Towards Intelligent Surveillance: Real-Time Anomaly Detection for Enhanced Public Safety Using a Deep Learning Approach

Sharanbabu B[1], Santhosh P[1], Subedha V[1]

[1] Department of CSE, Panimalar Engineering College, Chennai, 600123, India

sharanbabu545@gmail.com, santhosh929007@gmail.com, subedha@gmail.com

Abstract. Surveillance cameras are favored by people for maintaining high security levels in both public and private spaces. The surveillance operates continuously, and in the event of a crime, extensive manual review is necessary to inspect all recorded video footage, as a large amount of data is captured around the clock. In addition to the use of CCTVs for surveillance, some organization still employ someone to monitor those live feeds. Surveillance is only good as its monitoring and response system. Errors such as neglect, failure to check cameras regularly, and improper camera setup contribute to missed crime detection. An automated system that is capable of detecting anomalous activities happening around us by using the existing CCTV surveillance setup and alarm the law enforcements if anything unusual is detected. This research presents an automated video surveillance system that employs Autoencoder Neural Network, a deep learning technique for real-time anomaly detection. The dataset used is Kaggle's University of Central Florida (UCF) Crime Dataset. The system utilizes OpenCV for video capturing and processing and an Autoencoder Neural Network Architecture to learn normal behavioral patterns and identify potential anomalies in surveillance footage. Available over the internet browser as a surveillance dashboard, the system is capable of processing several camera inputs at a time and of sending out SMS's and E-Mails via SMTP and status alerts in real time. This includes addressing the increasing demand for intelligent surveillance systems that provide real time threat detection alerts in any open area. The results from the test showed that the use of the implementation in real time anomaly detection completed 99.5 % of the tasks with very few false alarms, hence it is much more feasible in real life security systems.

Keywords: Anomaly Detection, Surveillance, Video Feeds, Features, Alert Generation, Deep Learning, Convolutional Neural Networks (CNN)

1 Introduction

Since the 1940s closed circuit television systems (CCTV) have been, in use for surveillance purposes. With the introduction of video recording technologies, in the 1990s real time anomaly detection still relied on human oversight [2]. Security guards monitored video feeds. Used their own judgment to identify unusual or suspicious behavior. The increasing volume of video footage in the digital era led to a data deluge. It is challenging to manually find suspicious activities from the large amount of data available for surveillance purposes in case of crime investigations [2]. Thus, manual surveillance is labor-intensive and is prone to human error due to fatigue and attention limitations.

In early 2000s, alarm systems were integrated into some traditional CCTV setups, where predefined rules (such as motion detection) would trigger alerts sent to security teams. Such warnings by electronic systems were a common occurrence, but in many cases, they were provided late, and more often than not, numerous false alerts led the few, who traditionally responded to them, to treat real threats as standard operations [3]. This research solves the reviewed problems of enormous coverage and untimely warning systems by creating a self-operating device that changes all the time and can focus on several streams of video simultaneously to search for irregular activities without any interruptions.

1.1 Research Background

In recent times, there has been a significant rise in offensive and disruptive incidents. This sudden increase in crime and insecurity especially for women because of the lack in timely control of crimes. Crime prone areas have become more challenging to provide a faster service for anomalous events happened because of the rapid increase in the population in urban areas [4]. CCTV installations are widely used by various organizations and industries to monitor people and their behavior on a continuous basis. Analyzing surveillance videos for anomalies using manpower is a labor-intensive and tedious task due to the low occurrence of anomalous events compared to normal events. This makes it costly in terms of labor [2]. As such, it is almost unrealistic to expect authorities to keep a watchful eye on these surveillance videos in order to notice any suspicious activities since it requires resources and most importantly attention. There is an urgent need for some effort on the development of an appropriate automated system for this operation. Separation of the exact frames and spans of the video recordings which contain the suspicious or unusual events will speed up the research of any suspicious or abnormal activities. The saved time and effort from manually reviewing recordings would assist authorities in quickly identifying the cause of any abnormalities [5]. The installation of over 31000 security cameras in 11524 spots under 'Mission Trinetra' has solved over 360 criminal cases across the district of Noida [6]. Surveillance system with automated system of anomaly detection in real-time would increase the rate of crime prevention even more since it uses the existing surveillance cameras and is not dependent on a new device for surveillance purposes. A smart automated system that can spot behaviors helps address these problems by improving surveillance effectiveness and response time during emergencies. Anomaly detection is akin, to categorizing actions [7]. In surveillance settings, anomaly detection involves monitoring a location, for any behaviors that deviate from the patterns of behavior. Recent advancements in deep learning, particularly in computer vision and pattern recognition, have opened new possibilities for automated surveillance. Understanding anomaly detection in videos entails the deployment of algorithms within computer processing and pattern recognition procedures. Past strategies on the other hand would often apply supervised learning methods which needed great amounts of labelled anomalous events. In contrast, our method employs unsupervised learning with the use of autoencoders learning the typical behaviors and detecting an abnormality without the aid of abnormal data. The system has the ability to process a video and perform classification on a frame-by-frame basis. Each Frame is tagged as a given type of violence or crime: abuse, arrest, arson, assault, burglary, explosion, fighting, road accidents, robbery, shooting, shoplifting, stealing and vandalism [8].

1.2 Research Rationale

From the sayings of Simeon Preston "The biggest part of our digital transformation is changing the way we think". The primary motivation for this research is the need to develop an efficient surveillance system that can operate in real-time, minimizing the chances of missing critical events. In the Women's Peace and Security Index, for 2023 report shows that India is placed 128th out of 177 countries in terms of ranking. The index score for India is 0.58 which falls under the category when it comes to women safety according to the National Family Health Survey (NFHS) for this year reveals that around a third of women aged between 15 to 49, in India have encountered instances of social or domestic violence [9]. This system is particularly designed with women's safety in mind, offering a method to detect dangerous situations such as abuse or assault. The rationale for this research stems from several other factors such as the increasing number of surveillance cameras makes manual monitoring impractical, the need for 24/7 vigilance without human limitations is needed, the challenge of detecting subtle anomalies that human operators might miss, the requirement for a scalable and an automated solution that can handle multiple camera feeds and the importance of real-time detection and notification for immediate response.

1.3 Aims and Objectives

Aims:

To develop a robust, real-time anomaly detection system for video surveillance using deep learning techniques. This automated system depends on the process of segmentation of frames for anomaly detection which lead to classify the anomaly type. An enhanced machine learning algorithm is utilized for the classification process to get the ultimate results.

Objectives:

- To formulate and create a design and deploy an architecture based on autoencoder for detecting anomaly in video feeds.
- To evaluate how well the model worked compared to normal surveillance techniques in terms of accuracy, sensitivity, and specificity.
- To enhance the efficiency and accurate results. Thus, availing safety and timely interventions.
- To implement a web-application-based control interface used for supervision and management of the system in real-time.
- To build a Flask application which can visualize surveillance and live video stream with statistics.
- To allow for the system to be used in places where there are many cameras and in changing public spaces.
- To enable to run several cameras concurrently with the ability to process them at the same time.
- To provide an alarm systems for notifying the user at once when an abnormal event is detected and its location.
- To connect this system to SMS notification, sound notifications, email, and other notification systems.
- To enhance effective crime prevention and crime identification.
- To enable police officer to detect anomaly easily and classify its type from the live CCTV video feeds.
- To distinguish between normal and anomalous events by an efficient classifying algorithm.

The remainder of the paper is as follows. Section 2 proposes literature reviews. Section 3 presents a detailed description of real-time anomaly detection using a deep learning approach. Section 4 shows the results obtained from the model. Finally, concluded the paper in section 5 with the future direction.

2 Literature Survey

Anala [2] high lights the addition of spatial and time features to model video learning. In modeling, acquisition of spatial features is performed using CNN-CNN network and for learning sequence use a short-term LSTM network. The classification accuracy of the CNN-LSTM model was 85%. Its parameter classes are incapable as new anomalous classes could not be classified. Sultani [10] intended a novel approach to video abnormal and normal data processing with the purpose of being able to predict high negative scores for abnormal videos and effectively identify anomalies. On the contrary, the authors utilized a weakly labeled dataset where the video is marked as abnormal, even though only a few frames are bad with no phase annotations. Yaxiang Fan [11] proposed a 2-stream autoencoder, one stream for extracting spatial features and the other stream for extracting temporal features. The unsupervised learning model is competent in physical time but has a bad effect on new videos. Xu [12] presented novel unsupervised learning methodology using DeepNet that detects images and motion features from the input images and motion using DeepNet, image understanding, motion data, and shared representations using stacked autoencoders. It depends on the application, and SVM can determine the anomaly score for each of the inputs and calculate the final score. It was shown to be competitive when tested on two challenging datasets. Deepak Mane [13] proposed a method developed using MobileNet and Bi-LSTM to detect real-time anomalies correctly with the application of unsupervised learning technology. High accuracy is achieved due to the multimodal capabilities of MobileNet. This model only considers a few classes of parameters and does not use the latest deep learning techniques. Yuan Kai Wang [14] proposed an automatic scene detection system that uses image analysis to detect suspicious objects captured by cameras. This technology first reduces the features in various parts of the surveillance image, then detects abnormal situations by detecting changes in features when the image quality is low and the visuality changes. The situation analysis is done by calculating the changes over time. An online Kalman filter iteratively smooths the features and further reduces false positives caused by noise. This model has high accuracy in practical applications and rarely gives false alarms. Jerry Gao [15] uses neural network technology to identify crimes that occur in the real world. The model is trained to investigate property and arson, theft, and torture crimes. The models are trained using YOLOv5, YOLOv7, and YOLOv6 respectively. This project ensures people's safety without interfering with them and creates affordable security cameras to detect and identify crimes. The network system is used to receive alerts via Twilio communications when suspicious activity occurs in the community. This model is definitely less sensitive and has no monitoring potential. Ahmed Elmetwally [16] proposed a method for continuous detection of regular events based on the combination of inflated 3D convolutional networks (13D-ResNet50) and deep multiple comparison bounded learning (MIL). The results obtained from this model show that the AUC 0f is 82.85% after 10,000 iterations. The model seems to be better than other ways to see defects in live video. By using a deep FCNN to detect anomalies in video surveillance, the AD problem in video surveillance is solved. The network uses a weak training method. The algorithm used does not work well for low scores. In their research, Ulla et al. [17] introduced a convolutional neural network (CNN) model designed to extract spatiotemporal features from images.

These features can then be input into a multilayer bidirectional long-term memory (BDLSTM) model to differentiate between normal and abnormal events. The study obtained accuracies of 3.41% and 8.09% for UCF-Crime and UCF-Crime2 local data, respectively. Nevertheless, the accuracy of this model is less than that of truncation. Tian et al. [18] employed the Robust Temporal Feature Magnification (RTFM) model for normal/weakly labeled video clip classification. I3D or C3D was employed to extract features for segment training. When considering the UCF-Crime, UCSD-Peds, and XD-Violence datasets, the RTFM model outperforms many other existing methods and also exhibits superior capabilities in detecting confusion and extracting patterns. Pratik D. Waghere [19] focuses on real-time vulnerability detection to improve security using OpenCV on edge platforms. The OpenCV computer vision capabilities enable a business organization to unearth weaknesses that may prevail in the business environment. This system provides business security since it explains the situation and, therefore, responds in time to avoid accidents. The proposed system provides an improvement over traditional measures of security through live video analysis and detection of abnormal activities in real time. The anomaly detection system does not include existing industrial autonomous systems. Raut et al. [20] ensures machine safety using OpenCV to improve safety measures in work environments. He integrated computer vision technology to monitor equipment, detect potential hazards, and proactively address safety issues to create safer operations and reduce risks associated with machine operation. This study believes that negative detection aims to detect disruptions in the economy rather than detecting abnormal situations in the public sector. Manal Mostafa Ali [21] uses background subtraction (BS) by modeling each pixel as a mixture of Gaussians (MoG) to focus on foreground high learning only. The front end is equipped with an electronic autoencoder to filter abnormal cases from normal cases and automatically identify signs of threat and aggression on the fly. He introduced search objects throughout the scene and use bounding boxes to highlight areas of interest to minimize human intervention in the video stream. During the verification process, the network will generate alerts for existing vulnerabilities to warn against potential vulnerabilities. The system does not focus on the use of new equipment to improve the detection of anomalies in the business environment. Nithish [22] used YOLOv5, an object detection model combined with multiple deep learning methods, for anomaly detection in video surveillance. At the present, results of the experiment prove that the proposed theory is useful and powerful for the analysis and control of various defects-intrusions and anomalous motion and product abandonment. In the experiment, a training set consists of a small dataset containing only a few sets of anomalies. Dr. M. Senthil Kumaran [23] developed a new technique for face recognition and motion detection. The Raspberry Pi model is selected as the reference for initial storage of data and information. Local binary pattern (LBP) texture is used to provide a good representation of the face for face detection. It divides the face image into local regions to independently extract fine annotations from each region. Combination of adaptive background modeling and cascade classifier-based object detection system for video surveillance applications. The system cannot detect abnormalities in real-time video surveillance and cannot raise an alarm when abnormal conditions occur in the public. Seemantula Nischal [24] used deep learning models such as CenterNet and Graph Convolutional Networks (GCN) to detect and identify anomalies in CCTV footage. In case of any theft, traffic violation, illegal entry, and criminal arrest, the system will send notifications to the nearest police station. It integrates with the Twilio Video API to send real-time video notifications, video messages, as well as informal documents to employees. The system stores information about anomalies in a database referred to as MindsDB. This information includes type of anomaly, seriousness level, and latitude and longitude of location. The system makes fewer decisions about specific classes.

3 Proposed System

3.1 Overview

The architectural model includes an application of autoencoders for the purpose of video anomaly detection. The training is aimed at recognizing normal behavioral aspects so any deviation is marked as an anomaly. The system makes use of Twilio API to send out SMS alerts and the SMTP for emails and generates sound alerts locally on the machine when an anomaly is detected. Table 1 describes the classical and modern approaches of real-time anomaly detection from the life video stream.

Table 1. Comparison between the traditional and contemporary methods for real-time anomaly detection from live feeds.

Aspect	Conventional System	Proposed System
Detection Method	Relies on human monitoring.	Learns patterns from data to automatically detect anomalies in real-time.
Efficiency	Low; prone to human error, fatigue, and system inflexibility.	High; continuous and autonomous operation with real-time detection.
Accuracy	Moderate; high false positive/negative rates.	High; lower false alarm rates and improved precision in anomaly detection.
Resource Requirement	High; requires significant human resources and equipment.	Moderate; requires computational resources but operates autonomously after setup.
Accessibility	High; easy to implement but lacks advanced anomaly detection capabilities.	Growing; as deep learning tools become more accessible and easier to use.
Training & Expertise	Requires trained operators for monitoring and configuring rule-based systems.	Requires expertise in machine learning, but once deployed, needs minimal human input.
Subjectivity	High; human judgment can be inconsistent, leading to bias.	Low; data-driven, making detection more objective and consistent.
Scalability	Low; difficult to scale with many cameras due to manual monitoring.	High; easily scalable to thousands of camera feeds.
Processing Time	Slow; human reaction introduces delays in real-time detection.	Fast; real-time anomaly detection as video frames is processed instantly.

3.2 Dependencies

Software Requirements:
- Python – Primary programming language
- Anaconda Navigator – Environment

Core Frameworks used:
- Tensorflow/Keras – Model creation and training
- OpenCV – Video capturing and processing
- Flask – Web application for user interaction

Other Frameworks used:
- SQLite3 – Database to store user and camera information
- Twilio API – For SMS alerts
- SMTP – For email notifications

Frontend Technologies:
- HTML – User interface components
- CSS – For styles

3.3 Workflow

Video feeds with and without anomalies are included in a dataset of varied anomaly types. To improve model performance, the videos undergo video-processing techniques such as real-time frame capture, image preprocessing and feature extraction. A deep learning architecture such as Autoencoder Neural Network is chosen for training the dataset. After training, the model is deployed in the integrated system with user-friendly interface to get live input CCTV camera feed from the user and display the obtained anomaly status. Backend infrastructure is built for efficient inference and scalability. The ethical consideration regarding patient privacy, data security and regulatory compliance are ensured throughout the lifecycle of the system.

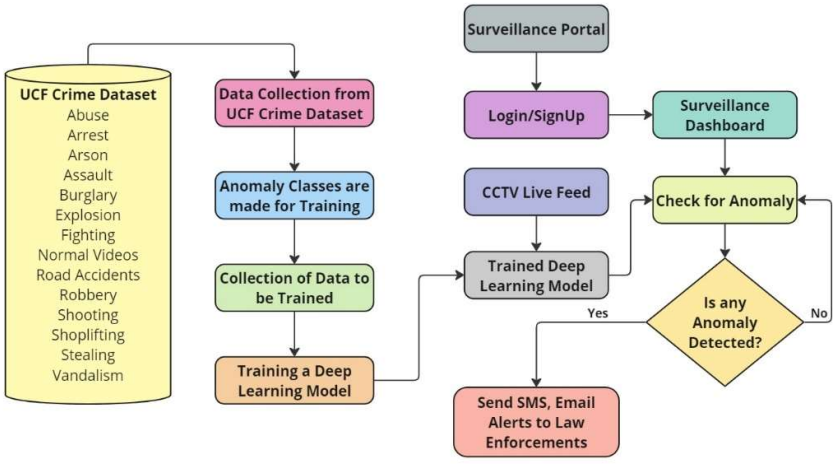

Fig. 1. Block Diagram

UCF Crime Dataset: The UCF Crime Dataset is an image annotation where several crime categories are depicted through the Means of the numerous video clips showing abusive behavior, assault, robbery, vandalism and so on, in addition to ordinary activities. This dataset is very important in training our deep learning model to detect outliers in live CCTV footage.

Data Collection & Preparation: Data from the UCF Crime Dataset is collected, capturing every video frame as the footage required is extracted from each video. These frames are then filtered through so as to do away with all the noise and enhance the quality so that the model is able to learn from the best data possible.

Anomaly Classes & Training: Different types of offending behavior (like robbery, fighting, arson, etc.,) are summed up in a distinction. Fairly significant samples from each category are gathered to ensure the model is not biased to any particular crime scenario. Samples are used for training the deep learning model with the assistance of deep learning methods like Autoencoder Neural Networks capable of learning the unexpected in the video outputs.

Deployment & Real-time Detection: After the model training is complete, the model is embedded in a simple user-friendly surveillance system. The system enables its users to log in, watch CCTV in real time and check updates about the recorded oddities. In case of any suspicious action, real time alert is activated through Text message (SMS), Email and sound.

Database: The system, for detecting anomalies uses SQLite as its database system because of its efficient design which makes it perfect for managing user and surveillance camera information. The database consists of three tables. Users for keeping user credentials and roles in check Cameras for overseeing camera locations and statuses. Alerts, for recording notifications triggered by identified anomalies. Each table is set up in a way that guarantees data reliability by maintaining primary and foreign key connections. Security protocols such, as password encryption and restricted access are in place to protect data and uphold user privacy and security within the system, for operations.

Ethical Considerations: At every stage in the lifecycle of development, we try to understand, assess and deal with ethical concerns such as privacy, security of information and regulatory compliance. It is important to protect information and use it sparingly in order to gain trust in the system.

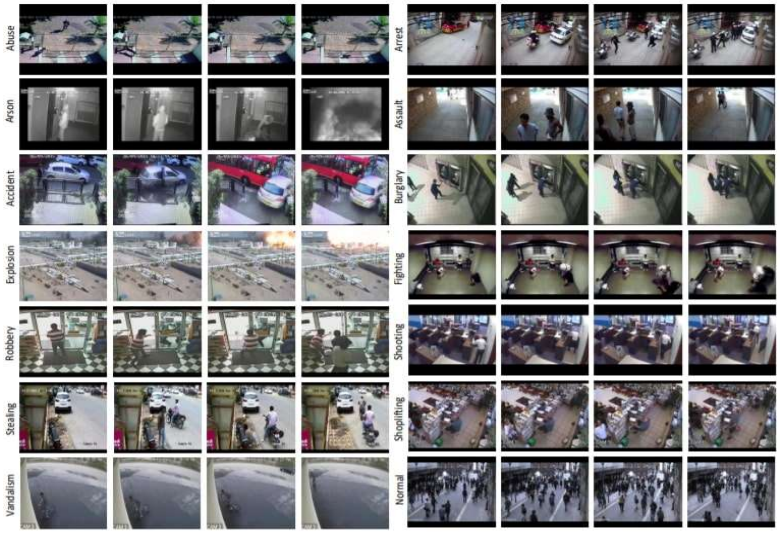

Fig. 2. UCF Crime Dataset

4 Result and Analysis

The whole set of anomaly detection on live video feeds from the Kaggle's UCF Crime Dataset are included in this section. Windows 11 64-bit is utilized with an 10th generation Core i3 PC equipped with 8GB of RAM. NVIDIA GPU can be helpful for faster processing. We employed 50 epochs and a 32-bit batch size.

The following Fig. 3 shows the Training-Validation Accuracy Loss graph obtained at the end of model training with a training accuracy of 99.5-99.8%, validation accuracy of 99.3-99.7% and average inference time of 30ms per frame.

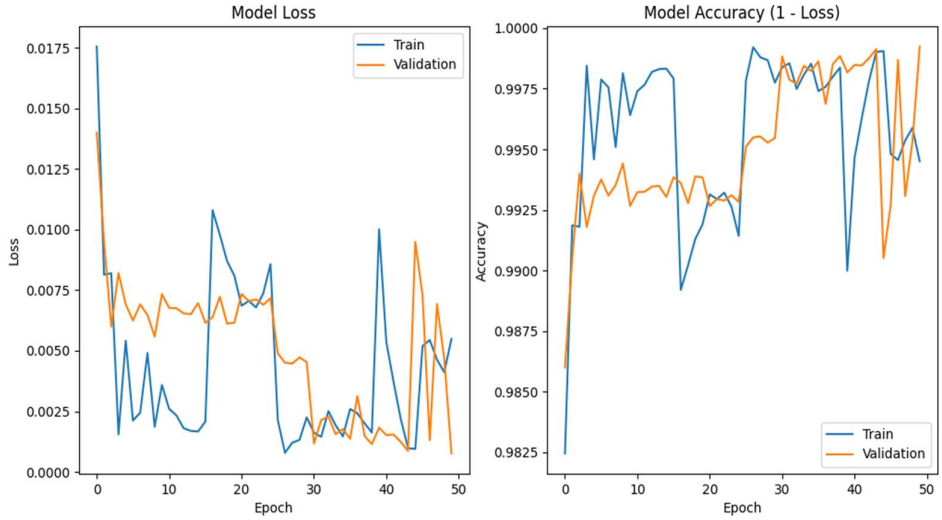

Fig. 3. Training-Validation Accuracy Loss Graph

The following Fig. 4, Fig. 5 shows the ROC Curve and Error Distribution Graph respectively:

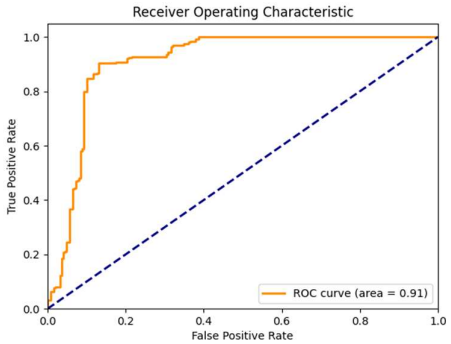

Fig. 4. ROC Curve

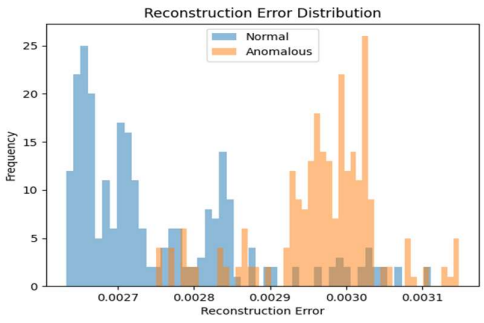

Fig. 5. Error Distribution Graph

The following Fig. 6 shows the Surveillance Dashboard after Login/Signup:

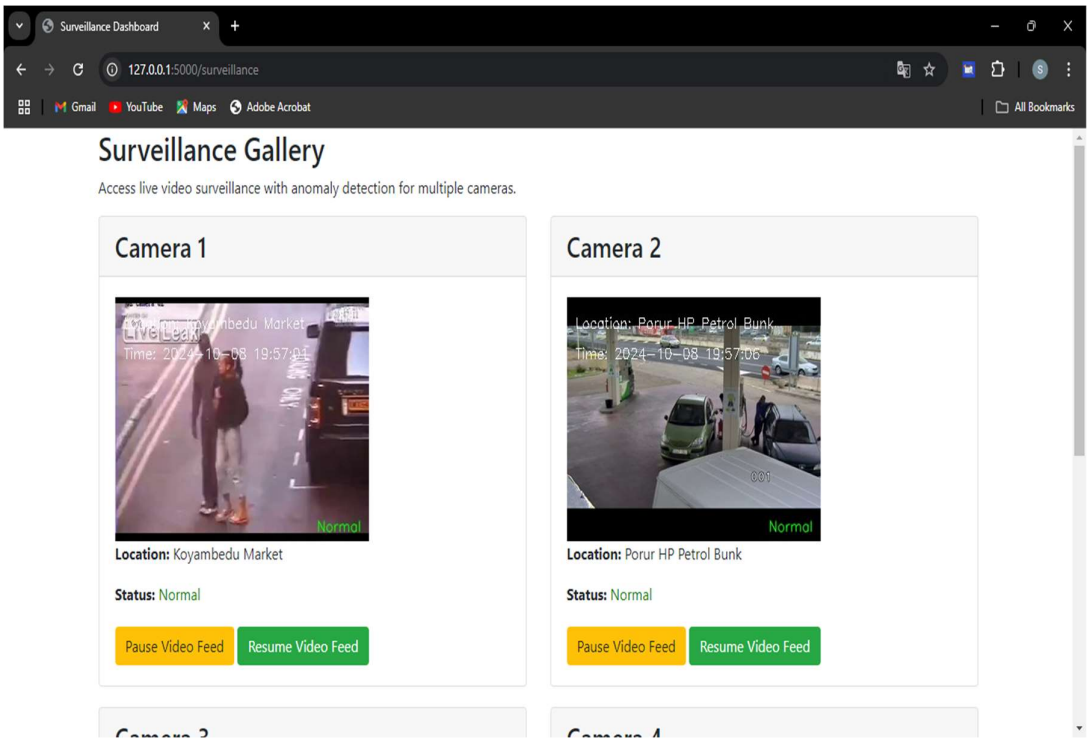

Fig. 6. Surveillance Dashboard

The following Fig. 7 shows the Normal and Anomaly Detected Status:

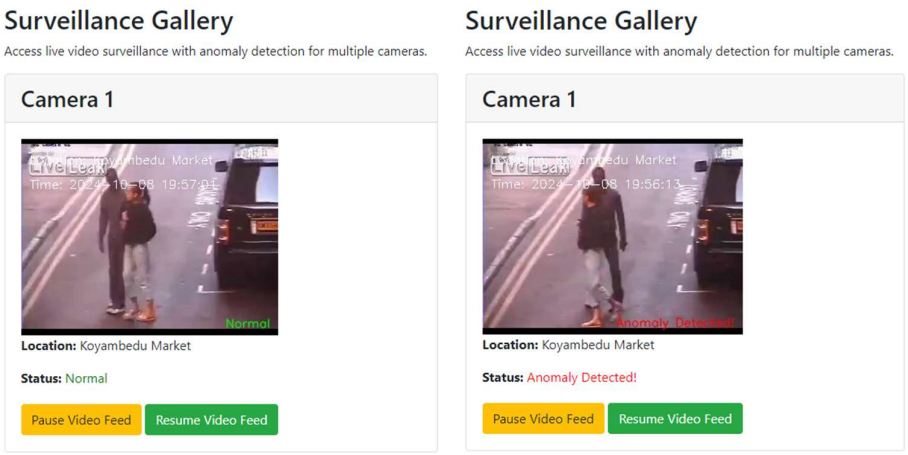

Fig. 7. Normal and Anomaly Detected Status

The following Fig. 8 shows the SMS and Email Alerts:

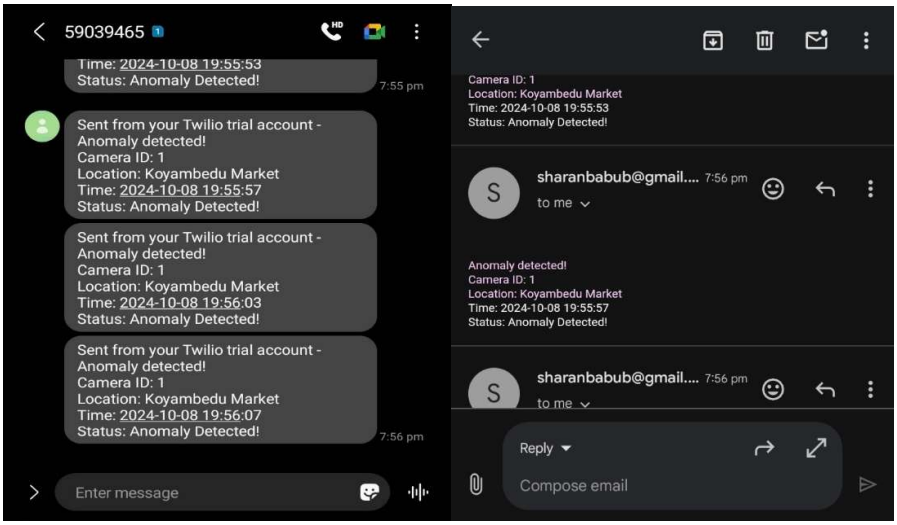

Fig. 8. SMS and Email Alerts

The following Fig. 9 depicts the Confusion Matrix and Classification Report:

```
Confusion Matrix:
 [[245   5]
 [230  20]]

Classification Report:
              precision    recall  f1-score   support

         0.0       0.52      0.98      0.68       250
         1.0       0.80      0.08      0.15       250

    accuracy                           0.53       500
   macro avg       0.66      0.53      0.41       500
weighted avg       0.66      0.53      0.41       500
```

Fig. 9. Confusion Matrix and Classification Report

5 Conclusions

In brief, the study proves how a real time anomaly detection in video surveillance can be accomplished using deep learning techniques, hence the safety in public places is improved. The ability to exploit an autoencoder in detecting anomalous events was established without the need of vast amounts of labelled data. The remote monitoring and control functions are also enhanced by the use of web interface, while the multi-threading feature allows for the supervision of several cameras' feeds efficiently. High accuracy and efficiency of the system allow timely detection and investigation of crimes thus enhancing the safety of the public. As regards this model, it is confined within these boundaries as it can be further and more actively improved and validated in practice. The future developments can also involve board range of object tracking, creating a mobile application for remote control and advanced analytics user interface.

References

1. Wikipedia, Closed-Circuit Television, https://en.wikipedia.org/wiki/Closed- circuit television.
2. Dr. Anala M.R, Malika Makker and Aakanksha Ashok, "Anomaly Detection in Surveillance Videos", 26th International Conference on High Performance Computing, Data, and Analytics Workshop (HiPCW), 2019.
3. Catarina Fontes, Ellen Hohma, Caitlin C. Corrigan and Christoph Lütge, "AI-powered public surveillance systems: why we (might) need them and how we want them", Technical University of Munich, School of Social Sciences and Technology, Institute for Ethics in Artificial Intelligence, München, 80333, Germany, Technology in Society 71, 2022.
4. Norkobil Saydirasulovich, S. Abdusalomov, A. Jamil, M.K. Nasimov, R. Kozhamzharova and D. Cho, "A YOLOv6-Based Improved Fire Detection Approach for Smart City Environments", Sensors 2023, 23, 3161.
5. Abhishek Kumar, Ayush Kumar, Aryan Shrivastava and Mudit Khandelwal, "Criminal Detection by Analysing Live CCTV Footages", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, http://www.ijert.org, IJERTV12IS050328, Vol. 12 Issue 05, May-2023.
6. Times of India, https://timesofindia.indiatimes.com/city/noida/murder-to-loot-how-cctv-cameras-helped-noida-police-solve-360-cases/articleshow/105768113.cms.
7. A. Sodemann, M. P. Ross and B. J. Borghetti, "A Review of Anomaly Detection in Automated Surveillance", IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 42, no. 6, pp. 1257-1272, Nov. 2012.
8. Deepak Mane, Sheetal Phatangare, Siddhant Nawale, Siddhesh Wani, Varun Gujarathi and Vaishnav Loya, "Real-Time Anomaly Detection in Video Surveillance: A Mathematical Modeling and Nonlinear Analysis Perspective with MobileNet and Bi-LSTM", Communications on Applied Nonlinear Analysis, ISSN: 1074-133X, Vol 31 No. 2s, 2024.
9. ForumIAS, https://forumias.com/blog/women-safety-in-india-significance-and-challenges-explained-pointwise/.
10. W. Sultani, C. Chen, and M. Shah, “Real-world anomaly detection in surveillance videos”, arXiv preprint arXiv:1801.04264, 2018.
11. Yaxiang Fan, Gongjian Wen, Deren Li, Shaohua Qiu and Martin D. Levine. “Video Anomaly Detection and Localization via Gaussian Mixture Fully Convolutional Variational Autoencoder”, arXiv preprint arXiv:1805.11223, 2018.
12. D. Xu, E. Ricci, Y. Yan, J. Song, and N. Sebe, “Learning Deep Representations of Appearance and Motion for Anomalous Event Detection”, arXiv:1510.01553v1 [cs.CV], 6 Oct 2015.
13. Deepak Mane, Sheetal Phatangare, Siddhant Nawale, Siddhesh Wani, Varun Gujarathi and Vaishnav Loya, "Real-Time Anomaly Detection in Video Surveillance: A Mathematical Modeling and Nonlinear Analysis Perspective with MobileNet and Bi-LSTM", Communications on Applied Nonlinear Analysis, ISSN: 1074-133X, Vol 31 No. 2s, 2024.
14. Yuan-Kai Wang, Ching-Tang Fan, Ke-Yu Cheng and Peter Shaouha Deng, "Real-time Camera Anomaly Detection for Real-World Video Surveillance”, International Conference on Machine Learning and Cybernetics, Guilin, 10-13 July, 2011.
15. Jerry Gao, Jingwen Shi, Priyanka Balla, Akshata Sheshgiri, Bocheng Zhang, Hailong Yu and Yunyun Yang, "Camera-Based Crime Behavior Detection and Classification", Smart Cities 2024, 7, 1169–1198, https://doi.org/10.3390/smartcities7030050.
16. Ahmed Elmetwally, Reem Eldeeb, Samir Elmougy, "Deep learning-based anomaly detection in real-time video", Multimedia Tools and Applications, https://doi.org/10.1007/s11042-024-19116-9.
17. Ullah W, Ullah A, Haq IU, Muhammad K, Sajjad M and Baik SW, "CNN features with bi-directional ISTM for real-time anomaly detection in surveillance networks", Multimedia Tools and Applications 80(11):16979–16995, 2021.

18. Tian Y, Pang G, Chen Y, Singh R, Verjans JW and Carneiro G, "Weakly-supervised video anomaly detection with robust temporal feature magnitude learning", Proceedings of the IEEE/CVF International Conference on Computer Vision, pp. 4975–4986, 2021.
19. Pratik D. Waghere, Sakshi Wagh and Archana L. Rane, "Enhancing Industrial Safety: Real-time Anomaly Detection with OpenCV on Edge Platforms", International Research Journal of Modernization in Engineering Technology and Science, Volume:06/Issue:05/May-2024.
20. Raut S, Hase V, Kotgire S, Dalvi S, and Malge A, "Enhancement of the Machine Safety Using OpenCV", Biennial International Conference on Future Learning Aspects of Mechanical Engineering (pp. 717-724), Springer Nature Singapore, August 2022.
21. Manal Mostafa Ali, " Real-time Video Anomaly Detection for Smart Surveillance", IET Image Processing published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology, DOI: 10.1049/ipr2.12720, 11 December 2022.
22. Nithish S, Kushaj Kumar, Anupama Sinha, Naman Sood and Vinay V Hegde, "YOLOv5: Anomaly Detection in Surveillance Videos using Deep Learning", International Journal of Creative Research Thoughts (IJCRT), www.ijcrt.org, ISSN: 2320-2882, Volume 12, Issue 6 June 2024.
23. Dr. M. Senthil Kumaran, Suraj S and Naga Dheeraj N, "Anomaly Detection using OpenCV", International Research Journal of Engineering and Technology (IRJET), www.irjet.net, e-ISSN: 2395-0056, p-ISSN: 2395-0072, Volume: 07 Issue: 05, May 2020.
24. Seemantula Nischal, Bhunesh K and Ashwin Sathappan V, "Real-time Anomaly Detection and Alert System for Video", International Research Journal of Engineering and Technology (IRJET), www.irjet.net, e-ISSN: 2395-0056, p-ISSN: 2395-0072, Volume: 10 Issue: 05, May 2023.