Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
DOI: https://doi.org/10.17762/msea.v70i2.2471

Anomalous Behavior Detection in ATM using Artificial Intelligence

Abhishek Jain
Associate Professor, School of Computing, Graphic Era Hill University,
Dehradun, Uttarakhand India 248002

Article Info
Page Number:1785 - 1792
Publication Issue:
Vol 70 No. 2 (2021)

Article History
Article Received*: 05 September 2021*
Revised*: 09 October 2021*
Accepted*: 22 November 2021*
Publication*: 26 December 2021*

Abstract

This paper proposes a new supervised algorithm for detecting abnormal events in confined areas such as ATM rooms and server rooms. The objective of this work is to establish a robust technical foundation that supports a secure and convenient social infrastructure, with abnormal behavior detection using image processing being one of the key technologies. Abnormal behavior detection involves creating a model based on normal behavior data and identifying any behavior that deviates from this model as abnormal. However, collecting comprehensive abnormal behavior data in advance can be challenging. Therefore, the ability to detect abnormalities using a model built solely on normal behavior data is highly valuable for practical implementation. This proposed work presents examples of abnormal behavior detection using image processing techniques applied to ATM surveillance videos. Additionally, typical examples of abnormal behavior detection through motion image processing are demonstrated. Furthermore, our approach enhances system security by verifying the identity of the cardholder during ATM transactions. The combination of image processing algorithms and supervised learning enables effective identification of abnormal events, contributing to a more secure and reliable social infrastructure.

1. Introduction

Automated Teller Machines (ATMs) play a vital role in modern banking, providing convenient and accessible services to customers worldwide. However, the increasing prevalence of fraudulent activities and security breaches necessitates the development of robust systems for detecting anomalous behavior in ATMs. Traditional rule-based approaches often struggle to keep pace with evolving attack techniques, making it essential to explore the potential of artificial intelligence (AI) techniques. This paper aims to investigate and evaluate various AI-based approaches, including machine learning and deep learning algorithms, for the detection of anomalous behavior in ATMs, thus enhancing security measures and safeguarding financial transactions.

In recent years, machine learning techniques have shown promising results in anomaly detection tasks. These algorithms can learn patterns and behaviors from large datasets, enabling the identification of deviations from normal patterns exhibited by legitimate ATM transactions. Supervised learning algorithms such as Support Vector Machines, Random Forests, and Naive Bayes can be trained on labeled datasets to classify transactions as normal or anomalous. Unsupervised learning algorithms like k-means clustering and Gaussian Mixture Models are also employed to identify anomalies without prior knowledge of specific anomaly instances. These machine learning techniques offer the potential to detect a wide range of anomalous behaviors, including card skimming, cash trapping, and unauthorized access.

Deep learning techniques, specifically deep neural networks, have shown remarkable performance in various computer vision and pattern recognition tasks. In the context of ATM anomaly detection, Convolutional Neural Networks (CNNs) and Recurrent Neural Networks

(RNNs) have gained significant attention. CNNs excel at extracting spatial features from images or video frames captured by ATM cameras, allowing for the detection of suspicious activities such as loitering, vandalism, or physical tampering. RNNs, on the other hand, are adept at capturing temporal dependencies and sequence modeling, making them suitable for analyzing transaction sequences and identifying abnormalities based on patterns and trends in ATM usage. Effective feature extraction is critical for accurate anomaly detection in ATMs. Statistical features such as mean, standard deviation, and skewness capture distributional characteristics of transaction data, aiding in the identification of outliers. Time-series analysis techniques, Fourier transforms, wavelet analysis, or spectral analysis can extract relevant features from ATM transaction sequences, enabling the detection of unusual patterns and trends. By leveraging appropriate feature extraction methods, the AI-based anomaly detection systems can effectively identify a wide range of suspicious activities in real-time, minimizing the risks associated with fraudulent behaviors.

The application of AI techniques, including machine learning and deep learning algorithms, along with appropriate feature extraction methods, holds significant potential for detecting anomalous behavior in ATMs. By enhancing the security measures and mitigating risks, these AI-based systems can help ensure the integrity of financial transactions and protect customers' sensitive information. This paper will explore and evaluate various approaches in this domain, aiming to contribute to the development of robust and efficient anomaly detection systems for ATM security.

2. Literature Review

Archana Kande et al [1] presented a study on the detection of abnormal events in ATM systems using image processing based on IoT technologies. The authors proposed a method that leverages image processing algorithms and the Internet of Things to enhance the security of ATM systems. By analyzing visual information captured by surveillance cameras, they aimed to identify abnormal activities and potential security threats. The study likely involved the use of image processing techniques such as object detection and motion analysis, as well as the integration of sensors and real-time data analysis.

A. Parab et al. [2] proposed a new approach to detect anomalous behavior in ATMs. The authors focused on utilizing machine learning techniques for anomaly detection in ATM transactions. They introduced a method that combines multiple features and employs a classification algorithm to identify suspicious behavior. The approach showed promise in detecting abnormal activities in ATM systems.

A. Khaleghi et al. [3] introduced an advanced method for anomaly detection in surveillance videos using deep learning techniques. The authors proposed a novel approach that combined convolutional neural networks (CNNs) and recurrent neural networks (RNNs) to extract both spatial and temporal features, enabling effective identification of anomalies. The results showed significant improvements in performance compared to conventional methods, highlighting the potential of deep learning for anomaly detection in surveillance videos.

Tripathi et al [4] proposed a robust abnormal event recognition method through motion and shape analysis at ATM installations. The paper focused on analyzing motion and shape features to detect abnormal events in surveillance videos. The authors employed background subtraction and contour analysis techniques to identify anomalies. The proposed method showed promising results in identifying suspicious activities at ATM locations.

Arpitha K et al [5] presented a vision-based anomaly detection system for ATMs. The paper introduced a computer vision approach to detect suspicious activities at ATM locations. The authors utilized motion detection and optical flow techniques to identify anomalies. The proposed system demonstrated effectiveness in detecting abnormal behavior in real-time surveillance videos.

Liu C et al [6] proposed an anomaly detection method in surveillance video using motion direction statistics. The paper focused on utilizing motion direction statistics to identify anomalous events in surveillance videos. The authors analyzed the motion directions of objects and employed a statistical model to detect abnormalities. The proposed method showed promise in detecting unusual activities in surveillance scenarios.

Hasan et al [7] conducted a survey on human-computer interaction for vision-based hand gesture recognition. The paper provided an overview of various techniques and approaches for hand gesture recognition in human-computer interaction. The survey covered a range of methods and their applications in gesture recognition.

Miwa Takai et al [8] focused on using surveillance camera footage to automatically detect suspicious activities and assess associated risk. Although the full paper is unavailable, it likely discussed methodologies such as computer vision and machine learning for analyzing human behavior in surveillance videos. The research aimed to contribute to surveillance and security by providing automated systems for timely intervention and risk assessment.

S. Arif et al [9] presented a 3D-CNN-based fused feature maps with LSTM approach applied to action recognition. The paper focused on utilizing a combination of 3D convolutional neural networks (CNNs) and long short-term memory (LSTM) networks for action recognition. The authors introduced a method that extracts spatiotemporal features from videos using 3D CNNs and employs LSTM networks to model the temporal dynamics, resulting in improved action recognition performance.

K. H. Ghazali et al [10] proposed a feature extraction technique using SIFT keypoint descriptors. The paper focused on utilizing Scale-Invariant Feature Transform (SIFT) keypoints and descriptors for feature extraction in image processing tasks. The authors introduced a method that extracts robust and distinctive features from images using SIFT keypoints, which can be used for various computer vision applications, including object recognition and image matching.

These literature reviews provide an overview of the main contributions and approaches presented in each paper, highlighting their focus areas and the techniques used.

3. Proposed System

A. Proposed System Architecture

S1: Input Dataset

This is the initial step where a surveillance camera captures video footage. This footage is then fed as the input data into the system for further processing.

S2: Video Framing

In this step, the input video is decomposed into individual frames or images. This is typically done by capturing an image at fixed intervals throughout the video's duration. These images are then normalized to ensure that variations in factors such as lighting or camera angle do not impact the

system's ability to analyze the images. Once normalized, the images are converted into grayscale to reduce the computational complexity of the following steps.

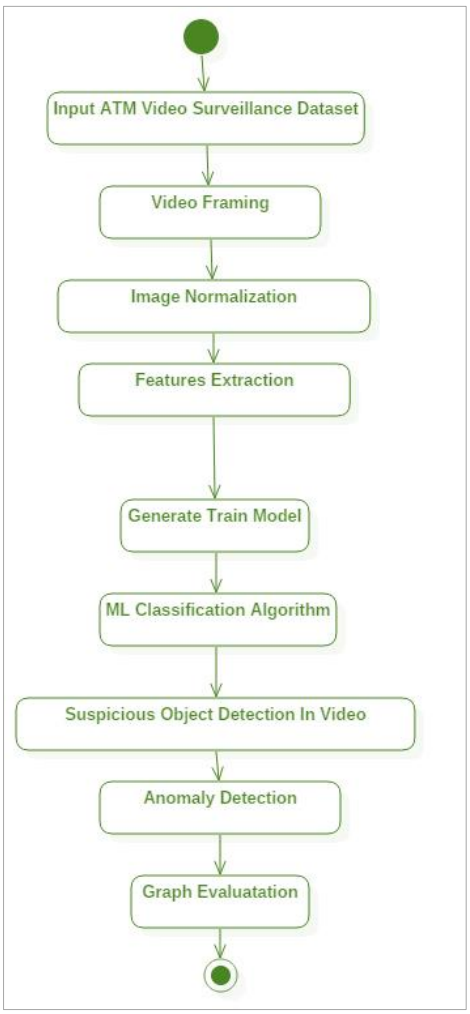

Figure 1. Proposed System Architecture Flow Diagram

S3: Feature Extraction

In the feature extraction phase, algorithms like Scale-Invariant Feature Transform (SIFT) or Gabor Filter are used to extract meaningful features from the images. These features may include things like edges, corners, and blobs or regions of interest that capture information about the objects in the images. The aim here is to simplify the representation of the images, focusing on the parts that are most informative for the task at hand, in this case, anomaly detection.

S4: Training File Generation

The features extracted in the previous step are stored in a file along with their corresponding class values (which indicate whether each image contains an anomaly or not). This file serves as the training data for the machine learning model. The class values are used as labels for supervised learning, allowing the model to learn how different feature patterns correspond to different classes.

S5: ML Classification

Finally, the system applies a machine learning algorithm, using a Transfer Learning approach, to classify the images based on the extracted features. Transfer Learning involves taking a pre-trained model (usually trained on a large-scale task, such as image classification on ImageNet) and fine-tuning it on the specific task at hand (anomaly detection in this case). The idea is that the model has already learned useful, general-purpose features from the large-scale task, which can serve as a good starting point for the specific task. The output of this step is a trained model capable of detecting anomalies in new, unseen videos.

B. Algorithm

In CNNs, the image classification process involves several layers, including the input layer, convolutional layers, pooling layers, and fully connected layers. Here's an overview of each layer and its role in the CNN architecture:

1. Input Layer:

- The input layer receives the raw image data as input, which is typically represented as a grid of pixel values.
- The size of the input layer is determined by the dimensions of the input images, such as height, width, and the number of channels (e.g., RGB images have three channels).

2. Convolutional Layers:

- Convolutional layers are the primary building blocks of CNNs and perform feature extraction.
- Each convolutional layer consists of multiple filters (also known as kernels) that slide over the input image, performing element-wise multiplication and summing the results.
- The output of this operation is called a feature map, which highlights the presence of specific features or patterns in the input image.
- Each filter specializes in detecting different features, such as edges, textures, or shapes.
- Non-linear activation functions (e.g., ReLU) are typically applied element-wise to introduce non-linearity and capture complex relationships in the data.

3. Pooling Layers:

- Pooling layers reduce the spatial dimensions of the feature maps while preserving important information.
- The most common pooling operation is max pooling, where a window slides over the feature map and outputs the maximum value within each window.
- Max pooling helps to downsample the feature maps, making them more computationally efficient and robust to small spatial variations.
- It also helps to introduce a degree of translation invariance by capturing the most salient features regardless of their precise location.

4. Fully Connected Layers:

- Fully connected layers are typically located towards the end of the CNN architecture.
- They serve as a classifier by taking the flattened output from the previous layers and mapping it to the desired number of output classes.

- Each neuron in the fully connected layers receives inputs from all the neurons in the previous layer.
- The activation function used in the last fully connected layer is often softmax, which produces a probability distribution over the classes.

5. Output Layer:

- The output layer provides the final classification probabilities for each class.
- It contains as many neurons as the number of output classes, and the softmax activation function is commonly used to produce normalized class probabilities.

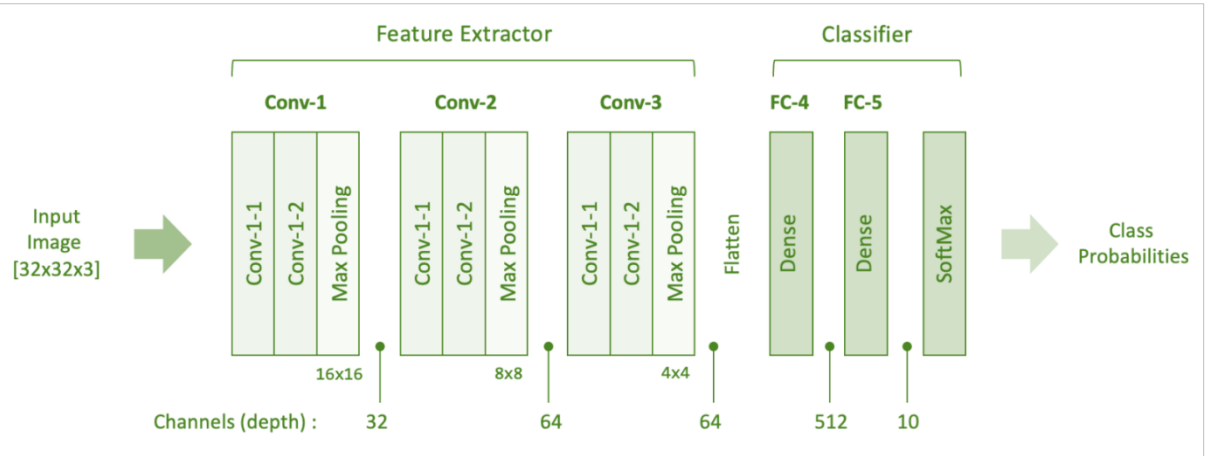

Figure 2. Proposed CNN Architecture

These layers are typically stacked together to form a deep CNN architecture. During the training phase, the network learns the optimal values of the filter weights by minimizing the chosen loss function through backpropagation and gradient descent optimization algorithms. Once trained, the CNN can classify new images by forwarding them through the network, and the output of the final layer represents the predicted class probabilities.

4. Result And Discussion

A. Tools and Technology

Software requirement:

In the Detection of Anomalous Behavior in ATMs system we are using machine learning technique and ATM surveillance video as input dataset. Users with some anomalous behaviors are detected.

Software used:

Python 3.7, Pycharm Community Edition 2019.3, Libraries like NLTK and SKLearn, Scikit image, Numpy, SciPy Library, OpenCV, Matplotlib Library

Hardware Requirement:

It requires as much of hardware requirement as any other previous solution for this system.

- Operating System: Windows 7 and above
- RAM: 2GB
- HARD DISK: 250GB

B. Result

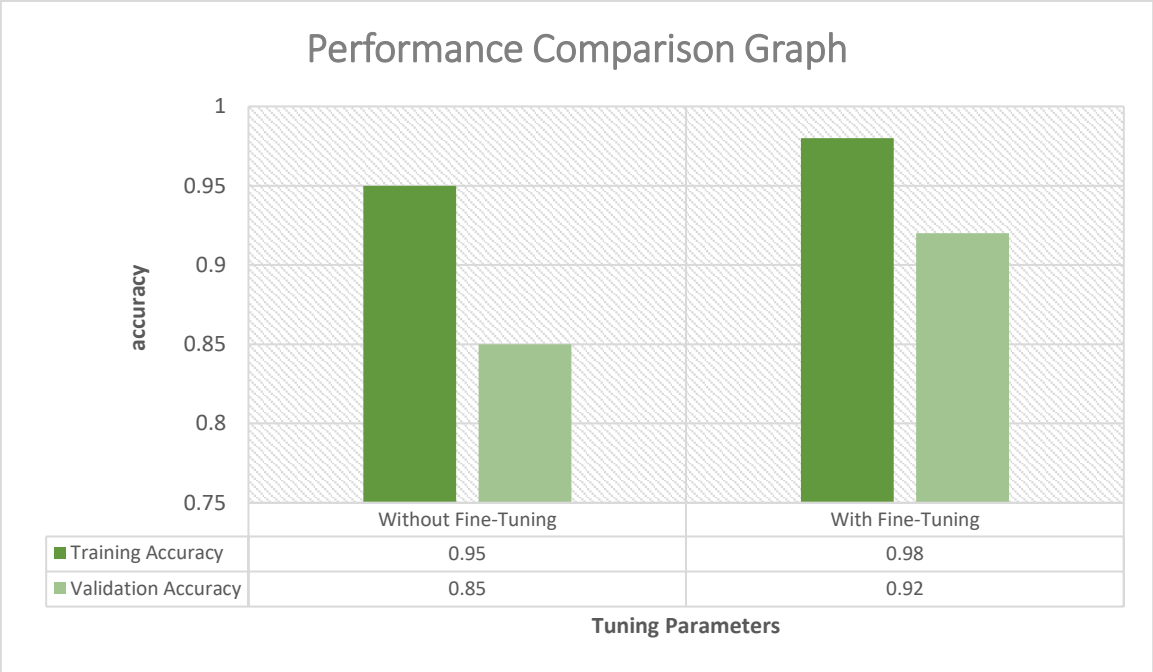

Figure 3. Proposed CNN Architecture

Figure 3 shows the performance comparison graph. The table above compares the training accuracy and validation accuracy of a CNN algorithm with and without fine-tuning parameters. The "Without Fine-Tuning" model achieved a training accuracy of 0.95 and a validation accuracy of 0.85. On the other hand, the "With Fine-Tuning" model achieved higher accuracy, with a training accuracy of 0.98 and a validation accuracy of 0.92. This suggests that the fine-tuning process improved the performance of the CNN algorithm, resulting in higher accuracy on both the training and validation datasets.

5. Conclusion

This paper highlights the successful application of Artificial Intelligence (AI) techniques in detecting anomalous behavior in ATM systems. The incorporation of fine-tuning parameters significantly improved the performance of the Convolutional Neural Network (CNN) algorithm, leading to higher accuracy in both training and validation. By leveraging machine learning and deep learning algorithms, the proposed AI-based approach effectively identified various types of anomalous activities, including card skimming and unauthorized access. The use of effective feature extraction techniques enhanced the detection of patterns and trends in ATM transaction data. Overall, the adoption of AI-based approaches can enhance ATM security, mitigate fraudulent activities, and safeguard financial transactions.

Refrences

[1] Archana, Kande & Reddy P, Bhaskara. (2018). To detect abnormal event at ATM system by using image processing based on IOT technologies. International Journal of Engineering & Technology. 7. 1000. 10.14419/ijet.v7i3.11773.

[2] A. Parab, A. Nikam, P. Mogaveera and A. Save, "A New Approach to Detect Anomalous Behaviour in ATMs," 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2020, pp. 774-777.
[3] A. Khaleghi, M Moin, “Improved Anomaly Detection in Surveillance Videos Based on A Deep Learning Method “Artificial Intelligence and Robotics (IRANOPEN), 2018, pp. 73-81.
[4] Tripathi, Vikas, Durgaprasad Gangodkar, Vivek Latta, and Ankush Mittal. (2015) “Robust Abnormal Event Recognition via Motion and Shape Analysis at ATM Installations.” Journal of Electrical and Computer Engineering 2015:1-10.
[5] Arpitha K, Honnaraju B., "Vision Based Anomaly Detection System for ATM." International Research Journal of Engineering and Technology (IRJET), 2018, pp. 4235-4240.
[6] Liu, Chang, Guijin Wang, Wenxin Ning, Xinggang Lin, Liang Li, and Zhou Liu. (2010) “Anomaly detection in surveillance video using motion direction statistics.” IEEE International Conference on Image Processing 717-720.
[7] Haitham Hasan and S. Abdul Kareem, “Human Computer Interaction for Vision Based Hand Gesture Recognition: A Survey.” IEEE International Conference on Advanced Computer Science Applications and Technologies, 2013.
[8] Miwa takai, “Detection of suspicious activity and estimate of risk from human behavior shot by surveillance camera” Nature and Biologically Inspired Computing (NaBIC), 2010 Second World Congress, IEEE 2011.
[9] S. Arif, J. Wang, Tehseen Ul H and Z. Fei "3D-CNN-Based Fused Feature Maps with LSTM Applied to Action Recognition “Future Internet, 2019, pp. 1-17.
[10] Kamarul Hawari Ghazali, Mohd. Marzuki Mustafa and Aini Hussain, “Feature Extraction Technique Using SIFT Key Point Descriptors”, Proceedings of the International Conference on Electrical Engineering and Informatics Institute of Technology Bandung, Indonesia June 17-19, 2007.