International Journal of Electrical and Electronics Engineers
Volume 18, Issue No. 01, Jan-June 2026
ISSN (0) 2321-2055 ISSN (P) 2321-2045

SMART SURVEILLANCE SYSTEM WITH ANOMALY DETECTION USING DEEP LEARNING TECHNIQUES

Mr. M. Srikanth[#1], *Associate Professor, Department of Computer Science and Engineering, Tirumala Engineering College, Jonnalagadda, Andra Pradesh, India - 522601.*

P. Navya Kanaka Durga[#2], SK. Abdul Ghani[#3], Y. Aparna[#4], Y. Sasi Kumar[#5]

Abstract— Public safety and security are major concerns due to increasing crime rates and suspicious activities in public places. Traditional surveillance systems rely on continuous human monitoring of CCTV footage, which is time-consuming and prone to errors. This project presents a Smart Surveillance System with Anomaly Detection using Deep Learning techniques to automatically detect abnormal activities such as violence, theft, fighting, and intrusion in real time. Using Computer Vision and Convolutional Neural Networks (CNN), video frames are analyzed and classified as normal or abnormal. If suspicious activity is detected, alerts are generated and important footage is stored. Implemented using Python, TensorFlow, Keras, OpenCV, and Flask, the system improves monitoring efficiency, reduces false alarms, and enables faster response to security threats.

Keywords— Smart Surveillance, Anomaly Detection, Deep Learning, Convolutional Neural Network (CNN), Computer Vision, Real-Time Monitoring, Violence Detection, Suspicious Activity Detection

I. INTRODUCTION

Security and surveillance play a major role in protecting people and property in modern society. CCTV cameras are widely installed in public places such as banks, malls, hospitals, schools, railway stations, airports, and offices for continuous monitoring. However, traditional surveillance systems only record video footage and require human operators to monitor multiple screens continuously.

Manual monitoring of surveillance footage is difficult, time-consuming, and highly prone to human error. Security personnel may miss important suspicious events due to fatigue, distraction, or the large number of cameras. This often leads to delayed responses and reduced security efficiency.

To solve this problem, intelligent surveillance systems are required. The Smart Surveillance System with Anomaly Detection Using Deep Learning is designed to automate surveillance monitoring and detect suspicious activities in real time.

The system identifies abnormal events such as violence, theft, fighting, burglary, assault, shooting, explosion, fall detection, and unauthorized motion detection. It uses Artificial Intelligence (AI), Deep Learning, and Computer Vision to analyze video frames and classify activities as normal or abnormal.

The system immediately generates alerts when suspicious behavior is detected, allowing faster action by security personnel. This provides a proactive approach to surveillance instead of passive recording.

II. LITERATURE SURVEY

Accurate anomaly detection in surveillance systems is essential for improving public safety and reducing crime. Several researchers have proposed machine learning and deep learning approaches for intelligent surveillance.

Menezes et al. developed a face tracking system using Haar-like features and Eigenfaces. Haar-like features were used for fast face detection, while Eigenfaces helped in face recognition using Principal Component Analysis (PCA). Their system provided the foundation for early surveillance applications, but it was sensitive to lighting conditions and pose variations.

Ling Shao et al. presented a survey on transfer learning techniques for visual categorization. Their work explained how pre-trained deep learning models such as VGG16 can be reused for new image classification tasks with limited datasets, which became highly useful for surveillance systems.

Kaiming He et al. proposed Deep Residual Learning (ResNet), which solved the vanishing gradient problem in deep neural networks using residual connections. This improved image classification accuracy and deep model training, although it required high computational resources.

Wazwaz et al. developed a low-cost face detection system using Haar Cascade and Raspberry Pi for real-time surveillance. The system was affordable and useful for small-scale applications, but its performance was affected by lighting and background variations.

Arya Paul et al. proposed an integrated smart surveillance system using VGG16 and MoveNet for face detection, object detection, and anomaly recognition. Their system improved detection efficiency and reduced storage requirements using edge-cloud architecture.

Although many methods exist, most systems focus only on specific tasks such as face detection or object recognition. A complete framework integrating motion detection, fall detection, anomaly recognition, and real-time alert generation is still required.

III. EXISTING SYSTEM

The existing surveillance systems mainly depend on traditional CCTV cameras and manual monitoring by human operators. These systems continuously record video footage but do not automatically detect suspicious activities or abnormal behavior.

Security personnel are required to monitor multiple camera screens for long hours, which is time-consuming, difficult, and prone to human error. Important events such as violence, theft, fighting, intrusion, and accidents may be missed due to fatigue, distraction, or lack of attention.

Most traditional systems only provide passive recording instead of active monitoring. They require large storage space for continuous video recording and do not generate instant alerts when suspicious activities occur. This results in delayed response to emergency situations and reduces overall security efficiency.

Some existing intelligent surveillance systems focus only on specific tasks such as face detection, object detection, or motion

detection, but they do not provide a complete solution for anomaly detection and real-time alert generation.

Therefore, there is a need for an automated smart surveillance system that can detect abnormal activities in real time, reduce human dependency, minimize storage usage, and improve public safety.

IV. PROPOSED SYSTEM

The proposed Smart Surveillance System with Anomaly Detection uses Deep Learning and Computer Vision techniques to automatically detect suspicious and abnormal activities in real time. The system is designed to improve public safety by reducing human dependency in traditional surveillance systems and providing faster response to security threats.

The system accepts input from CCTV cameras or uploaded video files and continuously monitors the video stream. It processes the video frames using image preprocessing techniques and applies a trained Convolutional Neural Network (CNN) model to classify activities as normal or abnormal. If suspicious behavior such as violence, theft, fighting, fall detection, intrusion, or abnormal movement is identified, the system immediately generates alerts and stores important event-based footage for future reference.

Unlike traditional surveillance systems that only record video, the proposed system performs active monitoring and real-time anomaly detection. This improves security efficiency and reduces the workload of security personnel.

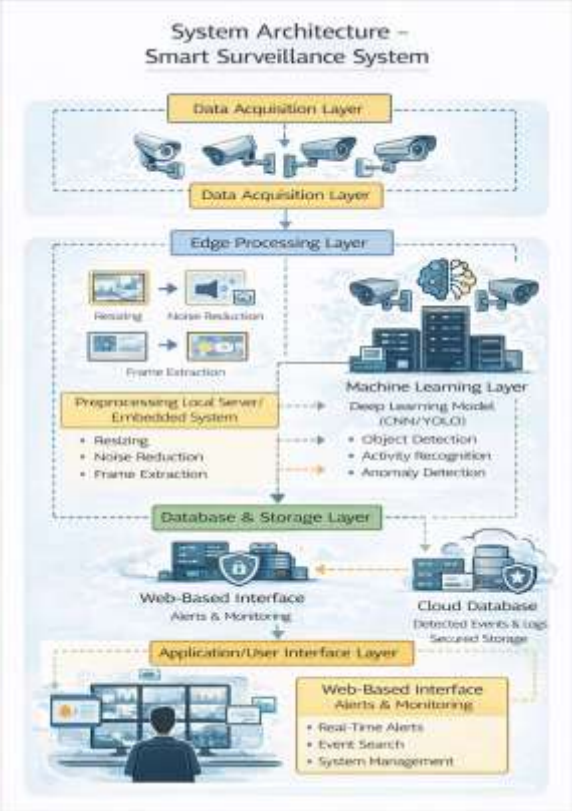


Fig: System Architecture

Modules of Proposed System

1. Motion Detection Module

This module detects suspicious movement in restricted or sensitive areas. It compares consecutive video frames to identify motion using frame differencing, grayscale conversion, thresholding, and contour detection. If unexpected movement is found, the system marks it as suspicious activity.

2. Fall Detection Module

This module is useful for hospitals, elderly care centers, and public safety environments. It detects whether a person has fallen by analyzing body posture and object dimensions. Using object detection methods such as YOLO, the system checks changes in height and width of the human body. If height decreases and width increases significantly, a fall is detected.

3. Object Detection Module

This module identifies suspicious objects such as weapons, masks, or unusual items that may indicate criminal behavior. It helps improve anomaly detection accuracy by recognizing dangerous objects present in the surveillance area.

4. CNN-Based Anomaly Detection Module

This is the main module of the system. The Convolutional Neural Network (CNN) model is trained using datasets containing normal and abnormal activities. It analyzes video frames and classifies activities into categories such as Fighting, Burglary, Assault, Shooting, Explosion, Abuse, and Stealing. The trained model improves detection accuracy and reduces false alarms.

5. Alert Generation Module

When abnormal activity is detected, the system immediately generates alerts such as on-screen warnings, alarm sounds, and notifications to security personnel. This enables quick response and improves emergency handling.

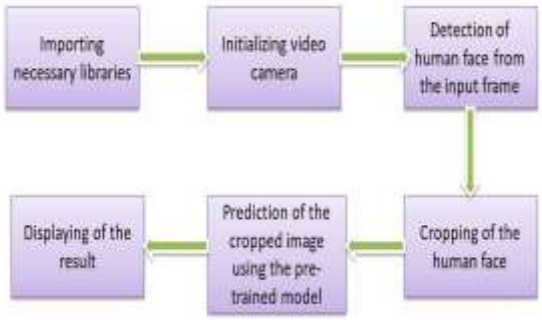
6. Event-Based Storage Module

Instead of storing complete continuous video footage, the system saves only anomaly frames, suspicious events, and event logs. This significantly reduces storage space and makes event tracking easier.

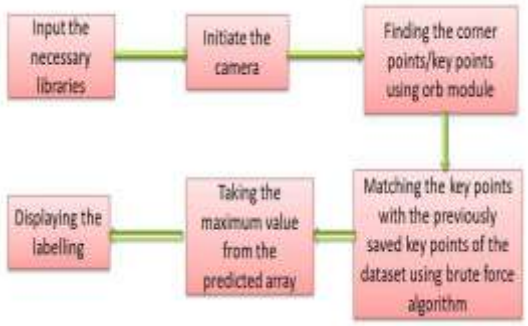
7. Web Interface Module

A Flask-based web application provides a user-friendly interface for video upload, live monitoring, alert viewing, and administrative control. This allows users to monitor surveillance activities efficiently through a simple dashboard.

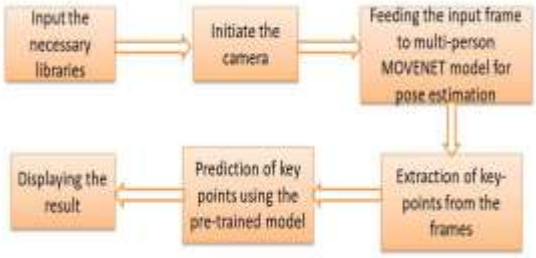
A. Face Detection



B. Object Detection



C. Pose Detection



Advantages of Proposed System

- Real-time anomaly detection
- Reduced human intervention
- Faster alert generation
- Improved security monitoring
- Lower false alarms
- Reduced storage consumption

• Easy deployment in smart cities, banks, airports, hospitals, schools, and public places

The proposed system provides an intelligent and cost-effective surveillance solution that improves public safety and supports smart monitoring environments.

V. METHODOLOGY

The methodology of the Smart Surveillance System with Anomaly Detection Using Deep Learning focuses on detecting abnormal activities automatically from live CCTV footage or uploaded video files. The system uses Computer Vision, Deep Learning, and image processing techniques to identify suspicious events in real time and generate alerts.

The complete working process of the system is divided into the following steps:

1. Video Collection

The system accepts input from CCTV cameras or uploaded video files. Live video streams are continuously captured from surveillance cameras installed in public places such as banks, hospitals, airports, malls, schools, and offices. Users can also upload recorded videos for anomaly detection and analysis.

2. Frame Extraction

The input video is divided into individual image frames for easier processing. Since Deep Learning models work efficiently on images rather than complete videos, frame extraction helps in analyzing activities step by step.

3. Frame Preprocessing

The extracted frames are preprocessed to improve detection accuracy. This includes:

• Resizing the frames to a fixed dimension

• Converting frames into grayscale

• Noise reduction using filtering techniques

• Normalization for better model performance

• Background subtraction for motion analysis

These preprocessing steps help remove unnecessary information and improve the quality of input data.

4. Motion Detection

The system compares consecutive frames to detect suspicious movement. Frame differencing and contour detection are used to identify motion in restricted or sensitive areas. This helps in detecting unauthorized entry or unusual movement without requiring deep learning training.

5. Fall Detection

Human objects are detected using object detection methods such as YOLO. The system analyzes body posture by checking height and width changes of the detected person. If the height decreases and width increases significantly, the system identifies it as a fall event.

6. Feature Extraction and CNN Analysis

The preprocessed frames are passed to the trained Convolutional Neural Network (CNN) model. The model extracts important features such as:

• Human posture

• Motion patterns

• Object movement

• Suspicious interactions

• Violent behavior patterns

The CNN model classifies the activities as normal or abnormal based on these extracted features.

7. Alert Generation

If abnormal activity is detected, the system immediately generates alerts such as:

• On-screen warning messages

• Alarm notifications

• Email or SMS alerts

This enables quick action by security personnel and reduces response time during emergencies.

8. Event-Based Storage

Instead of storing complete video footage continuously, the system saves only anomaly frames, suspicious events, and event logs. This reduces storage requirements and makes event retrieval easier for future investigation.

9. Web-Based Monitoring

A Flask-based web interface is provided for live monitoring, video upload, event history checking, and administrative control. This improves usability and allows efficient surveillance management.

The proposed methodology ensures accurate anomaly detection, faster alert generation, reduced storage usage, and improved security efficiency compared to traditional surveillance systems.

VI. RESULT ANALYSIS

1. Dataset Overview

The model was trained using the **UCF Crime Dataset**, which contains multiple crime-related video categories such as:

- Abuse
- Assault
- Burglary
- Explosion
- Fighting
- NormalVideos
- Shooting
- Shoplifting
- Stealing

Dataset Size

- Total images extracted: **12,66,345**
- The dataset was highly imbalanced, where **NormalVideos** had the highest number of samples.

Class Imbalance Handling

To avoid bias toward the majority class, the training dataset was balanced by:

- Reducing **NormalVideos** to **50,000 samples**
- Retaining the maximum available samples for other crime categories

This balancing improved the overall model performance and reduced classification bias.

2. Model Training Performance

The CNN model was trained for **5 epochs**.

Training and Validation Results

Epoch	Training Accuracy	Validation Accuracy	Validation Loss
1	66.4%	96.7%	0.1078
2	93.5%	98.0%	0.0665
3	94.9%	98.4%	0.0586
4	95.5%	98.4%	0.0592
5	95.8%	98.6%	0.0480

Observations

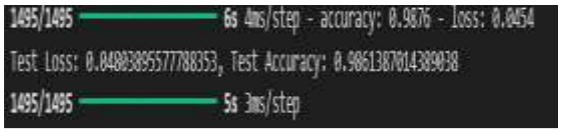
- Rapid improvement in accuracy after the first epoch
- Validation accuracy remained consistently high
- Validation loss steadily decreased
- No major overfitting was observed
- The model converged successfully and showed stable learning performance

3. Test Performance

Final Test Results

- **Test Accuracy:** 98.61%
- **Test Loss:** 0.0480

These results indicate excellent generalization capability of the model on unseen test data.



4. Classification Report Analysis

Class	Precision	Recall	F1-Score
Abuse	0.99	0.97	0.98
Assault	1.00	0.96	0.98
Burglary	1.00	0.99	0.99
Explosion	0.99	0.98	0.99
Fighting	1.00	0.98	0.99
NormalVideos	0.96	0.99	0.97
Shooting	0.99	0.97	0.98
Shoplifting	1.00	1.00	1.00
Stealing	0.99	1.00	0.99

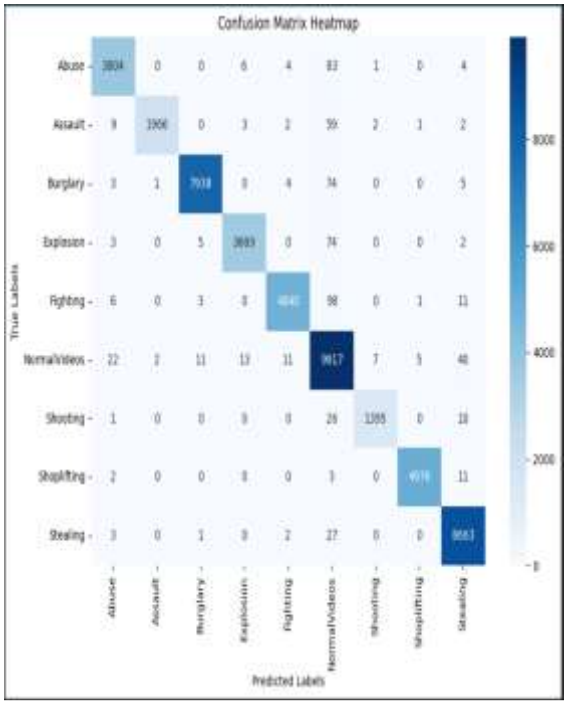
Overall Metrics

- **Accuracy:** 99%
- **Macro Average F1-Score:** 0.99
- **Weighted Average F1-Score:** 0.99

Interpretation

- Very high precision indicates fewer false positives
- High recall indicates fewer false negatives
- Excellent F1-score shows balanced model performance

The model performed very well across all crime categories and achieved highly reliable anomaly detection.

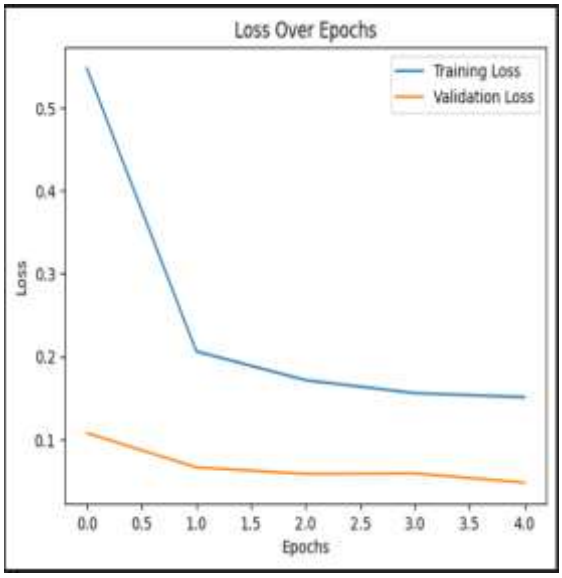


5. Graphical Analysis

From the generated training and evaluation graphs:

- The **loss curve** showed a steady decline, indicating successful learning
- The **accuracy curve** showed continuous improvement during training
- The **confusion matrix** showed minimal misclassifications between classes
- Dataset balancing significantly improved classification performance

These graphical results confirm that the proposed Smart Surveillance System is highly effective for real-time anomaly detection and provides strong performance for practical surveillance applications.



VII. CONCLUSION

The Smart Surveillance System with Anomaly Detection Using Deep Learning provides an efficient and intelligent solution for modern security challenges. Traditional surveillance systems rely on continuous human monitoring, which is time-consuming, error-prone, and often causes delayed responses during emergencies. The proposed system uses Computer Vision, Convolutional Neural Networks (CNN), and Deep Learning techniques to detect abnormal activities such as violence, theft, fighting, assault, burglary, and other suspicious behavior in real time. It also includes motion detection and fall detection modules to improve monitoring efficiency. Trained using the UCF Crime Dataset, the model achieved 98.61% test accuracy and 99% overall classification accuracy. By generating instant alerts and storing

only important event-based footage, the system reduces storage requirements and enables faster response from security personnel, making it suitable for banks, hospitals, airports, schools, and smart city environments.

VIII. REFERENCES

[1] P. Viola and M. Jones, "Rapid Object Detection using a Boosted Cascade of Simple Features," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR)*, 2001, pp. 511–518.

[2] N. Dalal and B. Triggs, "Histograms of Oriented Gradients for Human Detection," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR)*, 2005, pp. 886–893.

[3] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," in *Advances in Neural Information Processing Systems (NIPS)*, 2012, pp. 1097–1105.

[4] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You Only Look Once: Unified, Real-Time Object Detection," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016, pp. 779–788.

[5] R. Girshick, "Fast R-CNN," in *Proceedings of the IEEE International Conference on Computer Vision (ICCV)*, 2015, pp. 1440–1448.

[6] K. He, X. Zhang, S. Ren, and J. Sun, "Deep Residual Learning for Image Recognition," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016, pp. 770–778.

[7] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2015, pp. 815–823.

[8] G. Bradski, "The OpenCV Library," *Dr. Dobb's Journal of Software Tools*, vol. 25, no. 11, pp. 120–125, 2000.

[9] D. G. Lowe, "Distinctive Image Features from Scale-Invariant Keypoints," *International Journal of Computer Vision*, vol. 60, no. 2, pp. 91–110, 2004.

[10] T. Ojala, M. Pietikäinen, and T. Mäenpää, "Multiresolution Gray-Scale and Rotation Invariant Texture Classification with Local Binary Patterns," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 7, pp. 971–987, 2002