e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704182 |

Propounding First Artificial Intelligence Approach for Predicting Robbery Behavior Potential in an Indoor Security Camera

Ms.S.DHANALAKSHMI, SHARMILA T, PRIYA S, SOUNDHARYA P

Assistant Professor, Department of CSE, Muthayammal Engineering College (Autonomous), Rasipuram, Tamil Nadu, India

Department of CSE, Muthayammal Engineering College (Autonomous), Rasipuram, Tamil Nadu, India

Department of CSE, Muthayammal Engineering College (Autonomous), Rasipuram, Tamil Nadu, India

Department of CSE, Muthayammal Engineering College (Autonomous), Rasipuram, Tamil Nadu, India

ABSTRACT: The proposed video surveillance and security system, augmented by AI with the YOLO algorithm, marks a notable stride forward in the realm of crime prevention and detection. Through real-time object identification, behavior analysis, and contextual insight, the system offers a proactive means to bolster public safety and security. Its capacity to swiftly pinpoint potential threats, issue timely alerts, and adapt to evolving contexts positions it as a valuable asset across diverse sectors, spanning from public spaces and retail establishments to critical infrastructure and smart city initiatives. With its predictive prowess, practical versatility, and potential to revolutionize surveillance technology, this system stands poised to significantly elevate safety measures and mitigate security risks within communities.

KEYWORDS: Artificial Intelligence (AI), Video Surveillance, YOLO Algorithm, Crime Detection, Object Detection

I. INTRODUCTION

The use of surveillance cameras in private and public spaces has become increasingly prevalent in recent years for various purposes, including tracking, monitoring, and preventing violations. An anomaly, as defined in the surveillance field, refers to a deviation from common rules, types, arrangements, or forms and can be characterized as an uncommon event that deviates from “normal” behavior.

Detecting anomalies in surveillance videos is crucial to maintaining security in various applications, such as crime detection, accident detection, abandoned object detection, illegal activity detection, and parking area monitoring. However, the manual detection of anomalies in surveillance videos is a tedious and labor-intensive task for humans. This is due to the large amount of data generated by critical systems in security applications, making manual analysis an impractical solution.

In recent years, there has been a significant increase in the demand for automated systems for detecting video anomalies. These systems include biometric identification of individuals, alarm-based monitoring of Closed-Circuit Television (CCTV) scenes, automatic detection of traffic violations, and video-based detection of abnormal behavior [1]. Automated systems significantly reduce human labor and time, making them more efficient and cost-effective for detecting anomalies in surveillance videos.

Identifying and tracking anomalies in the recorded video comprise a growing research problem in surveillance. Many methods have been proposed by researchers in academia, including the use of machine learning algorithms and image processing techniques.

In recent times, the utilization of surveillance cameras in public and private areas has risen significantly, serving multiple objectives. Identifying abnormalities in surveillance footage is vital to upholding safety measures in diverse scenarios. Nonetheless, the manual identification of anomalies in surveillance footage can be arduous and laborious for humans. Researchers have proposed automated systems for detecting video anomalies to address this issue,

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704182 |

significantly reducing human labor and time. Despite the advancements that have been made, there is still room for improvement in the accuracy, reliability, and scalability in developing a flawless video surveillance system [2].

The Surveillance Video Anomaly Detection (SVAD) system is a sophisticated technology designed to detect unusual or suspicious behavior in video surveillance footage without human intervention. The system operates by analyzing the video frames and identifying deviations from normal patterns of movement or activity. This is achieved through advanced algorithms and machine learning techniques that can detect and analyze the position of pixels in the video frame at the time of an event.

Traditionally, anomaly detection methods have focused on identifying objects that deviate from normal trajectories. However, these methods need to be improved [3] for use in video surveillance due to the variety of objects that may be present in a video frame. As a result, two main approaches have been developed for video anomaly detection. The first approach involves measuring the magnitude of the error by calculating the reconstruction error of future frames. This is achieved by comparing the predicted future frames with the actual frames and identifying significant differences. The second approach involves predicting the future frames based on the previous frames and assigning a high anomaly score to any frame that deviates significantly from the predicted frame.

In recent years, with the advancement of hardware performance and the development of new models, smart learning techniques have become increasingly popular in video anomaly detection. However, the use of these techniques also brings several challenges. One of the major challenges is the production of big data, which requires a large amount of computational power for processing. High computational power also poses a significant challenge, requiring a significant resource investment [4].

:

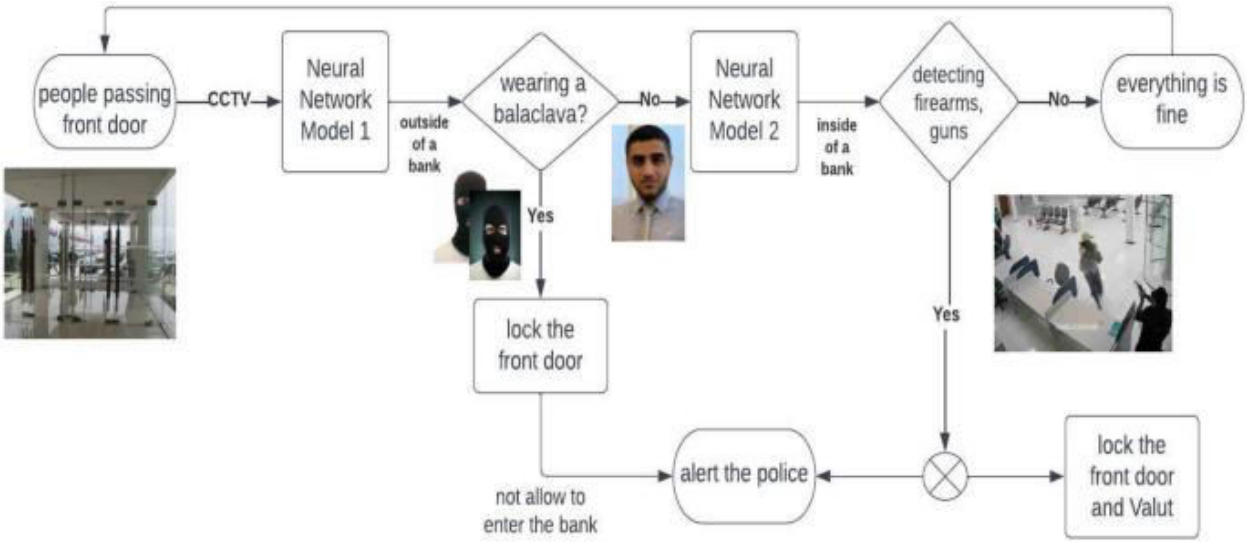

Fig 1: Improving video surveillance systems

Over the past two decades, a significant amount of research has been conducted on image and video processing to overcome these challenges. These studies have focused on developing new methods for anomaly detection that are more efficient and effective while also addressing the challenges associated with intelligent anomaly detection. Overall, understanding the issues of traditional anomaly detection methods and exploring new methods are crucial for the continued advancement of video surveillance.

This survey aimed to comprehensively examine the existing literature on Artificial Intelligence (AI) techniques for detecting abnormal events in surveillance videos. Specifically, the survey aimed to provide an overview of the most-commonly used datasets and evaluate their benefits and drawbacks. Additionally, the survey highlights key difficulties in the literature, providing insight into areas that require further research and development.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704182 |

First, it is important to note that the use of AI in surveillance video analysis has gained significant attention in recent years due to its potential to improve the effectiveness and efficiency of surveillance systems. This is particularly relevant in security and surveillance, where detecting abnormal real-time events is crucial for public safety.
Various approaches and techniques, based on evolving artificial intelligence methods, enable the analysis of surveillance videos and the identification of abnormal events such as suspicious behavior, criminal activities, and other potential threats. The contributions of our study are as follows

II. RELATED WORKS

There are many definitions of an anomaly. Frank E. Grubbs [5], in 1969, defined an outlier or an anomaly as "An outlying observation, or outlier, appears to deviate markedly from other members of the sample in which it occurs". Hawkins [6], in 1980, defined it as "an observation which deviates so much from other observations as to arouse suspicions that a different mechanism generated it". Barnett and Lewis [7], in 1994, defined it as "an observation (or subset of observations) which appears to be inconsistent with the remainder of that set of data".

In several situations, the same action can be interpreted as an abnormal or anomalous event because most anomaly detection techniques are based on the hypothesis that a pattern that deviates from previously acquired patterns is considered abnormal [8]. According to some studies [9,10,11], anomalies can be divided into three types:

Because of a lack of knowledge sufficient to generalize their characteristics and correctly classify them as outliers, most machine learning (ML) and expert systems frequently need help detecting and classifying these anomalies. These rare events make identification challenging and contribute to an imbalanced data classification [3,4].
Once predictive models are built and sufficient data labels are provided, anomaly detection is challenging, considering the binary classification problem. However, the data available for training a model are restricted to containing few or no anomalous events, and such labels are frequently infrequent or cumbersome [5].

SVAD aims to find abnormal frames or pixel parts that contain various spatial and temporal data [16]. Spatial features can be collected from a single frame, whereas temporal features can be collected from the data on object movement and the order of frames. Generally, there are three methods for estimating abnormalities in SVAD [7]: (1) The characteristics of both regular and irregular events are reflected in a shared space, and the anomaly is identified based on the margin of the spatial distribution. (2) A dictionary was trained using the semantic properties of the event patterns. This dictionary is then used for anomaly calculation. (3) Anomalies are found through errors made during the prediction and reconstruction of prior or subsequent frames using various feature extractors trained to do so.

III. METHODS

SL acquires knowledge from pre-existing labeled datasets or "the training set", then compares the predicted output to the known labels. A high-level training set is always required to build a model that works effectively, but more is needed to ensure that the final product will be satisfactory; the training procedure is also a crucial element in creating a reliable predictor. A classifier model is first developed in SL through training, and after that, it can forecast either discrete or continuous outputs. The ASL model's performance, such as accuracy, is typically validated before prediction to demonstrate its dependability. Additionally, classification and regression techniques can be used to categorize SL tasks.

The training data are first divided into separate categories in the classification technique. It then calculates the probability of test samples falling into each category and chooses the category with the most votes. This probability represents the likelihood that a sample is a class member. Credit scoring and medical imaging are examples of typical applications. The regression technique uses input factors such as temperature changes or variations in electricity demand to forecast continuous responses, often in quantity. Forecasting power load and algorithmic trading are examples of typical applications. While the regression model can calculate the root-mean-squared error, the classification model can quantify the percentage of accurate predictions. Nevertheless, a discrepancy between the expected and actual values is acceptable since the output data are continuous.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704182 |

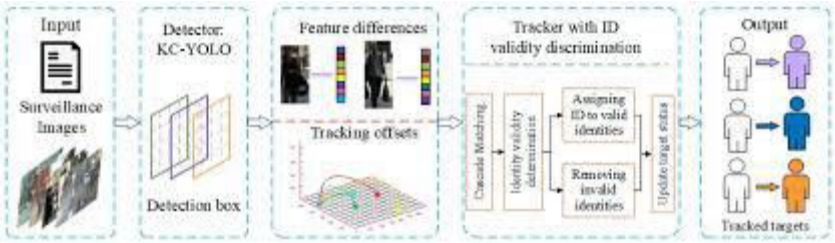

Fig 2: Propounding First Artificial Intelligence Approach

Several works have been performed with SL. One of the suggestions in this area is presented by the study. They proposed a unique way to identify fights or violent acts based on learning the temporal and spatial information from consecutive video frames that are evenly spaced. Using the proposed feature fusion approach, features with many levels for two sequential frames are retrieved from the first and last layers of the Convolutional Neural Network (CNN) and fused to consider the action knowledge. They also suggested a "Wide-Dense Residual Block" to learn the unified spatial data from the two input frames. These learned characteristics are subsequently consolidated and delivered to long-term memory components to store temporal dependencies. Using the domain adaptation strategy, the network may learn to efficiently merge features from the input frames, improving the results' accuracy. They evaluated their experiments by using four public datasets, namely HockeyFight, Movies, ViolentFlow, and BEHAVE, to show the performance of their model, which was compared with the existing models. There are several important learning techniques in SL, such the Hidden Markov Model (HMM), Support Vector Machine (SVM), Gaussian Regression (GR), Multiple Instance Learning (MIL), and Long Short-Term Memory (LSTM). It is clear that each technique has advantages and disadvantages in anomaly detection, and it is impossible to say that one technique can solve all problems efficiently.

IV. RESULT ANALYSIS

Once the features have been extracted, the next step is to train a classifier to distinguish between normal and anomalous video frames or segments. Several classifiers have been proposed in the literature, including traditional machine learning classifiers, such as Support Vector Machines (SVMs), random forests, k-Nearest Neighbors (kNNs), and deep learning-based classifiers: CNNs and RNNs. The choice of the classifier will depend on the specific application and the type of features that have been extracted.

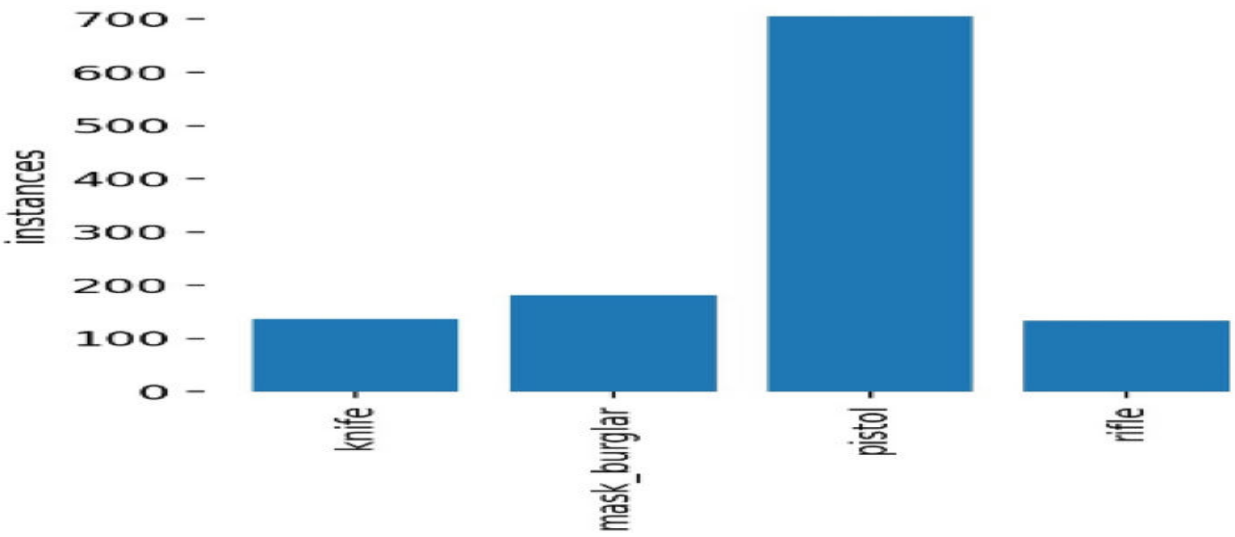

Fig 3: Result analysis Improving video surveillance systems

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704182 |

After the classifier has been trained, it can classify new video frames or segments as normal or anomalous. The classifier will output a score or probability for each frame or segment, indicating the likelihood that it is normal or anomalous. A threshold is usually set to make a final decision, and any frames or segments with a score below the threshold are considered anomalous.

One of the main advantages of classification-based methods for video anomaly detection is that they can be fine-tuned to a specific application by selecting appropriate features and classifiers. However, one of the main challenges is that these methods require a large amount of labeled training data to be effective. Additionally, they may be unable to detect anomalous events significantly different from the training data
Reconstruction-based methods are a variation of adversarial generative methods. Generative-Adversarial-Network (GAN)-based networks consist of two neural networks: a Generator (G) and a Discriminator (D). The generator network creates new examples in the target domain by mapping examples from the source domain to the target domain. The discriminator network then tries to distinguish between examples created by the generator and examples from the target domain. Through this process, the generator network learns to create examples indistinguishable from examples in the target domain.

V. CONCLUSIONS

In conclusion, this survey article provided a comprehensive overview of the current state-of-the-art in the field of SVAD and the various AI techniques that have been applied to this problem. The review highlighted the methods, datasets, challenges, and future directions explored in previous studies. The need for automated systems for detecting abnormal events in real-time has been driven by the increasing use of CCTV and other video recording systems, leading to an overwhelming amount of video data being produced. The ability to learn from new observations and continuously improve anomaly detection capabilities is also paramount in video surveillance.

The field of SVAD is expected to see significant advancements in the coming years, thanks to the rapid progress in AI techniques and the availability of reasonably priced hardware. The survey has shown that prediction-based and reconstruction-based techniques are at the forefront of AI-based SVAD and are expected to provide improved anomaly detection capabilities and enable real-time monitoring of large-scale video surveillance systems.

It is also worth noting that the field of SVAD is still an active area of research, and there is still much room for improvement. Future research should focus on developing more robust and efficient algorithms and addressing existing methods' limitations. Additionally, more comprehensive and diverse datasets should be used to evaluate the performance of the proposed methods. Using large-scale datasets with various types of anomalies and scenarios will help improve the generalization capabilities of the proposed methods.

REFERENCES

1. Kumari, P.; Bedi, A.K.; Saini, M. Multimedia Datasets for Anomaly Detection: A Survey. *arXiv* **2021**, arXiv:2112.05410. [Google Scholar]
2. Verma, K.K.; Singh, B.M.; Dixit, A. A review of supervised and unsupervised machine learning techniques for suspicious behavior recognition in intelligent surveillance system. *Int. J. Inf. Technol.* **2019**, *14*, 397–410. [Google Scholar] [CrossRef]
3. Zhao, Y. Deep Learning in Video Anomaly Detection and Its Applications. Ph.D. Thesis, The University of Liverpool, Liverpool, UK, 2021. [Google Scholar]
4. Abu Al-Haija, Q.; Zein-Sabatto, S. An Efficient Deep-Learning-Based Detection and Classification System for Cyber-Attacks in IoT Communication Networks. *Electronics* **2020**, *9*, 2152. [Google Scholar] [CrossRef]
5. Grubbs, F.E. Procedures for detecting outlying observations in samples. *Technometrics* **1969**, *11*, 1–21. [Google Scholar] [CrossRef]
6. Hawkins, D.M. *Identification of Outliers*; Springer: Berlin/Heidelberg, Germany, 1980; Volume 11. [Google Scholar]
7. Barnett, V.; Lewis, T. *Outliers in Statistical Data*; Wiley Series in Probability and Mathematical Statistics. Applied Probability and Statistics; Wiley: New York, NY, USA, 1984. [Google Scholar]
8. Wan, B.; Jiang, W.; Fang, Y.; Luo, Z.; Ding, G. Anomaly detection in video sequences: A benchmark and computational model. *IET Image Process.* **2021**, *15*, 3454–3465. [Google Scholar] [CrossRef]

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704182 |

9. Aldayri, A.; Albattah, W. Taxonomy of Anomaly Detection Techniques in Crowd Scenes. *Sensors* **2022**, *22*, 6080. [Google Scholar] [CrossRef]
10. Pannirselvam, P.M.; Geetha, M.K.; Kumaravelan, G. A Comprehensive Study on Automated Anomaly Detection Techniques in Video Surveillance. *Ann. Rom. Soc. Cell Biol.* **2021**, *25*, 4027–4037. [Google Scholar]
11. Chandola, V.; Banerjee, A.; Kumar, V. Anomaly detection: A survey. *ACM Comput. Surv. (CSUR)* **2009**, *41*, 1–58. [Google Scholar] [CrossRef]

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com