e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:03/March-2024 Impact Factor- 7.868 www.irjmets.com

SUSPICIOUS ACTIVITY DETECTION USING DEEP LEARNING APPROACH

Aruna Bali[*1], Deepu AB[*2], Inchara P[*3], Rithesh KT[*4], Yogaprakash MG[*5]

[*1,2,3,4]ACU, Department Of Information Science Engineering, BGSIT, BG Nagar, Karnataka, India.

[*5]Ass. Prof., Department Of Information Science Engineering, BGSIT, BG Nagar, Karnataka, India.

DOI : https://www.doi.org/10.56726/IRJMETS49934

ABSTRACT

In the contemporary world, Video Surveillance holds a crucial role, leveraging advancements in technologies such as artificial intelligence, machine learning, and deep learning. These innovations contribute to the development of sophisticated systems capable of discerning various suspicious behaviors in real-time image monitoring. Given the inherent unpredictability of human behavior, distinguishing between normal and suspicious activities poses a significant challenge. This paper introduces a classification system for human activities, categorizing them into normal (e.g., sitting, walking, jogging, hand waving) and suspicious (e.g., running, boxing, fighting). The classification is achieved through the utilization of convolutional neural networks, extractiing high-level features from images. The convolutional network's classification, along with the final pooling layer result, is considered to make the ultimate prediction, especially in the context of AI-based suspicious activity detection and criminal case identification from video input.

Keywords: AI Based Suspicious Activity Detection, Video Input, Criminal Case Detection.

I. INTRODUCTION

In the contemporary landscape, despite widespread surveillance cameras, escalating crime emphasizes the necessity for a model that swiftly detects suspicious behavior. The proposed solution involves developing a robust deep learning model capable of accurately identifying and classifying such activities within video surveillance footage. Objectives include enhancing the model's recognition of anomalous behavior patterns, implementing real-time processing, seamless integration with existing surveillance systems, and conducting thorough testing for optimal performance in diverse scenarios. The problem statement underscores the limitations of traditional surveillance methods, urging the need for an advanced, adaptive deep learning system to address the complexity and diversity of suspicious activities, mitigate false positives, and enhance security in various environments.

II. METHODOLOGY

1. Introduction

Brief overview of the proposed methodology and its focus on automatic detection of suspicious activities in video streams.

2. Deep Learning Model Selection: Convolutional Neural Network (CNN)

Explanation of the chosen CNN architecture for the detection task.

3. Transfer Learning for Enhanced Performance

Description of how pre-trained models were utilized through transfer learning to improve the detection model's performance.

4. Training on Annotated Dataset

Details on the training process, emphasizing the importance of the annotated dataset.

5. Feature Extraction: Temporal and Spatial Features

Explanation of the extraction process for temporal and spatial features, crucial for capturing nuanced patterns related to suspicious behavior.

6. Real-time Video Processing

Overview of the system's implementation for swift and accurate detection through real-time video processing.

Ensure to provide detailed explanations under each subheading to maintain clarity and uniqueness in your content.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:03/March-2024 Impact Factor- 7.868 www.irjmets.com

III. MODELING AND ANALYSIS

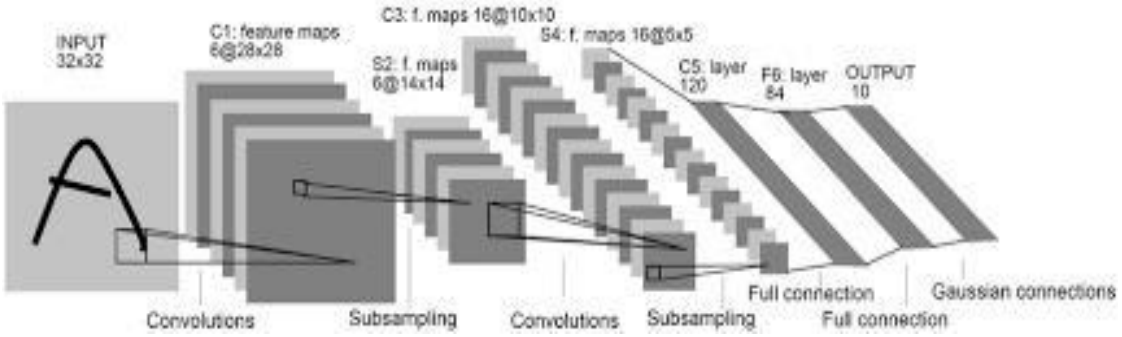

Figure 1: Layers Of CNN

This section details the model and materials used, adhering to the prescribed format. Figure 1 illustrates the layers of the convolutional neural network (CNN). Layer configurations are presented, including specifications such as kernel size, stride, and the number of kernels. For instance, Layer 1 consists of a 3x3 convolutional layer with six kernels, resulting in a 26x26x6 image. The subsequent layers involve pooling, convolutional, and dense layers, each with specific configurations and total parameters. Notably, Layer 6 employs a dense sheet with 128 parameters and Layer 7 culminates in a fully connected Softmax output layer with two units.

IV. RESULTS AND DISCUSSION

The proposed framework was implemented in Python 3.2 with the OpenCV library. The system hardware specifications are as follows: Intel(R) Core (TM) i5-8300H @ 2.30GHz, 8.00GB RAM, Windows Operating System (64-bit). The training dataset consisted of 10700 frames of nonsuspicious (safe) activity and 96800 frames of suspicious activity

V. CONCLUSION

We provided a detection tool based on frames extracted from videos and deep learning-based algorithms in this article. To detect the operation, this novel and special method necessarily require the use of minimal computational resources. It is versatile and mobile due to the lack of special hardware components. As a result, this cost-effective tool can be easily.

VI. REFERENCES

[1] Sudhir Goswami, Jyoti Goswami, Nagresh Kumar, “Unusual Event Detection in Low Resolution Video for enhancing ATM security”, 2nd International Conference on Signal Processing and Integrated Networks (SPIN), 2015.

[2] Saleem Ulla Shariff ; Maheboob Hussain; Mohammed Farhaan Shariff, “Smart unusual event detection using low resolution camera for enhanced security”, 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 17-18 March 2017

[3] Jignesh J. Patoliya ; Miral M. Desai, “Face detection based ATM security system using embedded Linux platform”, 2017 2nd International Conference for Convergence in Technology (I2CT), 7-9 April 2017.

[3] Sharayu Sadashiv Phule; Sharad D. Sawant, “Abnormal activities detection for security purpose un attainded bag and crowding detection by using image processing”, 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), 15-16 June 2017.

[4] G. Renee Jebaline, S. Gomathi, “A Novel Method to Enhance the Security of ATM using Biometrics,” 2015 International Conference on Circuit, Power and Computing Technologies [ICCPCT] 978-1-4799-7075-9/15/$31.00 ©2015 IEEE.

[5] Vikas Tripathi, Durgaprasad Gangodkar, Vivek Latta, and Ankush Mittal, “Robust Abnormal Event Recognition via Motion and ShapeAnalysis at ATM Installations”, Journal of Electrical and Computer.

[6] S.Shriram, Swastik B.Shetty, Vishnuprasad P. Hegde, KCR Nisha, Dharmambal V, “Smart ATM Surveillance System”, 2016 International Conference on Circuit, Power and Computing Technologies [ICCPCT].