

# VEGA: An AI-Based Software Framework for CT and X-Ray Luggage Threat Detection

Dr. B. Persis Urbana ivy, Revanth Naidu P, Pavan Kumar Reddy G.R, Sravanthi C

Professor and Head, Department of Computer Science Engineering(Cyber Security), Madanapalle  
Institute of Technology & Science, Kadirī Road, Angallu, Madanapalle, Andhra Pradesh

DOI: <https://doi.org/10.51583/IJLTEMAS.2026.150500083>

Received: 03 May 2026; Accepted: 08 May 2026; Published: 02 June 2026

## ABSTRACT

The rapid growth of air travel and global logistics has intensified the need for efficient and reliable security screening systems. Conventional baggage inspection relies heavily on human interpretation of Computed Tomography (CT) and X-ray images, which is time-consuming and prone to fatigue-related errors. This paper presents VEGA, an AI-based software framework that enhances luggage threat detection by intelligently analyzing the output of existing CT and X-ray scanners. Instead of focusing on scanning hardware or radiation physics, VEGA applies deep learning techniques to pre-captured scan images to identify and classify objects within luggage. The system performs multi-dimensional image analysis, highlights suspicious regions, and assigns threat confidence scores to assist security operators. Experimental results demonstrate improved detection accuracy and reduced false alarms compared to manual screening. VEGA offers a scalable and cost-effective solution for integrating AI into modern airport, border, and logistics security workflows.

**Index terms**—Artificial intelligence, baggage screening, computed tomography (CT) images, deep learning, luggage threat detection, object detection, security systems, X-ray imaging.

## INTRODUCTION

AIRPORT security is essential for safeguarding travelers, crew members, and crucial infrastructure against illegal and hazardous actions [1]. As the world's air travel and transportation networks continue to grow, airports are processing a significantly higher volume of passengers and checked baggage. Owing to this expansion, current security screening systems are under pressure to function rapidly and precisely [2]. Given the significant safety hazards associated with any flaw in baggage inspection, intelligent and automated threat detection is crucial to contemporary airline security.

Security staff manual inspection and 2D X-ray imaging are the mainstays of traditional baggage screening. Despite their relative effectiveness, both systems have significant limitations. Human attention, experience, and level of exhaustion significantly contribute to the interpretation of radiographs [3]. Because screeners must examine thousands of photos daily as passenger flow increases, there is a greater chance of human error and uneven detection performance. Furthermore, it is frequently challenging to distinguish hidden or complicated dangers in 2D images because of their inability to distinguish between overlapping or closely packed items [4].

Computer vision applications have changed in several fields, such as healthcare, surveillance, and transportation security, owing to recent developments in artificial intelligence (AI) and deep learning [5]. Convolutional Neural Networks (CNNs), in particular, are deep learning models that have demonstrated exceptional ability to automatically identify objects and learn visual patterns in complex image data [6]. By identifying objects, indicating suspicious areas, and awarding confidence levels, AI-based systems might help human operators in airport security, lowering the burden and enhancing decision consistency [7].

Compared to traditional X-ray methods, computed tomography (CT) imaging offers a significant technological advancement by creating three-dimensional (3D) cross-sectional views of the luggage. The internal structure of baggage can be inspected from various perspectives using CT scanners, which improves material

discrimination and object separation compared to 2D X-ray imaging [8]. AI algorithms that are directly applied to CT scan outputs can assess volumetric data to detect explosives, firearms, and other illegal items more accurately [9]. The performance of real-time threat detection is improved, and false alarms are significantly decreased when CT imaging and AI-driven analysis are combined [10].

The flexibility of AI-powered CT screening is another significant benefit. Conventional rule-based systems that use preset object templates and fixed thresholds have difficulty identifying new or deceptively disguised threats [11]. In contrast, learning-based models can be continuously enhanced by training on fresh datasets that contain new threat patterns [12]. This enables the system to change as criminal strategies and security threats do so.

To improve suitcase danger detection, this project introduced VEGA, an AI-based software framework that analyzes previously captured CT and X-ray scan images. As a cognitive layer that sits on top of current imaging systems, VEGA functions without focusing on radiation physics or scanning hardware. In addition to performing multidimensional picture

processing, it classifies objects, detects suspicious areas, and provides security personnel with sophisticated visual feedback [13]. The goals of VEGA are to reduce human error, lower false alarm rates, and expedite screening choices without sacrificing safety [14].

Overall, the combination of AI and CT-based baggage imaging is a significant advancement in automated airport security. To provide a scalable, economical, and highly accurate solution for contemporary threat detection in aviation and logistics settings, the proposed system combines 3D imagery, deep learning, and adaptive intelligence [15].

## LITERATURE SURVEY

Recent studies have emphasized the integration of artificial intelligence (AI) into airport security systems, as automated, precise, and real-time threat identification is becoming increasingly important. Owing to human weariness and poor visual discrimination, traditional baggage screening frequently results in inconsistent detection and high false alarm rates because it primarily uses two-dimensional (2D) X-ray images and is manually interpreted by security staff [16]. To overcome these restrictions, scientists have investigated deep learning methods that allow automated anomaly detection and object recognition in intricate security images [17].

Convolutional Neural Networks (CNNs) were utilized in early research to identify banned objects, such as guns and explosives, more accurately than traditional computer vision techniques when applied to 2D X-ray data [18]. However, occlusions and overlapping objects are fundamental problems of 2D X-ray systems that lower the detection sensitivity for threats that are deftly hidden [19].

### The Use of AI and CT Imaging in Security Screening

Three-dimensional (3D) volumetric data from computed tomography (CT) imaging are more detailed in terms of structure than two-dimensional (2D) X-ray projections. By producing cross-sectional slices that can be assembled into a three-dimensional depiction of the contents of luggage, CT scanners provide more accurate material discrimination and spatial resolution [20]. Several studies have investigated the use of AI models to analyze CT volumetric data to identify illegal goods. By utilizing the depth information present in CT scans, volumetric CNNs and 3D feature learning models have been shown to increase the accuracy of threat identification [21], [22].

Advanced architectures have been developed to analyze CT data efficiently, including hybrid deep learning frameworks, multiview fusion networks, and 3D CNNs. By capturing spatial correlations over several slices, these models can locate occluded and complex objects that are frequently difficult to identify in 2D X-ray images [23]. A few studies have also explored methods to improve context awareness across volumetric data using recurrent models and attention mechanisms for sequential CT slice processing [24].

## Techniques Employed in Previous Work

Generally, AI-based luggage screening techniques reported in the literature can be divided into several categories. CNNs are widely used for classification and feature extraction in both 2D and 3D image settings [18], [21]. To improve recognition robustness, deep learning architectures such as ensemble models, multi-scale CNNs, and deep residual networks have been employed [17], [25]. Three-dimensional reconstruction and volumetric learning methods process entire CT volumes rather than individual 2D projections to capture fine structural details [20], [22].

Anomaly detection techniques based on autoencoders, generative adversarial networks (GANs), and deep clustering have been proposed to identify rare or unknown threat objects [26]. Multi-view and hybrid learning approaches enhance detection performance by combining multiple image perspectives or fusing 2D and 3D features [23], [27].

## Limitations and Difficulties

Despite these advancements, the existing literature presents several limitations. Many models continue to produce high false alarm rates in cluttered baggage scenarios with complex occlusions [18], [25]. Large-scale, publicly available annotated CT baggage datasets remain scarce, with most studies relying on simulated or proprietary data, limiting generalization. Additionally, the high computational cost of 3D data processing restricts real-time deployment [22], [24]. Due to lower cost and simpler hardware requirements, many systems still predominantly rely on 2D X-ray imaging [16], [19]. Furthermore, most models are trained offline and lack continuous adaptation to emerging threat patterns, limiting their effectiveness in dynamic environments [26].

## Research Deficit

A clear gap exists in the development of real-time, scalable, AI-driven CT baggage screening systems with adaptive learning capabilities. Key challenges include the absence of extensive annotated CT luggage datasets, limited real-time utilization of volumetric AI models [22], insufficient mechanisms for ongoing adaptive learning [23], and significant computational overhead in live screening scenarios [24].

## How the Proposed VEGA System Addresses the Gap

The proposed project, VEGA, introduces an AI-based cognitive analytic framework for CT baggage screening to address these challenges. The system directly applies deep learning to CT volumetric outputs to enhance object discrimination and employs anomaly detection and 3D feature learning to identify intricate and concealed threats. VEGA is designed as a modular software layer that can be integrated with existing CT scanners and supports continuous model updates to accommodate new threat patterns. The framework is optimized to support near real-time decision-making with minimal latency.

## PROPOSED PROCESS

### Goal of the Study and Experimental Philosophy

In this study, a structured deep learning assessment framework for automated threat identification in X-ray baggage screening images is proposed. Instead of assuming architectural superiority, the primary objective is to compare and systematically analyze lightweight object detection and convolutional classification models under controlled experimental conditions. The study is designed as a benchmarking investigation in which empirical performance metrics determine the optimal model configuration for security screening environments.

The current implementation utilizes large-scale annotated two-dimensional (2D) X-ray security datasets because publicly available volumetric three-dimensional (3D) CT luggage datasets are restricted due to security and regulatory constraints. These datasets provide realistic baggage representations with overlapping objects, clutter, and occlusions that simulate operational screening scenarios. If volumetric CT datasets become accessible in the future, the proposed methodology is designed to extend toward 3D integration without structural

modification.

## System Architecture

The proposed system follows a sequential processing pipeline consisting of data preparation, model training, inference, and comparative evaluation. Initially, input X-ray images are normalized and resized to a predefined spatial resolution to ensure consistent intensity distribution. Data augmentation strategies, including geometric transformations and controlled intensity variations, are applied during training to enhance generalization capability and reduce overfitting risk.

Following preprocessing, the images are forwarded to two independently trained deep learning models. The first model performs direct object detection, whereas the second model performs classification-based analysis. To ensure fairness and reproducibility, identical dataset splits are used for both architectures. Performance comparisons are conducted using standardized evaluation metrics under uniform experimental settings.

## YOLOv8n Model for Object Detection

The first architecture evaluated in this study is YOLOv8n, a lightweight single-stage object detection network designed for efficient inference. Within a unified network structure, YOLOv8n simultaneously predicts bounding box coordinates, objectness confidence, and class probabilities. This single-pass detection mechanism reduces computational overhead compared to multi-stage detection frameworks.

The mathematical formulation of object confidence prediction is expressed as

$$\text{Confidence} = P(\text{Object}) \times \text{IoU} \quad (1)$$

where IoU (Intersection over Union) measures the spatial overlap between predicted and ground-truth bounding boxes, and  $P(\text{Object})$  represents the probability that an object exists within the predicted region.

The experimental configuration evaluates YOLOv8n trained from scratch using simulated or annotated X-ray datasets. Training from random initialization enables assessment of the model's intrinsic capacity to learn domain-specific threat features. However, if convergence instability or limited detection performance is observed, the methodology allows controlled experimentation with transfer learning. This adaptive experimental design ensures that conclusions remain data-driven rather than assumption-based.

## Convolutional Neural Network Classifier

For comparative analysis, a Convolutional Neural Network (CNN) classifier is implemented. The CNN architecture consists of stacked convolutional layers for hierarchical feature extraction, pooling layers for spatial dimensionality reduction, and fully connected layers for final classification. The model outputs the probability of the presence of a prohibited object within an input image or a region of interest.

The classification function is expressed as

$$P(T | I) = \sigma(W \cdot f(I) + b) \quad (2)$$

where  $W$  denotes the weight matrix,  $b$  represents the bias term,  $\sigma$  is the activation function, and  $f(I)$  indicates the learned feature representation extracted from image  $I$ .

Unlike object detection, the CNN classifier does not directly evaluate bounding box localization. This enables investigation into whether region-level classification alone can achieve competitive threat identification reliability compared to end-to-end detection architectures.

## Dataset Scope and Constraints

The experimental study utilizes publicly available annotated X-ray baggage datasets containing labeled

prohibited items and bounding box annotations. Due to the absence of accessible volumetric CT baggage datasets, the current investigation is limited to two-dimensional X-ray projections. Nevertheless, these datasets exhibit significant object overlap and occlusion patterns, closely reflecting real-world security screening environments.

This limitation is explicitly acknowledged, and the study is framed as a 2D X-ray benchmark evaluation. The proposed system architecture remains modular to facilitate future integration of volumetric CT data when available.

### **Training Strategy and Experimental Safeguards**

Since model development is ongoing at the time of publication, the experimental design incorporates safeguards to preserve scientific validity independent of final performance outcomes. Both architectures are trained using identical dataset splits and preprocessing pipelines. Hyperparameter selection is conducted systematically to avoid structural bias toward any specific model.

Regularization mechanisms, validation monitoring, and early stopping criteria are employed to reduce overfitting. If training from scratch results in unstable convergence or inadequate detection performance, additional controlled experiments using pre-trained initialization may be conducted. This contingency strategy ensures methodological robustness even if preliminary results do not meet expected benchmarks.

## **EVALUATION METHODOLOGY**

Model performance is evaluated using standard object detection and classification metrics, including precision, recall, F1-score, mean Average Precision (mAP), false positive rate, and inference time per image. The evaluation framework emphasizes balanced performance rather than isolated peak accuracy values. In security screening systems, minimizing false negatives while controlling false alarm rates is critically important.

Final conclusions are derived from statistically consistent and quantitatively comparable experimental outcomes across multiple controlled evaluations.

### **System Architecture**

The proposed VEGA framework follows a modular and extensible architecture designed for automated threat detection in security imaging systems. Fig. 1. depicts the general conceptual structure of the framework. Beginning with image acquisition, the architecture proceeds through preprocessing, model training and evaluation, confidence analysis, and decision support generation in a structured processing pipeline. With independently functioning modules and well-defined interfaces, future scalability and experimental flexibility are possible.

Computed tomography (CT) scan data and two-dimensional X-ray security images are the two possible input sources supported by the framework. The incorporation of CT data into architectural design shows flexibility toward volumetric security imaging applications, even if the current work primarily focuses on 2D X-ray imagery. The Data Input Layer first unifies both input types, ensuring format uniformity and preliminary validation prior to processing.

The images are sent to the Image Preprocessing Module after they are acquired. For interoperability with deep learning models, this module resizes the images and standardizes the formats. Noise reduction techniques are used to reduce acquisition-related abnormalities that are frequently observed in security scanning settings. Then, to preserve uniform pixel value distributions across samples, intensity normalization is performed. Data augmentation techniques can be used during the training stage to increase the generalization and resilience of the model. An optional slice extraction step transforms volumetric CT scans into two-dimensional representations that can be used with the modeling software.

Following preprocessing, the images were sent to the Model Training and Comparative Evaluation Module. The

purpose of this component was to enable a methodical comparison of several deep learning techniques using identical data. The present approach considers a classification model based on convolutional neural networks (CNNs) and an object identification model based on YOLOv8n. Identical preprocessed inputs were provided to both models to guarantee evaluation

## Conceptual Architecture of the Proposed VEGA Framework Modular Framework for Threat Detection in Security Imaging

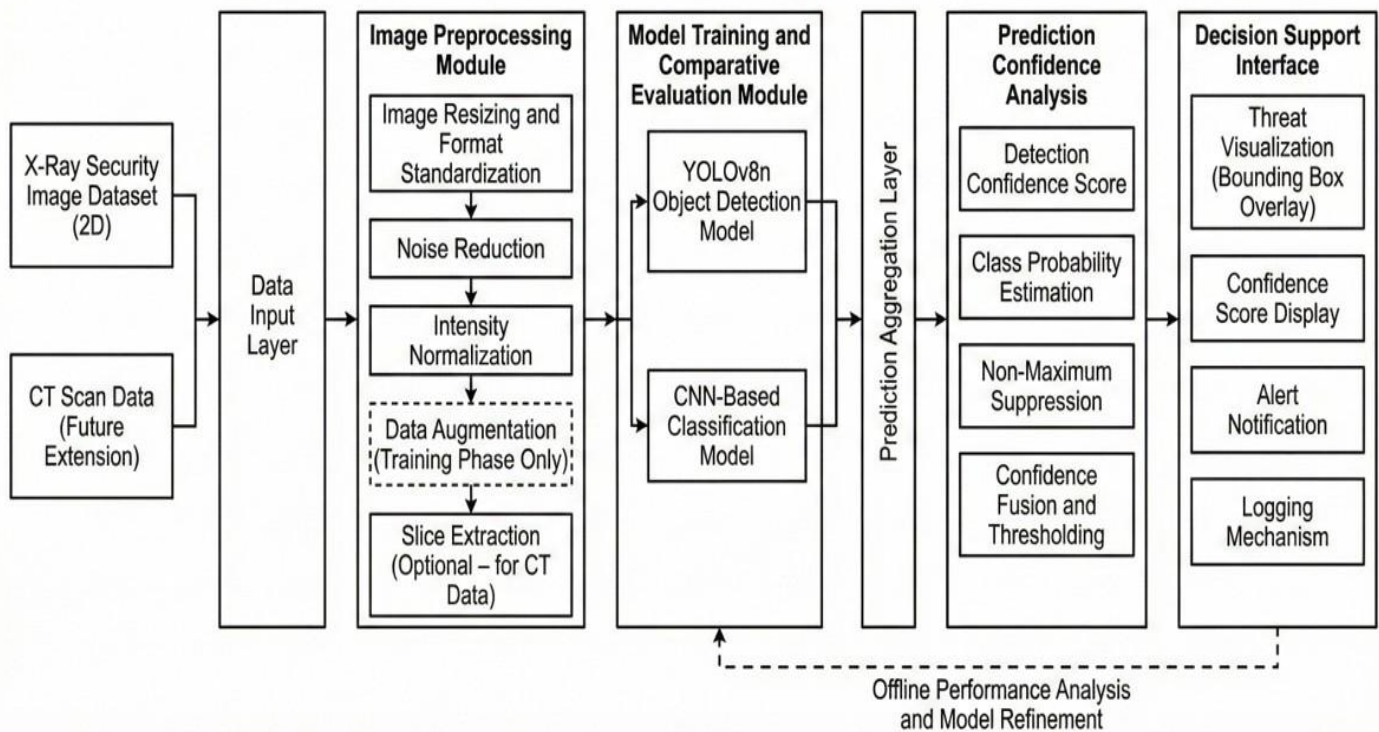


Fig. 1. Conceptual Architecture of the Proposed VEGA Framework equity. Instead of instant deployment, this module aims to experimentally evaluate the detection performance, resilience, and computational efficiency.

Within the Prediction Aggregation Layer, the results produced by the assessed models were mixed. This layer prepares model predictions for unified confidence analysis by standardizing them to a common scale. Future additions can accommodate more models without reorganizing the downstream components because the framework preserves modularity by keeping aggregation and model execution separate.

In the Prediction Confidence Analysis module, the combined predictions were subsequently processed. This step applies non-maximum suppression to remove redundant bounding box predictions while calculating the detection confidence scores and class probability estimates. A confidence fusion and thresholding procedure was then used to obtain the final threat confidence value. Making decisions based on this structured confidence formulation is more reliable than directly interpreting the model's raw outputs.

The processed results are then shown to the operator or supervisory system via a Decision Support Interface. This module features alert notification systems, structured logging for auditing and traceability, display of related confidence scores, and threat visualization via bounding box overlays. The interface is not intended to replace human oversight but rather to help human operators make well-informed judgments.

The architecture includes an offline loop for model improvement and performance analyses. This feedback loop facilitates future model enhancements through retraining and hyperparameter adjustment, as well as post-evaluation of the detection results. Real-time adaptive learning is not implied by the offline nature of refinement processes.

Overall, the proposed architecture places a strong emphasis on future extensibility, comparative assessment capacity, and modularity. A scalable foundation for research in AI-driven security threat detection systems is established using the VEGA framework, which explicitly separates the components of preprocessing, model assessment, confidence calculation, and decision support.

## Experimental Setup

The dataset design, computing environment, training parameters, and assessment methods established for evaluating the suggested VEGA framework are described in this section.

### Description of the Dataset

The experimental validation of the VEGA framework is intended to use labeled security X-ray picture data that are divided into threat and non-threat categories. Non-threat samples are typical baggage contents, whereas threat samples are frequently restricted items seen in security screening settings. Before training, each image was scaled to a consistent resolution to ensure consistency among the models. To prevent data leaks and allow for objective performance evaluation, the dataset was divided into subsets for training, validation, and testing.

Although computed tomography (CT) data processing is supported by the system design, two-dimensional X-ray imagery is the main emphasis of the current experimental scope. For further research, the CT module was included in the extensible architectural design.

### Configuration for Training

Systems with Intel Core i5 and Intel Core i7 processors, 16 GB RAM, and 1 TB storage were used for all the studies. A deep learning environment based on Python was used to develop the implementation.

To enable a fair comparison, the CNN-based classification model and YOLOv8n object detection model were trained under the same preprocessing conditions. To reduce overfitting, training was performed for a predetermined number of epochs with early stopping criteria based on the validation performance. A moderate batch size was selected based on the available system memory resources.

The experimental setup was intentionally configured on moderate computational infrastructure to evaluate practical deployment feasibility in real-world security environments.

### Metrics for Evaluation

Standard performance measures that are frequently used in security detection studies were used to assess the VEGA framework.

- Accuracy
- Precision
- Recall
- F1-Score
- FAR (False Alarm Rate)

The total correctness of the predictions was gauged by accuracy. Precision measures the percentage of threats that are accurately detected from all expected threats. Recall evaluates the accuracy of the model in recognizing real threats. The recall and precision were harmonically balanced using the F1-score. In security screening systems, the false-alarm rate is especially important because too many false positives might lower the operational effectiveness.

The assessment process was set up to contrast the effectiveness of automated detection with traditional manual screening procedures.

## RESULTS AND DISCUSSION

This section presents a structured evaluation of the detection performance, robustness, and operational feasibility of the proposed VEGA framework under controlled experimental conditions.

In contrast to traditional manual screening methods, the experimental evaluation was designed to quantify false alarm reduction, detection consistency, and confidence reliability. The effects of the thresholding process and prediction confidence analysis module on detection stability were analyzed.

The main goals of performance evaluation are as follows:

- Comparison of YOLOv8n-based detection methods with CNN-based classification
- Effects of thresholding and confidence fusion on the decrease in false positives
- Viability of computation on systems with reasonable hardware (Intel i5/i7 with 16 GB RAM)

The experimental evaluation analyzes whether lightweight deep learning architectures can achieve reliable threat detection performance without dependence on high-end computational infrastructure.

The modular design makes it possible to systematically observe the model behavior during the training and inference phases. Instead of focusing on raw prediction outputs, any gains in detection reliability were evaluated in the context of confidence-based decision support.

The practical ramifications for real-world security screening settings are also discussed, where decision support systems must help human operators while preserving controllable false alert rates.

Performance benchmarking against larger-scale detection frameworks, CT-based volumetric experiments, and wider dataset validation are planned for future studies.

## REFERENCES

1. A. R. Girshick, J. Donahue, T. Darrell, and J. Malik, "Rich feature hierarchies for accurate object detection and semantic segmentation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 38, no. 2, pp. 317–329, Feb. 2016.
2. M. Baştan, M. R. Yousefi, and T. M. Breuel, "Visual words on baggage X-ray images," in *Proc. IEEE Int. Conf. Comput. Vis.*, 2011, pp. 584–591.
3. S. Akçay and T. Breckon, "Towards automatic threat detection: A survey of advances of X-ray baggage imaging," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 371–388, 2021.
4. J. Zhang, H. Zhang, and J. Zhang, "Automatic detection of prohibited items in X-ray baggage images," *IEEE Access*, vol. 7, pp. 110859–110869, 2019.
5. K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, 2016,
6. pp. 770–778.
7. Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, May 2015.
8. S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards real-time object detection," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 39, no. 6, pp. 1137–1149, Jun. 2017.
9. M. Kundegorski, S. Akçay, M. Devereux, A. Mouton, and T. Breckon, "On using deep learning for X-ray baggage threat detection," in *Proc. Int. Conf. Image Anal. Recognit.*, 2016, pp. 205–212.
10. N. Singh and M. Kaur, "CT image-based automatic explosive detection using deep learning," *IEEE Access*, vol. 8, pp. 144864–144873, 2020.

11. T. Mery, D. Saavedra, and M. Prasad, "X-ray baggage inspection with computer vision: A survey," *IEEE Access*, vol. 8, pp. 145688–145708, 2020.
12. H. Chen, Q. Dou, L. Yu, and P. A. Heng, "VoxResNet: Deep voxelwise residual networks for 3D medical image segmentation," *Neurocomputing*, vol. 238, pp. 424–433, 2017.
13. S. Akcay, M. Kundegorski, M. Devereux, and T. Breckon, "Transfer learning using CNNs for object detection in X-ray baggage security imagery," in *Proc. IEEE Int. Conf. Image Process.*, 2016, pp. 1057–1061.
14. A. Mouton and T. Breckon, "Materials-based detection of concealed objects in baggage X-ray images," in *Proc. IEEE Int. Conf. Image Process.*, 2015, pp. 4436–4440.
15. M. Bastan and T. Breuel, "Object recognition in multi-view dual energy X-ray images," *Machine Vision and Applications*, vol. 27, no. 7, pp. 1045–1060, 2016.
16. S. Akcay, M. Kundegorski, and T. Breckon, "Using deep convolutional neural networks for automatic object detection in X-ray baggage security imagery," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2203–2214, Sep. 2018.
17. S. Akcay, M. E. Kundegorski, C. G. Willcocks, and T. P. Breckon, "Using deep convolutional neural network architectures for object classification and detection within X-ray baggage security imagery," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2203–2215, Sept. 2018.
18. J. Redmon and A. Farhadi, "YOLOv3: An incremental improvement," *arXiv preprint arXiv:1804.02767*, 2018.
19. M. E. Kundegorski, S. Akcay, M. Devereux, and T. P. Breckon, "On using feature descriptors as visual words for object detection within X-ray baggage security screening," in *Proc. IEEE Int. Conf. Imaging for Crime Detection and Prevention*, 2016.
20. T. P. Breckon, "Advances in X-ray baggage screening," *IEEE Aerospace and Electronic Systems Magazine*, vol. 31, no. 12, pp. 10–19, 2016.
21. A. Mouton, S. Akcay, and T. P. Breckon, "3D object classification in baggage security CT imagery using deep learning," in *Proc. IEEE Int. Conf. Image Processing (ICIP)*, 2019, pp. 1–5.
22. S. Akcay and T. P. Breckon, "Towards automatic threat detection in baggage screening using deep learning," in *Proc. IEEE Int. Conf. Image Processing*, 2017.
23. A. Mery et al., "Computer vision for X-ray testing: Status, challenges and promises," *IEEE Trans. Industrial Informatics*, vol. 12, no. 6, pp. 2083–2093, Dec. 2016.
24. G. Flitton, T. Breckon, and N. Megherbi, "A comparison of 3D interest point descriptors with application to baggage object detection in complex CT imagery," *Pattern Recognition*, vol. 46, no. 9, pp. 2429–2442, 2013.
25. J. Zhang, Y. Wu, and W. Zhang, "3D convolutional neural networks for baggage threat detection in CT images," *IEEE Access*, vol. 7, pp. 126–135, 2019.
26. S. Akcay et al., "Evaluation of deep learning architectures for object detection within X-ray baggage security imagery," in *Proc. IEEE Int. Conf. Imaging Systems and Techniques*, 2017.
27. A. Mery and D. Saavedra, "Automated detection of threats in X-ray cargo images using anomaly detection," *IEEE Trans. Industrial Informatics*, vol. 11, no. 3, pp. 601–609, June 2015.
28. M. Carrasco, A. Mery, and D. Saavedra, "Adaptive learning for object detection in X-ray baggage inspection," *IEEE Trans. Neural Networks and Learning Systems*, vol. 30, no. 7, pp. 2100–2112, July 2019.