International Journal of Research in Engineering, Science and Management
Volume 7, Issue 5, May 2024
https://www.ijresm.com | ISSN (Online): 2581-5792

Suspicious Activity Detection using LSTM and MobileNetV2

N. N. Namithadevi[1], S. D. Bhuvana[2*], M. D. Tarun[3], K. Seema Reddy[4], P. Shreyas Gowda[5]
[1]Assistant Professor, Department of Computer Science and Engineering, Vidya Vikas Institute of Engineering and Technology, Mysore, India
[2,3,4,5]Student, Department of Computer Science and Engineering, Vidya Vikas Institute of Engineering and Technology, Mysore, India

***Abstract*: For the prevention of security issues in publicly accessible areas, it is necessary to integrate computer vision and AI into an automatic video identification system. In detecting abnormal behaviour, traditional surveillance methods are insufficient and a system needs to be automated. The objective of the project is to use deep learning techniques, especially CNN models, for analysing video footage posted on a web site in order to make surveillance more efficient. In addition, it involves segmenting the video into frames, extracting features using MobileNetV2 and identifying irregular or suspicious activities. The system's functions include background and foreground extraction and anomaly detection that allows for a distinct distinction in the behaviour of normal and irregular activities on surveillance video. The study seeks to bridge the gap between surveillance technology by involving computer vision, image processing and artificial intelligence so as to be able to quickly identify unusual actions on video. In addition, when detecting potential security threats, it ensures that timely alerts are sent via email. This research demonstrates the importance of addressing emerging security challenges in today's cities, contributing to enhancing surveillance systems.**

***Keywords*: Classification, Deep Learning, CNN, MobileNetV2, LSTM, Anomaly Detection, Web Application, email.**

1. Introduction

In today's world criminal activities across urban and suburban landscapes have increased the pressing need for more reliable and efficient surveillance systems.

To address the ever-evolving challenges of monitoring and identifying unusual behaviours effectively, this project focuses on creating a cutting-edge web application integrated with a Convolutional Neural Network (CNN) model. This pioneering initiative aims to transform surveillance capabilities by harnessing advanced technologies such as computer vision and artificial intelligence to automatically detect anomalies in uploaded videos in real-time.

Urban areas are experiencing a significant increase in criminal activity, prompting the need for enhanced surveillance solutions. Traditional surveillance approaches heavily rely on manual monitoring, which struggles to keep up with the evolving complexities of security challenges. The proposed web application aims to revolutionize this scenario by incorporating state-of-the-art CNN models for rapid video analysis. This initiative aims to address crucial deficiencies in security infrastructure by offering an automated system capable of accurately distinguishing between normal and suspicious behaviour, thereby improving overall security measures.

This project aims to redefine the landscape of surveillance systems through the application of advanced deep learning techniques and CNN models. By seamlessly integrating cutting-edge algorithms into an intuitive web-based platform, the project endeavours not just to identify but also to promptly notify users of any unusual activities in real-time. Such a groundbreaking initiative holds the promise of transforming surveillance practices across diverse domains, including enhancing security in public transportation and effectively managing crowds in urban areas. Ultimately, this innovation seeks to cultivate a safer and more secure environment for everyone.

2. Related Works

In the cited study [1], the researchers adopt a hybrid approach, integrating background subtraction, Convolutional Neural Networks (CNNs), and Long Short-Term Memory (LSTM) networks to detect anomalous activities in video streams. Their methodology is centered on differentiating irregular actions from regular human behaviour patterns. By leveraging these techniques, the model is designed to differentiate between typical and atypical actions observed in surveillance footage. This methodology strengthens the system's capability to flag suspicious behaviours by comparing identified actions with expected norms, thereby offering a more robust analysis of unusual occurrences in video surveillance.

In their study, K. Kranthi Kumar and colleagues (2022) [2] introduced a novel system designed for detecting suspicious activities in video surveillance footage using Convolutional Neural Networks (CNNs). The system was trained on a dataset consisting of images portraying both normal and suspicious behaviors, enabling it to accurately classify actions observed in surveillance videos. The reported accuracy of the model ranges from 70% to 74%, underscoring its effectiveness in distinguishing between routine and potentially threatening activities. Leveraging machine learning methodologies, particularly CNNs trained on specialized datasets, this approach significantly enhances the surveillance system's capacity to

*Corresponding author: bhuvanasd20@gmail.com

identify anomalies and potential security risks with high precision.

This article [3] examines the complexities inherent in conventional video surveillance practices, where the manual processing of vast data sets can lead to the inadvertent loss of critical information, especially in identifying anomalous behaviors indicative of security threats. The proposed framework is dedicated to bolstering intelligent surveillance capabilities by introducing specialized algorithms tailored to discern two primary human activities: walking and running. Notably, the research imposes no constraints on the number of individuals or motion trajectories but is confined to analyzing indoor color video footage captured by stationary cameras. Detection of moving entities, suggestive of suspicious conduct, is facilitated through a background subtraction technique. Essential attributes for activity categorization encompass the rate of displacement of segmented foreground regions' centroids and the dynamics of their size alterations. The investigative approach involves a sequential series of methodologies, encompassing video frame partitioning, segregation of background and foreground elements, noise mitigation via morphological operations, and mathematical analyses to identify frames indicative of suspicious behavior. The efficacy of the proposed algorithms is underscored by their commendable accuracy rates in activity classification, thereby augmenting the efficacy of intelligent surveillance systems for security-centric applications.

The paper [4] discusses the widespread utilization of anomaly detection systems in tandem with machine learning and artificial intelligence for behavioral analysis. These systems serve a critical function in detecting and forecasting anomalies across diverse domains, including enterprise operations, intrusion detection, system health monitoring, fraud detection in financial transactions, and fault detection in operational environments. With escalating global crime rates and heightened concerns regarding human security, numerous nations, such as India with a crime index of 42.38, are embracing advanced anomaly detection systems. The paper underscores that conventional security measures, like CCTV installations, fall short, necessitating modern anomaly detection systems equipped with optimized versions featuring predictive capabilities. The research delves into the utilization of Convolutional Neural Network (CNN) models to enhance anomaly detection and prediction, thereby fortifying security measures.

This research paper [5] delves into the fusion of deep learning methodologies, a subset within the realm of machine learning, to tackle diverse challenges within the field of artificial intelligence. It underscores the pivotal role of machine learning in crafting algorithms that leverage data patterns and historical associations. The investigation concentrates particularly on harnessing image processing techniques and deep learning algorithms within a machine learning framework to detect fire outbreaks, identify unauthorized vehicles, and recognize individuals. Furthermore, the proposed model extends its utility to remotely manage electrical equipment, ensuring preemptive measures against fire hazards and unauthorized intrusions. The primary aim is to develop an intelligent neural network trained to track specific occurrences and furnish a scalable machine learning solution. The research methodology encompasses frame capture, data preprocessing, and the utilization of pre-existing datasets to identify recurring patterns. Additionally, a user-friendly web interface is devised for presenting predictive analyses, while simulations are carried out to evaluate the model's efficacy. By amalgamating deep learning and machine learning, the objective is to establish a robust and dependable security infrastructure for organizations, thereby mitigating the risks associated with fire outbreaks and unauthorized access, while also enabling remote device management through a web interface.

This study [6] delves into the pressing demand for heightened surveillance in public spaces amid escalating instances of violence, including shootings, knife assaults, and acts of terrorism on a global scale. Employing a deep learning methodology, specifically leveraging Convolutional Neural Networks (CNN), the research scrutinizes images and videos to identify potentially suspicious behaviors. It examines diverse CNN architectures, comparing their efficacy to offer valuable insights into model performance. The paper presents the blueprint of a system engineered to analyze real-time video feeds from surveillance cameras, with the ability to predict the likelihood of observed activities being suspicious. Notably, the integration of Fast AI, a deep learning framework, bolsters the system's functionality. Furthermore, the paper delineates prospective advancements aimed at propelling the domain of suspicious activity detection through deep learning techniques.

This study [7] delves into the real-time detection of potentially suspicious human behavior within CCTV footage using neural networks, with a particular emphasis on the utilization of Convolutional Neural Networks (CNNs). The research addresses the persistent challenge of accurately predicting the positions of human body parts or joints from images or video streams. Identifying suspicious human activity holds significant importance across various domains of computer vision, including video surveillance, behavior analysis, and human-computer interaction. Due to limitations associated with the use of low-cost depth sensors in existing systems, the proposed solution relies on neural networks to effectively address these challenges. The primary objective of this research is to contribute to the evolving field of image processing and computer vision by enhancing the capability to recognize suspicious activities in surveillance videos. The proposed intelligent video surveillance system is engineered to monitor public spaces in real-time, distinguishing between typical and atypical activities, and issuing alerts for potential threats or criminal behavior. It is noteworthy that this paper highlights the unique contribution of CNNs in detecting suspicious activities, setting it apart from prior research that predominantly focuses on image rather than video data.

This research [8] underscores the significant role of video monitoring in contemporary technological landscapes, leveraging artificial intelligence (AI), machine learning (ML), and deep learning to amplify its functionalities. It specifically addresses the challenge of distinguishing between typical and

suspicious human behaviors, recognizing the inherent unpredictability of human actions. The proposed methodology employs deep learning techniques, notably integrating LSTM (Long Short-Term Memory) models, to discern between suspicious and normal activities within academic settings. The surveillance mechanism operates by analyzing successive frames extracted from video recordings, and its framework comprises two primary components. Initially, features are extracted from the video frames, followed by a classifier that predicts the nature of observed activities—whether they are suspicious or normal—based on these extracted features. The integration of LSTM models introduces a temporal aspect to the analysis, allowing the system to capture prolonged patterns in human behavior, thereby facilitating more precise predictions.

This study [9] delves into the utilization of neural networks, specifically Convolutional Neural Networks (CNN), in identifying potentially suspicious human behavior within surveillance footage. The primary aim is to tackle the challenges inherent in monitoring public spaces, such as bus terminals, train stations, airports, and similar venues, to mitigate risks like terrorism, accidents, vandalism, and other anomalous activities. Given the impracticality of continuous human oversight in such environments, intelligent video surveillance emerges as a crucial solution. The proposed framework harnesses CNN, a deep learning architecture, to analyze video streams and distinguish between typical and atypical human actions. The overarching goal is to trigger alerts for unusual behavior, thus facilitating a proactive security approach and risk mitigation in public locales. The incorporation of CNN underscores the system's reliance on convolutional layers for efficient feature extraction and discernment of patterns pertinent to suspicious activity detection.

This study explores the implementation of an algorithm for identifying potentially hazardous human behaviors, with a focus on anomaly detection. The central objective is to enhance individual safety in light of escalating risks, ranging from intentional violence to unforeseen accidents. Conventional closed-circuit television (CCTV) systems are considered inadequate due to their dependence on continuous human surveillance, which often leads to inefficiencies. To address this shortfall, the proposed framework introduces a fully automated security solution capable of promptly detecting anomalous activities in real-time, thereby offering immediate assistance to potential victims. Leveraging machine learning methodologies, particularly Convolutional Neural Networks (CNN), the system scrutinizes CCTV footage in real-time to identify suspicious human actions. Alerts are promptly generated upon detection of abnormal activities. Empirical findings, derived from experiments conducted on a dataset encompassing both typical and anomalous behaviors, underscore the efficacy of the proposed approach. The adoption of CNN underscores the emphasis on leveraging convolutional layers for robust feature extraction, facilitating accurate detection of suspicious activities.

3. Methodology

- User Registration: Users register to the website by giving required details.
- User Login: User login to the website using login credentials.
- Upload Video: Users employ the web application interface to upload surveillance videos. It contains both normal and suspicious activities.
- Video Preprocessing: Upon upload, the backend system starts video preprocessing, segmenting the video into individual frames. Resize and preprocess each frame to fit the input requirements of MobileNetV2.
- Feature Extraction: MobileNetV2 is used to extract spatial features from each pre-processed frame. These features represent the content of each frame and are extracted efficiently using the MobileNetV2 architecture.
- Temporal Modeling and Training: Leveraging a pre-existing CNN model, LSTM specialized in detecting suspicious activities, the system analyses each segmented frame. The LSTM learns to capture temporal dependencies and patterns across the sequence of frames. The LSTM model is trained using the labeled video data, the model learns to differentiate between normal and suspicious activity by analyzing the temporal patterns in the input sequence of special features.
- Identification of Suspicious Behavior: The trained LSTM and MobileNetV2 model is deployed to analyze new video streams in real-time. Continuously feed each frame through the preprocessing pipeline, extract spatial features using MobileNetV2, and pass the sequence of features through the LSTM for suspicious activity detection.
- Alert Activation: Upon the model's identification of suspicious behavior in any frame, an alert mechanism is triggered.
- Email Notification: This alert mechanism activates the sending of an Email alert to the user's mobile device or PC, promptly notifying them of the identified irregular activity.
- Integration with Web Service Providers' APIs: The Email alerting functionality is seamlessly integrated using Web service providers' APIs. This integration ensures rapid and efficient delivery of notifications to the user's device.

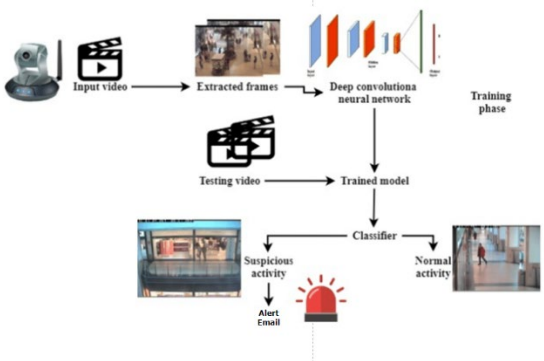

Fig. 1. System architecture

4. Proposed System

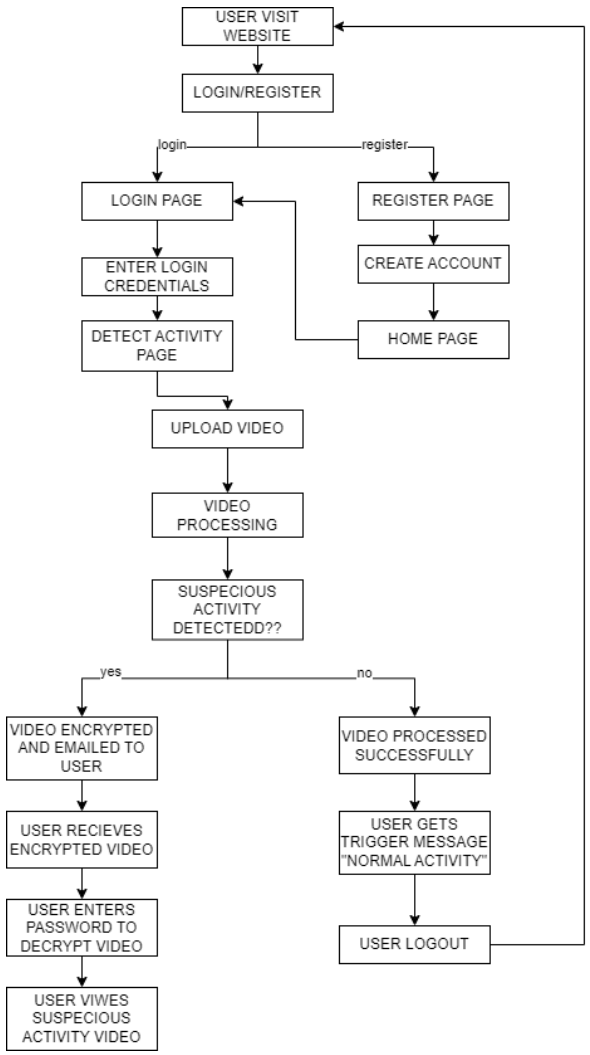

Fig. 2. Flow chart

The proposed system aims to transform security monitoring through the utilization of cutting-edge technologies to automate the identification of potentially concerning behavior within videos uploaded to an online platform. A fundamental aspect is its capacity to autonomously identify suspicious activities without requiring human intervention. Through the employment of machine learning algorithms trained on annotated datasets, the system can acquire the ability to identify patterns associated with a range of suspicious behaviors, including but not limited to unauthorized entry, property damage, or theft. This capability facilitates the proactive detection of security breaches as they unfold, thereby reducing response times and mitigating potential threats.

Furthermore, this platform provides real-time detection functionalities, enabling users to monitor video feeds in live mode for any indications of irregular behavior. This is especially crucial in environments prone to heightened risks, where prompt intervention might be crucial in averting security breaches or minimizing potential harm. Moreover, the platform integrates robust user verification mechanisms to guarantee that solely authorized personnel can view and upload videos, thereby bolstering the security and confidentiality of the system.

In addition, this system incorporates an email alert feature designed to promptly notify pertinent parties in the event of any potentially suspicious activity being identified. This facilitates the swift dissemination of security incidents to the relevant authorities, thereby enabling rapid response and necessary intervention. Through the integration of advanced video analytics, continuous real-time monitoring, robust user authentication protocols, and automated email notifications, this system presents a holistic solution for bolstering security measures and addressing risks across diverse environments, including commercial premises, public areas, and residential communities.

5. Future Enhancement

Future enhancements may entail refining the detection algorithms to enhance their precision and dependability. This might involve leveraging cutting-edge deep learning methodologies or integrating supplementary datasets for training purposes. Additionally, broadening the spectrum of suspicious activity detection to encompass various scenarios or industry-specific contexts could augment its relevance. Furthermore, introducing real-time alerts via SMS or mobile notifications alongside email notifications could offer users more immediate updates. Finally, integrating mechanisms for user feedback and reporting could facilitate ongoing enhancements to the detection system, informed by user insights and evolving threat landscapes.

6. Conclusion

The fusion of computer vision and artificial intelligence within automated video detection systems signifies a significant advancement in bolstering security protocols across public spaces. Traditional surveillance methodologies often demonstrate limitations in accurately pinpointing unusual behaviours, underscoring the necessity for more advanced solutions. This project introduces an innovative strategy leveraging deep learning methodologies, specifically LSTM (Long Short-Term Memory) and MobileNetV2 models. These models facilitate the segmentation of video footage, extraction of pertinent features, and real-time detection of irregular or suspicious activities, thus heralding a transformative approach to surveillance.

References

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

[2] 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, no. 6, pp. 2373-2377, June 2022.

[3] 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, 2021.

[4] 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, vol. 2, no. 4, 216-221, 2020.

[5] 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, 2023.

[6] Rachana Gugale, Abhiruchi Shendkar, Arisha Chamadia, Swati Patra, Deepali Ahir, "Human Suspicious Activity Detection using Deep Learning", International Research Journal of Engineering and Technology, vol. 7, no. 6, June 2020.

[7] Vedant Saikhede, Kiran Shende, Yuvraj Darekar, Hemant Thorat, Snehal. S. Shinde, "Deep Learning Approach for Suspicious Activity Detection from Surveillance Video", International Research Journal of Engineering and Technology, vol. 10, no. 12, Dec. 2023.

[8] Sonali Suryavansh, Rohit Shinde, Sarthak Kathe, Akash Phad, C.H. Patil, "Using Surveillance Video Detection of Suspicious Activity Based on Deep Learning," International Research Journal of Modernization in Engineering Technology and Science, vol. 5, no. 5, May 2023.

[9] 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, vol. 2, no. 4, May 2022.

[10] Tejashri Subhash Bora, Monika Dhananjay Rokade, "Human Suspicious Activity Detection System Using CNN Model for Video Surveillance", IJARIIE, vol. 7, no. 3, 2021.