

SUSPICIOUS HUMAN ACTIVITY TRACKING AI CAMERA USING BLACK BOX

¹Leenashruthi H M, ²Kusuma N A, ³Meghana P, ⁴Michelle Johnson, ⁵Monisha M U

¹Professor, ^{2,3,4,5}Students

Department of CSE

East West Institute of Technology

Bengaluru, India

Abstract: *The rapid advancements in artificial intelligence (AI) have paved the way for innovative applications in surveillance and security systems. This paper introduces a novel approach to suspicious human activity tracking using an AI-powered camera system integrated with a black box for enhanced functionality and privacy preservation. The proposed system employs deep learning algorithms to analyze real-time video streams and detect anomalies in human behavior that may indicate potential security threats. The AI camera utilizes convolutional neural network (CNN) architecture for efficient object detection and tracking. The model is trained on a diverse dataset to recognize normal and suspicious activities based on motion patterns, object interactions, and spatial relationships. To augment the system's adaptability, a black box component is introduced, encapsulating the core AI algorithms and ensuring a transparent and auditable decision-making process. The black box serves multiple purposes, including safeguarding sensitive information, addressing ethical concerns related to privacy, and facilitating regulatory compliance. It acts as an isolated module that processes and interprets video feeds without exposing raw data or compromising individual privacy. The integration of the black box also enables the logging of decision-making processes, contributing to accountability and traceability in the system's operations. Furthermore, the proposed system incorporates a feedback mechanism, allowing users to provide input to the black box to improve the AI model's accuracy over time. This iterative learning approach enhances the system's ability to adapt to evolving threats and reduces the risk of false positives or negatives.*

Indexwords: *Artificial Intelligence, AI Camera, Convolutional Neural Network (CNN)*

I. INTRODUCTION

In recent years, the integration of artificial intelligence (AI) into surveillance systems has transformed the landscape of security and public safety. This paper introduces an innovative solution for tracking suspicious human activities through the utilization of an AI camera system augmented with a sophisticated black box component. This amalgamation of cutting-edge technology aims to enhance the accuracy and

efficiency of threat detection while addressing critical concerns related to privacy and ethical considerations. The relentless evolution of AI technologies has enabled the development of advanced algorithms capable of analyzing complex visual data in real-time. The proposed system leverages deep learning algorithms, particularly a Convolutional Neural Network (CNN), to discern patterns and anomalies within video streams. By focusing on motion patterns, object interactions, and spatial relationships, the AI camera strives to identify behaviors indicative of potential security threats. Crucially, the integration of a black box within the system serves as a pivotal advancement. This black box encapsulates the core AI algorithms, creating a secure and transparent processing environment. This approach not only protects sensitive information but also ensures that decision-making processes are isolated and auditable, contributing to a heightened level of accountability in the deployment of surveillance technologies. Privacy preservation is a paramount concern in any AI-driven surveillance system. The black box architecture plays a key role in this regard by acting as a safeguard against unwarranted intrusion into individual privacy. By processing and interpreting video feeds within the black box, raw data exposure is minimized, mitigating concerns associated with data privacy.

II. LITERATURE SURVEY

A literature survey for a suspicious human activity tracking AI camera using a black box would involve reviewing existing research and publications related to AI in surveillance, anomaly detection, privacy preservation, and ethical considerations. These studies provide a foundation for understanding the state of the art in AI surveillance, anomaly detection, privacy preservation considerations. Continuing the literature survey without the emphasis on a black-box model, the examination should focus on existing research that explores various transparent or interpretable AI models for suspicious human activity tracking in surveillance systems. This involves reviewing literature on explainable AI (XAI) techniques, interpretable machine learning algorithms, and methodologies that prioritize transparency in model decision-making.

Title	Authors	Year	Objectives	Advantages	Disadvantages
A Review of Deep Learning-based Human Activity Recognition on Benchmark Video Datasets.	Vijeta Sharma, Manjari Gupta, Anil Kumar Pandey, Deepti Mishra and Ajai Kumar	2022	To present a comparative review of vision-based identification of human activity with the main focus on deep learning techniques on various benchmark video datasets comprehensively.	The paper summarizes the strengths and weakness of different methods, and compares their performance on four popular benchmark datasets.	The paper does not include any experimental results or code implementation of the reviewed methods, which may limit the reproducibility and verification of the paper.
Suspicious Activity Detection Network for Video Surveillance Using Machine Learning	Komal V Shivthare, Purvaja D Bhujbal, Akshada P Darekar, Prof. Yuvraj N N	2021	Used to design a Network for identifying suspicious activities in video surveillance employing learning techniques.	The proposed method can achieve high precision and efficiency in detecting suspicious activities from surveillance video.	The proposed method may not be able to generalize well to different environments and contexts where the definition of suspicious activity may vary.
Machine Learning Approach for Suspicious Activity Detection	Kadam P, Gawande S, Thorat A, Mule R.	2021	To use a dataset of frames in which suspicious and non-suspicious movements are seen to instruct the machine learning model.	The alternative approach can be able to handle multiple activities occurring simultaneously.	The proposed method may require a large amount of labeled data for training the machine learning model, which may be costly and time consuming to obtain.
Deep Learning Approach for Suspicious Activity Detection from Surveillance Video	Amrutha C.V, C. Jyotsna Amudha J.	2020	It sends an alert message to the relevant jurisdiction predicting a suspicious activity.	The proposed method can reduce the manual intervention and human errors in monitoring the video surveillance system.	The proposed approach may not be able to handle complex and dynamic scenarios where multiple activities are occurring simultaneously.

<p>Abnormal event detection based on analysis of movement information of video</p>	<p>Wang, Tian, Meina Qiao, Huan Wang,</p>	<p>2018</p>	<p>It detecting abnormal events in video monitoring for security, as an alternative systems.</p>	<p>An alternative algorithm is suggested efficiently that solves the problem using an image descriptor that encrypts information.</p>	<p>The suggested approach has been evaluated on an many different videos and has been to work well.</p>
--	---	-------------	--	---	---

III. CONCLUSION

In conclusion, the implementation of the suspicious activity tracking AI camera represents a significant stride towards enhancing security and safety in various domains. The robust capabilities of the AI system enable real-time identification and tracking of suspicious behavior, contributing to proactive threat prevention. The project's applications span across sectors such as public security, retail, industrial safety, transportation, and more, showcasing its versatility.

REFERENCES

1. Bouma, H.; Baan, J.; Burghouts, G.J.; Eendebak, P.; Van Huis, J.R.; Dijk, J.; Van Rest, J.H.C. Rest Automatic detection of suspicious behavior of pickpockets with track-based features in a shopping mall. In Optics and Photonics for Counterterrorism, Crime Fighting, and Defence X; and Optical Materials and Biomaterials in Security and Defence Systems Technology XI; SPIE: Washington, DC, USA, 2014; Volume 9253. [CrossRef]
2. Bouma, H.; Schutte, K.; Hove, J.-M.T.; Burghouts, G.J.; Baan, J. Flexible human-definable automatic behavior analysis for suspicious activity detection in surveillance cameras to protect critical infrastructures. In Counterterrorism, Crime Fighting, Forensics, and Surveillance Technologies II; SPIE: Washington, DC, USA, 2018; Volume 108020N. [CrossRef]
3. Kadam, P.; Gawande, S.; Thorat, A.; Mule, R. Suspicious Activity Detection using Image Processing. *J. Sci. Technol.* 2021, 6, 114–119. [CrossRef]
4. Scaria, E.; Aby Abahai, T.; Isaac, E. Suspicious Activity Detection in Surveillance Video using Discriminative Deep Belief Network. *Int. J. Control Theory Appl.* 2016, 9, 1–7.
5. Loganathan, S.; Kariyawasam, G.; Sumathipala, P. Suspicious Activity Detection in Surveillance Footage. In Proceedings of the 2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA), Ras Al Khaimah, United Arab Emirates, 19–21 November 2019; pp. 1–4. [CrossRef]
6. Bora, T.S.; Rokade, M.D. Human suspicious activity detection system using CNN model for video surveillance. *Int. J. Adv. Res. Innov. Ideas Educ.* 2021, 7, 688–694.
7. Shivthare, K.V.; Bhujbal, P.D.; Darekar, A.P. Suspicious activity detection network for video surveillance using machine learning. *Int. J. Adv. Sci. Res. Eng. Trends* 2021, 6, 88–90.
8. Elhamod, M.; Levine, M.D. Automated Real-Time Detection of Potentially Suspicious Behavior in Public Transport Areas. *IEEE Trans. Intell. Transp. Syst.* 2013, 14, 688–699. [CrossRef]
9. Alavudeen Basha, A.; Parthasarathy, P.; Vivekanandan, S. Detection of Suspicious Human Activity based on CNN-DBNN Algorithm for Video Surveillance Applications. In Innovations in Power and Advanced Computing Technologies (i-PACT); IEEE: Toulouse, France, 2019; pp. 1–7. [CrossRef]
10. Amrutha, C.; Jyotsna, C.; Amudha, J. Deep Learning Approach for Suspicious Activity Detection from Surveillance Video. In Proceedings of the 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, India, 5–7 March 2020; pp. 335–339. [CrossRef]
11. Singh, V.; Singh, S.; Gupta, P. Real-Time Anomaly Recognition Through CCTV Using Neural Networks. *Procedia Comput. Sci.* 2020, 173, 254–263. [CrossRef]
12. Saba, T.; Rehman, A.; Latif, R.; Fati, S.M.; Raza, M.; Sharif, M. Suspicious Activity Recognition Using Proposed Deep L4-Branched- Actionnet with Entropy Coded Ant Colony System Optimization. In IEEE Access; IEEE: Toulouse, France, 2021; Volume 9, pp. 89181–89197. [CrossRef]
13. Mehmood, A. LightAnomalyNet: A Lightweight Framework for Efficient Abnormal Behavior Detection. *Sensors* 2021, 21, 8501. [CrossRef] [PubMed]