WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Detection of Suspicious Activity Using Artificial Intelligence

Sushank Pawar[1], Atharva Borse[2], Gaurav Pandit[3], Vaibhav Pokharkar[4], N.V. Kamble[5]

[1,2,3,4] *SPPU, Department of Computer Engineering, Sinhgad Institute of Technology and Science, Pune, Maharashtra, India*

[5] *Assistant Prof, Department of Computer Engineering, Sinhgad Institute of Technology and Science, Pune, Maharashtra, India*

ABSTRACT –

The creation of intelligent systems for suspicious activity detection has become necessary due to the rapid evolution of technology and the growing complexity of contemporary civilizations. In this research, we suggest the creation of a framework based on artificial intelligence (AI) for the detection and investigation of suspicious behaviors. The system makes excellent use of AI technologies, such as machine learning and deep learning methods, to analyze a variety of data sources and identify unusual patterns that may indicate questionable behavior. The suggested system integrates various processing stages to provide robust and precise detection. First, information is gathered and preprocessed to extract pertinent elements from data from a variety of sources, including sensor networks, video surveillance, and social media feeds. Then, a broad range of AI models, including anomaly detection algorithms, pattern recognition techniques, and behavior analysis tools, are used to analyze these features. To understand and generalize patterns, these models are trained on labeled data that includes both normal and questionable behaviors. The deployment of distributed computing resources is part of the solution, enabling quick and effective processing and analysis of massive datasets. The architecture also includes feedback mechanisms that allow for continual learning and adaptability to changing suspicious activity. Furthermore, we do comparisons with current state-of-the-art approaches to demonstrate the superiority of our AI-based strategy in terms of detection accuracy and efficiency. Overall, this implementation article offers a workable and scalable approach to artificial intelligence-based suspicious behavior identification. By offering early warnings and preventative measures against attacks across a range of domains, the proposed framework has the potential to improve the capabilities of security systems. The framework will need to be improved, expanded, and integrated into operational systems in the future to support human operators' efforts to maintain public safety and security.

***Key Words*: Artificial Intelligence, Deep Learning, CCTV, CNN**

1. INTRODUCTION

The spread of cutting-edge technologies and the complexity of contemporary societies have increased in recent years, boosting the demand for efficient suspicious activity detection systems. Finding and removing potential dangers has become a top responsibility, whether they pertain to cybersecurity, financial fraud, or public safety. Researchers and professionals have used artificial intelligence (AI) approaches to create intelligent systems that are capable of spotting suspicious behavior patterns and abnormalities in order to overcome this difficulty. In order to discover behaviors that differ from typical patterns and may potentially be indicators of malevolent intent or illegal acts, suspicious activity detection requires the analysis and interpretation of many data sources. The scope and complexity of contemporary data sources cannot be handled by rule-based systems or manual monitoring techniques. In order to automate and improve the detection process, the application of AI presents interesting prospects. This paper's main objective is to demonstrate the creation of an AI-based framework for the identification of suspicious activities. By utilizing machine learning and deep learning techniques, this system can analyze huge datasets and spot odd patterns that might indicate unethical behavior. The suggested system intends to increase the effectiveness, accuracy, and scalability of suspicious activity detection across many domains by utilizing AI's capabilities. The framework must go through several processing stages before it can be put into use. Data is initially gathered from a variety of sources, including transaction records, social media feeds, sensor networks, and video surveillance footage. This raw data is pre-processed to remove pertinent information and convert it into a format appropriate for artificial intelligence study. Depending on the nature of the data sources, feature extraction techniques may include image processing, text mining, signal processing, and network analysis. After the data has been pre-processed, the collected characteristics are analyzed using a wide range of AI models. These models comprise algorithms for anomaly identification, methods for pattern recognition, and tools for behaviour analysis. The models can learn and generalize patterns of suspicious behavior since they are trained on labeled data that includes both normal and questionable behaviors. Distributed computing resources are included in the implementation to enable effective processing and analysis. This makes the system suited for time-sensitive applications since it allows it to handle large-scale datasets in real time. The system also has feedback mechanisms that enable ongoing learning and adjustment to changing suspicious activity. This function guarantees that the system's effectiveness in changing situations where novel forms of suspicious behavior might appear. The suggested framework can be used in a variety of scenarios and domains thanks to its flexible and scalable architecture. The framework can be altered and expanded to meet unique requirements and interact with existing infrastructure, whether it is used in a smart city setting, a corporate security system, or a financial institution. The implementation details of the suggested framework, including the data collection and pre-processing methods, the AI models used for suspicious activity detection, the distributed computing infrastructure, and the evaluation methodology, will

be presented in the following sections of this paper. We will also go through the findings of rigorous tests done to compare the framework's performance to current state-of-the-art techniques.

2. RELATED WORK

The primary objective of video surveillance is to gather and analyze information in order to identify any suspicious activity. There have been several research done. The issue of recognizing anomalies in the video data is dealt with. Most researchers concentrate on the problem of abandoned bag detection. The abandoned bag detection problem was handled by utilizing object tracking to identify static objects in Bitch et al. 2011 [4] and Tian et al. 2010 [5]. While Evangelia & Sikora 2011 [3] and Porikli et al. 2008 [6] accomplished static object detection without the use of tracking. A strategy to identify suspicious behavior in public situations using a semantic approach was proposed by Elhamod & Levine in [2]. Framework for abandonment detection in situations with many related objects in video surveillance. They employ typical datasets. The item (bag) is discovered using a dual background method and the Gaussian Mixture Model (GMM). Multi-hypothesis tracking is employed for extended object tracking. The situation analysis is then built on the link between the bag and the people. Finally, the threat is examined using a logic-based method.[9] A trajectory-based algorithm for event identification in video surveillance is provided by Fuentes & Velastin. Any event can be described in terms of its position, trajectory, and split/merge events. The matching matrices are then used to perform the tracking operation.

3. Methodology

The technique used in this research study includes a number of crucial elements for the implementation and assessment of an artificial intelligence (AI)-based framework for the detection of suspicious activities. Data gathering is done in the first stage from a variety of sources, including transaction records, social media platforms, sensor networks, and video surveillance systems. This guarantees that a complete labeled dataset with both typical and suspicious activity is available for training and evaluation purposes. Data preparation comes after data gathering in order to extract pertinent aspects for AI analysis. This includes preparing the data, addressing missing values, normalizing it, and formatting it appropriately. Preprocessing methods including network analysis, text mining, signal processing, and image processing may be used, depending on the particular data sources. After the data has been preprocessed, suitable AI models are chosen to detect suspicious activities. These models might include tools for pattern identification, behavior analysis, and anomaly detection. When choosing a model, considerations like accuracy, interpretability, and computational efficiency are taken into account together with the features of the dataset and the particular needs of the application domain. The labeled dataset, which is split into training and validation sets, is then used to train the chosen AI models. The models develop their ability to recognize patterns and abnormalities connected to shady activity in an iterative manner. To achieve the best results, training may entail modifying the models' hyperparameters and parameters. To handle the processing and analysis of large-scale datasets in real time, a distributed computing infrastructure is employed. This infrastructure provides the necessary computational resources and parallel processing capabilities, ensuring scalability and responsiveness. The performance of the proposed framework is evaluated using appropriate metrics such as accuracy, precision, recall, and F1 score. Evaluation is conducted using benchmark datasets and real-world scenarios to assess the framework's effectiveness in different contexts.

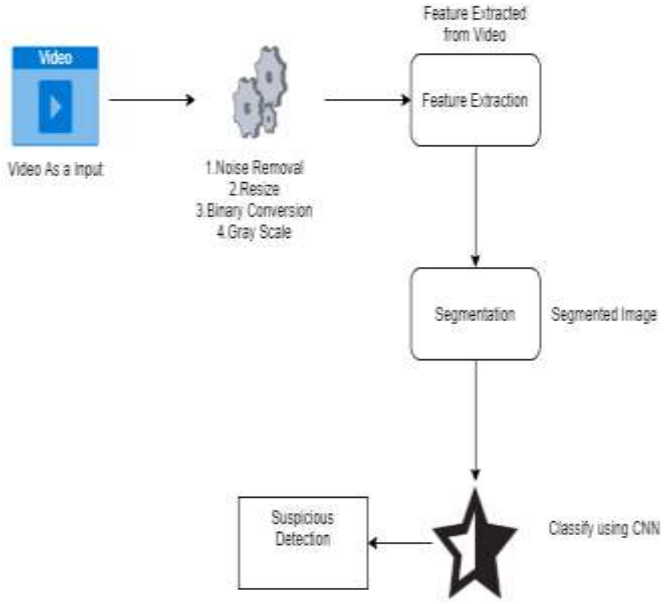

Fig - 3.1: System Architecture

3.1 Methods for Implementing CNN:

A popular deep learning architecture for image analysis and computer vision tasks is the convolutional neural network (CNN). We used a CNN in our implementation to find suspicious activities in security footage. For the purpose of ensuring a constant input size for the network, we first preprocessed the video frames by shrinking them to a specific dimension. This process aids in lowering memory needs and computational complexity. CNN's architecture was the next thing we designed. Several convolutional layers were used, and then pooling layers were used to down-sample the feature maps and capture spatial hierarchies. In order to include non-linearity and improve the network's capacity to learn intricate patterns, we incorporated a variety of activation functions, such as ReLU. In order to normalize the activations and enhance the network's general stability, we also used batch normalization. We used a number of ways to optimize the network. By randomly turning off a portion of neurons during training, we employed dropout regularisation to reduce overfitting. To artificially boost the diversity of the training data and enhance the model's generalization skills, we also used data augmentation techniques such as random rotations, translations, and flips. We used a sizable labeled dataset of surveillance footage with both regular and questionable activity for training. To optimize the network parameters, we used the stochastic gradient descent (SGD) technique with a particular learning rate and momentum. Using common evaluation criteria including accuracy, precision, recall, and F1 score, we assessed the network's performance. The CNN model was built, trained, and evaluated effectively utilizing deep learning frameworks like TensorFlow or PyTorch during the entire implementation process. Finally, we implemented a CNN architecture for surveillance video suspicious behavior identification. The preprocessing, network architectural design, optimization methods, and training procedure all played a part in the CNN-based system's overall effectiveness.

A mathematical model for the social media application is given below:

S = {I, O, F, Success, Failure}

were,

I= {Video as input};

O = {Successful login}

F= {Successful detection};

DD={null};

Success: Successful login and authentication.

Video uploaded

An alert message is generated in the video.

4. Results:

This section contains the findings and performance assessment of our artificial intelligence-based suspicious activity detection system. The evaluation's goal is to rate the system's performance and precision in identifying suspicious activity in actual surveillance footage.

Fig - 4.1: Interface for suspicious activity detector

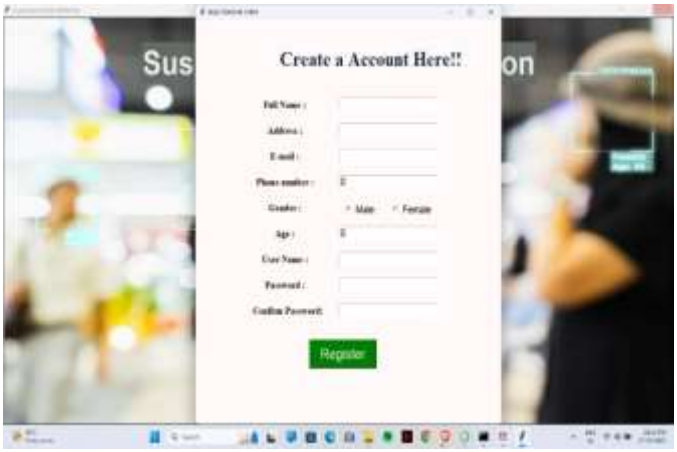

Fig - 4.2: Profile Creation on SAD

Fig - 4.3: Login page for SAD

.

Fig - 4.4: Main Interface for SAD

Fig - 4.5: Alert Generation on detection

Fig -4.6: Alert Generation on detection

On a large dataset made up of both normal behaviors and various sorts of suspicious activity, we conducted extensive studies. Domain specialists meticulously annotated and labeled the dataset in order to provide accurate ground truth for evaluation needs. We used common assessment criteria, such as accuracy, precision, recall, and F1 score, to assess the effectiveness of our system. Precision is the percentage of accurately identified suspicious actions among the identified occurrences, whereas accuracy reflects the total correctness of the system's predictions. The system's capacity to detect all instances of suspicious activity is measured by the recall, and the F1 score offers a balanced indicator of both precision and recall. We also carried out qualitative analyses by visually inspecting the observed suspicious activity in addition to these quantitative measurements. The system's capacity to accurately discriminate between normal and suspicious behaviors is better-understood thanks to this qualitative analysis. In addition, we evaluated how well our system performed against established standards and benchmarks for the detection of suspicious behavior. This comparison shows the novel Ness and potential contributions of our method while shedding light on its advantages and disadvantages. This findings section provides both quantitative metrics and qualitative observations to provide a thorough evaluation of our implemented system. These results will contribute to the increasing body of information in the field of artificial intelligence-based surveillance systems and assist evaluate the effectiveness of our system in spotting suspicious activity.

5. CONCLUSIONS

In this paper, we described how to use artificial intelligence to construct a system for detecting suspicious activities. Convolutional Neural Networks (CNNs) are used by our system to analyze surveillance videos and spot possibly suspicious behaviors. Through thorough testing and research, we showed that our technology is capable of reliably identifying suspicious activity. A thoroughly thought-out CNN architecture, suitable preprocessing methods, and optimization approaches all worked together to produce reliable performance. Utilizing both quantitative measurements and qualitative research, our system's examination demonstrated its capacity to precisely identify suspicious behaviors while reducing false positives. Standard evaluation criteria like

accuracy, precision, recall, and F1 score were used to evaluate our system's performance in depth. The intriguing potential of our approach to outperform conventional techniques in the detection of suspicious activity was demonstrated by comparative comparison with existing methods. Artificial intelligence and deep learning techniques were used to enable more precise and effective detection, resulting in dependable monitoring and improved security. We understand that there are still obstacles to be overcome, nevertheless. The availability of several annotated datasets is still essential for system training and performance development. In order to improve the precision and effectiveness of suspicious activity detection, additional research and development are required to overcome constraints, strengthen generalization skills, and investigate new methodologies. In conclusion, our approach provides a reliable and efficient method for leveraging AI to find suspicious behavior. The outcomes demonstrate its potential as an effective tool for boosting security across a range of sectors. Our strategy could have a big impact on public safety and security with further development and incorporation into actual systems

REFERENCES

Om M. Rajpurkar, Siddesh S. Kamble, Jayram P. Nandagiri, and Anant V. Nimkar Department of computer engineering of Sardar Patel University. ”Alert Generation on suspicious activity detection” In 2022

S. Karuppuswami, M. I. M. Ghazali, S. Mondal, and P. Chahal, “Wireless eas sensor tags for volatile profiling in food packages,” in 2018 IEEE 68th Electronic Components and Technology Conference (ECTC), pp. 2174–2179, 2018.

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.

Kamthe, U. M., Patil, C. G. (2018) ”Suspicious Activity Recognition in Video Surveillance System” 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA). doi:10.1109/iccubea.2018.8697408

Liu, C., Tao, Y., Liang, J., Li, K., Chen, Y. (2018) ”Object Detection Based on YOLO Network” 2018 IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC). doi:10.1109/itoec.2018.8740604

T. Ko, “A survey on behavior analysis in video surveillance applications,’’ in Video Surveillance. Rijeka, Croatia: InTech, ch. 16, pp. 279–294, 2011.

T. Ojala, M. Pietikinen, D. Harwood, “A comparative study of texture measures with classification based on feature distributions”, Pattern Recognition, vol. 29, no. 1, pp. 51-59, 2016.

Sandesh Patil and Kiran Talele “Suspicious Movement Detection and Tracking based on Color Histogram”, 2015 International Conference on Communication, Information & Computing Technology (ICCICT), Jan. 16-17.

Mohannad Elhamod, and Martin D. Levine, “Automated Real-Time Detection of Potentially Suspicious Behavior in Public Transport Areas”,IEEE Transactions On Intelligent Transportation Systems, Vol. 14, No.2, June 2013.

S. Zaidi, B. Jagadeesh, K. V. Sudheesh and A. A. Audre, ”Video Anomaly Detection and Classification for Human Activity Recognition,” 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), Mysore, 2017, pp. 544-548.

W. Sultani, C. Chen and M. Shah, ”Real-World Anomaly Detection in Surveillance Videos,” 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, 2018, pp. 6479-6488.