Survey on Suspicious Activity Detection using Deep Learning

Namithadevi N N, Bhuvana S D, M D Tarun, Seema Reddy K, Shreyas Gowda P
Department of Computer Science and Engineering
Vidya Vikas Institute of Engineering and Technology, Mysore, India
namithadevi19@gmail.com, bhuvanasd20@gmail.com, mdtarun1008@gmail.com
seemareddy004@gmail.com, shryasegowda@gmail.com

Abstract*: The integration of computer vision and artificial intelligence in an automated video detection system is crucial for preventing security issues in public places. Traditional surveillance methods are insufficient in detecting abnormal behaviors, so an automated system is needed. The project aims to revolutionize surveillance by using deep learning techniques, particularly CNN models, to analyze video footage uploaded through a web application. This involves segmenting the video into frames, extracting features using CNN, and identifying irregular or suspicious activities. The system's functionality includes background and foreground extraction, motion estimation, and anomaly detection, allowing for efficient differentiation between normal and abnormal behaviors in surveillance videos. This study aims to bridge the gap in surveillance technology by integrating computer vision, image processing, and artificial intelligence, enabling swift identification and flagging unusual actions in surveillance footage. It also ensures prompt alerts via email upon detecting potential security threats. This research contributes to the enhancement of surveillance systems and highlights the importance of addressing evolving security challenges in contemporary urban environments.*

Keywords: Classification, Deep learning, CNN, Anomaly Detection, Web Application, email

I. INTRODUCTION

The escalating rates of criminal activities across urban and suburban landscapes have underscored the pressing need for more sophisticated surveillance systems. Traditional methods have proven inadequate in addressing the evolving challenges of monitoring and identifying anomalous behaviours effectively. To bridge this gap, this project centers on the development of a groundbreaking web application equipped with a Convolutional Neural Network (CNN) model. This innovative approach aims to revolutionize surveillance capabilities by leveraging advanced technologies like computer vision and artificial intelligence for automated, real-time anomaly detection within uploaded videos.

Urban environments have witnessed an unprecedented surge in criminal incidents, demanding more robust and efficient surveillance mechanisms. Conventional surveillance methods rely heavily on manual monitoring, making it increasingly challenging to keep pace with the complexities of modern security needs. The proposed web application seeks to transform this landscape by integrating cutting-edge CNN models to swiftly analyse video footage. By doing so, the project endeavours to bridge critical gaps in security infrastructure, providing a seamless and automated system capable of accurately discerning irregular activities from routine behaviour.

By using deep learning techniques and CNN models, this project envisions a paradigm shift in surveillance systems' capabilities. The integration of sophisticated algorithms within a user-friendly web application promises not only to detect but also to alert users in real-time about suspicious activities. This innovation could potentially revolutionize surveillance across various sectors, from public transportation security to crowd management in public spaces, fostering a safer and more secure urban environment for all.

II. RELATED WORKS

Abhishek Mohite et al. (2020) [1], introduces a novel approach using a "motion influence map" to represent human activities within crowded scenes. By leveraging OpenCV Python with Machine Learning, the study focuses on

DOI: 10.48175/IJARSCT-17542

recognizing human activities and categorizing them as usual, unusual, or suspicious. The "motion influence map" serves as a unique representation method to analyse activities within densely populated areas, allowing for the identification of anomalies or suspicious behaviour amidst crowded scenes. This innovative approach enhances the ability to detect unusual activities within complex environments and contributes to the development of more effective surveillance systems.

In this study [2], the researchers employ a combination of background subtraction, Convolutional Neural Networks (CNNs), and Long Short-Term Memory (LSTM) networks to identify abnormal activities in video footage. Their methodology focuses on discerning unusual behaviour based on typical human behaviour patterns. By utilizing these techniques, the model aims to distinguish between normal and abnormal actions within surveillance videos. This approach enhances the system's ability to identify suspicious activities by contrasting detected behaviours against expected or normal behaviours, providing a more comprehensive understanding of unusual events within video surveillance.

K. Kranthi Kumar et al. (2022) [3], presented here proposes a system for suspicious activity detection from video surveillance using a Convolutional Neural Network (CNN). This system is trained on images depicting suspicious activities to classify normal and suspicious actions within surveillance footage. The reported accuracy rate falls between 70% to 74%, signifying the effectiveness of the model in differentiating between regular and suspicious activities. By employing machine learning techniques, particularly CNNs trained on specific datasets, this approach enhances the surveillance system's ability to identify potential threats or anomalies accurately.

Amrutha et al., [4] describe the pre-trained model VGG-16. The system was designed to monitor the student’s behaviour in examinations using neural networks and Gaussian distribution. In the first phase, the features were computed from video frames. And in the second phase, based on the obtained features, the classifier predicts the class as normal or suspicious. But the system was limited to academic areas which can be extended to the public as well as private sector. It can also be used in any scenario. Suspicious individuals can be suspected from suspicious activity.

Sathyajit et al., [5] proposed the model in which the captured images were used for training purposes. The advantage of this method is that detection of abandoned baggage was computationally efficient. For each frame the computational time was considerably smaller. But improvement is needed to detect the guns in real time.

The paper [6] introduces a recognition methodology named dynamic bag-of-words, which focuses on analysing spatio-temporal features. This signifies a departure from static representations and considers the sequential nature of human activities. By incorporating dynamic bag-of-words, the system aims to better capture the evolving patterns of activities over time, enhancing the accuracy and robustness of recognition. Their primary concern is recognizing events early (for instance, a man picking up a gun with his hand). A probabilistic activity prediction problem is formulated, and new methodologies are introduced to solve it. Spatio-temporal features are analysed using an integral histogram. As a result of considering the sequential nature of human activities and handling noisy data, they named their new recognition methodology dynamic bag-of-words.

This paper [7] addresses the challenges faced by traditional video surveillance operations due to the manual handling of large amounts of information and the potential loss of crucial data, particularly related to detecting abnormal behaviours representing security risks. The proposed system focuses on supporting smart surveillance by introducing algorithms designed to detect two human activities: walking and running. The study places no restrictions on the number of people or motion directions but is limited to indoor colour videos captured by a stationary camera. The detection of moving objects, representing suspicious activity, employs a background subtraction algorithm. Key features for activity classification include the displacement rate of segmented foreground areas' centroids and the rate of change in their size. The study utilizes a sequential set of procedures, involving video frame division, background-object separation, noise removal through morphological operations, and mathematical operations to determine images containing suspicious activity. The proposed algorithms demonstrate a high accuracy rate in determining the type of activity, enhancing the effectiveness of smart surveillance for security purposes.

This paper [8] highlights the extensive use of anomaly detection systems in conjunction with machine learning and artificial intelligence for behavioural analysis. These systems play a crucial role in identifying and predicting anomalies across various domains, including enterprise, intrusion detection, system health monitoring, fraud detection in financial transactions, and fault detection in operational environments. The increasing global crime rates and concerns about human security have led many countries, including India with a crime index of 42.38, to adopt advanced anomaly detection systems. The paper emphasizes that traditional security measures, such as CCTV installations, are insufficient, and modern anomaly detection systems, incorporating optimized versions with predictive capabilities, are essential. The study explores the application of Convolutional Neural Network (CNN) models in enhancing anomaly detection and prediction for improved security measures.

This research [9] addresses the critical need for suspicious pre- and post-activity detection in crowded areas to prevent potential incidents. Traditionally, surveillance cameras capture footage that authorities later investigate for suspicious activities, requiring significant human intervention. The paper suggests the adoption of machine learning (ML) and deep learning (DL) techniques to create a pre-incident warning alarm system. The focus is on predicting suspicious activities based on human gestures and detecting unusual behaviour. While existing ML and DL methods have been proposed, the paper introduces an Enhanced Convolutional Neural Network (ECNN)-based system, aiming for higher accuracy, precision, and lower false-positive and false-negative rates. Experimental results, analysed using the Statistical Package for the Social Sciences (SPSS) tool, demonstrate promising outcomes. The ECNN model achieved a mean accuracy of 97.050%, mean precision of 96.743%, mean false-positive rate of 2.957%, and mean false-negative rate of 2.927%. A comparison with the traditional Convolutional Neural Network (CNN) algorithm further supports the effectiveness of the proposed ECNN-based system. The research suggests practical applications for enhancing pre-suspicious activity alert security systems, contributing to improved safety in crowded environments.

This paper [10] explores the integration of deep learning algorithms, a subset of machine learning, to address various challenges in artificial intelligence. It emphasizes the importance of machine learning in building algorithms based on data trends and historical connections. The study specifically focuses on utilizing image processing and deep learning methods within a machine learning system to identify fire, unauthorized vehicles, and individuals. The proposed model extends its application to control electrical equipment remotely, ensuring protection against fire and unauthorized access. The objective is to create an intelligent, trained neural network capable of tracking specific events and providing a scalable machine learning solution. The study involves capturing frames, preprocessing the data, and utilizing pre-trained sets to track recurring events. A web interface is developed for presenting predictions, and simulations are conducted to analyse the model's performance. The combination of deep learning and machine learning aims to establish an effective and reliable security system for organizations, mitigating risks related to fire incidents and unauthorized access while also controlling device statuses through a web interface.

This paper [11] addresses the increasing need for detecting suspicious activities in public places, given the rising incidents of shootings, knife attacks, and terrorist activities globally. It adopts a deep learning approach, specifically employing Convolutional Neural Networks (CNN), to analyse images and videos for identifying suspicious behaviours. The research explores various CNN architectures and compares their accuracy, providing insights into the effectiveness of different models. The paper introduces the architecture of a system designed to process real-time video footage from cameras, predicting whether observed activities are suspicious. The inclusion of Fast AI, a deep learning library, enhances the system's capabilities. Additionally, the paper outlines future developments for advancing the field of suspicious activity detection using deep learning methods.

This paper [12] focuses on the detection of suspicious human activity in real-time CCTV footage using neural networks, particularly emphasizing the application of Convolutional Neural Networks (CNNs). The project addresses the longstanding challenge of predicting body part or joint locations of a person from images or videos. Recognizing suspicious human activity is crucial in various computer vision applications, such as video surveillance, behaviour understanding, and human-computer interaction. The use of low-cost depth sensors in existing systems has limitations, prompting the proposed solution's reliance on neural networks to overcome these challenges. The research aims to contribute to the active area of image processing and computer vision dedicated to recognizing suspicious activities in surveillance videos. The proposed intelligent video surveillance system is designed to monitor public places in real-time, categorizing activities as usual or unusual and generating alerts for potential threats or criminal behaviour. Notably, the paper underscores the unique contribution of employing CNNs for detecting suspicious activities, distinguishing it from existing research that often focuses on images rather than video data.

This paper [13] emphasizes the crucial role of video surveillance in today's advanced technological landscape, incorporating artificial intelligence, machine learning, and deep learning to enhance its capabilities. It particularly explores the challenge of distinguishing between suspicious and normal human behaviour, acknowledging the inherent unpredictability of human actions. The proposed system utilizes deep learning approaches, specifically employing LSTM (Long Short-Term Memory) models, to detect suspicious or normal activities within academic environments. The surveillance system operates through consecutive frames extracted from video footage, and the overall framework is divided into two key parts. In the initial phase, features are computed from the video image, and in the subsequent phase, a classifier predicts the class of the observed activity as either suspect or normal based on the extracted features. The adoption of LSTM models adds a temporal dimension to the analysis, enabling the system to capture long-term dependencies in human behaviour for more accurate predictions.

This paper [14] focuses on the application of neural networks, particularly Convolutional Neural Networks (CNN), for detecting suspicious human activity from surveillance videos. The primary goal is to address the challenges associated with monitoring public areas, such as bus stations, railway stations, airports, and more, to prevent various incidents like terrorism, accidents, vandalism, and other suspicious activities. The utilization of intelligent video surveillance becomes essential due to the difficulty of continuous human monitoring in public spaces. The proposed system employs CNN, a deep learning model, to analyse video footage and categorize human activities as either usual or unusual. The objective is to generate alerts for unusual activities, providing a proactive approach to security and risk prevention in public settings. The adoption of CNN signifies the system's reliance on convolutional layers for effective feature extraction and pattern recognition in the context of suspicious activity detection.

This paper addresses [15] the application of recognizing suspicious human activities, focusing on anomaly detection. The primary concern is the safety of individuals, given the rising threats from deliberate violence to accidents. Traditional CCTV installations are deemed insufficient as they rely on continuous human monitoring, leading to inefficiencies. The proposed system aims to overcome this limitation by introducing a fully automated security system capable of real-time detection of anomalous activities, providing immediate assistance to potential victims. The system utilizes machine learning techniques, specifically Convolutional Neural Networks (CNN), to examine and detect suspicious human actions in real-time CCTV footage. Alerts are generated promptly when abnormal activities are identified. The experimental results on a dataset containing both normal and anomaly activities showcase the effectiveness of the proposed method. The adoption of CNN signifies the reliance on convolutional layers for robust feature extraction and accurate detection of suspicious activities.

According to [16] Sparse coding has constructed anomaly detection which showed better performance, even containing the theories of feature learning, sparse representation, and dictionary learning. In this paper, an innovative neural network is proposed for anomaly detection which is also labelled as Anomaly Net by deeply accomplishing feature learning, sparse representation as well as dictionary learning in three joint neural processing blocks. Specifically, to learn improved features, the authors design a motion fusion block accompanied by a feature transfer block to relish the benefits of eliminating background noise, capturing motion and improving data insufficiency.

According to [17] A suspicious activity is any observation of action that could state a person may be involved in a crime or is about to commit a certain criminality. Anomaly detection is the process of detecting suspicious activity. Surveillance cameras are one of the best solutions to the issue of security in various places. Present-day system needs manpower for monitoring the system as detecting and identifying criminal and abnormal activity is so challenging. So, this paper carries out a survey on anomaly detection for video surveillance using different concepts like deep learning, RNN etc.

This paper [18] automates the detection of anomalous actions within long video series is challenging due to the uncertainty of how such events are defined. The authors tactic the problem by learning generative models that can discover anomalies in videos using restricted supervision. Projected end-to-end trainable complex Convolutional Long Short-Term Memory (Conv-LSTM) networks that are able to predict the development of a video sequence from a minor number of input frames.

According to the paper [19], authors inspired by the capability of sparse coding based suspicious detection, projected a Temporally-coherent Sparse Coding (TSC) where they implement similar neighbouring frames encoded with similar reconstruction coefficients. Then mapped the TSC with a distinct type of stacked Recurrent Neural Network (sRNN). The contributions of the paper are- i) proposed a TSC, which can be recorded to a sRNN which facilitates the parameter optimization and speeds up the doubtful prediction. ii) Build a very huge dataset that is even larger than the summation of all existing dataset for finding anomalous activity.

This paper [20] presented an efficient technique for identifying anomalies in videos. Recently applications of convolutional neural networks have shown possibilities of convolutional layers for object detection and recognition, specifically in images. Though, convolutional neural networks are supervised and have need of labels as learning signals. Authors as well as proposed a spatiotemporal architecture for suspicious detection in videos with crowded scenes.

III. METHODOLOGY

The methodology of the web application revolves around a sequential process initiated upon video upload. Firstly, upon a user uploading a surveillance video through the application interface, the backend system comes into play. This backend infrastructure is responsible for the video preprocessing phase, where the uploaded video undergoes segmentation into individual frames to prepare them for analysis. Once segmented, the system leverages a pre-existing Convolutional Neural Network (CNN) model, trained specifically for detecting anomalous or suspicious activities within these frames.

The CNN model's role is pivotal; it scrutinizes each frame, utilizing its trained algorithms and learned patterns to discern any predefined abnormal behaviours or actions. The model's expertise in recognizing these predefined activities, such as carrying weapons or erratic movement, aids in the identification of suspicious occurrences within the video footage. Upon detection of such suspicious behaviour in any frame, the system activates an alert mechanism. This mechanism initiates an email alert, swiftly notifying the user of the identified irregular activity. This alerting functionality can be seamlessly integrated using the APIs provided by web service providers, ensuring prompt email notifications to the user's mobile device or PC. Ultimately, this methodology integrates video preprocessing, CNN analysis, and email alerting, offering users rapid notifications when suspicious activities are detected within the uploaded surveillance videos.Furthermore, the system is fortified with live detection capabilities, enabling the real-time streaming and analysis of videos. During live detection, the identical machine learning model continuously scrutinizes video frames for any indications of suspicious behaviour. Upon detecting such anomalies, the system promptly triggers email notifications to the respective users.

IV. CONCLUSION

The integration of computer vision and artificial intelligence in automated video detection systems represents a critical advancement in enhancing security measures in public places. Traditional surveillance methods often fall short in effectively identifying abnormal behaviours, necessitating the development of more sophisticated solutions. Through the utilization of deep learning techniques, particularly Convolutional Neural Network (CNN) models, this project proposes a revolutionary approach to surveillance by segmenting video footage, extracting features, and detecting irregular or suspicious activities in real-time.

REFERENCES

[1] Mohite, A., D. Sangale, P. Oza, T. Parekar, and M. Navale. "Unusual Human Activity Detection Using OpenCV Python with Machine Learning." CLIO An Annual Inter disciplinary Journal of History 6, no. 3 (2020): 183-187.

[2] Nandini Fal Dessai, Prof. Shruti Pednekar. "Surveillance-based Suspicious Activity Detection: Techniques, Application and Challenges." International Journal of Creative Research Thoughts (IJCRT), 2023.

[3] K. Kranthi Kumar, B. Hema Kumari, T. Saikumar, U. Sridhar, G. Srinivas, G. Sai Karan Reddy. “Suspicious activity detection from video surveillance”, International Journal of Research Publication and Reviews, Vol 3, Issue 6, pp 2373-2377, June 2022.

[4] Amrutha C.V, C. Jyotsna, Amudha J. : “Deep Learning Approach for Suspicious Activity Detection from Surveillance Video” Second International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2020) IEEE Xplore Part Number: CFP20K58-ART; p:335-339.

DOI: 10.48175/IJARSCT-17542

[5] Sathyajit Loganathan, Gayashan Kariyawasam, Prasanna Sumathipala : “Suspicious Activity Detection in Surveillance Footage ” 2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA).

[6] N. Bordoloi, A. K. Talukdar and K. K. Sarma, "Suspicious Activity Detection from Videos using YOLOv3" 2020 IEEE 17th India Council International Conference (INDICON), 2020, pp. 1-5, doi: 10.1109/INDICON49873.2020.9342230.

[7] Salem, Fathia G. Ibrahim, Reza Hassanpour, Abdussalam Ali Ahmed, and Aisha Douma. "Detection of suspicious activities of human from surveillance videos." In 2021 IEEE 1st International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering MI-STA, pp. 794-801. IEEE, 2021.

[8] Bhambri, Pankaj, Sachin Bagga, Dhanuka Priya, Harnoor Singh, and Harleen Kaur Dhiman. "Suspicious human activity detection system." Journal of IoT in Social, Mobile, Analytics, and Cloud 2, no. 4 (2020): 216-221.

[9] Selvi, Esakky, Malaiyalathan Adimoolam, Govindharaju Karthi, Kandasamy Thinakaran, Nagaiah Mohanan Balamurugan, Raju Kannadasan, ChitapongWechtaisong, and Arfat Ahmad Khan. "Suspicious actions detection system using enhanced CNN and surveillance video." Electronics 11, no. 24 (2022): 4210.

[10] Ahamad, Shahanawaj, B. Bhaskara Rao, K. Srikanth, V. P. Gopal, Pritika Mehra, and Malik Bader Alazzam. "Machine learning approach to enhance performance of suspicious activity detection system." In AIP Conference Proceedings, vol. 2587, no. 1. AIP Publishing, 2023.

[11] Rachana Gugale, Abhiruchi Shendkar, Arisha Chamadia, Swati Patra, Deepali Ahir, “Human Suspicious Activity Detection using Deep Learning”, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056, Volume: 07 Issue: 06 | June 2020

[12] Vedant Saikhede, Kiran Shende, Yuvraj Darekar, Hemant Thorat, Prof. Snehal. S. Shinde, “Deep Learning Approach For Suspicious Activity Detection From Surveillance Video”, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 10 Issue: 12 | Dec 2023

[13] Sonali Suryavansh, Rohit Shinde, Sarthak Kathe, Akash Phad, Prof. C.H. Patil, “Using Surveillance Video Detection Of Suspicious Activity Based On Deep Learning” e-ISSN: 2582-5208, International Research Journal of Modernization in Engineering Technology and Science Volume:05/Issue:05/May-2023

[14] Prof. Malan Sale, Arvind Patkal, Harshal Mahale, Jyoti Lavhale, Sunayana Apsingekar, “Deep Learning Approach for Suspicious Activity Detection from Surveillance Video”, International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Volume 2, Issue 4, May 2022

[15] Tejashri Subhash Bora, Monika Dhananjay Rokade, “Human Suspicious Activity Detection System Using Cnn Model for Video Surveillance”, IJARIIE-ISSN(O)-2395-4396, Vol-7 Issue-3 2021

[16] Joey Tianyi Zhou, Jiawei Du, Hongyuan Zhu, Xi Peng, Rick Siow Mong Goh, ”AnomalyNet: An Anomaly Detection Network for Video Surveillance, 2019.

[17] Monika D. Rokade and Tejashri S. Bora, "Survey On Anomaly Detection for Video Surveillance" 2021, International Research Journal of Engineering and Technology(IRJET).

[18] Jefferson Ryan Medel, Andreas Savakis, “Anomaly Detection in Video Using Predictive Convolutional Long Short-Term Memory Networks”, Jan 2020.

[19] W. Luo, W. Liu, and S. Gao, “A revisit of sparse coding based anomaly detection in stacked rnn framework,” in The IEEE International Conference on Computer Vision (ICCV), Oct 2021.

[20] Y. S. Chong and Y. H. Tay, “Abnormal event detection in videos using spatiotemporal autoencoder,” in International Symposium on Neural Networks. Springer, 2020, pp. 189–196