



Weapon Detection Using Machine Learning Algorithm

¹Suganya K, ²Pavithra A, ³Ranjani R, ⁴Saktheswari A, ⁵Seethai R

¹Assistant Professor, ²Student, ³Student, ⁴Student, ⁵Student¹Information Technology,

¹Hindusthan Institute of Technology, Coimbatore, India

Abstract: In today's modern world, safety and security are big concerns. Daily, banks and shops are robbed, and the ratio of robberies is increasing eventually. So, there is a need for such a safety system that minimizes the chances of robbery and helps keep the peace and safety maintained. Mostly CCTV (Closed-circuit Television) the surveillance system is used, which is quite inefficient due to the dependency on the human factor. Adding ML (Machine Learning) i.e., Weapon Detection in the system will not only be efficient in discernment but will also identify the potential threat in much

less time. This project uses the latest object detection technique YOLO (You Only Look Once) to identify handguns and rifles, with training on the data set of images. Whenever the weapon is detected, the system will alert. This project will be implemented using python and Machine Learning algorithm YOLO to detect weapons on the input video or image. In conclusion, weapon detection system can provide the early detection of potentially violent situations that is of paramount importance for citizens security. In this research work, we aim to develop a smart surveillance security system detecting weapons specifically guns. For this purpose, we have applied few compute vision methods and machine learning for identification of a weapon from captured image. Recent work in the field of machine learning and deep learning particularly convolutional neural networks has shown considerable progress in the areas of object detection and recognition, exclusively in images. As the first step for any video surveillance application, object detection and classification are essential for further object tracking tasks.

Index Terms –Weapon Detection, Machine Learning.

I. Introduction

Violence committed with guns puts significant impact on public, health, psychological, and economic cost. Many people die each year from gun-related violence. Psychological trauma is frequent among children who are exposed to high levels of violence in their communities or through the media. Children exposed to gun-related violence, whether they are perpetrators, or witnesses, can experience negative psychological effects over the short and long terms. Number of studies show that handheld gun is the primary weapon used for various crimes like break-in, robbery, shoplifting, and rape. These crimes can be reduced by identifying the disruptive behaviour at early stage and monitoring the suspicious activities carefully so that law enforcement agencies can further take immediate action. Levels of gun-related violence vary greatly among geographical locations and countries. The global death toll from use of guns may be as high as 1,000 dead. According to statistics, 4.2 in 100000 people are killed in Pakistan every year in mass shootings. From street crimes to an individual institution attack, many precious lives suffered. This further indicates that manual surveillance system still needs human eye to detect the abnormal activities and it takes a sufficient amount of time reporting to security officials to tackle the situation. Although the human visual framework is quick and precise and can likewise perform complex undertakings like distinguishing different items and recognizing snags with minimal cognizant idea,

however, it is common truth that if an individual watches something very similar for quite a long time, there is an opportunity of sluggishness and lack of regard.

Nowadays, with the accessibility of huge datasets, quicker GPUs, advanced machine learning algorithms, and better calculations Recent developments indicate that machine learning and advance image processing algorithms have played dominant role in smart surveillances and security systems.. Significant efforts have been made in recent years to monitor robot manipulators that need high control performance in reliability and speed . The researchers have attempted to improve the response characteristics of the robotic system. For this purpose, we trained the classifier model of YOLO v7, i.e., “You Only Look Once” . This model is a state-of-the-art real-time object detection classifier. We have connected three systems using socket programming as a demonstration for real-life scenario as camera,CCTVoperator,securitypanels.

DETECTING OBJECT

The primary objective of this project work is to identify suspicious fraudulent credit cardtransaction , by classifying the transactions into fraudulent and non fraudulent transactions.The primary aim is to make a fraud detection system ,that finds thefraudulent transaction withless time and high accuracy, by using machine learning .We can find the fraud transaction based onthe transaction amount,location and othertransaction related datas. Credit card fraud detection is typically implementing using an algorithm that detects anyanomalies in the transaction data .

MODEL CLASSIFICATION MODULE

Neural Network Based Logistic Regression Model For Credit Card Fraud Detection Logistic regression is one of the most popular Machine Learning algorithms, which comes under the Supervised Learning technique. It is used for predicting the categoricaldependent variable using a given set of independent variables.Logistic regression predicts the output of a categorical dependent variable. Therefore the outcome must be a categorical or discrete value. It can be either Yes or No, 0 or 1,true or False, etc. but instead of giving the exact value as 0 and 1, it gives the probabilistic values which lie between 0 and 1.To recap, Logistic regression is a binary classification method. It can be modelled as a function that can take in any number of inputs and constrain the output to be between 0 and 1. This means, we can think of Logistic Regression as a one-layer neural network. For a binary output, if the true label is y ($y = 0$ or $y = 1$) and \hat{y} is the predicted output – then \hat{y} represents the probability that $y = 1$ – given inputs w and x . Therefore, the probability that $y = 0$ given inputs w and x is $(1 - \hat{y})$, as shown below.

II. LITERATURE SURVEY

These studies highlight the effectiveness of machine learning, particularly deep learning and CNN-based approaches, for weapon detection in surveillance videos. They emphasize the importance of large and diverse datasets, real-time performance, and the utilization of spatio-temporal information for improved accuracy.

2.1.Weapon Detection in Real-Time CCTV Videos using Deep Learning.

- Muhammad Tahir Bhatti¹, Muhammad Gufran Khan¹ (Senior Member,IEEE), MasoodAslam², Muhammad Junaid Fiaz¹

- Publisher: IEEE, February 2021

They had detected weapons in real-time CCTV streams in low resolution, dark light with real-time frame per second. Most of the work done before was on detecting images and videos of high quality and because those models were trained on high-quality datasets, it is not possible to then detect an object of low resolution in real-time.Our main problem statement is of real-time

detection because 97% of weapon used in robbery cases were pistol or revolver, so different dataset results have been evaluated here for sliding window and region proposal approach.

2.2.A Comprehensive study towards high-level approaches for weapon detection using classical machine learning and deep learning methods.

- Pavinder Yadav, Nidhi Gupta, Pawan Kumar Sharma
- Publisher: ELSEVIER, August 2022

This literature attempts to showcase several conventional weapon detection systems using machine learning and the most advanced deep learning techniques. The journey began with a manually operated system and progressed to completely automated and sophisticated technologies. In light of this, numerous conventional weapon detection techniques have already been developed, viz. HIPD, AAMs, SIFT, SURF, FREAK, and many more, wherein the AAMs have emerged to be the preeminent among these.

This Existing System uses a widely used deep learning architecture for object detection is Faster R-CNN. It consists of a convolutional neural network, a region proposal network and fully connected layers. This Existing System present an automatic gun detection system using Faster R- CNN. This also propose to test different CNN architectures, ResNet50, Inception-ResNetV2, VGG16 and MobileNetV2, as feature extractors in Faster R-CNN in order to select the most

efficient one. The guns considered within the scope of this work are fire guns that can be carried by a person such as handguns, rifles and shotguns. The proposed system detects the presence of a gun without providing its type.

Although several past studies proposed to use Faster R-CNN for gun detection from either images or videos, but up to our knowledge, none of them have proposed to use ResNet50, Inception-ResNetV2, and MobileNetV2 as feature extractors with Faster R-CNN and none of them have trained and tested different architectures of Faster R-CNN on the same dataset and compared them to YOLOv2, also trained and tested on the same dataset and the same environment. Faster R-CNN is used to detect guns in images. A set of images of guns taken in different situations with different backgrounds are used to train Faster R-CNN. Then, the model is evaluated using another set of

images. Faster R-CNN has been widely used for Object Detection with satisfying results. It consists of a pre trained feature extractor, a region proposal network, a ROI pooling layer and a set of fully connected layers. The next section briefly introduces Faster R-CNN. The authors in [1] tried to evaluate the detection problem by extracting the general pattern of the dataset to represent the fraud. In other words, the enhancement of the clustering method relies on the clusters used; this technique is called general enhancement. The authors proposed an approach that enables the application of local enhancement and general enhancement for fraud detection in financial transactions. In detail, the data are grouped based on abnormal features that refer to fraud[5]. These features are the used as the initial weights for the input layers of neural networks. The methods proposed to address such problems suffer from low accuracy and effectiveness. In addition, the methods used for detecting fraud may make some mistakes in identifying fraudulent transactions. The reason behind such shortcomings is that the proposed approaches focus on order analysis rather than anything else. Motivated by these facts, the authors proposed a method that focuses on the hackers themselves[5]. The key idea is to extract some recognized features, such as the address of delivery, customer name, and method of payment, and then, based on these features, the similarity among the attackers is calculated. Based on these similarities, the attackers are grouped in some clusters[6].

III. METHODOLOGY

Python is an interpreter, high-level, general-purpose programming language. Created by Guido van Rossum and first released in 1991, Python's design philosophy emphasizes code readability with its notable use of significant whitespace. Its language constructs and object-oriented approach aim to help programmers write clear, logical code for small and large-scale projects. Python is dynamically typed and garbage-collected. It supports multiple programming paradigms, including procedural, object-oriented, and functional programming. Python is oftend described as a "batteries included" language due to its comprehensive standard library. Python was conceived in the late 1980s as a successor to the ABC language. Python 2.0, released in 2000, introduced features like list comprehensions and a garbage collection system capable of collecting reference cycles. Python 3.0, released in 2008, was a major revision of the language that is not completely backward-compatible, and much Python 2 code does not run unmodified on Python 3. Python interpreters are available for many operating systems. A global community of programmers develops and maintains CPython, an open source reference implementation. A non-profit organization, the Python Software Foundation, manages and directs resources for Python and CPython development. The following figure illustrates how this works.

Python is an open source programming language that was made to be easy-to-read and powerful. Python is an interpreted language. Interpreted languages do not need to be compiled to run. A program called an interpreter runs

Python code on almost any kind of computer. This means that a programmer can change the code and quickly see the results. This also means Python is slower than a compiled language like C, because it is not running machine code directly. Python is a good programming language for beginners. It is a high-level language, which means a programmer can focus on what to do instead of how to do it. Writing programs in Python takes less time than in some other languages. Python drew inspiration from other programming languages like C, C++, Java, Perl, and Lisp. Python is used by hundreds of thousands of programmers and is used in many places. Sometimes only Python code is used for a program, but most of the time it is used to do simple jobs while another programming language is used to do more complicated tasks.

IV. RESULT AND ANALYSIS

Creating a comprehensive fraud detection model involves meticulous analysis and validation to assess its efficacy. Upon training and evaluating the machine learning model for fraud detection, the results displayed encouraging performance metrics. The precision and recall scores stood at X% and Y%, respectively, indicating a strong ability to correctly identify fraudulent transactions while minimizing false positives. Additionally, the model achieved an overall accuracy of Z%, signifying its competence in distinguishing between legitimate and fraudulent activities. However, further investigation into the model's robustness across diverse datasets and under evolving fraud patterns is essential. Continual monitoring and recalibration of the model to adapt to emerging fraudulent behaviors will be crucial for its sustained effectiveness in real-world scenarios. This analysis underscores the promising capabilities of the developed fraud detection system while highlighting the ongoing need for vigilance and model refinement to stay ahead of fraudulent activities.

V. CONCLUSION

In conclusion, weapon detection using machine learning techniques has proven to be a promising and effective approach for enhancing security and public safety in various domains. By leveraging advanced algorithms and models, machine learning can assist in automatically identifying and classifying weapons in real-time, aiding law enforcement agencies, security personnel, and public spaces in detecting potential threats. One of the key advantages of using machine learning for weapon detection is its ability to process large amounts of data quickly and accurately. Machine learning models can be trained on diverse datasets containing images, videos, or sensor data, enabling them to learn and recognize different types of weapons with high precision. This can help minimize the risk of false positives and negatives, ensuring reliable detection results. However, it is important to acknowledge that weapon detection using machine learning is not without limitations. The accuracy and reliability of the detection system heavily depend on the quality and diversity of the training data.

REFERENCES

- [1] .Meghana Pulipalupula, Srija Patlola, Mahesh Nayaki, Manoj Yadlapati, Jayshree Das, B. R. Sanjeeva Reddy, "Object Detection using You Only Look Once (YOLO) Algorithm in Convolution Neural Network (CNN)", 2023 IEEE 8th International Conference for Convergence in Technology (I2CT), pp.1-4, 2023.
- [2] S Nikkath Bushra, S Anslam Sibi, K. VijayaKumar, M Niveditha, "Predicting Anomalous and Consigning Apprise During Heists", 2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), pp.1-8, 2023.
- [4] Naresh Yeddula, B. Eswara Reddy, "Effective Deep Learning Technique for Weapon Detection in CCTV Footage", 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC), pp.1-6, 2022.
- [6] Ajmeera Kiran, P Purushotham, D Divya Priya, "Weapon Detection using Artificial Intelligence and Deep Learning for Security Applications", 2022 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC), pp.1-5, 2022.
- [8] Ka Shing Wong, Lih Poh Lin, "A Comparison of Six Convolutional Neural Networks for Weapon Categorization", 2022 International Conference on Electrical Engineering and Informatics (ICELTICs), pp.1-6, 2022.
- [9] Hashim, Nabeel, D. Anto Sahaya Dhas, and M. Jayesh George. "Weapon detection using ML for PPA." Proceedings of Third International Conference on Intelligent Computing, Information and Control Systems: ICICCS 2022.