Suspicious Activity Detection in ATM

Deepali Ahir[1], Vaibhav Shinde[2], Ashutosh Devanpalli[3], Aniket Dhole[4], Aditya Wagh[5]

Modern Education Society's Wadia College Of Engineering

Abstract— In today's volatile culture, video surveillance systems are critical for ensuring both inside and outdoor security. Real-time applications can benefit from video surveillance characteristics such as behavior identification, comprehension, and the capacity to classify actions as normal or suspicious. People are at risk when it comes to the potential dangers posed by suspicious actions. As crime rates rise, it is critical to detect criminal behavior in urban and suburban areas in order to reduce such incidents. Initially, people conducted surveillance manually, which was extremely exhausting because suspicious activity was unusual in comparison to regular operations. Automated Teller Machines (ATMs) provide convenient access to financial activities without the need for interaction with bank authorities. However, ATM attacks remain a significant issue, despite security precautions in place. The current study focuses on a survey of preventive measures taken to prevent ATM theft. To prevent ATM thefts and respond quickly, a completely automated system is needed.

Keywords— Suspicious behavior, Anomaly Detection, Machine Learning, Video surveillance

I. INTRODUCTION

Worldwide, crime and violence have increased in recent years. A range of tools are used to reduce or eliminate the problem. Video surveillance is the appropriate solution for both public and private places. The video surveillance system is considered effective when it successfully detects abnormal or suspicious activity. Humans manage the vast majority of today's monitoring systems. As a result, in order to detect any curious activity, they require continuous human inspection. When humans are involved, the system's effectiveness eventually decreases due to human weariness. Video surveillance automation can help to tackle this problem. Computer vision works to create intelligent apps that perceive images and movies similarly to people. Computer vision focuses on detecting, recognizing, and tracking. Detection and recognition are frequently utilized in several applications, including security, surveillance, and traffic control. One goal is to monitor and recognize people's physical activities. To detect suspicious human activity, it's necessary to detect and track individuals across several video frames. Effective video surveillance detects aberrant or suspicious activity efficiently. The majority of surveillance systems nowadays are operated by humans. We are implementing an algorithm to improve detection, recognition, and tracking.

For almost 30 years, consumers have relied on and trusted ATMs to meet their financial needs. ATMs are often positioned in public areas, making them vulnerable to attacks, as they do not require constant monitoring by humans.

Automated teller machines aid humans with financial transactions during emergencies. Detecting human activity in busy situations is a difficult job in computer vision. Crowd scene analysis is critical in computer vision since detecting individual human activities remains difficult. Anomaly detection is becoming more significant in a variety of businesses, including prisons, fire departments, public safety organizations, and finance.

Existing ATM systems require automatic security warning systems that allow customers to securely access the ATM. Despite the fact that the government and financial authorities have put in place a variety of safety measures, the human security system continues to cost more. Suspicious actions are defined using a semantic method, based on understanding by humans.

Here, a low-cost, real-time automated ATM security system based solely on video surveillance detection is proposed. The study's purpose is to check for a variety of unusual activities, such as a large number of people using the ATM, removing cameras from the system (even if some camera masking is used), and even detecting instances of persons using the system while wearing helmets.

II. Scope

- The scope would involve analyzing ATM video footage, using computer vision algorithms to spot unusual behavior, and enhancing security procedures to prevent unauthorized access.

- To enhance ATM security, detect suspicious behavior in real time, and safeguard users against fraud.

Disrelated Work

In 2022, et al Sridevi S have researched A method for recognizing unauthorized ATM users is proposed. By polishing their features and storing the datasets, several assumptions are made, one of which is the identity context. However, not everyone will be suspected. suspicious activity on ATMs in isolated places and to reduce the potential of fraudulent acts, such as taking out cash with someone else's card. Several video surveys and image processing approaches have been discussed in the context of surveillance.

In 2022, et al. Valarmathi R have explained the proposed strategy can help to prevent ATM robberies. Criminals utilize multiple tactics to steal money from ATMs. The suggested system seeks to prevent all of these tactics, including the most prevalent one employed by thieves, stabbing victims, even though there is no practical remedy and the money was stolen. The initiative's main objectives are to detect and prevent ATM fraud.

In 2023, et al. Sheelambigai P have researched Criminal activity and suspicious situations are on the rise on the earth. Humans cannot monitor all of the illegal activity that occurs on a daily basis. To avoid manual monitoring, the automated monitoring system for suspicious activities is activated. The major purpose of this proposed activity monitoring system is to use machine learning to identify and warn users when problematic conduct is detected. YOLO is used in this study to detect a number of problematic behaviors, including chain snatching.

In 2020, et al. Nipunjita Bordoloi have researched Human activity detection for video systems is an automated way of studying video sequences and drawing precise conclusions about the actions in the film. It is one of the rapidly emerging topics of artificial intelligence and computer vision. Suspicious activity detection is the practice of detecting unwanted human behavior in specific areas and situations. This is performed by converting video into frames, which are then used to assess human activities. Detecting humans has always been challenging since human bodies are flexible and can change shape at will.

In 2018, .Ms.U.M.Kamthe have researched This study uses a hierarchical approach to detect a variety of suspicious behaviors, including but not limited to loitering, fainting, and unauthorized access. The motion characteristics of the various components serve as the basis for this method. First, the semantic approach is utilized to define the different dubious actions. Object detection is then carried out using background subtraction. The detected goods are then classified as non-living (bag) or living (person). These things must be tracked, which is done using the correlation technique. Ultimately, the episodes are classified as normal or suspicious based on the motion features and temporal data.

III. Objective

.

- To generate machine learning Model with better accuracy.

- Identify unusual patterns and anomalies.

- Improve customer confidence in using ATM’s.

V. Algorithm

CNNs are a type of deep learning algorithm that is often used to analyze images and videos. The Convolutional Neural Network (CNN) is an important tool for detecting suspicious activity in ATM video data. CNN is a deep learning system capable of analyzing images and videos. Using CNN in this

study aids in detecting trends, anomalies, and probable fraudulent behavior in real time from video data.

1.Data Preparation: The video might illustrate how video footage captured by ATMs is preprocessed. This can include procedures such as reducing frames, converting them to grayscale, and separating the video into individual frames.

2. Convolutional Layers: The video demonstrates that the CNN algorithm applies convolutional layers to extract information from each frame. These layers apply filters to the frames, highlighting patterns and edges that can help spot suspect activity.

3. Pooling Layers: The video may show how pooling layers reduce maps of features generated by convolutional layers. Pooling reduces the spatial dimensions of the features while retaining the most important data.

4. Fully Connected Layers: The video shows how flattened and pooled attributes are fed into fully connected layers. These layers investigate the deep relationships between features and make predictions based on them.

5.Training: The video might demonstrate how the CNN algorithm is trained on labelled video data.

6.Suspicious Activity Detection: The video can explain how the trained CNN model is then applied to new video footage from ATMs. It explains how the model uses learned patterns and attributes to determine whether an observed action is suspicious or not.

VI. System Architecture

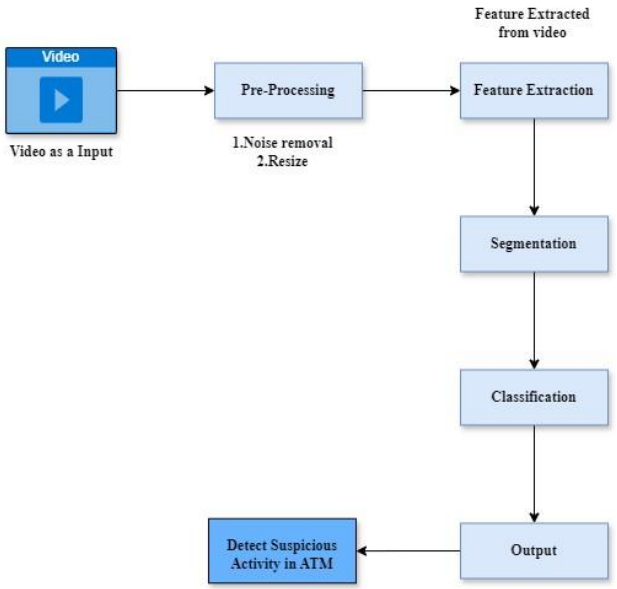

Fig: System Architecture

VII. Proposed Work

1. Data Collection: The first step is to collect video footage from ATMs.

2. Preprocessing: The collected video data needs to be preprocessed to enhance its quality and extract relevant information. This can involve tasks like resizing the frames, converting them to grayscale, and removing any noise or distortions.

3. Feature Extraction: Features are extracted from each frame to capture important information.

Model Training: A machine learning model, such as a CNN, is trained using labeled data. The model learns to recognize patterns and distinguish between normal and suspicious activities.

VIII. Conclusion

In Conclusion , To improve security processes and ensure ATM users' safety. The technology may recognize suspicious patterns or actions by analyzing video footage in real time, extracting features, and training machine learning models. This allows you to investigate and respond immediately to activities that have been identified. However, it is necessary to address limits such as ethical considerations, interpretability concerns, and data quality. Human knowledge is required for further analysis and decision-making. Over time, updating and improving the model can help to boost the system's effectiveness. Overall, the technology has a great deal of potential to improve ATM

security and protect users from potential threats. Users from potential risks.

IV. References

1. Sridevi, S., K. M. Monica, G. A. Senthil, R. Prabha, A. Sathya, and J. Ramya. "Third Generation Security System for Face Detection in ATM Machine Using Computer Vision." In *2022 International Conference on Computer, Power and Communications (ICCPC)*, pp. 143-148. IEEE, 2022.

2. Valarmathi, R., M. Divya, S. Divyashree, and U. Vidhyashree. "ATM Fraud Detection Using Human Activity Recognition." In *2022 1st International Conference on Computational Science and Technology (ICCST)*, pp. 798-802. IEEE, 2022.

3. Raja, D. Prem, P. Sheelambigai, and K. Valarmathi. "Suspicious activity monitoring system using machine learning." In *2023 8th International Conference on Communication and Electronics Systems (ICCES)*, pp. 1-5. IEEE, 2023.

4. Bordoloi, Nipunjita, Anjan Kumar Talukdar, and Kandarpa Kumar Sarma. "Suspicious activity detection from videos using yolov3." In *2020 IEEE 17th India Council International Conference (INDICON)*, pp. 1-5. IEEE, 2020.

5. Kamthe, U. M., and C. G. Patil. "Suspicious activity recognition in video surveillance system." In *2018 Fourth international conference on computing communication control and automation (ICCUBEA)*, pp. 1-6. IEEE, 2018.

6. S. Loganathan, G. Kariyawasam and P. Sumathipala, "Suspicious Activity Detection in Surveillance Footage," *2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, Ras Al Khaimah, United Arab Emirates, 2019, pp. 1-4, doi: 10.1109/ICECTA48151.2019.8959600.

7. S. S. Gurav and V. V. Khandare, "Performance Evaluation of Automatic Suspicious Activity Detection Method," *2023 International Conference for Advancement in Technology (ICONAT)*, Goa, India, 2023, pp. 1-4, doi: 10.1109/ICONAT57137.2023.10080627.

8. C. V. Amrutha, C. Jyotsna and J. Amudha, "Deep Learning Approach for Suspicious Activity Detection from Surveillance Video," *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, Bangalore, India, 2020, pp. 335-339, doi: 10.1109/ICIMIA48430.2020.9074920.

9. . S. Dileep, N. S. S., S. S., F. K. and S. S., "Suspicious Human Activity Recognition using 2D Pose Estimation and Convolutional Neural Network," *2022 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET)*, Chennai, India, 2022, pp. 19-23, doi: 10.1109/WiSPNET54241.2022.9767152.

10. H. Samir, H. E. Abd El Munim and G. Aly, "Suspicious Human Activity Recognition using Statistical Features," *2018 13th International Conference on Computer Engineering and Systems (ICCES)*, Cairo, Egypt, 2018, pp. 589-594, doi: 10.1109/ICCES.2018.8639457.