INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 1321-1324

e-ISSN : 2583-1062

Impact Factor: 5.725

"AUTOMATICALLY DETECT SUSPICIOUS HUMAN ACTIVITY BY USING VARIOUS TOOLS AND TECHNOLOGIES"

Raj Kumar Gupta[1]

[1]Assistant Professor Madhyanchal Professional University, Faculty Of Engineering And Technology, School Of Computer Science Engineering, Bhopal, M.P, India.

ABSTRACT

Detecting suspicious behavior using a combination of deep learning techniques, particularly LRCN (Long-term Recurrent Convolutional Network). This method allows for the analysis of temporal data in video frames, which is crucial for identifying anomalies in human activity.

Using a combination of Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), the model can effectively extract relevant features from video data and classify behavior as suspicious or not. The process involves several key stages, including research, data collection and preprocessing, model design and training, and performance evaluation.

It's great that we've utilized datasets like KTH and Kaggle to train and validate your model. By leveraging these resources, you've been able to achieve an impressive accuracy of 86% in detecting suspicious events. Additionally, as you continue to expand your dataset, it's reasonable to expect further improvements in accuracy. Seems well-structured and promising for enhancing public safety and security through the automated detection of suspicious behavior in real-time video footage.

Keywords: LRCN, Convolutional Neural Networks, Deep learning techniques, video footage

1. INTRODUCTION

Project is focused on developing an automated system for detecting suspicious human behavior in real-time using image data. This is indeed a critical application, especially in public spaces where safety and security are paramount.

To create a framework for identifying abnormal activity, you'll likely need to employ techniques from computer vision and machine learning. These could include methods like object detection, tracking, anomaly detection, and possibly even deep learning approaches for more complex behaviors.

The technology you're aiming to develop should be capable of analyzing video footage and identifying behaviors that deviate from normal patterns. This could include actions such as loitering in a certain area for an extended period, sudden movements, unusual interactions between individuals, or any other behaviors that may raise suspicion.

Evaluation of your system will be crucial to assess its effectiveness. This involves testing it on a dataset of video footage containing both normal and suspicious behaviors. You can compare the results of your system with those from earlier trials or existing systems to demonstrate its improvements or advantages. Project has the potential to significantly enhance security measures in various public spaces, providing real-time detection and response to suspicious activities. project focused on enhancing security through the detection of suspicious human behavior in surveillance video footage. Here's a breakdown of the provided information:

Significance:

- ❖ Detection of suspicious human behavior is crucial for enhancing results significantly.
- ❖ The main goal is to contribute to the creation of an effective and precise system for detecting abnormal activity in surveillance video footage.
- ❖ The suggested system can be implemented in various real-world settings, including public safety and homeland security.
- ❖ Its implementation may lead to a decrease in criminal and terrorist activities.

Purpose:

- ❖ The primary purpose of the project is to enhance the accuracy of detecting anomalous activities.
- ❖ It aims to identify suspicious human behavior to enhance security and safety in public areas.
- ❖ The system could be implemented in various open locations, such as theaters and train stations, to provide real-time information about crowd sentiment, identify concerning or suspicious individuals, and issue alerts for potential hazards.

Figure 1 Various Human Activities

2. METHODOLOGY

Automatically detecting suspicious human activity involves employing a combination of tools and technologies from various domains such as artificial intelligence, machine learning, computer vision, data analytics, and cyber security.

Data Collection: Gather data from diverse sources such as surveillance cameras, sensors, social media feeds, network logs, and transaction records.

Preprocessing: Clean and preprocess the data to ensure consistency and compatibility across different sources. This may involve data normalization, transformation, and filtering.

Feature Extraction: Extract relevant features from the data that can provide insights into human behavior. For example, in video data, features like motion patterns, facial expressions, and object interactions can be extracted.

Model Development: Utilize machine learning and statistical models to build algorithms that can identify patterns indicative of suspicious activity. This could involve techniques such as anomaly detection, pattern recognition, and classification.

Training: Train the models using labeled data to recognize different types of suspicious behavior. Supervised learning techniques can be used where labeled examples of both normal and suspicious activities are provided.

Real-time Monitoring: Implement systems capable of monitoring the data streams in real-time. This may involve deploying algorithms on edge devices for faster processing and immediate response to detected anomalies.

Alerting Mechanism: Develop an alerting mechanism to notify relevant authorities or security personnel when suspicious activity is detected. Alerts can be sent via email, SMS, or integrated with existing security systems.

Continuous Improvement: Regularly update and refine the models based on feedback and new data. This involves analyzing false positives/negatives and adjusting the algorithms to improve accuracy and reduce false alarms.

Integration with Existing Systems: Integrate the automated detection system with existing security infrastructure such as intrusion detection systems (IDS), security cameras, access control systems, etc., to enhance overall security measures.

Compliance and Privacy: Ensure that the implementation complies with relevant regulations and privacy laws. Implement measures to safeguard sensitive data and respect individuals' privacy rights.

Usage of Technology

The methodology described in the chapter utilizes cutting-edge technologies in the field of computer vision and machine learning, particularly focusing on deep learning techniques. Deep learning, a subset of machine learning, involves training artificial neural networks with multiple layers to learn representations of data.

Specifically, the image classification methodology leverages a combination of deep learning and machine learning methods, such as Long Short-Term Memory Recurrent Convolutional Networks (LRCN). LRCN is a hybrid model that combines convolutional neural networks (CNNs) for feature extraction from images and recurrent neural networks (RNNs), particularly LSTM (Long Short-Term Memory), for sequential data processing. This combination makes LRCN well-suited for tasks involving both spatial and temporal information, such as video analysis. By employing deep learning techniques like LRCN, the research aims to develop a robust system capable of identifying suspicious behavior in video surveillance footage. Deep learning models excel at learning complex patterns and features from large datasets, which is crucial for tasks like image and video classification in security applications.

Machine learning:- Machine learning is a broad field of study that focuses on developing algorithms and techniques that allow computers to learn from and make predictions or decisions based on data, without being explicitly programmed to do so. It encompasses various methods such as supervised learning, unsupervised learning, semi-supervised learning, reinforcement learning, and deep learning.

In essence, machine learning algorithms learn patterns and relationships from data and use them to make predictions or decisions without explicit programming instructions. These algorithms are used in various applications across industries, including but not limited to image and speech recognition, natural language processing, recommendation systems, autonomous vehicles, medical diagnosis, and financial forecasting.

Deep learning:- Deep learning is a subset of machine learning, which is a branch of artificial intelligence (AI). It's based on the concept of neural networks, which are algorithms inspired by the structure and function of the human brain. Deep learning algorithms attempt to model high-level abstractions in data by using multiple layers of nonlinear processing units. These layers form a hierarchy of features, where each layer's output serves as the input to the next layer.

Deep learning has gained immense popularity and success in recent years due to several factors:

Big Data: Deep learning models require large amounts of data to learn complex patterns and relationships within the data.

Advancements in Hardware: The availability of powerful GPUs (Graphics Processing Units) and specialized hardware like TPUs (Tensor Processing Units) has accelerated the training of deep learning models.

Algorithms and Architectures: There have been significant advancements in algorithms and architectures, such as convolutional neural networks (CNNs) for image recognition, recurrent neural networks (RNNs) for sequential data, and transformers for natural language processing.

Transfer Learning: Pre-trained models and transfer learning techniques allow leveraging knowledge gained from one task or domain to another, reducing the need for large amounts of labeled data.

Deep learning technology finds applications in various fields such as computer vision, natural language processing, speech recognition, healthcare, finance, and autonomous vehicles, among others. Its ability to automatically learn hierarchical representations from data makes it a powerful tool for solving complex problems across different domains.

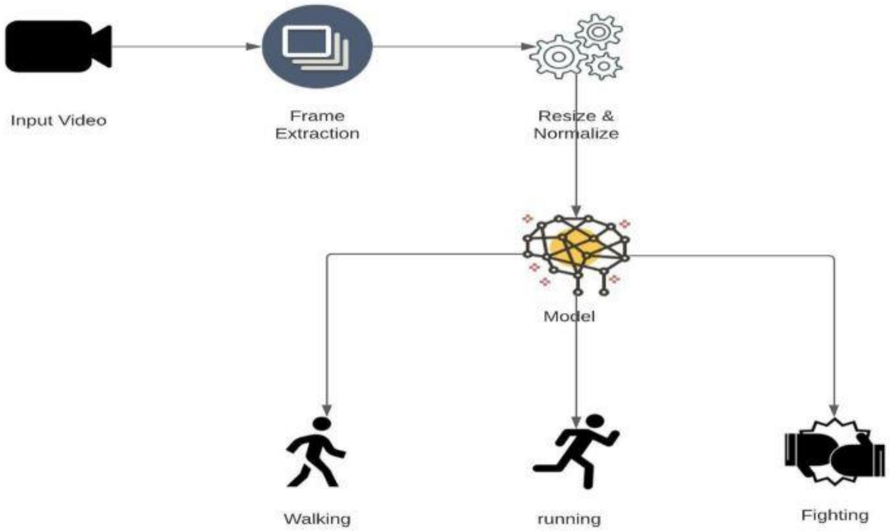

Figure 2 action of human activity

3. RESULT

Several improvements to your model for detecting suspicious behavior in videos. Reducing the number of layers in the LSTM architecture from 16 to 12 is likely to have sped up processing significantly while still maintaining a high level of accuracy at 86%. Resizing frames from 224px to 64px would also have helped conserve memory without sacrificing too much detail, especially if the primary focus is on detecting overall behavior rather than fine-grained visual details.

Adding more videos to the dataset, especially those depicting both suspicious behavior like fighting and typical behavior like walking and running, is a smart move. A diverse dataset helps ensure that the model learns to generalize well across different scenarios, leading to more robust performance in real-world applications.

Describing a training process for a machine learning model, possibly a neural network. The "train loss" typically refers to the loss function evaluated on the training dataset, which quantifies how well the model is performing on that dataset during training. Epochs represent one complete pass through the entire training dataset during the training process. The vertical line, often referred to as the y-axis, usually represents the value of the loss function, which is a measure of how well the model's predictions match the actual targets in the training data. Each point on the graph represents the loss (error) at a particular epoch during training. By observing how the loss changes over epochs, you can understand how the model's performance improves or deteriorates during training.

4. CONCLUSION

An impressive achievement! Incorporating more relevant data sounds like a promising approach to further improve the model's performance. There are several avenues you could explore:

Data Augmentation: You can synthetically increase your dataset by applying transformations to existing images, such as rotation, scaling, or adding noise. This can help generalize the model better.

More Diverse Data: Collecting data from a wider range of sources and environments can help the model learn to handle various scenarios and conditions. This might involve different lighting conditions, camera angles, or even cultural contexts.

Fine-tuning Pre-trained Models: If you're using pre-trained models, fine-tuning them on your specific dataset can often yield better results. This involves training the model on your data while keeping the initial weights from the pre-trained model.

Ensemble Methods: Combining predictions from multiple models can often lead to better performance than any individual model. You could try ensemble methods like bagging or boosting to improve accuracy.

Advanced Architectures: Experimenting with more complex architectures or state-of-the-art models in the field of computer vision, such as Transformers or more advanced variants of CNNs, could also lead to improvements.

Data Cleaning and Balancing: Ensuring that your dataset is clean and balanced can significantly impact model performance. Removing noisy or irrelevant data and balancing the classes can prevent the model from being biased towards the majority class.

Regularization Techniques: Applying techniques like dropout or L2 regularization can help prevent over fitting, especially when dealing with large amounts of data.

Hyper parameter Tuning: Optimizing the hyper parameters of your model, such as learning rate, batch size, and optimizer choice, can often lead to performance improvements.

5. REFERENCES

[1] C. V. Amrutha, C. Jyotsna, J. Amudha (2020) Deep learning Approach for suspicious activity detection from surveillance video, Publisher IEEE Bangalore www.ieeexplore.ieee.org/document/9074920 (Original work published 2020)

[2] Jason Brownlee, Introduction to the adam-optimization-algorithm-for-deep-learning [python], Latest update on January 13, 2021. www.machinelearningmastery.com/adam-optimization-algorithm-for-deep-learning (Original work published 2017)

[3] Mark Daoust (2022). Sequential model, Model Creation [python].Tensor Flow is a platform that makes it easy to build and deploy ML models. www.tensorflow.org/guide/keras/ (Original work published on 2022)

[4] Sik-Ho Tsang (2022) LRCN: Long-term Recurrent Convolution Networks[Python] https://sh-tsang.medium.com/brief-review-lrcn (Original work published on 2022. 41

[5] Dinesh Jackson, “suspicious activity detection in surveillance video using discriminative deep belief network,” International Journal of Control Theory and Applications, Volume 10, Number 29 - 2017.

[6] P. Bhagya Divya, Sravya Reddy, published an article in the International Research Journal of Engineering and Technology titled “Inspection of suspicious human activity in the crowdsourced areas captured in surveillance cameras”, December 2017.

[7] Elizabeth Scaria, Aby Abahai T and Elizabeth Isaac, “Suspicious Activity Detection in surveillance Video using Discriminative Deep Belief Netwok”, International Journal of control Theory and Applications Volume 10, Number 29 ---2017