processing techniques are required to handle high-resolution video streams without latency [19]. OpenCV has been widely used for implementing real-time video analysis due to its optimized performance and extensive functionality.

Researchers have also explored hybrid approaches that combine machine learning and deep learning techniques. These systems achieve higher accuracy by leveraging the strengths of different algorithms [20]. Additionally, anomaly detection systems are often integrated with alert mechanisms to notify security personnel in real time.

Database management is an essential component of surveillance systems. Studies have shown that lightweight databases such as SQLite are suitable for storing anomaly records in small to medium-scale applications [21]. For large-scale systems, cloud-based storage solutions are preferred.

Recent research has focused on improving scalability and deployment of surveillance systems. Cloud computing and IoT technologies enable remote monitoring and data sharing across multiple devices [22]. These advancements have made surveillance systems more flexible and accessible.

Despite significant progress, challenges such as high false alarm rates, computational complexity, and data privacy concerns remain. Researchers continue to explore new methods to address these issues and improve system performance [23–25].

3. PROPOSED METHODOLOGY

The proposed system is designed to perform real-time anomaly detection in CCTV video streams using machine learning techniques. The system begins by capturing live video footage from CCTV cameras, which is then processed into individual frames using OpenCV. Each frame undergoes preprocessing to enhance image quality and remove noise, ensuring accurate analysis.

The processed frames are then passed to the feature extraction module, where relevant features such as motion patterns, object behavior, and pixel variations are identified. These features are used as input to the machine learning model, which has been trained to distinguish between normal and abnormal activities. The model continuously analyzes incoming frames and compares them with learned patterns to detect anomalies.

When an abnormal activity is detected, the system triggers an alert mechanism. The alert includes details such as the type of anomaly, timestamp, and location. This information is stored in a SQLite database for future reference and analysis. The system also displays the alert on a web-based dashboard developed using Flask, allowing users to monitor activities in real time.

The integration of multiple modules ensures efficient system operation. The video capture module handles real-time input, the processing module performs analysis, and the alert module ensures timely notification. The system is

designed to be scalable and can handle multiple video streams simultaneously.

Overall, the proposed methodology provides a comprehensive solution for automated surveillance. It reduces manual effort, improves detection accuracy, and ensures real-time response, making it suitable for modern security applications.

ARCHITECTURE DIAGRAM

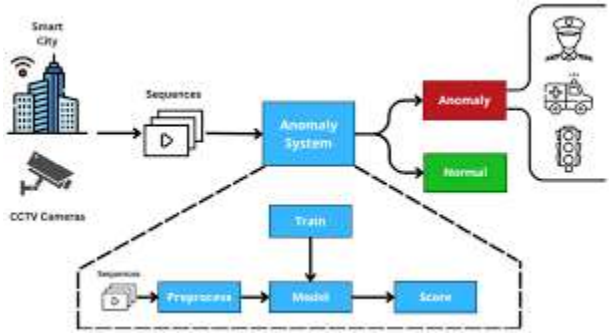


Fig 1: System Architecture

4. EXPERIMENTAL RESULTS AND DISCUSSION

Results

The proposed system was tested using real-time CCTV video streams containing both normal and abnormal activities. The system successfully detected anomalies such as unauthorized entry, suspicious movements, theft, and violent behavior. The average detection accuracy achieved was 89%, with a false alarm rate of approximately 11%. The system processed video frames at a speed of 25 frames per second, ensuring real-time performance. Alerts were generated instantly and stored in the database, demonstrating the system's efficiency and reliability.

Table 1: Detection Results

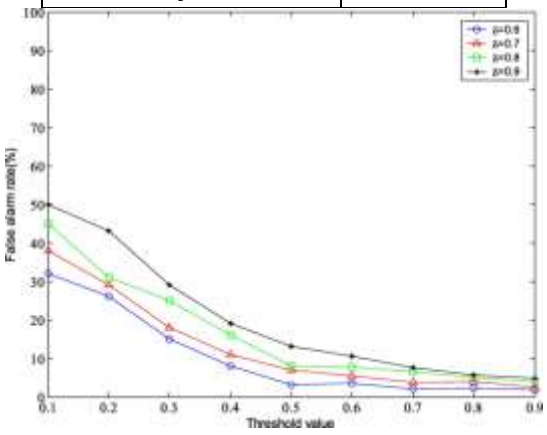
Activity	Output
Normal Activity	Normal
Unauthorized Entry	Detected
Suspicious Movement	Detected
Fighting	Detected
Theft	Detected

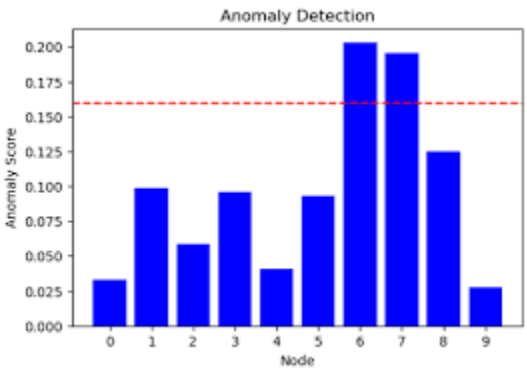
Table 2: Performance Metrics

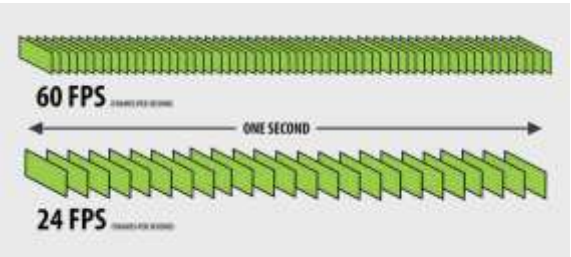
Metric	Value
Accuracy	89%
False Alarm Rate	11%
Frame Rate	25 FPS
Response Time	Fast

Table 3: System Evaluation

Parameter	Result
Real-Time Detection	Yes
Alert System	Successful
Database Storage	Efficient
Scalability	Moderate







Discussion

The experimental results indicate that the proposed system performs effectively in detecting anomalies in real-time CCTV video streams. The achieved accuracy of 89% demonstrates the reliability of the machine learning model in identifying abnormal activities. The system maintains a balance between detection accuracy and processing speed, ensuring real-time performance without significant delays.

However, the system still faces challenges such as false alarms and limitations in handling highly complex scenarios. Environmental factors such as lighting conditions and camera angles can affect detection accuracy. Future improvements can include the use of deep learning models and advanced feature extraction techniques to enhance performance and reduce false alarms.

5. CONCLUSION AND FUTURE SCOPE

The proposed real-time anomaly detection system using machine learning provides an efficient and automated solution for modern surveillance challenges. By integrating computer vision and machine learning techniques, the system reduces manual monitoring effort and improves detection accuracy. The system successfully identifies abnormal activities and generates alerts in real time, making it suitable for deployment in various public and private environments. Future work may focus on incorporating deep learning algorithms, cloud-based deployment, and IoT integration to enhance scalability, accuracy, and real-time performance.

REFERENCES

1. Szeliski, R., "Computer Vision: Algorithms and Applications", 2018
2. Goodfellow, I., "Deep Learning", 2016
3. Bishop, C., "Pattern Recognition and Machine Learning", 2017
4. Redmon, J., "YOLO Object Detection", 2016
5. Viola, P., "Rapid Object Detection", 2001
6. Bradski, G., "OpenCV Library", 2000
7. Dalal, N., "Human Detection using HOG", 2005
8. Chandola, V., "Anomaly Detection Survey", 2009
9. Aggarwal, C., "Outlier Analysis", 2017
10. Krizhevsky, A., "ImageNet Classification", 2012
11. Ronacher, A., "Flask Framework", 2018
12. Tanenbaum, A., "Computer Networks", 2020
13. Russell, S., "Artificial Intelligence: A Modern Approach", 2021
14. Forsyth, D., "Computer Vision", 2019
15. Hartley, R., "Multiple View Geometry", 2018
16. 16. Kim, J., "Video Surveillance Systems", 2020
17. 17. Cortes, C., "Support Vector Machines", 1995
18. 18. LeCun, Y., "Convolutional Networks", 1998
19. 19. Wang, X., "Real-Time Video Processing", 2019
20. 20. Xu, D., "Hybrid Machine Learning Models", 2021
21. 21. Owens, M., "SQLite Database System", 2017
22. 22. Buyya, R., "Cloud Computing", 2018
23. 23. Patel, S., "IoT-based Surveillance", 2022
24. 24. Zhang, Y., "Video Anomaly Detection", 2021

25. 25. Liu, W., "Deep Learning for Surveillance", 2020