Suspicious Activity Recognition Using Machine Learning

PROJECT SYNOPSIS

BACHELOR OF TECHNOLOGY

Artificial Intelligence and Data Science

Submitted By:

Harshul, 2121723
Aarzoo Sharma, 2121695
Deepakshi Sharma, 2121714

Guided By:

Ms. Chaahat Gupta

Chandigarh Group of Colleges

College of Engineering, Landran

Jan,2024

Introduction

Background

This project revolves around the critical task of promptly identifying potentially suspicious human behavior in real-time, leveraging the ubiquity of image capture and the abundance of available data. The escalating demand for automated systems capable of swiftly detecting abnormal activities becomes particularly imperative in public areas such as bustling shopping malls, frequented public parks, and busy train stations, where the assurance of security and safety is paramount [5]. The primary and overarching objective is to meticulously establish a comprehensive framework proficient in recognizing and promptly flagging unusual activities.

The ultimate pinnacle of achievement for this project lies in the development of cutting-edge technology meticulously crafted to precisely pinpoint suspect human behavior as it unfolds in the dynamic realm of real-time scenarios. Through a rigorous evaluation process, employing a diverse and extensive dataset comprising video footage capturing various scenarios, the project's outcomes are methodically scrutinized and compared with results obtained from prior trials. This ambitious endeavor aspires to make a substantial and tangible contribution to the continuous enhancement of the efficacy of surveillance and security measures in a diverse array of public spaces.

In essence, the project not only aims to address the pressing need for rapid identification of suspicious activities but also endeavors to push the boundaries of technological innovation, serving as a pioneering force in the ongoing evolution of surveillance systems designed to uphold safety and security in our ever-evolving urban landscapes.

Furthermore, the technological strides made in this project extend beyond the immediate objective of recognizing unusual behaviors in real-time. The developed framework is poised to act as a catalyst for advancing the broader field of artificial intelligence and computer vision applications. By pushing the boundaries of innovation, this project seeks to set a precedent for the seamless integration of cutting-edge technology into existing surveillance infrastructures, fostering a symbiotic relationship between human operators and automated systems.

Project Milestones

Research and Literature:

The initial phase of the project involves undertaking research and conducting a thorough literature review to acquire a profound comprehension of the current state of detecting suspicious human activity. This includes an exploration of various deep learning-based strategies that have been proposed in the existing body of knowledge.

Data Acquisition:

The next crucial step involves the compilation of a comprehensive data set comprising labeled videos, intended for training, and testing the suggested system. Assemble a set of labeled videos to be utilized for both training and testing the proposed system. The dataset should encompass a diverse array of abnormal behaviors, as well as typical activities, to facilitate comparative analysis.

Image Pre-Processing:

It is of paramount importance to undergo meticulous pre-processing of the video clips before integrating them into the deep learning framework. This critical step encompasses a series of tasks, including the enlargement of frames, selective cropping of pertinent areas, and the normalization of pixel values. These measures collectively contribute to optimizing the input data for enhanced interpretability and efficacy within the deep learning model.

Model Design:

During the model design phase, a sophisticated deep learning architecture is crafted, likely incorporating both Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN). RNNs are adept at temporal analysis, discerning patterns over time, while CNNs excel in extracting robust features, enhancing the model's ability to capture intricate details within the data. This synergistic approach ensures a comprehensive model design tailored for effective identification of suspicious human behavior.

Model Training & Testing:

The collected dataset plays a crucial role in training and testing the model, assessing its performance through metrics like recall, accuracy, and precision. This approach enables iterative refinement and fine-tuning of the model, enhancing its capacity to detect and respond to suspicious human behavior. By systematically adjusting parameters based on performance metrics, the model evolves, ensuring an optimized and effective system for the identification and mitigation of potential security threats in public spaces.

Significance

The identification of suspicious human behavior presents a transformative opportunity to significantly enhance outcomes. The primary goal is to actively contribute to developing a sophisticated and precise system for detecting abnormal activities in surveillance video footage, with applications in public safety and homeland security. This envisioned system aims to seamlessly integrate into real-world settings, promising a tangible reduction in criminal and terrorist activities.

To achieve this goal, advanced behavioral analysis algorithms will discern intricate patterns and swiftly identify deviations, indicating potential threats. Integrating multi-modal data, including video feeds, audio, and sensor data, is pivotal for a comprehensive understanding of the surveillance environment. Emphasizing anomaly detection, distinguishing between benign and hazardous anomalies, refines the system's effectiveness.

Real-time processing capabilities are crucial, ensuring prompt identification and response to anomalies, minimizing vulnerability windows. The system's scalability and adaptability are paramount, accommodating diverse environments and evolving threat landscapes. Privacy concerns are addressed through measures like anonymization and encryption, ensuring individual rights are safeguarded. This envisioned system aspires to redefine surveillance paradigms for a safer and more secure future.

Purpose

This project aims to significantly enhance anomaly detection accuracy, focusing on identifying suspicious human behavior to bolster security in public spaces. The tailored system provides real-time crowd sentiment information, issuing hazardous signals for prompt response to potential threats. Its adaptability and proactive monitoring contribute to a comprehensive solution, elevating security standards across diverse public settings. Here's an explanation of each term in the context of the project:

Abuse: This refers to instances of verbal, physical, or emotional mistreatment that may pose a threat to public safety. Detection of aggressive or harmful behavior is crucial for preemptive intervention.

Arrest: This indicates the apprehension of individuals engaging in unlawful activities. The project may involve identifying behaviors leading to potential arrests, contributing to law enforcement efforts.

Arson: This involves the deliberate act of setting fire to property. Detecting signs of arson is vital for preventing potential harm to people and structures, making it a target for the project's surveillance capabilities.

Assault: This refers to intentional acts of physical harm. The project seeks to identify and address aggressive behavior that may lead to assaults, thereby contributing to public safety.

Burglary: This involves unauthorized entry into premises with the intent to commit a crime. The project aims to detect suspicious behavior associated with burglary, aiding in the prevention of property crimes.

Explosion: This signifies a sudden and violent release of energy. Detecting indicators of potential explosive activities is crucial for mitigating the risk of harm in public areas.

Fighting: The project aims to identify and address physical altercations or "fighting" scenarios. Detecting early signs of confrontations contributes to the prevention of violence in public spaces.

Road Accidents: Detection of "road accidents" involves monitoring and responding to traffic incidents. This aspect of the project contributes to public safety on roadways by identifying and responding to accidents promptly.

Robbery: This entails the use of force or threats to commit theft. Detecting suspicious behavior associated with robbery is critical for preventing crimes against individuals.

Shooting: The project focuses on the identification of gun-related activities or "shooting" incidents. Early detection can lead to a swift response and the prevention of potential casualties.

Shoplifting: This involves stealing merchandise from retail establishments. Detecting signs of shoplifting contributes to loss prevention and ensures the safety of both customers and store personnel.

Stealing: This term broadly refers to the act of taking something unlawfully. In the context of the project, it involves identifying suspicious behavior associated with theft or stealing in public areas.

Vandalism: This pertains to the willful destruction or defacement of property. Detecting signs of vandalism contributes to the preservation of public spaces and structures.

In conclusion, the project strives to pioneer an advanced surveillance system, adept at swiftly identifying and responding to diverse suspicious activities, bolstering public safety and security. By incorporating a comprehensive array of terms, the framework promises a holistic approach to risk detection across various public settings. This initiative not only aims to elevate real-time anomaly identification but also sets new benchmarks in technology integration, contributing significantly to the ongoing evolution of surveillance systems for safer, more resilient urban environments.

Methodology/ Planning of work

Data Collection and Preprocessing (Weeks 1-4):

Outline the process for data collection, including any necessary permissions or ethical considerations. Plan for data preprocessing tasks, such as cleaning, normalization, and feature extraction.

Feature Selection and Model Selection (Weeks 5-8):

Detail the criteria for selecting relevant features for suspicious activity detection. Allocate time for any necessary model fine-tuning and hyperparameter optimization.

Training the Model (Weeks 9-12):

Divide the dataset into training and validation sets. Implement the selected model and train it on the prepared data. Monitor and adjust the training process as needed to ensure optimal performance.

Evaluation Metrics and Testing (Weeks 13-16):

Define the evaluation metrics that will be used to assess the model's performance. Analyze the results and make any necessary adjustments to improve performance.

Documentation and Reporting (Weeks 17-20):

Document the entire project, including methodologies, codebase, and results. Prepare a comprehensive report summarizing the project's findings, challenges, and contributions.

Review and Iteration (Weeks 21-22):

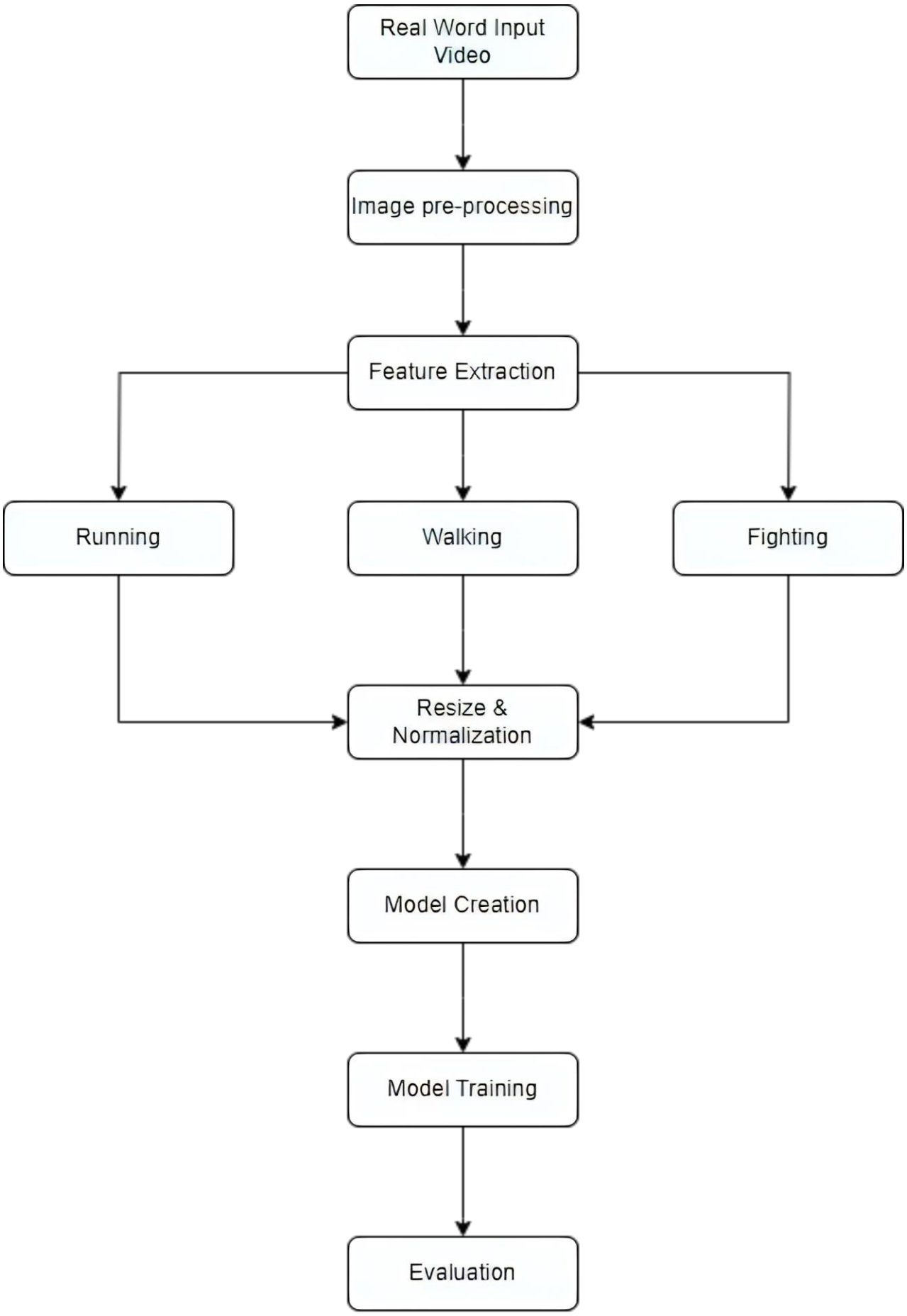
Conduct a thorough review of the project, seeking feedback from peers or mentors. Identify any areas for improvement or further iterations.

Conclusion and Future Work (Week 23):

Summarize the overall project, highlighting achievements and insights gained.

Discuss potential avenues for future work or enhancements to the system.

State Diagram



Facilities

Google Colab

Google Colab stands as a cloud-based powerhouse for training machine learning models, offering an ideal environment for tasks spanning machine learning, coding, and analysis. Particularly noteworthy is its integration of Graphical Processing Units (GPUs), a critical feature for expedited model training, especially in the context of larger neural networks. Leveraging Google Colab, the project focuses on training deep learning models specialized in classifying suspicious activities. Furthermore, the platform serves as a version control tool, aiding in the meticulous tracking of different model versions and iterations, ensuring a streamlined development process.

Python

Python, a dynamically typed and garbage-collected programming language, plays a pivotal role in the project's ecosystem. Renowned for its versatility, Python finds application in diverse domains, encompassing software development, website creation, automation, computation, and data analytics. Python frameworks such as Flask and Django contribute to the seamless development of applications with varied functionalities, adding to the project's adaptability and efficiency.

Sklearn

Sklearn, integrated for its compatibility with scientific and numerical libraries, enriches the project with an array of clustering, classification, and regression methods, facilitating robust model development. TensorFlow, another integral component, is a comprehensive machine learning platform that supports distributed and multi-GPU processing. It provides essential features such as automatic differentiation, model development, training, assessment, and multidimensional numerical calculations.

NumPy

NumPy is a powerful numerical computing library in Python, providing support for large, multi-dimensional arrays and matrices, along with a collection of mathematical functions to operate on these arrays. It facilitates efficient data manipulation and mathematical operations, crucial for tasks in data science, machine learning, and scientific research. NumPy's array-oriented computing paradigm enhances code readability and execution speed.

TensorFlow

TensorFlow serves as a fundamental technology for developing and training deep learning models. Its capabilities in distributed processing and multi-GPU support are crucial for accelerating the training of complex models designed to classify suspicious activities. This framework plays a pivotal role in achieving the project's objective of enhancing accuracy in detecting anomalous activities and contributes to the overall success of the machine learning-based surveillance system.

OpenCV

OpenCV (Open-Source Computer Vision Library) is a versatile open-source computer vision and machine learning software library. Developed in C++ and Python, it provides a rich set of tools for image and video analysis, including algorithms for object detection, facial recognition, and image processing. Its extensive functionality, ease of use, and active community support make it a preferred choice for researchers and developers working on various computer vision applications.

Keras

Keras, a modular neural network library, is instrumental in the project for its seamless integration with TensorFlow. Prioritizing quick experimentation, Keras simplifies the development of intricate neural network architectures. Its high-level abstraction allows for swift model prototyping, making it an ideal choice for the project's goal of classifying suspicious activities. Leveraging Keras on top of TensorFlow enhances efficiency, enabling rapid iteration.

References

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

(Original work published 2020)

[2] Mark Daoust (2022). Sequential model, Model Creation [python], TensorFlow is a platform that makes it easy to build and deploy ML models.

https: www.tensorflow.org/guide/keras/

(Original work published on 2022)

[3] Sik-Ho Tsang (2022) LRCN: Long-term Recurrent Convolution Networks [Python]

https://sh-tsang.medium.com/brief-review-lrcn

(Original work published on 2022)

[4] CVPR (Conference on Computer Vision and Pattern Recognition), ICCV (International Conference on Computer Vision), or ACM Multimedia for research papers on video analysis and anomaly detection.

https://pubmed.ncbi.nlm.nih.gov/

(Original work published on 2022)