

AI-BASED AUTOMATIC CRIME DETECTION SYSTEM

Patoliya Priya P. OM Engineering College, Junagadh, India

Pithva Dhara C. OM Engineering College, Junagadh, India

Prof. Megha. K. Chavda OM Engineering College, Junagadh, India

Abstract

In India, Video surveillance plays an important role in today's world. Technology has evolved tremendously as artificial intelligence, machine learning and deep learning become mainstream. Using a combination of the above, there are various systems that help in distinguishing different types of suspicious behavior from live videos. The most unpredictable thing is the behavior of a person and it is very difficult to find out whether it is suspicious or normal. A deep learning approach is used to detect suspicious or unusual activity in the academic environment and send alert messages to the appropriate authorities if suspicious activity is detected. Surveillance is often done using a series of frames captured from a video. All frames are divided into two parts. In the first part, the features are calculated from the video frames, and in the second part, based on the extracted features, the classifier predicts the class as suspicious or normal.

Keywords: Suspicious Activity, Video Surveillance, Deep Learning, Anomaly detection, RNN, CNN, LSTM.

INTRODUCTION

A finds many applications in real-world human behavior recognition, intelligent video surveillance, and shopping behavior analysis. The advantages of video surveillance include effective surveillance, less labor, cost-effective surveillance capabilities, adoption of new security trends, etc. Now tracking is done by humans. Because we are dealing with a large amount of video data, it is easy for people to feel overwhelmed and manual intervention will also introduce errors. It greatly affects the efficiency of the system. This is solved by automating video surveillance. Human behavior detection in video surveillance systems is an automated way to

easily find suspicious objects activity. Airports, Railway Stations, Banks, Offices, Exam Halls etc. There are several effective algorithms to automatically detect human behavior in public spaces such as video surveillance for artificial intelligence, machine learning and deep learning. Artificial intelligence helps computers think like humans. An important component of machine learning is learning from training data and predicting future data. Today, there are GPU (Graphics Processing Unit) processors and large databases, so the concept of deep learning is used.

The combination of computer vision and video surveillance will ensure public safety and security. Computer vision techniques include the following steps: environment modeling, motion detection, moving object classification, tracking, behavior understanding and interpretation, and data fusion from multiple cameras. This method requires a lot of work to extract features in different video sequences. Supervised and unsupervised classification



methods. Supervised classification uses manually defined training data, while unsupervised classification is fully computer-driven and does not require human intervention.

In India, crime is increased daily in various forms/Methods. It is necessary to control these activities. Hence, we required control mechanism to stop these or we can have system, which is able to detect criminal activities before crime happens. This proposed system will use to Human activities can be monitored in sensitive and public areas by video surveillance. Find out whether activity is suspicious or normal. Send alert messages to the appropriate authorities if suspicious activity is detected.

- 1. **Crime Prediction:** By analyzing historical crime data and patterns, the system can predict potential crime hotspots, helping law enforcement agencies allocate their resources more efficiently and proactively respond to potential criminal activity.
- 2. **Real-Time Monitoring:** The system constantly monitors live feeds from surveillance cameras and other sources to identify ongoing criminal activities, enabling law enforcement to respond promptly and prevent crimes from escalating.
- 3. **Anomaly Detection:** The AI system can detect unusual behaviors or patterns that deviate from normalcy, which may indicate criminal activities like burglaries, thefts, or other suspicious activities.
- 4. **Forensic Analysis:** The system can assist in forensic investigations by rapidly processing vast amounts of data and providing valuable insights to law enforcement agencies to help solve crimes more effectively.
- 5. **Social Media Monitoring:** With the prevalence of social media, criminals often leave digital footprints. The system can analyze social media content to track potential threats, monitor gang activities, and gain insights into criminal networks.
- 6. **Alerts and Notifications:** Whenever the system identifies a potential crime or suspicious behavior, it generates real-time alerts and notifications, allowing law enforcement personnel to take immediate action.

It is important to note that an AI-Based Automatic Crime Detection System is designed to augment the capabilities of law enforcement agencies and not replace human judgment. Law enforcement officers remain an integral part of the decision-making process and validate the system's outputs before taking any actions.

The deployment of such advanced crime detection systems raises important considerations related to data privacy, ethics, and bias. Ensuring that the AI algorithms are fair, transparent, and respectful of individuals' privacy rights is crucial to maintaining public trust and acceptance.

In conclusion, the AI-Based Automatic Crime Detection System represents a significant leap forward in law enforcement technology, enabling more efficient crime prevention and enhanced public safety through the power of artificial intelligence and real-time data analysis.

MATERIAL AND METHODS

1. Dataset & Pre-processing

• Dataset:

Phase	No. Of Samples		Doncont
	Abnorm al	Normal	Percent age



International Journal of Advanced Research in IT and Engineering

	Training	112	126	70%	
	Validatio	24	27	15%	
n					
	Testing	24	27	15%	
Total Samples Of Normal Activity : 180					
Total Samples Of Abnormal Activity : 160					
Total Samples : 340					

Note: This dataset will be strengthened in future.

Normal Activity: Boxing, Handclapping, Handwaving, Jogging, Running, Walking **Abnormal Activity:** Fighting, Harassment, Slapping, Punching, Shooting, Attack with Weapons, Forcefully Hand or Head Catch, Falling, Coercion.

- Video detect
- Video to frame conversion (using different methods)
- Preprocessing: Some powerful image preprocessing techniques include noise reduction, contrast enhancement, image resizing, color correction, segmentation, feature extraction, etc.

2. Machine Learning

- Feature Classification
- Machine learning models (CNN, RNN, LSTM etc.)

CNN:

CNN stands for Convolutional Neural Network, and it is a type of deep learning architecture widely used in machine learning and computer vision tasks. CNNs are specifically designed to process and analyze visual data, such as images and videos. They are inspired by the human visual system, which can detect patterns and features in a hierarchical manner.

RNN:

Recurrent neural networks (RNNs) are a class of neural network that are helpful in modeling sequence data. Derived from feed forward networks, RNNs exhibit similar behavior to how human brains function.

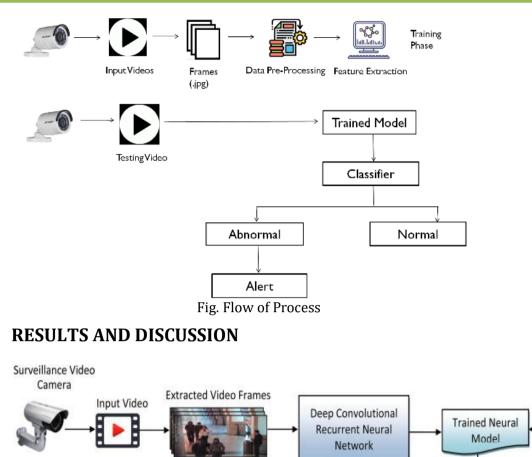
LSTM:

It is used for processing, predicting, and classifying on the basis of time-series data. Long Short-Term Memory (LSTM) is a type of Recurrent Neural Network (RNN) that is specifically designed to handle sequential data, such as time series, speech, and text.

3. Activities

- Result of Classification
- Find Normal/Abnormal
- Alert Generate





The aim of the project is to use CCTV videos for suspicious activities and to alert security in case of suspicious incidents. This is done by extracting features from the frame using CNN. After extraction, LSTM architecture is used to classify frames as suspicious or normal class.

Detected Activity to Security Section

Collecting video sequences from CCTV footage, removing frames from films, pre-processing the images, creating training and validation sets from the datasets, and training and testing are the steps involved in establishing the entire system. The system notifies the appropriate authority through SMS when it detects suspicious behaviour. Python was used to develop the system on an open source platform. By registering a Twilio account and installing the Twilio library in Python, you can send SMS messages. Twilio enables programmatic sending and receiving of text messages, as well as making and receiving phone calls.

Training:

The videos used as input are from the dataset. Many videos of various suspicious and regular conduct have been gathered. Frames are retrieved from the recorded videos as part of the pre-

Testing Videos

Classifier

Normal Activity

Suspicious Activity



processing procedure. VGG-16 is the pre-trained model that our system uses, and we employ its lessons to solve the challenge. Based on our needs, the final layer of this model was deleted, and LSTM architecture is employed for classification. It has been trained using our dataset. For testing, CCTV video footage of various circumstances is taken and rendered into frames. The trained model receives the stored frames, and then the classifier determines whether the video depicts suspicious or typical activity.

Testing:

Test Data:

Gather a diverse and representative dataset that encompasses different types of crime incidents, environmental conditions, lighting variations, and other relevant factors. This dataset should cover a wide range of scenarios to ensure the system's effectiveness.

Integration Testing:

If the system is designed to integrate with existing law enforcement or emergency services systems, test the integration to ensure seamless communication and data sharing. Verify that the system can properly interface with external systems and provide timely notifications or alerts as needed.

ACKNOWLEDGEMENT

First of all, we would like to thank our college **OM ENGINEERING COLLEGE, JUNAGADH** for giving us the opportunity to develop this project.

We want to thank a number of people at our institute for helping us to solve the queries of subject related and finding the solution of various critical problems that we face during developing this project.

We want to thank many of our faculties at our college for taking been interest in this project, helping us to solve many queries, suggesting guidelines, feedback and suggestions to shape this project better.

REFERENCES

- [1] D. D. M. Dinama, Q. A'yun, A. D. Syahroni, I. A. Sulistijono, and A. Risnumawan, "Human detection and tracking on surveillance video footage using convolutional neural networks," in 2019 International Electronics Symposium (IES), pp. 534–538, 2019.
- [2] M. Popa, L. Rothkrantz, Z. Yang, P. Wiggers, R. Braspenning, and C. Shan, "Analysis of shopping behavior based on surveillance system," in 2010 IEEE International Conference on Systems, Man and Cybernetics, pp. 2512–2519, 2010.
- [3] N. Dawar and N. Kehtarnavaz, "Continuous detection and recognition of actions of interest among actions of non-interest using a depth camera," in 2017 IEEE International Conference on Image Processing (ICIP), pp. 4227–4231, 2017.
- [4] C.-H. Chuang, J.-W. Hsieh, and K.-C. Fan, "Suspicious object detection and robbery event



analysis," in 2007 16th International Conference on Computer Communications and Networks, pp. 1189–1192, 2007.

- [5] Y. Kaneko, "Fractal analysis of a grocery store shopping path," in 2015 2nd Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE), pp. 1–7, 2015.
- [6] H. Valecha, A. Varma, I. Khare, A. Sachdeva, and M. Goyal, "Prediction of consumer behaviour using random forest algorithm," in 2018 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), pp. 1– 6, 2018.
- [7] Y. Zuo, K. Yada, T. Li, and P. Chen, "Application of network analysis techniques for customer in-store behavior in supermarket," in 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 1861–1866, 2018.
- [8] Y. Zuo and K. Yada, "Using statistical learning theory for purchase behavior prediction via direct observation of in-store behavior," in 2015 2nd Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE), pp. 1–6, 2015.
- [9] S. Peker, A. Kocyigit, and P. E. Eren, "An empirical comparison of customer behavior modeling approaches for shopping list prediction," in 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp.1220–1225,2018.
- [10] Shreyash Chole, Rishabh Nath Tiwari, Samiullah Siddique, Piyush Jain, Prof. Sagar Mane," Detecting Suspicious Activities In Surveillance Videos Using Deep Learning Methods," in 2023 Dept. Of Computer Science & Engineering, NBN Sinhgad School Of Engineering Ambegaon, Pune, India.
- [11] Mohammed Boukabous, Mostafa Azizi, "Image and video-based crime prediction using object detection and deep learning," Mathematics, Signal and Image Processing, and Computing Research Laboratory (MATSI), Superior School of Technology (ESTO), Mohammed First University, Oujda, Morocco.
- [12] Venu Majji1, Dr. Vanitha Kakollu2, Mpj Santosh Kumar3, K Naga Soujanya4, Dr. B. Kanthamma5, Dr. G. Babu Rao6, "Video behavior Possible Identification And Recognition Of Abnormalities And Normal Behavior Profiling For Anomaly Detection Using Cnn Model," UX Manager, Assistant Professor ASG Technologies, Department of CS, Department of CSE, Department of EECE, GITAM (Deemed to be University) Visakhapatnam.



Biography of Authors

 Prof. Megha K. Chavda Head & Assistant Professor, Department of Computer Engineering, Om Engineering College, Junagadh, Gujarat, India Published international paper in journal named INTERNATIONAL JOURNAL OF ADVANCE ENGINEERING AND RESEARCH DEVELOPMENT (IJAERD) with title "Third party Identity Diffuser technique for the Private Location Based Query using Third Party Identity Diffuser" in June 2015. Published paper in journal named INDIAN JOURNAL OF APPLIED RESEARCH with title "Private Location Based Query Using Third Party Identity Diffuser: A Review" in December 2014. Published paper in journal named INTERNATIONAL RESEARCH JOURNAL OF ENGINEERING AND TECHNOLOGY (IRJET) with title "Importance of Artificial Intelligence in Industry: A Review" in December 2021.
 Published Chapters in Book named Futuristic Trends in Artificial Intelligence with chapter titles "Artificial intelligence (AI): how the technology transform the world from human to machine" and "Artificial intelligence (AI): overview, background and tools in ai" in November 2022.
Priya Patoliya Student of B.E (Computer Engineering)
Dhara Pithva Student of B.E(Computer Engineering)