Performance Enhancement of Video Surveillance In Fortifying Banking Security Through Darknet Analysis

Dr. P. Suresh Kumar[1], Pranav Kumar S[2], Ratheesh M[3]
[1]Professor, Dept of Electronics and Communication Engineering
[2, 3]Dept of Electronics and Communication Engineering
[1, 2, 3] Chennai Institute of Technology (Autonomous), Chennai

Abstract- *This research paper is on the application of non-linear neural networks, YOLOv5, object-detection framework with the Darknet architecture to design a standout Intelligent Video Image Processing and Monitoring Control System that increases efficiency in the banking industry. Leveraging the real-time object detection capabilities of YOLO v5, the system supports efficient monitoring and surveillance among various areas of bank premises, with a directed attention on detecting probable security threats like knives, guns, and individuals, who are wearing robbery masks.*

The Darknet establishes the eventual image's operational core, making it possible to yield real-time performance and effortlessly monitor the banking premises with its fast processing. It plans to do so by implementing this integration which will help to create instant and precise alerts for suspicious activities or threats, including carried knives, guns, and people wearing a robbery mask. Introducing this method of security monitoring into the banking sector proactively, helps banking institutions to notice and respond to security incidents swiftly. As a result, it enhances the security environment in the banking sector.

YOLOv5-Darknet represents a major progress in bank security, through its capacity of real-time video detection carried out with high accuracy and efficiency by detecting knives, guns, and robbery masks. This system, based on deep learning and neural network frameworks, will be a responsive asset against security risks in the bank territory and subsequently will be a part of the initiatives aiming at improving the security measures within the financial institutions.

Keywords- YOLO v5, Darknet architecture, Intelligent Video Image Processing, Monitoring Control System, Banking security, Real-time object detection, Knives, Guns, Robbery masks, Surveillance capabilities

I. INTRODUCTION

Features of detecting objects in the computer vision go beyond lettering of the image stuff only. The technique is achieving its objective of imitating human image processing, thus making machines not only capable of recognizing elements within an image but also of detecting their precise locations. Not only it brings from the surface the straightforward subject of the image but also it can reveal the hidden layers of the photo. It aims to solve the questions of "where" and "what" by the method of classification using bounding boxes.

Object identification transmits the level a bit further from understanding the simple content of the picture. Deep learning, being a potent tool in the computer vision and machine learning domain, uses these techniques with the help of deep learning models, which provide far superior accuracy, to solve two key functions. In the first instance, the device location objects are like how humans as to the scene perception. It is building up computers to detect objects from an image, involving a broad choice of objects like cars, people, animals, and common items. Besides their discovery identification is a necessary but not a decisive factor. In object detection, there is another important complication called localization along with it the exact location of the object within the image is located. This is usually carried out by labelling the detected objects with boxes, which, are referred to as bounding boxes. Here, the two tasks being undertaken together provide a more informed interpretation of the overall visual world of the image. YOLO (You Only Look Once) the leap object detection made since its birth in 2015, owing to its easiest and fastest single-stage architecture. Unlike the methods that are to be performed repeatedly over an image, YOLO analyses the entire image at once, producing an excellent fast time and showing high applicability in real-time usage. From YOLOv1 to the state-of-the-art YOLOv8, the History of YOLO is illustrated by a selfless seeking of accuracy and efficiency.

YOLOv1, the first version, which is a single-stage detection approach, provides real-time detection and lower performance than multi-stage with more robustness. While YOLOv2 dropped in 2016, the accuracy had increased, while the performance was still within the real-time. In the very first version of the algorithm, batch normalization was used and the anchor boxes were introduced in an attempt that not only benefited from better accuracy metrics but also from better problem-solving abilities. Additionally, developments of YOLOv3 in 2018 brought more intricate architecture than the previous model attaining a gratifying effort of speed and accuracy. This particular model played an instrumental role in considerably elevating the YOLO algorithm's position among the top object detectors in the market.

Next year, the YOLOv3's release of YOLOv4 added another marque to its history since it included different variations aimed at different uses. The lightweight YOLOv4-Tiny is geared toward lookout operations where quick response is the main feature while the highly accurate YOLOv4-X represents cases where precision is the main feature. This cultivated flexibility helped YOLO to offer a satisfactory range of deployment requirements.

YOLOv5, which was released the same year by Ultralytics, aimed to have a simpler model and make the codebase less complex, but still get high-level accuracy. This time around, the emphasis lay on developer-friendliness, which included engaging several measures such as simplifying the implementation process and making YOLO available to a potentially broader range of stakeholders.

YOLOv1, the first version, which is a single-stage detection approach, provides real-time detection and lower performance than multi-stage with more robustness. While YOLOv2 dropped in 2016, the accuracy had increased, while the performance was still within the real-time. In the very first version of the algorithm, batch normalization was used, and the anchor boxes were introduced in an attempt that not only benefited from better accuracy metrics but also from better problem-solving abilities. Additionally, developments of YOLOv3 in 2018 brought more intricate architecture than the previous model attaining a gratifying effort of speed and accuracy. This model played an instrumental role in considerably elevating the YOLO algorithm's position among the top object detectors in the market.

Next year, the YOLOv3's release of YOLOv4 added another marque to its history since it included different variations aimed at different uses. The lightweight YOLOv4-Tiny is geared toward lookout operations where quick response is the main feature while the highly accurate YOLOv4-X represents cases where precision is the main feature. This cultivated flexibility helped YOLO to offer a satisfactory range of deployment requirements.

YOLOv5, which was released the same year as Ultralytics by Ultralytics, aimed to have a simpler model and make the codebase less complex, but still get high-level accuracy. This time around, the emphasis lay on developer-friendliness, which included engaging several measures such as simplifying the implementation process and making YOLO available to a potentially broader range of stakeholders.

With YOLO constantly changing Yolo encourages ongoing search for technology in the field of CV. The key ideas in object detection and neural networks such as YOLO imply that computers are capable of not only distinguishing objects but also interpreting the world around us by using these methods. They also show that the latest technology is advancing in this direction.

II. LITERATURE REVIEW

[1] C. Ryan et al., "Real-Time Multi-Task Facial Analytics With Event Cameras," in IEEE Access, vol. 11, pp. 76964-76976, 2023, doi: 10.1109/ACCESS.2023.3297500.

[2] G. Gallego, T. Delbrück, G. Orchard, C. Bartolozzi, B. Taba, A. Censi, et al., "Event-based vision: A survey", IEEE Trans. Pattern Anal. Mach. Intell., vol. 44, no. 1, pp. 154-180, Jan. 2022.

[3]] H. U. Khan, M. Z. Malik, S. Nazir and F. Khan, "Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector: A Systematic Analysis," in IEEE Access, vol. 11, pp. 80181-80198, 2023, doi: 10.1109/ACCESS.2023.3298824.

[4] C. Ryan, F. Murphy and M. Mullins, "End-to-end autonomous driving risk analysis: A behavioural anomaly detection approach", IEEE Trans. Intell. Transp. Syst., vol. 22, no. 3, pp. 1650-1662, Mar. 2021

[5] F. Becattini, F. Palai and A. D. Bimbo, "Understanding human reactions looking at facial microexpressions with an event camera", IEEE Trans. Ind. Informat., vol. 18, no. 12, pp. 9112-9121, Dec. 2022.

[6] H. Hu, Y. Fang, M. Han and X. Qi, "Multi-Scale Adaptive Graph Convolution Network for Skeleton-Based Action Recognition," in IEEE Access, vol. 12, pp. 16868-16880, 2024, doi: 10.1109/ACCESS.2024.3359234.

[7] V. Asha, "Real-Time Face Mask Detection in Video Streams Using Deep Learning Technique," 2023 4th International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2023, pp. 1254-1259, doi:10.1109/ICOSEC58147.2023.10276166.

[8] N. T J and K. Thinakaran, "An Enhanced Forensic Analysis and Security Surveillance Using Deep Reinforcement Learning," 2023 Second International Conference On Smart Technologies For Smart Nation (SmartTechCon), Singapore, Singapore, 2023, pp. 361-365, doi: 10.1109/SmartTechCon57526.2023.10391428.

[9] M. Balakrishnan, R. M, P. V. Kumar, S. Subramaniam and L. R, "Potato Plant Leaf Disease Detection and Recognition Using R-CNN Model," 2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN), Salem, India, 2023, pp. 605-609, doi: 10.1109/ICPCSN58827.2023.00106.

[10] N. T. J and K. Thinakaran, "Deep Neural Network-based Crime Scene Detection with Frames," 2023 Eighth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), Chennai, India, 2023, pp. 1-8, doi: 10.1109/ICONSTEM56934.2023.10142449.

III. PROPOSED SYSTEM

3.1 YOLO_v5:

Description:

In the area of banking security, this suggested system integrates Darknet with YOLO v5 to provide intelligent video image processing and surveillance. To improve monitoring capabilities within bank premises and enable real-time identification of security risks and suspicious actions, the system will make use of cutting-edge technologies. Here, they list the essential elements and features of the suggested system:

- Input Interface
- Data Conditioning
- Attribute Extraction
- Image Repository
- Object Detection Framework (YOLO)

Training Details:

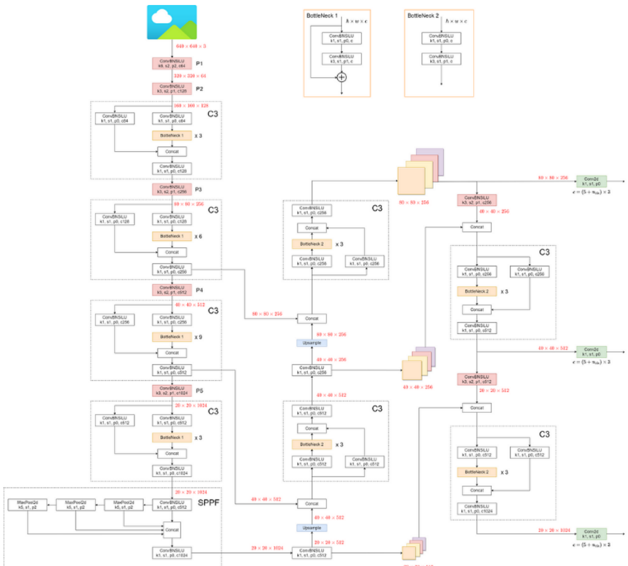
Training YOLOv5 requires a few essential steps. To ensure diversity and balance, the dataset is first constructed using annotated photos in the COCO format. With multiple versions (e.g., YOLOv5s, YOLOv5m, YOLOv5l, YOLOv5x) available, the model architecture consists of a CNN backbone for feature extraction, a neck for aggregating features, and a head for predicting bounding boxes and class probabilities. Transfer learning is applied using pre-trained weights during training, and robustness is improved by data augmentation methods such as random transformations and mosaic augmentation. Adam or SGD optimizers are used to optimize the model, together with an early halting mechanism and a learning rate scheduler. Lastly, evaluation is carried out with hyperparameters adjusted for best results, utilizing metrics such as mean Average Precision (mAP), precision, recall, and F1-score.

Benefits:

- **Processing in Real-time :**The capacity of YOLOv5 to process data in real time is essential for banking security since it allows for the quick identification of questionable activity like fraudulent transactions, illegal access, or possible security breaches. By acting quickly, situations are stopped before they get worse, protecting the bank's and its clients' safety.
- **Precision :**High object detection and classification accuracy are provided by YOLOv5, which is crucial in a banking setting where accuracy is paramount. Because the model can reliably detect faces, behaviors, and objects under a variety of situations, there is a decreased likelihood of false positives and negatives in surveillance systems.
- **Enhanced Productivity :**The monitoring procedure is streamlined in banking security systems by implementing YOLOv5. Its capacity to swiftly identify irregularities and scan numerous video feeds at once lessens the burden on human operators, freeing them up to verify and address actual threats instead of going through hours' worth of material.
- **Adaptability :**Because of its adaptable architecture, YOLOv5 may be integrated into a wide range of financial security applications, including extensive surveillance networks and teller stations as well as ATMs. This flexibility guarantees that the model can accommodate a wide range of security requirements in various contexts and branches.
- **Possibility of Adjusting :**Because of the model's adjustable nature, banks can tailor YOLOv5 to meet their unique security needs. Banks can improve the model's performance for specific scenarios, such as identifying fraud types or distinguishing known security concerns related to their operations, by training it on private datasets.

- **Open-source Accessibility :** The open-source nature of YOLOv5 offers banks an affordable way to improve their security measures. Because the model is open-source, the community can continuously contribute to its improvement and updates, keeping it up to speed with the most recent developments in object detection and machine learning.

Figure 1. Ultralytics, the company behind YOLO, released the architecture of YOLOv5



Source: https://sh-tsang.medium.com/brief-review-yolov5-for-object-detection-84cc6c6a0e3a

Flow Of Execution:

1. Obtaining Data:

Data acquisition in the banking security industry entails gathering a broad spectrum of visual data from multiple sources, including ATMs, surveillance cameras, and other monitoring devices. This dataset is comprehensive and depicts the variety of scenarios found in banking environments because it consists of photos and video recordings taken under various conditions and at different times.

2. Annotation of Data:

An important phase in the process is data annotation, in which the collected data is painstakingly tagged to identify things of interest, like faces, unauthorized individuals, suspicious activity, and other pertinent entities. By labeling the locations and classes of these items in every frame, a comprehensive and organized dataset is produced, which YOLOv5 may use for training. Precise annotation guarantees that the model acquires the ability to identify

3. YOLOv5 Instruction Training:

YOLOv5 for banking security trains the model to identify and categorize items with high accuracy using the annotated dataset. Transfer learning is used in the training phase, where the model is adjusted using the particular banking dataset once initial weights have been pre-trained. The model's robustness is increased by strategies like data augmentation, and optimal performance is attained by combining learning rate schedulers with optimization techniques like Adam or SGD.

YOLOv5 Single-Stage Detection Algorithm

For effective, real-time object detection, YOLOv5 employs a single-stage detection technique. Important actions consist of:

1. **Input Processing:** Adjust the input image's size and normalization.

2. **Feature Extraction:** To extract features, use a CNN backbone.

3. **Neck Architecture:** Use Path Aggregation Network (PANet) to improve features.

4. **Head Network**: Estimate class probabilities and bounding boxes.

5. **Anchor Boxes:** Compute the sizes and placements of objects.

6. **Predictive Bounding Box:** Adjust box coordinates.

7. **Class Prediction:** Ascertain which class is most likely.

8: **Non-Maximum Suppression (NMS):** Eliminate unnecessary discoveries.

9. **Output:** Present bounding boxes, confidence ratings, and class labels for items that have been discovered.

4 Assessment and Implementation:

To make sure the YOLOv5 model satisfies the required accuracy and reliability standards, it is thoroughly assessed after training using measures like mean Average Precision (mAP), precision, recall, and F1-score. The model is implemented throughout the bank's security architecture after it has been verified. This involves incorporating it into real-time monitoring settings such as ATMs, live surveillance systems, and other systems where it can function in real-time and improve security by promptly and precisely identifying possible threats. To sustain and enhance the model's efficacy over time, occasional retraining and ongoing monitoring are used.

IV. IMPLEMENTATION DETAILS :

4.1 Configuring the collaborative workspace:

Install necessary libraries and dependencies, including PyTorch, torchvision, and YOLOv5 repository.

4.2 Downloading YOLOv5 model weights:

The YOLOv5 model weights, users can navigate to the official repository for YOLOv5 variants. They can choose from different options tailored to specific requirements.The YOLOv5s pre-trained weights (yolov5s.pt) to current directory. Can replace yolov5s.pt with other model weights (e.g., yolov5m.pt, yolov5l.pt, or yolov5x.pt) if needed. After selecting the desired variant, users can download the corresponding model weights file and upload it to their Colab workspace for further utilization.

4.2. Preparing data:

Collect and label the dataset in the YOLO format (images and corresponding .txt files with bounding box annotations).

Organize the data into train, val, and test directories.

4.3. Script for person detection:

First, the YOLOv5 model and weights are loaded into the notebook. Subsequently, a function is defined for image loading and pre-processing, particularly if utilizing a custom dataset. Another function is implemented for person detection, where the image is loaded using the previously defined function or by providing a test image path. Inference with the YOLOv5 model is performed to obtain detections, followed by processing of the detections to identify people and person-like objects through bounding boxes and confidence scores. Optionally, detections can be visualized by drawing bounding boxes and labels ("person") on the image using libraries like OpenCV.

V. RESULTS AND DISCUSSION

Training the system:

Run the dataset and train the dataset repeatedly to improve the focal loss graph by pulling the curve of gamma value first setting it to 1 and increasing it step by step until the confidence curve of the predicted result improves.

Fig : Train batch_0

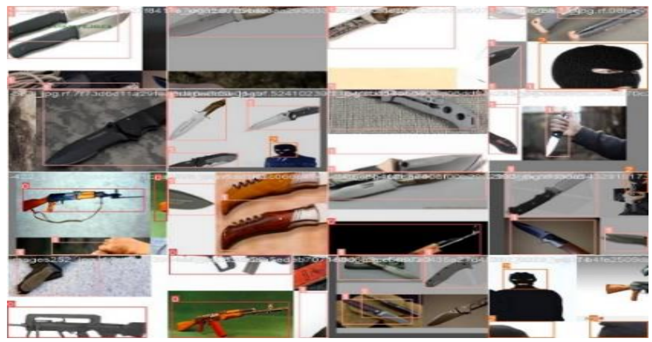


Fig : Train batch_2

Fig: Train batch-150

Predicted results:

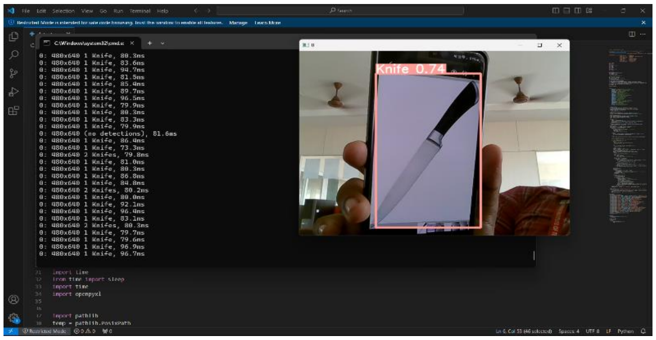


Fig:Value batch_0

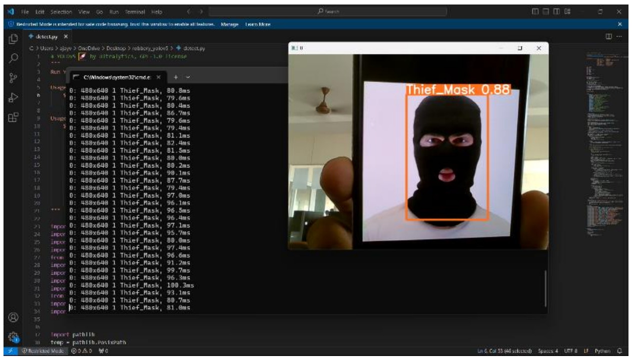
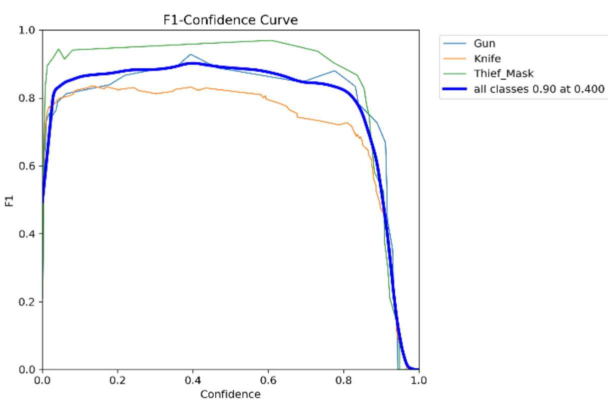


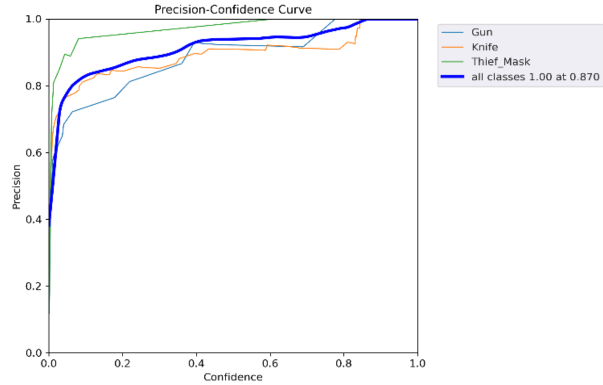
Fig:Val bactch_2,this fig shows the predcited output by training the images & valuing it which gives the output of detecting the person and person like objects from the given dataset.

7.1 Graph curve:

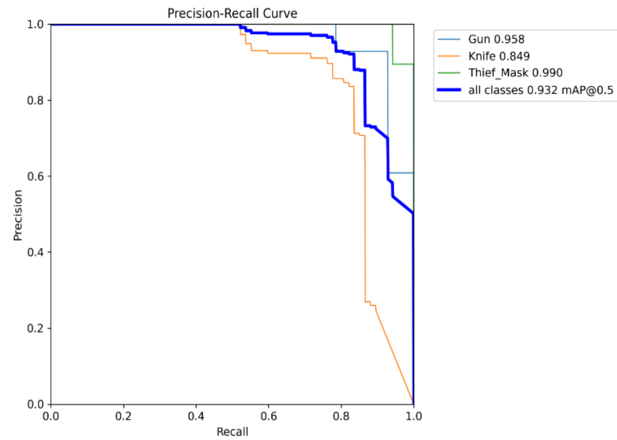
Confidence Curve:



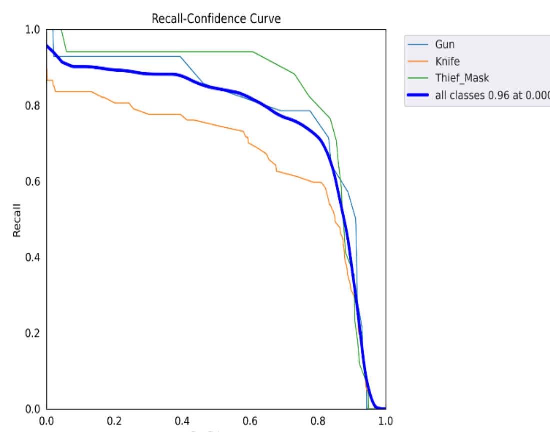
Precision confidence curve:



Precision recall curve:



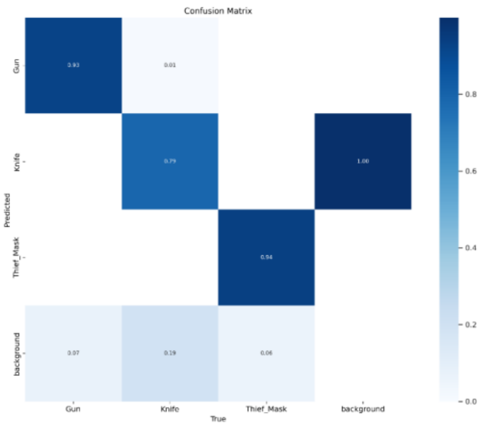
Recall confidence curve:



7.2 Confusion Matrix Analysis:

Understanding Predictions:

The confusion matrix, a powerful tool for dissecting model predictions, dissects the outcomes into four categories: true positives, true negatives, false positives, and false negatives. This visual representation elucidates areas where the model excels and those where improvements may be warranted. Examining the confusion matrix facilitates a granular understanding of the ensemble model's strengths and areas for refinement.



IX. CONCLUSION

This paper delves into the utilization of YOLOv5, a cutting-edge deep learning model, for real-time detection of people and person-like objects within images. Key modules include data acquisition, annotation, YOLOv5 training, and optional fine-tuning. A diverse dataset encompassing various factors such as poses, lighting conditions, and backgrounds was crucial for model training, impacting its performance and generalization. Each image in the dataset underwent meticulous annotation with bounding boxes around people and person-like objects, a time-consuming yet essential step. The YOLOv5 framework facilitated model training, utilizing a single-stage detection approach for faster processing speeds compared to multi-stage detectors. During training, the model learned to identify patterns and relationships within the data, enabling it to detect similar objects in new images. Fine-tuning, if required, involved leveraging pre-trained weights and training the model again on the specific dataset to potentially enhance accuracy for unique use cases.

Predicted results include accurate detection, real-time applicability, and adaptability. The system aims to accurately identify and localize people and person-like objects within images with high precision, minimizing false positives and negatives. YOLOv5's speed enables real-time processing of video streams or image sequences, suitable for applications requiring quick responses. Additionally, the framework offers functionalities for customizing the training process through user-defined configurations, allowing for fine-tuning of the model to specific scenarios beyond the initial dataset. This adaptability opens doors for various applications across diverse domains.

The successful implementation of this project holds promising applications in fields reliant on real-time person detection. Security systems can benefit from improved monitoring with real-time alerts for unauthorized intrusions. Crowd analysis can utilize accurate person counting and tracking for better resource allocation and safety measures in events or public spaces. Autonomous systems can enhance navigation and interaction with the environment, ensuring safe operation by accurately detecting people and person-like objects to avoid collisions. Overall, this project explores the potential of YOLOv5 for person and person-like object detection, contributing to advancements in computer vision tasks requiring real-time processing and adaptability to diverse scenarios.

REFERENCES

[1] C. Ryan et al., "Real-Time Multi-Task Facial Analytics With Event Cameras," in IEEE Access, vol. 11, pp. 76964-76976, 2023, doi: 10.1109/ACCESS.2023.3297500.

[2] G. Gallego, T. Delbrück, G. Orchard, C. Bartolozzi, B. Taba, A. Censi, et al., "Event-based vision: A survey", IEEE Trans. Pattern Anal. Mach. Intell., vol. 44, no. 1, pp. 154-180, Jan. 2022.

[3] H. U. Khan, M. Z. Malik, S. Nazir and F. Khan, "Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector: A Systematic Analysis," in IEEE Access, vol. 11, pp. 80181-80198, 2023, doi: 10.1109/ACCESS.2023.3298824.

[4] C. Ryan, F. Murphy and M. Mullins, "End-to-end autonomous driving risk analysis: A behavioural anomaly detection approach", IEEE Trans. Intell. Transp. Syst., vol. 22, no. 3, pp. 1650-1662, Mar. 2021

[5] F. Becattini, F. Palai and A. D. Bimbo, "Understanding human reactions looking at facial microexpressions with an event camera", IEEE Trans. Ind. Informat., vol. 18, no. 12, pp. 9112-9121, Dec. 2022.

[6] H. Hu, Y. Fang, M. Han and X. Qi, "Multi-Scale Adaptive Graph Convolution Network for Skeleton-Based Action Recognition," in IEEE Access, vol. 12, pp. 16868-16880, 2024, doi: 10.1109/ACCESS.2024.3359234.

[7] V. Asha, "Real-Time Face Mask Detection in Video Streams Using Deep Learning Technique," 2023 4th International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2023, pp. 1254-1259, doi:10.1109/ICOSEC58147.2023.10276166.

[8] N. T J and K. Thinakaran, "An Enhanced Forensic Analysis and Security Surveillance Using Deep Reinforcement Learning," 2023 Second International Conference On Smart Technologies For Smart Nation

(SmartTechCon), Singapore, Singapore, 2023, pp. 361-365, doi: 10.1109/SmartTechCon57526.2023.10391428.

[9] M. Balakrishnan, R. M, P. V. Kumar, S. Subramaniam and L. R, "Potato Plant Leaf Disease Detection and Recognition Using R-CNN Model," 2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN), Salem, India, 2023, pp. 605-609, doi: 10.1109/ICPCSN58827.2023.00106.

[10] N. T. J and K. Thinakaran, "Deep Neural Network-based Crime Scene Detection with Frames," 2023 Eighth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), Chennai, India, 2023, pp. 1-8, doi: 10.1109/ICONSTEM56934.2023.10142449.

[11] T. J. Nandhini and K. Thinakaran, "An Improved Crime Scene Detection System Based on Convolutional Neural Networks and Video Surveillance," 2023 Fifth International Conference on Electrical, Computer and Communication Technologies (ICECCT), Erode, India, 2023, pp. 1-6, doi: 10.1109/ICECCT56650.2023.10179852.

[12] M. Rahevar, A. Ganatra, T. Saba, A. Rehman and S. A. Bahaj, "Spatial–Temporal Dynamic Graph Attention Network for Skeleton-Based Action Recognition," in IEEE Access, vol. 11, pp. 21546-21553, 2023, doi: 10.1109/ACCESS.2023.3247820.

[13] T. Anagnostopoulos, P. Kostakos, I. Salmon, Y. Psaromiligkos, K. Ntalianis and S. R. Jino Ramson, "Spatiotemporal Authentication System Architecture for Smart Campus Safety," 2022 4th International Conference on Smart Sensors and Application (ICSSA), Kuala Lumpur, Malaysia, 2022, pp. 155-160, doi: 10.1109/ICSSA54161.2022.9870931.

[14] B. Oztas, D. Cetinkaya, F. Adedoyin, M. Budka, H. Dogan and G. Aksu, "Perspectives from Experts on Developing Transaction Monitoring Methods for Anti-Money Laundering," 2023 IEEE International Conference on e-Business Engineering (ICEBE), Sydney, Australia, 2023, pp. 39-46, doi: 10.1109/ICEBE59045.2023.00024.

[15] S. G, D. Chandrasekaran, M. D. Sre and M. Sathiyanarayanan, "Predicting Abnormal User Behaviour Patterns in Social Media Platforms based on Process Mining," 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bengaluru, India, 2023, pp. 204-209, doi: 10.1109/IITCEE57236.2023.10091025.

[16] X. Luo, X. Han, W. Zuo, Z. Xu, Z. Wang and X. Wu, "A Dynamic Transaction Pattern Aggregation Neural Network for Money Laundering Detection," 2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Wuhan, China, 2022, pp. 818-826, doi: 10.1109/TrustCom56396.2022.00114.

[17] B. Oztas, D. Cetinkaya, F. Adedoyin and M. Budka, "Enhancing Transaction Monitoring Controls to Detect Money Laundering Using Machine Learning," 2022 IEEE International Conference on e-Business Engineering (ICEBE), Bournemouth, United Kingdom, 2022, pp. 26-28, doi: 10.1109/ICEBE55470.2022.00014.

[18] D. Balakrishnan, U. Mariappan, S. S. Seerla, P. V. Tej, Y. E. Vani and S. Fazi, "Isolation Forest based Fraud Detection for Cryptocurrency Transaction," 2023 International Conference on Integrated Intelligence and Communication Systems (ICIICS), Kalaburagi, India, 2023, pp. 1-6, doi: 10.1109/ICIICS59993.2023.10421325.

[19] S. Kaushik and N. E. Madhoun, "Analysis of Blockchain Security: Classic Attacks, Cybercrime and Penetration Testing," 2023 Eighth International Conference On Mobile And Secure Services (MobiSecServ), Miami Beach, FL, USA, 2023, pp. 1-6, doi: 10.1109/MobiSecServ58080.2023.10329210.

[20] K. Kalra and R. G. Tiwari, "Exploring Common Areas and Types of Cybercrime in Today's Digital Landscape," 2023 3rd Asian Conference on Innovation in Technology (ASIANCON), Ravet IN, India, 2023, pp. 1-6, doi: 10.1109/ASIANCON58793.2023