Technical Report

Technical Report for Real-time Anomaly Detection in Video Surveillance

I. Introduction

The increasing use of surveillance cameras in the United States, driven by technology and security concerns, has led to a reliance on human operators for monitoring and anomaly detection. However, human operators have limitations such as fatigue and distraction. To address this, real-time automatic anomaly detection in video surveillance is crucial. This system can continuously monitor and promptly respond to unusual activities, enhancing security by detecting crimes like shootings, shoplifting, assault, and robbery. Furthermore, it serves as an early threat detection tool, identifying suspicious events like robbery, unusual vehicle movements, etc. Rapid anomaly detection enables quicker responses from security personnel and law enforcement, reducing the risk of danger or damage.

II. Data Preprocessing

Preprocessing video data for real-time anomaly detection in video surveillance involves several steps to ensure that the data is prepared, cleaned, and transformed in a way that facilitates accurate anomaly detection. Here are the key steps:

1. **Data Collection:** Gather video data from surveillance cameras, which can be in the form of video streams or recorded footage. Ensure that the data is timestamped to maintain temporal information.
2. **Frame Extraction:** To working with video streams, extract individual frames from the video to process them individually.

```
# frame extraction
video_capture = cv2.VideoCapture("video_stream.mp4")
```

3. **Removing duplicate frames:** Eliminate identical frames to reduce redundancy. This will significantly decrease number of frames to process.
4. **Data Normalization:** Normalize the extracted features to have consistent scales and distributions. This step is crucial for ensuring that different features are treated equally during anomaly detection.
5. **Data Splitting:** Splitting the data into train, test, and validation datasets. So that we can train the model with these datasets.

III. Data Analysis

1. **Temporal Analysis:** Analyze the temporal behavior of objects or regions of interest across multiple frames. Detect anomalies by identifying deviations from typical object behavior over time.
2. **Thresholding:** Set appropriate thresholds for anomaly scores or probabilities to classify detected anomalies as genuine or false positives.

3. **Model Updating:** Periodically update the background models, feature extraction methods, and anomaly detection algorithms to adapt to changing environmental conditions and maintain accuracy.
4. **Evaluation and Fine-tuning:** Continuously evaluate the performance of the anomaly detection system and fine-tune parameters and algorithms to minimize false positives and improve detection accuracy.

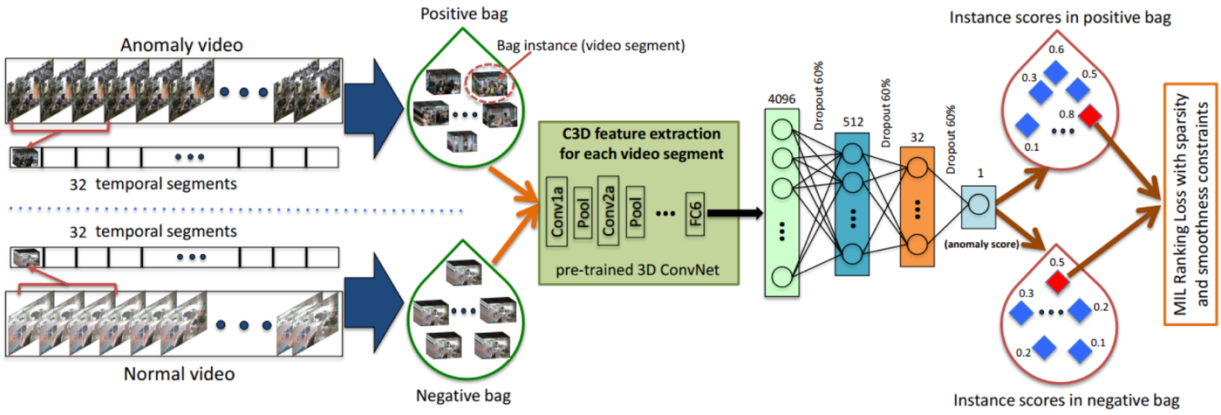
IV. Notification and Logging

1. **Alert Generation:** Generate alerts or notifications when anomalies are detected. This may involve sending alerts to security personnel or triggering other actions to address the anomaly. Some ways are through email, message through subscripted phone, and notification through application.
2. **Logging and Storage:** Log the detected anomalies and associated information for future analysis and auditing. Store the preprocessed video data, anomalies, and alerts for reference and evidence.

V. Methodology

- **I3D (Inflated 3D ConvNet)**
  - 3D Convolutional Layers: I3D uses 3D convolutional layers that operate on video data, capturing spatial and temporal features simultaneously.
  - Inflated Weights: Initializing the 3D convolutional layers with 2D convolutional filters pretrained on large-scale image classification datasets. These pretrained weights helps in transfer learning and faster convergence.
  - Two-Stream Architecture: I3D typically employs two parallel streams of networks: one for RGB frames and another for optical flow. This enables the model to analyze both frame content and motion patterns.
- **Video Explainity Methods**
  - Use LIME, sharp, or CLAD to explain why the detection decision was made

VI. Model Visualization



[1] Figure 1. The flow diagram of proposed anomaly detection

VII. Conclusion

In conclusion, this paper has underscored the critical importance of real-time anomaly detection in video surveillance systems, emphasizing its role in enhancing societal security. We have discussed the significance of early threat detection, scalability, reduced false positives, proactive response, and emergency notification as key objectives in the context of this technology.

VIII. References

[1] https://www.crcv.ucf.edu/projects/real-world