Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/180103

Strengthening the Security of the Kuwait International Airport by Detecting Threats in X-ray Images

Abdallah S. Mohamed[1], *Adel A. Sewisy*[1], *Khaled F. Hussain*[1] *and Ahmed I. Taloba*[2,*]

[1]Department of Computer Science, Faculty of Computers and Information, Assiut University, Assiut, Egypt
[2]Information System Department, Faculty of Computers and Information, Assiut University, Assiut, Egypt

Received: 1 Sep. 2023, Revised: 11 Oct. 2023, Accepted: 15 Nov. 2023
Published online: 1 Jan. 2024

Abstract: The substantial number of false positives in X-ray analysis of images is one of the current problems, which causes delays and adds to the responsibilities of security staff. Maintaining security measures to confront growing threats and new technology is a continuing concern. Using a Convolutional Neural Network-Gated Recurrent Unit (CNN-GRU) model, this research suggests a novel strategy for upgrading the safety precautions at Kuwait International Airport. This research tackles the requirement for more precise and efficient threat detection, which is crucial for airport security. Utilizing the advantages of CNNs and GRUs is the goal of the CNN-GRU approach. The GRU, a recurrent neural network, can evaluate the ordered sequence of X-ray scans and keep context across time. At the same time, the CNN element is skilled at extracting features and can interpret X-ray images to identify potential hazards. With the help of this communication, the model is better equipped to identify hidden risks and is more accurate. This research involves a thorough analysis of the effectiveness of the suggested model via intensive training and testing. The findings show that the CNN-GRU model works better than traditional approaches in recognizing threats in X-ray pictures, considerably lowering false positives and increasing safety precautions at Kuwait International Airport. The CNN-GRU model's deployment reflects an innovative approach to security at airports, offering a reliable and flexible instrument to protect passengers and staff successfully. This study contributes to continuing attempts to maintain and improve airport security in a threat environment that is always changing.

Keywords: Threat Detection, Convolutional Neural Networks (CNNs), Gated Recurrent Units (GRUs), X-ray images.

1 Introduction

Considering the growing dangers to society in the current period, safeguarding the security of airports is of the utmost significance. The aviation industry, one of the key forms of transportation, is always being watched, and maintaining security requirements is becoming more difficult. The X-ray examination of carry-on luggage has emerged as a crucial part of airport security protocols among the numerous safety measures [1]. The uneven and chaotic character of luggage articles might make the X-ray imaging examination of baggage contents difficult, labour-intensive, and much more challenging [2]. Danger identification in X-ray pictures has to be automated and effective. This article aims to increase airport security by utilizing cutting-edge technologies to recognize possible dangers in X-ray pictures. [3] The main goal is to make air travel more convenient and secure while accelerating the safety inspection procedure. Airport security continues to be a source of worry since threats are always evolving, and new weaknesses must be covered. Older manual inspection techniques require a lot of effort and are prone to mistakes made by humans. Additionally, the rise in air travel requires a quick and efficient inspection procedure [4]. X-ray imaging is one of the main tools used in luggage inspection. However, the X-ray pictures of carry-on items are frequently messy and complicated, with haphazardly overlapping. This intricacy can make it difficult for human inspectors to detect possible hazards effectively, especially in situations with significant blockings [5]. Convolutional neural networks (CNNs), in particular, that were trained on widely used visual recognition datasets were challenged to function satisfactorily in this difficult situation. Innovative technologies are crucial in addressing the shortcomings of conventional checks for security. In particular, increasing and automating the identification of dangers in X-ray pictures has shown promise when using deep learning and

* Corresponding author e-mail: Taloba@aun.edu.eg

computer vision approaches [6]. When used to identify specific danger items, deep learning models like You Only Look Once (YOLO) may greatly increase the precision and effectiveness of recognizing threats [7].

Deep learning models are especially well-suited for time safety checks since they can quickly process and evaluate X-ray pictures. In addition, Generative Adversarial Networks (GANs) can create synthetic X-ray pictures to enhance datasets, allowing for the training of more reliable threat identification models [8]. This method can make it easier to identify numerous hazardous objects frequently used in conjunction with various sorts of hazardous devices, strengthening security procedures. The airport security area must adapt as threats change and stay on the cutting edge of technology [9]. There is tremendous potential to increase detection accuracy by creating automated and realistic threat picture projection models that consider variations in orientation, color schemes, and other item attributes regarding the backdrop. Furthermore, a potential direction for future study is changing the layers and architectures of deep learning models to improve their effectiveness in various settings. The detection of shared characteristics across multiple threat items may be improved by utilizing transfer learning approaches with similar datasets, such as X-ray pictures of different weapons [10]. The integration of cutting-edge technologies into the constantly changing environment of airport security is essential for safeguarding the safety of air travellers [11]. One promising avenue is 3D scanning and tomography systems, which provide a more intricate and layered view of carry-on items [12]. The capacity of this technology to show an object's underlying structure greatly helps discover concealed hazards, such as harmful materials or hidden weapons. Additionally, deep learning models may be complemented by machine learning methods, such as support vector machines (SVMs) and random forests, to analyze X-ray pictures, adding a layer of protection. Because of their prowess in pattern recognition, these algorithms can recognize suspicious-looking items or materials based on a variety of visual clues [13].

Additionally, integrating spectroscopy and chemical analysis devices alongside X-ray machines enhances security screening by providing valuable insights into the chemical composition of items within luggage [14]. This is particularly effective in detecting explosive materials or other hazardous substances that may not be immediately obvious from their visual appearance. Furthermore, advancements in biometrics and facial recognition systems for passenger identification enhance security and streamline the airport screening process [15]. These systems cross-reference passenger data with watch lists and databases to swiftly identify potential threats or persons of interest, further tightening security measures. Automated threat recognition systems come into play for a holistic approach to security, harnessing AI and machine learning to scrutinize X-ray images for patterns, shapes, and densities that indicate potential threats. This not only automates the detection process but also ensures that suspicious items are swiftly flagged for further inspection by security personnel. Enhance airport security. It utilizes Convolutional Neural Networks (CNN) and Gated Recurrent Units (GRU) to improve threat detection accuracy in X-ray images of luggage and passenger belongings. The CNN is employed for efficient feature extraction from the X-ray images, while the GRU, a type of recurrent neural network, is used to analyze the temporal aspects of the scanned items. By combining these two deep learning architectures, the system can better identify potential security threats, such as prohibited items or contraband, thereby enhancing airport security measures at Kuwait International Airport.

The recommended work's main contributions are,

1. In the context of X-ray image analysis at Kuwait International Airport, the research presents a unique Convolutional Neural Network-Gated Recurrent Unit (CNN-GRU) model built particularly for enhancing security precautions.
2. The CNN-GRU model takes advantage of both the CNNs' and GRUs' advantages. While GRUs can analyze X-ray scan sequences while keeping context over time, CNNs are superior at extracting features from and interpreting X-ray pictures.
3. Using the CNN-GRU model significantly lowers the number of false positives in X-ray picture analysis.
4. It addresses the constant need to adjust security measures to changing threats and technology breakthroughs, successfully protecting passengers and employees.
5. This study contributes to the larger initiatives to preserve and upgrade airport security in a dangerous, changing environment by providing a potential and novel method for enhancing safety measures.
6. This study provides a thorough solution to the issue of false positives in X-ray image analysis, with particular emphasis on practicality, operational effectiveness, and the capacity to adjust to changing security issues.

This research significantly contributes to the " Strengthening the Security of International Airports by Detecting Threats in X-ray Images," introducing a comprehensive approach to developing sophisticated deep learning architectures. The paper is structured to include an exhaustive review of related work (Section 2), a clear definition of the problem (Section 3), a detailed exploration of the proposed CNN-GRU architectures (Section 4), an in-depth analysis of experimental results (Section 5), and a conclusive summary (Section 6). These contributions collectively aim to improve the accuracy and effectiveness of Strengthening the Security by Detecting Threats in X-ray Images".

2 Related Work

For computer vision techniques in this field, resolving the innate data distribution imbalance in X-ray security pictures is a considerable problem. Numerous earlier research failed to include this important factor, which limited their capacity to be used in real-world situations. Dumagpi and Jeong [16] explore the effects of applying picture augmentation or visual synthesis techniques based on Generative Adversarial Networks to improve the performance of algorithms for computer vision when handling unbalanced X-ray samples. Cycle-GAN converts camera photos of potential threats into X-ray images, and Deep Convolutional GAN (DCGAN) is used to create fresh X-ray images of potential threats. Researchers created new X-ray protection images by fusing dangerous objects with background X-ray pictures, which are utilized to expand the dataset. Then, utilizing different augmentation techniques, I built various faster (region-based Convolutional neural network) R-CNN models, assessing their efficacy on a sizable experimental X-ray picture dataset. However, irrespective of the augmentation technique employed, a rather high true positive rate (TPR) of roughly 94% was preserved. A significant difficulty will be balancing the demand for accurate threat prediction and computational efficacy.

Due to significant overlap, an unorganized backdrop, and rapid throughput, detecting forbidden objects during X-ray security inspections is difficult. Numerous deep-learning algorithms have been presented in recent years and have shown good results. However, the efficacy of these techniques significantly depends on the provided datasets. Additionally, manually gathering and classifying pictures to create a large-scale X-ray imaging collection is unacceptably costly and takes time. Liu and Lin [17] propose a text-driven system based on generative adversarial networks (GAN) for synthesizing X-ray security inspection pictures. A conditional GAN is initially generated to create realistic pictures of banned things using labels for classes. The next phase is implementing a revised model based on a pix-to-pix GAN to transform natural photos into X-ray scans. Third, a different HD pix-to-pixel GAN creates high-resolution benign backdrop pictures combined with the produced images of forbidden objects to generate X-ray inspection images. The suggested approach is then tested using SOTA object identification techniques like YOLO-v5, which results in 4.6% promotion for mAP0.5 and 15.9% for mAP0.50.95. The experimental findings show that, during X-ray security screening, the picture synthesis system can successfully supplement the datasets of restricted goods and enhance the efficiency of deep learning techniques. The suggested technique's key drawbacks are its reliance on the excellence and variety of synthesized images and the impending challenges in generalizing to everyday life, untested circumstances.

Object recognition has a lot of promise for usage in various applications, such as security, surveillance, and human-computer interactions, especially in bio-inspired object detection (BOD). Although deep learning (DL) algorithms have achieved outstanding results in identifying objects, performing thorough experiments to assess the effectiveness of DL models designed particularly for BOD is still challenging. This lack of research prevents the creation of more precise and successful object detection techniques motivated by biological structures, like many seen in nature. Taking on this problem can result in novel methods and enhanced object identification skills in bio-inspired technologies. Ajagbe et al. [18] use six (6) performance indicators to examine the effectiveness of DL models in BOD. According to the published research, eight popular DL models were chosen for the study. The bio-inspired datasets utilized to recognize objects and pictures on MATLAB 2018a included Beetles Bee and Morder Hornet. In terms of obtained training time, detection quality, specificity, sensitivity, and precision measures, the outcomes demonstrate that CNN excelled in the other seven deep-learning models. The results presented here point to CNN as the most effective model to take into consideration the job at hand. The next directions of this study include modifying the layered structures of the eight DL models to examine their efficacy in various settings. The primary drawback is the lack of specific findings or research addressing the suggested model adjustments.

Davis et al. [19] establish a unique study paradigm for investigating observing behavior (complacency) and performance in a simulated x-ray testing task. The 'Wizardof-Oz' automated assessment feature was integrated with an X-ray screening. In 80% of the cases, the computerized system in the x-ray task gave people a trustworthy suggestion to inspect the checked luggage (hazardous goods found) or clear it (no dangerous weapons discovered). The frequency with which users choose to request information by clicking a "Request Info" button to confirm the process's automation was used to gauge their complacency. Surveillance actions, or the proportion of trials when the user asked the robot for more details, were low. It was, however, considerably greater if the automated made a wrong suggestion. The results show that individuals exhibited bias toward automation or the propensity to concur with a computerized support system. Participants also showed boredom while working, ceasing to actively track the system. Consumers may have realized the algorithm wasn't accurate due to the rise of tracking behavior in inaccurate suggestion examinations. However, they accepted the automation instead of visually searching the luggage for proof. This shows a particular threat to security in such fields, in which consumers may rely on subpar computerization over their skills whenever they suspect a thing is wrong. The extra data provided via the button could have been less useful in making choices; instead, it was probably improvised.

Although it is time-consuming for human inspectors, security checks through the X-ray scanning of baggage are essential for public safety. The foundation of visual computing, known as deep learning, has made it possible to automate checks for safety. However, the haphazard overlapping of objects within baggage results in noisy X-ray pictures with significant obstructions, making conventional CNN-based algorithms trained on conventional image recognition datasets useless. To solve these issues, 8885 X-ray pictures from 5 categories of the often-found forbidden item ”cutters” make up the initial superior banned X-ray object identification data set, called OPIXray. The photos were taken from an airport, and qualified inspectors physically tagged these illegal objects. This annotation serves as a standard for training models and helps future research. Tao et al. [20] suggest an over-sampling de-occlusion attention network comprising a unique focus component and an innovative over-sampling training technique to enhance occluded X-ray object recognition. The over-sampling training method requires the system to place greater value on these challenging specimens, including those objects with significant occlusion levels, making them more appropriate for this situation. In particular, de-occlusion module, particularly DOAM, simultaneously uses the various visual characteristics of the prohibited items. Thoroughly tested DOAM-O on the OPIXray dataset, demonstrating that this algorithm could consistently beat numerous widely-used strategies for attention and enhance the efficiency of renowned detection techniques such as SSD, YOLOv3, and FCOS. The data set may not be completely annotated manually or accurately reflect all actual-world events. The manually performed dataset annotation may not accurately reflect all real-world circumstances and might require much effort.

The idea of a ”smart city” and its accompanying amenities are being thoroughly researched regarding the development of innovation and the use of technology ideas. The safety of individual lives and possessions vulnerable to terrorist activity and planned crime is one of the major issues with encouraging smart living. Avoiding bombings in public areas is given a lot of focus, particularly regarding IED (Improvised Explosive Device) detection. Chamnanphan et al. [21] focuses on developing an algorithm for analytical analysis that can accurately determine the existence or lack of IEDs in X-ray images of baggage or other objects. The idea provides an alternative to current approaches that can’t locate covert or concealed devices. For this specific task, experts generate sample images that span a range of situations encountered during activities during the last 10 years. After that, a deep learning model is created using these images. Then, various data augmentation techniques are used to overcome the problem of having too few training examples. The suggested model often produces greater accuracy rates for unnoticed samples than a comparable study using neural networks, with the greatest accuracy rate of 0.985. An empirical analysis also establishes the ideal training set size for high prediction performance. The study finds that a big training set could not produce the greatest outcomes besides consuming many resources since it might point to overfitting. Methods for transfer learning are suggested as a viable way to improve the efficiency of the existing models.

Limitations from the research above include the urgent need for comprehensive, large-scale, and diversified datasets that accurately depict the complexities and challenges of identifying improvised explosive devices (IEDs) in smart cities and security-sensitive environments. Robust and practical solutions are required to address overfitting, scalability, and the difficulties involved with IED detection in complicated urban areas.

3 Problem Statement

The problem raised in the research above is that X-ray security inspections present several difficulties, including an inherent data distribution imbalance, a lack of datasets, and the need for more precise and effective object recognition in X-ray images [18]. Generative Adversarial Networks (GANs) for picture synthesis, developing deep learning models for bio inspired object recognition, and investigating automation in X-ray screening to reduce human error are just a few of the solutions put forth by researchers [20]. In the context of smart city security, there is an emphasis on enhancing object recognition in noisy X-ray images, particularly for locating hidden objects like Improvised Explosive Devices (IEDs) [19]. There is a need for comprehensive, large-scale, and diverse datasets that accurately represent the real-world scenarios and challenges of detecting Improvised Explosive Devices (IEDs) in smart cities and security-sensitive environments. Robust and practical solutions to mitigate overfitting, scalability, and challenges. These studies aim to improve the efficiency of computer vision techniques in X-ray security, addressing problems including data imbalance, dataset constraints, and the requirement for more precise and automated detection methods.

4 Methodology

A diversified collection of X-ray images, comprising potential threats, harmless things, and non-threat objects, are gathered and pre-processed using the suggested methods. Feature extraction and sequential analysis are combined in a CNN-GRU model to detect threats effectively. The algorithm is trained, verified, and assessed on several datasets to guarantee reliable performance. To meet new threats while upholding the highest security requirements at Kuwait International Airport, the model has been implemented in real-time, linked to the airport’s protection infrastructure, and

subject to continual refinement. Fig. 1 explains the overall methodology.

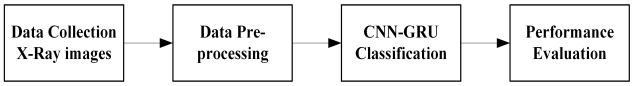

Fig. 1: Overall Methodology.

4.1 Data Collection

The Rapiscan 620DV X-ray inspection equipment focuses on aerospace and high-security operations. It comprises 640 mm wide by 430 mm high tunnels with 160 kV / 1 mA X-ray sources that can resolve wires to roughly 80 micrometers (40 US Wire Gauge) and penetrate steel up to 33 mm. Due to the X-ray sources' fan-shaped beams' nearly orthogonal orientation, the scanner creates two images. The vertical and horizontal views of the thing under examination produced by the projections can be utilized to determine what is in a bag. X-ray detectors collect low and high X-ray energy information, enabling material classification [22].

4.2 Data Pre-processing

They prefer to utilize the pre-processed RGB coloring commonly displayed to human TSOs, even though entering the high- and low-energy image scans directly into the model would be feasible. This coloring alters the image so material characteristics can be more easily determined. For instance, organic substances typically have low Z. In contrast, metallic substances typically have higher Z. This color uses the relationship between the coefficient of linear attenuation and the energy of photons to calculate the operational atomic numbers (Z). Rapiscan has a unique color scheme that tints organic substances orange, metal things blue, and substances with an effective Z (Z_{ef}) among both of these in green. Because weapons, sharp objects, and blunts, for example, frequently contain metal-based components, utilizing this false coloring as the input accomplishes two goals: (i) encoding more human understanding of material characteristics, which is extremely useful for threat detection and (ii) coordinating the image input colors distribution more closely with the pre-trained weights, that had been developed on RGB scenes from nature.

The RGB images have been pre-processed to identify the first region of interest (ROI) wherein the threat may be found. Initially, the regional entropy image is thresholded to separate the bag portion of the image from the initial image. A greyscale version of the initial RGB X-ray image calculates the localized entropy image. The degree of complexity in a certain neighborhood, often identified by a structural element, is connected to the local entropy [23]. The structure element calculates the entropy filter utilizing the next formula, which may detect minute fluctuations in the regional grey-level distributions:

$$h = -\sum_{i=0}^{255} p_{0i} log_2 p_{0i} \tag{1}$$

where p_{0_i} is the likelihood (seen in the image's normalized localized histograms) connected to the grey level, i.

4.3 CNN-GRU

Convolutional Neural Network

Convolutional Neural Networks (CNNs) are considered the most advanced neural network architectures for image recognition, delivering outstanding performance in various applications such as controlling unmanned helicopters, analyzing X-ray cargo scans, and many others. A CNN is comprised of an input layer for the pixel matrix, an output layer for class labels, and multiple hidden layers. The final layers are fully connected, typically using a SoftMax activation function. Each hidden layer generally includes convolution, activation, and pooling operations. The convolutional layer captures pixel-dependent image regions, creating a representation of the input image by applying 2D sliding filters. This filtered image is then combined through pooling to reduce the input size [24]. The final result gets flattened into a list following a series of hidden layers that conduct convolution, activation, and pooling before being transferred to a traditional fully linked layer to categorize the image.

The two-channel, 16-bit integer's precision X-ray pictures that the proposed classifications system processes are of low and high energy. It proposed to classify the components into six distinct groups: history, weak natural, lightweight organic, light metallic elements, metals that are heavy, and unbreakable. One training specimen is a collection of patches made from the same material but in various sizes. The patches are 3 x 3, 5 x 5, 7 x 7, 9 x 9, and 15 x 15 in size. Since material properties are not operationally specified, label every collection of training patches with the relevant characteristics. It is significant to highlight that various patch sizes of the input information might have very varied statistical features, making it challenging for a single, sequential approach to directly encapsulate such an image. They require a multi-scale model to help us better understand multi-channel and multi-scale input information and combine them to provide basic characteristics to address this challenge. They present a variant of the multiple scales network with 5 inputs supplied with various patch sizes to provide a final materials class on the result,

influenced by deep CNN and multiple scales architectures [25]. Five smaller networks make up the suggested network, and based on the dimensions of the source patch, each has a distinct topology. As described, they modified the model's smaller networks to match the quality of incoming patches to enhance the effectiveness of the CNN. The subnet grows deeper and larger as the patch's quality rises. Every subnetwork produces a characteristic vector as its output. Both layers with full connectivity (FC), finalized by the softmax layer, get the concatenation vectors of features across all five subnetworks. This makes it possible to develop CNNs using various source scales.

Gate Recurrent Unit

GRU is a better RNN than the standard one. GRU uses both the update gate and the reset gate, two gates, to address the issue of vanishing gradients that plague a normal RNN. In essence, both vectors determine the damage that must be conveyed to the outputs. GRUs are capable of deleting undesired data while holding onto valuable historical data. It has two gates: update gate (i) and reset gate (ii). The resultant gate of an LSTM is comparable to the update gate. It determines the amount of outdated data that should be kept and forwarded to the following step. The combined impact of both the input and forgetting gates in an LSTM is comparable to that of the reset gate. It takes charge of the amount of outdated data you remember.

Recurrent neural networks (RNNs) have a GRU subtype. This is also intended to address issues with long-term memory with gradient in reverse propagation, similar to LSTM. In the Gate Recurrent Unit -Long Short-Term Memory variation, the forget and input gates are combined to create one updated gate. The last version is easier than the conventional LSTM model since it also combines the cell information and the state that is hidden in addition to making other specific alterations. Based on the results of experiments in research, there is little efficiency difference between LSTM and GRU on datasets with historical correlation. In certain datasets, GRU models are even rated as having better results. Early GRU research has demonstrated that GRU elements determine fewer parameters than LSTM, which suggests that model inference and training can be completed more quickly. Additionally, the study demonstrates that GRU requires less time for inference and training than LSTM for various datasets.

For the reasons stated earlier, the Gate Recurrent Unit was chosen as the primary hidden component of the neural network framework. The condition of the preceding instant about the present moment t is represented by h_{0t-1}. The current inputs and outputs of the GRU modules are x_{0t} and h_{0t}, accordingly. Two essential GRU modules structures, the reset gate and the update gate, are designated as r_{0t} and z_{0t}. The gate is a straightforward neural network. Additionally, the activation procedure of the neural network uses a sigmoid function of eqn. (2) to set the result of the gate between zero and one. The resultant candidate value following reset gates processing is $\hat{h}_{0_t}$ [26]. The following formula describes how the GRU modules is structured from eqn. (3-6):

$$S_0(x) = \frac{1}{1+e^{-x}} \tag{2}$$

$$r_{0t} = \sigma(W_{r_0 h_0} h_{0t-1} + W_{r_0 x_0} x_{0t} \tag{3}$$

$$z_{0t} = \sigma(W_{z_0 h_0} h_{0t-1} + W_{z_0 x_0} x_{0t} \tag{4}$$

$$\hat{h}_{0_t} = \tanh[W_{h_0 h_0}(r_{0_t} \circ h_{0t-1}) + W_{h_0 x_0} x_{0t}] \tag{5}$$

$$h_{0t} = (1 - z_{0t}) \circ \hat{h}_0 + z_{0_t} \circ h_{0t-1} \tag{6}$$

$W_{h_0 h_0}$ and $W_{h_0 x_0}$ are the variables in the procedure to get the outcome applicant range h_{0t}, and the modulo operator $\circ$ is used to multiply each of the collection components in chance. $W_{z_0 h_0}$ and $W_{z_0 x_0}$ are the variables in the updating gate. Fig. 2 shows the architecture of CNN-GRU.

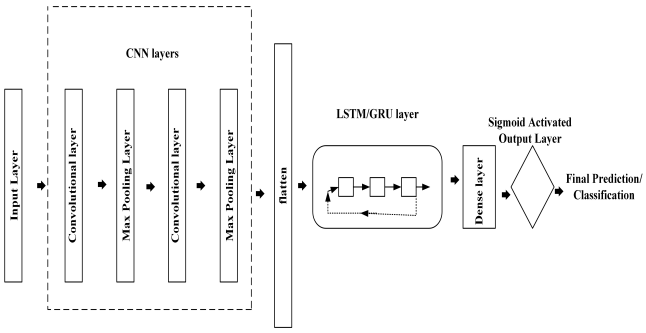

Fig. 2: CNN-GRU Architecture.

5 Results and Discussion

At Kuwait International Airport, the CNN-GRU algorithm's installation increased security by significantly increasing the accuracy of threat identification. The model's accuracy in detecting hidden dangers resulted in fewer false positives, improving screening effectiveness and passenger comfort while significantly raising overall safety. The model's incorporation into the airport's security architecture improved operational effectiveness and made Kuwait International Airport a hub that is safer and more welcoming to travelers.

5.1 Performance Evaluation

Achieving a high level of precision and recall is essential in airport security. High recall guarantees that serious threats are not ignored, while high precision helps to eliminate false alerts [27]. But precision and recall frequently have to be traded off, and the F1-Score can assist in striking the correct balance. The model's performance at different threshold settings is seen more broadly by the AUC-ROC score, which can be significant in real-world applications. The model's performance could be fine-tuned and understood more effectively due to the confusion matrix, which provides in-depth insights regarding its efficacy [28].

Precision

The precision measures the proportion of accurate positive forecasts to all positive predictions. It evaluates how accurately the model's optimistic predictions came true. It provides information on the proportion of objects that are genuinely dangers in the context of threat detection. High accuracy suggests that false alarms are infrequent, as expressed in Equation (7).

$$Precision\ (P) = \frac{T^{pos}}{T^{pos} + F^{pos}} \tag{7}$$

Recall

Recall is the proportion of accurate forecasts to all actual threats. Recall gauges a technique's capacity to recognise dangers. It reveals how many actual threats are accurately discovered in threat detection. High recall shows that the model effectively identifies real threats as expressed in Equation (8).

$$R = \frac{T^{pos}}{T^{pos} + F^{pos}} \tag{8}$$

F1-score

The harmonic average of recall and precision is known as the F1-Score. It offers a mix of recall and precision. The performance of the model is summarised by a single measure that is provided in Equation (9)

$$F1 = 2 * \frac{P \bullet R}{P + R} \tag{9}$$

Table 1: Performance Measure of CNN-GRU.

Techniques	Precision	Recall	F1 Score
CNN [29]	0.94	0.96	0.98
FCN-SSD [30]	0.93	0.92	0.90
R-CNN with ResNet101 [31]	0.95	0.92	0.89
Proposed (CNN-GRU)	0.95	0.96	0.94

The precision, recall, and F1 Score metrics for several image analysis and object detection approaches are concisely compared in Table 1 for each technique. According to [29], the "CNN" technique performs well at correctly distinguishing between threats and non-threats, as seen by its high precision (0.94), recall (0.96), and F1 Score (0.98). The "FCN-SSD" technique, described in [30], obtains a slightly lower F1 Score (0.90), showing a balanced performance while maintaining strong precision (0.93) and recall (0.92) metrics. The precision (0.95) and F1 Score (0.89) of "R-CNN with ResNet101" [31] are significantly higher, while the recall (0.92) and F1 Score are just slightly lower. The "Proposed (CNN-GRU)" technique, which emphasizes the effectiveness of the CNN-GRU architecture for reliable threat detection and visual evaluation tasks, records consistent precision (0.95) and recall (0.96) values, yielding a noteworthy F1 Score (0.94).

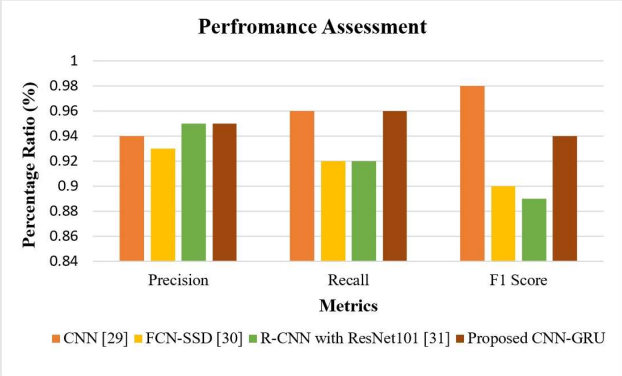

Fig. 3: Performance Assessment of the Proposed Approach.

Fig. 3 provides a visual representation of a comparison of the precision, recall, and F1 Score metrics for several image evaluation and object detection approaches. The effectiveness of "CNN," "FCN-SSD," "R-CNN with ResNet101," and the "Proposed (CNN-GRU)" approach are highlighted. Especially noteworthy is that the "CNN [29]" technique has remarkable precision, recall, and F1 Score, suggesting its greater accuracy in correctly differentiating dangers and non-threats. "FCN-SSD" demonstrates a somewhat lower F1 Score but maintains a strong balance between precision and recall. The F1 Score for "R-CNN with ResNet101" is somewhat lower but exhibits impressive precision, possibly indicating a trade-off between precision and recall. In contrast, the "Proposed (CNN-GRU)" technique outperforms the competition on all measures, demonstrating the CNN-GRU architecture's potential for powerful picture analysis and accurate threat identification.

Confusion Matrix

A confusion matrix (table 2) assesses the categorization approach efficacy. The number of accurate and erroneous classifications for each class in a binary classification problem and a thorough analysis of the model's predictions are provided. A confusion matrix is made up of four basic parts:

1. *True Negative* (T^{Neg}) reflects the total amount of accurately identified non-threat categories.
2. *False Positive* (F^{pos}) reflects the number of things misclassified as threats while not being vulnerabilities.
3. *False Negative* (F^{Neg}) reflects the number of identified threats misclassified as non-threats.
4. *True Positive* (T^{pos}) reflects the quantity of threats that have been accurately identified as threats.

Table 2: Confusion Matrix.

	Predicated Negative	**Predicated Positive**
Actual Negative	*True Negative* (T^{Neg})	
Actual Positive	*False Negative* (F^{Neg})	*True Positive* (T^{pos})

AUC-ROC Curve

When assessing the effectiveness of a binary classification model, such as the one employed for threat detection in X-ray pictures, it's possible to employ the Area Under the Receiver Operating Characteristic (AU-ROC or simply AUC-ROC) metric [32],[33]. The model's capacity to differentiate between the positive class (such as threats) and the negative class (such as non-threats) at various threshold values is represented graphically by the ROC curve. AUC-ROC measures the model's overall capacity to distinguish between these two classes [34],[35]. A model without discriminating power will have an AUC of 0.5 and a ROC curve, a diagonal line (the "no discrimination" line) running from the bottom left to the top right. The "perfect discrimination" line on the ROC curve of a model with perfect discrimination has an AUC of 1, and the ROC curve runs straight up to the top left and then straight over to the top right. Fig. 4 displays the proposed method's AUC-ROC curve.

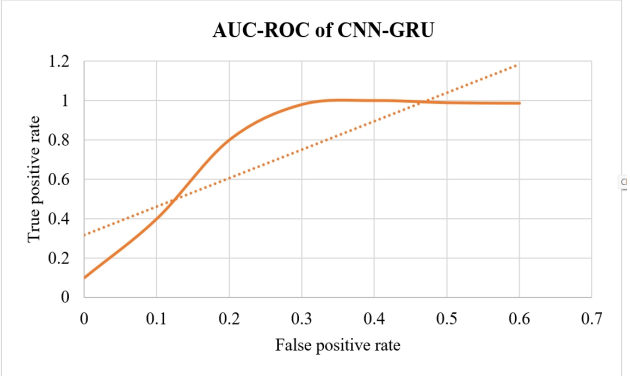

Fig. 4: AUC-ROC Curve.

5.2 Accuracy Comparison

Accuracy measures the proportion of correctly classified instances out of the total instances in the dataset. It provides a general idea of how well the model is performing. However, accuracy can be misleading if there is a class imbalance (i.e., if there are many more non-threat items than threat items), as the model might achieve high accuracy by simply predicting the majority class was expressed in Equation (10).

$$Accuracy = \frac{No.of\ Accurate\ Predictions}{Total\ Number\ of\ Predictions} \quad (10)$$

Table 3: Accuracy Comparison.

Techniques	**Accuracy**
CNN [29]	97.6%
FCN-SSD [30]	60.5%
R-CNN with ResNet101 [31]	66%
Proposed (CNN-GRU)	98.62%

The accuracy attained by various image analysis and object detection approaches is compared in Table 3 of this article. Convolutional neural networks' efficiency was demonstrated by the "CNN [36] " approach, which had a 97.6% accuracy rate. While "R-CNN with ResNet101 [37]" achieved an accuracy of 66%, the "FCN-SSD [38]" method only managed to reach a lesser accuracy of 60.5%. Notably, the "Proposed (CNN-GRU)" technique exceeds the competition with an accuracy of 98.62%, demonstrating the CNN-GRU architecture's potential to improve threat detection and image evaluation applications. Fig. 5 displays each strategy's accuracy rates and compares their performance. Among the given techniques, the "Proposed (CNN-GRU)" method seems to have the highest accuracy.

6 Conclusion and Future Work

Consequently, the CNN-GRU model has been successfully applied to strengthen the security measures

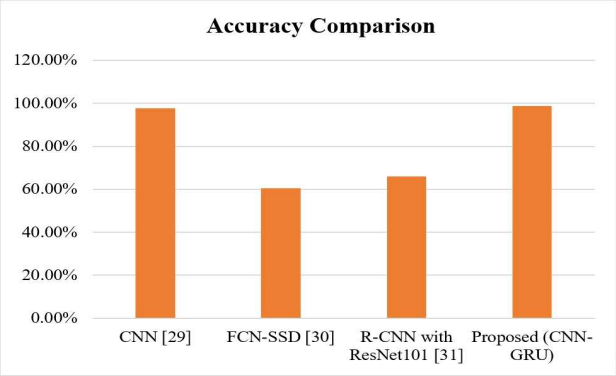

Fig. 5: Accuracy Comparison.

at Kuwait International Airport. This research has developed a new technique that considerably improves the precision and efficiency of threat identification, a crucial concern in airport security, to address the ongoing difficulty of false positives in X-ray picture analysis. The CNN-GRU model has shown its ability to accurately identify concealed risks within X-ray images and reduce the occurrence of false positives, thereby mitigating delays and minimizing the workload of security staff. These accomplishments were made possible by combining the strengths of CNNs and GRUs. This unique strategy offers a trustworthy, flexible tool to protect customers and employees, serving as a model for other cutting-edge security measures in the airport industry. This study adds to the continuous effort to preserve and enhance airport security as security threats continue to grow along with technology breakthroughs, guaranteeing that Kuwait International Airport can withstand ever-evolving difficulties. Furthermore, it establishes a standard for the wider aviation sector to use cutting-edge technologies and sophisticated procedures to guarantee a safer and more effective travel experience for every passenger, eventually strengthening the security of airports worldwide.

The development of real-time threat detection systems, the investigation of image fusion and machine learning techniques for improved threat assessment, the protection of passenger privacy and ethical considerations, and the integration of X-ray detection with biometric authentication techniques for a quick but secure passenger screening process should be the main objectives of future work in airport security using X-ray detection technology. To enhance the efficiency of cutting-edge security technology, research should also look at human-AI collaboration in security operations, the resistance of AI systems to hostile assaults, and the usability and training of security employees. Future research to construct a comprehensive and effective airport security framework must also focus on creating international norms, rules, and AI technologies for analyzing passenger behavior.

Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this article.

References

[1] E. N. Omweno, Legal, regulatory and technical responses to terrorism in the aviation industry in kenya, *Science Mundi* **2**(1) (2022) 1–21.

[2] K. A. Yener, *The domestication of metals: the rise of complex metal industries in Anatolia* (Brill, 2021).

[3] J. H. Tan and T. Masood, Adoption of industry 4.0 technologies in airports–a systematic literature review, *arXiv preprint arXiv:2112.14333* (2021).

[4] R. Tailor and S. Khan, Robotic process automation (rpa) in the aviation sector, in *Global Air Transport Management and Reshaping Business Models for the New Era*, (IGI Global, 2022) pp. 289–300.

[5] P. Priyadarshini, G. Jeevanandan, L. Govindaraju and E. Subramanian, Clinical evaluation of instrumentation time and quality of obturation using paediatric hand and rotary file systems with conventional hand k-files for pulpectomy in primary mandibular molars: a double-blinded randomized controlled trial, *European Archives of Paediatric Dentistry* **21** (2020) 693–701.

[6] D. Pandiar, P. Ramani, R. P. Krishnan and Y. Dinesh, Histopathological analysis of soft tissue changes in gingival biopsied specimen from patients with underlying corona virus disease associated mucormycosis (cam), *Medicina Oral, Patología Oral y Cirugía Bucal* **27**(3) (2022) p. e216.

[7] E. Kim, J. Lee, H. Jo, K. Na, E. Moon, G. Gweon, B. Yoo and Y. Kyung, Shomy: Detection of small hazardous objects using the you only look once algorithm., *KSII Transactions on Internet & Information Systems* **16**(8) (2022).

[8] P. Verma and S. Muthuswamy Pandian, Bionic effects of nano hydroxyapatite dentifrice on demineralised surface of enamel post orthodontic debonding: in-vivo split mouth study, *Progress in Orthodontics* **22** (2021) 1–8.

[9] L. Florido-Benítez, Identifying cyber security risks in spanish airports, *Cyber Security: A Peer-Reviewed Journal* **4**(3) (2021) 267–291.

[10] T. Hassan, M. Shafay, S. Akçay, S. Khan, M. Bennamoun, E. Damiani and N. Werghi, Meta-transfer learning driven tensor-shot detector for the autonomous localization and recognition of concealed baggage threats, *Sensors* **20**(22) (2020) p. 6450.

[11] M. Kumar, Optimized application of artificial intelligence (ai) in aviation market., *International Journal of Recent Research Aspects* **9**(4) (2022).

[12] D. Velayudhan, T. Hassan, E. Damiani and N. Werghi, Recent advances in baggage threat detection: A comprehensive and systematic survey, *ACM Computing Surveys* **55**(8) (2022) 1–38.

[13] M. D. Barma, M. A. Indiran, P. Kumar, A. Balasubramaniam and M. S. Kumar, Quality of life among head and neck cancer treated patients in south india: a cross-sectional study, *Journal of Oral Biology and Craniofacial Research* **11**(2) (2021) 215–218.

[14] J. Li, B. Xiong, R. Qin and A. Gruen, A flexible inference machine for global alignment of wall openings, *Remote Sensing* **12**(12) (2020) p. 1968.

[15] D. Ezhilarasan, T. Lakshmi, M. Subha, V. Deepak Nallasamy and S. Raghunandhakumar, The ambiguous role of sirtuins in head and neck squamous cell carcinoma, *Oral Diseases* **28**(3) (2022) 559–567.

[16] J. K. Dumagpi and Y.-J. Jeong, Evaluating gan-based image augmentation for threat detection in large-scale xray security images, *Applied Sciences* **11**(1) (2020) p. 36.

[17] J. Liu and T. H. Lin, A framework for the synthesis of x-ray security inspection images based on generative adversarial networks, *IEEE Access* (2023).

[18] S. A. Ajagbe, O. A. Oki, M. A. Oladipupo and A. Nwanakwaugwum, Investigating the efficiency of deep learning models in bioinspired object detection, in *2022 International conference on electrical, computer and energy technologies (ICECET)*, IEEE2022, pp. 1–6.

[19] J. Davis, A. Atchley, H. Smitherman, H. Simon and N. Tenhundfeld, Measuring automation bias and complacency in an x-ray screening task, in *2020 Systems and Information Engineering Design Symposium (SIEDS)*, IEEE2020, pp. 1–5.

[20] R. Tao, Y. Wei, H. Li, A. Liu, Y. Ding, H. Qin and X. Liu, Over-sampling de-occlusion attention network for prohibited items detection in noisy x-ray images, *arXiv preprint arXiv:2103.00809* (2021).

[21] C. Chamnanphan, S. Vorapatratorn, T. Boongoen, N. Iam-On and K. Kirimasthong, Improvised explosive device detection using cnn with x-ray images, *Journal of Advances in Information Technology* **14**(4) (2023) 674–684.

[22] K. J. Liang, J. B. Sigman, G. P. Spell, D. Strellis, W. Chang, F. Liu, T. Mehta and L. Carin, Toward automatic threat recognition for airport x-ray baggage screening with deep convolutional object detection, *arXiv preprint arXiv:1912.06329* (2019).

[23] D. Vukadinovic, M. R. Osés and D. Anderson, Automated detection of inorganic powders in x-ray images of airport luggage, *Journal of Transportation Security* **16**(1) (2023) p. 3.

[24] A. Petrozziello and I. Jordanov, Automated deep learning for threat detection in luggage from x-ray images, in *Analysis of Experimental Algorithms: Special Event, SEA^2 2019, Kalamata, Greece, June 24-29, 2019, Revised Selected Papers*, Springer2019, pp. 505–512.

[25] E. Benedykciuk, M. Denkowski and K. Dmitruk, Material classification in x-ray images based on multi-scale cnn, *Signal, Image and Video Processing* (2021) 1–9.

[26] H. Ma, J. Cao, B. Mi, D. Huang, Y. Liu and S. Li, A gru-based lightweight system for can intrusion detection in real time, *Security and Communication Networks* **2022** (2022).

[27] A. Paul, M. A. S. Tajin, A. Das, W. M. Mongan and K. R. Dandekar, Energy-efficient respiratory anomaly detection in premature newborn infants, *Electronics* **11**(5) (2022) p. 682.

[28] A. R. M. Forkan, I. Khalil, Z. Tari, S. Foufou and A. Bouras, A context-aware approach for long-term behavioural change detection and abnormality prediction in ambient assisted living, *Pattern Recognition* **48**(3) (2015) 628–641.

[29] M. Xu, H. Zhang and J. Yang, Prohibited item detection in airport x-ray security images via attention mechanism based cnn, in *Pattern Recognition and Computer Vision: First Chinese Conference, PRCV 2018, Guangzhou, China, November 23-26, 2018, Proceedings, Part II 1*, Springer2018, pp. 429–439.

[30] M. Subramani, K. Rajaduari, S. D. Choudhury, A. Topkar and V. Ponnusamy, Evaluating one stage detector architecture of convolutional neural network for threat object detection using x-ray baggage security imaging., *Rev. d'Intelligence Artif.* **34**(4) (2020) 495–500.

[31] Y. F. A. Gaus, N. Bhowmik, S. Akçay, P. M. Guillén-Garcia, J. W. Barker and T. P. Breckon, Evaluation of a dual convolutional neural network architecture for object-wise anomaly detection in cluttered x-ray security imagery, in *2019 international joint conference on neural networks (IJCNN)*, IEEE2019, pp. 1–8.

[32] A. Alsirhani, M. M. Alshahrani, A. Abukwaik, A. I. Taloba, R. M. Abd El-Aziz and M. Salem, A novel approach to predicting the stability of the smart grid utilizing mlp-elm technique, *Alexandria Engineering Journal* **74** (2023) 495–508.

[33] N. Omer, A. H. Samak, A. I. Taloba and R. M. Abd El-Aziz, A novel optimized probabilistic neural network approach for intrusion detection and categorization, *Alexandria Engineering Journal* **72** (2023) 351–361.

[34] R. Chawla, H. K. Konda, A. A. Deshmukh, K. D. Sagar, M. S. Al Ansari and A. I. Taloba, A hybrid optimization approach with deep learning technique for the classification of dental caries, *International Journal of Advanced Computer Science and Applications* **13**(12) (2022).

[35] K. Ravikumar, P. Chiranjeevi, N. M. Devarajan, C. Kaur and A. I. Taloba, Challenges in internet of things towards the security using deep learning techniques, *Measurement: Sensors* **24** (2022) p. 100473.

[36] A. Saif Alghawli and A. I. Taloba, An enhanced ant colony optimization mechanism for the classification of depressive disorders, *Computational Intelligence and Neuroscience* **2022** (2022).

[37] R. M. Abd El-Aziz, A. I. Taloba and F. A. Alghamdi, Quantum computing optimization technique for iot platform using modified deep residual approach, *Alexandria Engineering Journal* **61**(12) (2022) 12497–12509.

[38] A. Abozeid, R. Alanazi, A. Elhadad, A. I. Taloba, A. El-Aziz, M. Rasha *et al.*, A large-scale dataset and deep learning model for detecting and counting olive trees in satellite imagery, *Computational Intelligence and Neuroscience* **2022** (2022).