Indian Journal of Cryptography and Network Security (IJCNS)
ISSN: 2582-9238 (Online), Volume-4 Issue-2, November 2024

IoT Sensor-Based Convolutional Neural Network System for Concealed Weapon Detector for Security Enhancement

Moradeke Grace Adewumi, Ese Sophia Mughele, Akinribido Comfort Tomiye, Rowland Ogunrinde, Stella Chinye Chiemeke, Olumide Sunday Adewale

***Abstract:** Security has been a major concern in our societies due to the rise in crime rate, most especially in a crowded area. Concealed weapons have been posing a significant threat to government, law enforcement, security agencies, and civilians. Existing weapons detection systems seem to be not culpable of detecting concealed weapons without the cooperation of the person being searched. There remains a need for a weapons detector that can detect and identify concealed weapons for security enhancement in Nigeria. For this purpose, computer vision methods and a deep learning approach were applied for the identification of a weapon from captured images downloaded from the internet as a prototype for the study. Recent work in deep learning and machine learning using convolutional neural networks has shown considerable progress in the areas of object detection and recognition. The CNN algorithms are trained on the collected datasets to identify and differentiate between weapons and non-weapons. We built a concealed weapon detection system prototype and conducted a series of experiments to test the system's accuracy, precision, and false positives. The models were compared by evaluating their average values of sensitivity, specificity, F1 score, accuracy, and the area under the receiver operating characteristic curve (AUC). The experimental findings clearly demonstrated that the ResNet-50 model performed better than the VGG-16 and AlexNet models in terms of sensitivity, specificity, and accuracy.*

***Keywords:** Concealed Weapon, Detector, Insecurity, Internet of Things.*

I. INTRODUCTION

Insecurity has been a major threat to Nigerians for the past decade.

Manuscript received on 12 January 2024 | Revised Manuscript received on 10 November 2024 | Manuscript Accepted on 15 November 2024 | Manuscript published on 30 November 2024.

*Correspondence Author(s)

Moradeke Grace Adewumi, Department of Computing and Information Science, Bamidele Olumilua University of Education, Science and Technology Ikere-Ekiti. Ekiti State Nigeria. Email ID: adewumi.moradeke@bouesti.edu.ng ,ORCID ID: 0000-0003-4608-5057

Ese Sophia Mughele, Department of Cyber Security, University of Delta, Agbor. Delta State, Nigeria. ORCID ID: 0000-0002-9765-0135

Akinribido Comfort Tomiye*, Department of Computing and Information Science, Bamidele Olumilua University of Education, Science and Technology Ikere-Ekiti. Ekiti State Nigeria. Email ID: comforttomiye@gmail.com, ORCID ID: 0009-0003-3379-6367

Rowland Ogunrinde, Department of Computing and Information Science, Bamidele Olumilua University of Education, Science and Technology Ikere-Ekiti. Ekiti State Nigeria. ORCID ID: 0000-0002-9642-0979

Stella Chinye Chiemeke, Department of Cyber Security, University of Delta, Agbor. Delta State, Nigeria. ORCID ID: 0000-0001-5577-4028

Olumide Sunday Adewale, Department of Computer Science, Federal University of Technology, Akure. Ondo State, Nigeria. ORCID ID: 0000-0003-4642-0150

The use of weapons for manslaughter began in Nigeria when a parcel containing a bomb was delivered to Dele Giwa in his house in 1986, which took his life untimely. This action fully gained its momentum in Nigeria on Friday, August 26th, 2011, in Abuja, when a suicide bomber detonated a vehicle packed with explosives, followed by the Abuja police headquarters being bombed the same year. The effectiveness of weapons has impaired many coalition operations in Nigeria. This has brought suffering, pain, and death to the people, thus keeping the nation in a state of anarchy and lawlessness to date [11].

Indeed, terrorism's global incarnation has been visible in Africa, particularly Nigeria. The employment of improvised explosive devices, targeted assassinations, ambushes, drive-by shootings, suicide bombings, and kidnappings are among the terrorists' tactics.

The sectarian insurgency has caused substantial damage to the nation, especially through the barbaric use of weapons for the purpose of murder. Terrorism is a true example of collective violence; it is committed by organizations who believe that doing so will help them achieve their objectives. Terrorism is the unjustified aggression of individuals, groups, or states against humans. It also encompasses any violent act or threat carried out as part of an individual or group of criminals strategy to terrorize or hurt individuals or to jeopardize their lives, liberty, or security in order to instill fear in governments and the general public [9]. This has led to a severe crisis for those who have been affected. Many people were killed, others lost loved ones, and many properties were damaged. Nigerians are still reeling from the effects of these terrorists. They are not afraid of anything; they are made up of both male and female members; they strike at will, and they are skilled at what they do. Hence the need for weapon detection.

A weapon is any device utilized to gain an advantage over an opponent or target that is hostile in nature. This could be achieved through tactical, strategic, material, or psychological means. Weapons range from simple implements such as knives, axes, guns, and swords to complicated modern firearms, tanks, intercontinental ballistic missiles, biological weapons,

and cyber weapons. A convolutional neural network (CNN) is a fundamental component of deep learning that is employed for intelligent processing, accuracy, and data improvement. The system consists of a multi-data processing layer that trains data representation through an abstraction of different layers.

CNN has been used in various research studies, such as human pose segmentation, face recognition, image classification, image detection, speech recognition, and others [12].

According to [17], Nigeria's security agencies appear to be ill-equipped for the task of maintaining law and order through crime detection, prosecution, prevention, and control due to poor information flow between the agencies and the public as well as collective mobilization in their respective spatial locations. On this note, there should be a precautionary measure for an individual and for crowded areas for concealed weapon detection, which calls for this study.

A. Objective of the Study

This study aims to design a detection model for concealed weapons based on Internet of Things connectivity.

B. Sensors and Internet of Things.

A sensor is a device that accepts energy from one system and transmits it to another, converting a physical variable into a signal variable. A sensor is a device that can be activated by receiving input from one or more transmission media and subsequently producing a corresponding signal for one or more transmission systems. A sensor generates a functional output based on a given input, which may be monitored and may pertain to physical or mechanical aspects. Sensors are useful in the development of a detection system. Several sensors, such as the ultrasonic sensor, infrared sensor, radar sensor, and structured light, have been used for improvised explosive device detection [16]. Sensors can be classified as active and passive based on the power or energy supply requirement of the sensors. Active sensors are devices that necessitate an external power source for their operation, whereas passive sensors are capable of detecting and responding to specific inputs from the surrounding physical environment. Passive sensor technologies gather data through the detection of vibrations, light, radiation, heat, or other phenomena occurring in the environment. In contrast to active sensors, which utilize transmitters to emit signals such as light wavelengths or electrons that interact with the target and are subsequently reflected, passive sensors collect data based on the reflections received. The Internet of Things (IoT) refers to a network of interconnected devices that have sensors, software, network connectivity, and necessary electronics. This network enables the interchange of data between these devices. It is an architectural framework that enables integration and data sharing between the physical environment and computer systems using current network infrastructure. Some people see IoT as an independent technology, whereas it cannot work in isolation from other independent technologies that make fundamental components of IoT [8].

The Internet of Things (IoT) paradigm primarily focuses on intelligent nodes that self-configure and connect within an interconnected and worldwide network infrastructure. It is considered one of the most revolutionary technologies, enabling situations of widespread and all-encompassing computing. IoT can be viewed as physical objects distributed widely in the real world, characterized by limited storage and processing capabilities, while also encompassing considerations related to reliability, performance, security, and privacy. IoT can alternatively be perceived as a global network comprising interconnected objects, each uniquely identifiable and utilizing standardized communication protocols, all converging through the internet as a central point. The Internet of Things is driven by recent progress in many gadgets and communication technologies, including mobile phones and everyday items such as food, clothing, furniture, paper, landmarks, monuments, artworks, and others. These things serve as either sensors or actuators, enabling interaction among themselves to achieve common objectives. IoT can also be regarded as the evolution of the internet, introducing machine-to-machine (M2M) learning into the equation. Consequently, IoT establishes connectivity for both individuals and all kinds of objects. Within this framework, IoT imbues the internet with a level of intelligence that enables connected objects to communicate, share information, make decisions, initiate actions, and offer remarkable services.

C. Weapon Detection

A system for automatically detecting weapons holds crucial significance in ensuring the early identification of potentially dangerous situations, greatly contributing to the security of citizens. One method employed to avert these scenarios involves the identification of hazardous items like handguns and knives within surveillance videos. However, the detection of such objects has been enhanced by the use of deep learning techniques, most especially the Convolutional Neural Networks (CNNs). The process of weapon detection was executed by amalgamating a region proposal technique with a classifier, thereby consolidating these components into a single model.

D. Deep Learning

This is a part of machine learning that imparts computers with the ability to acquire knowledge through experiential learning, a process innate to humans. Unlike conventional modeling techniques, which rely on predetermined equations, machine learning algorithms extract information directly from data.

Deep learning excels at image recognition, which is crucial for tackling tasks such as facial recognition, motion detection, and the advanced technologies that support autonomous driving, including lane detection, pedestrian identification, and autonomous parking.

It harnesses neural networks to glean valuable data representations directly from the input data. These neural networks consist of multiple layers of nonlinear processing, akin to the operations of biological nervous systems.

Deep learning models excel in achieving cutting-edge accuracy in object classification, sometimes surpassing human-level performance. This accomplishment is facilitated by training models on large collections of labelled data and incorporating neural network layers that consist of multiple layers, most especially the convolutional layers.

E. Convolutional Neural Networks

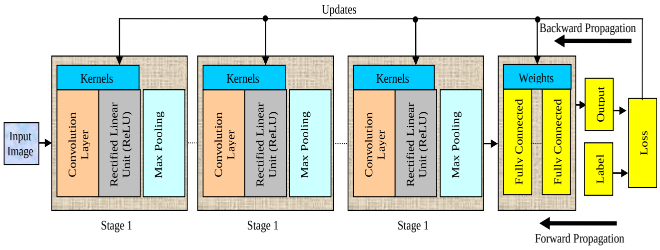
Convolutional neural networks, often referred to as ConvNets, are extensively employed in the realm of deep learning. Their primary function involves taking an image as input and ascribing significance, in the form of learnable weights and biases, to distinct elements within the image, facilitating their

Indian Journal of Cryptography and Network Security (IJCNS)
ISSN: 2582-9238 (Online), Volume-4 Issue-2, November 2024

discernment from one another. These networks leverage a feed-forward neural network architecture to scrutinize visual images, processing data in a grid-like topology. It is worth noting that ConvNets are versatile and can be applied to various other domains beyond images, including text analysis, signal processing, and the evaluation of continuous responses. ConvNets differ from other types of neural networks in some ways: Convolutional neural networks are inspired from the biological structure of a visual cortex, which contains arrangements of simple and complex cells [5]. These cells are activated based on sub-regions of a visual field that are called receptive fields. The neurons in a convolutional layer were connected to the sub-regions of the layers instead of being fully-connected as it was in other types of neural networks. These neurons are not responsive to the image outside these sub-regions. If these sub-regions are overlap, then the neurons of a ConvNet will produce spatially-correlated outcomes. But in other types of neural networks, the neurons do not share common connections which result into production of independent outcomes. More also, in a neural network with fully-connected layers, the number of parameters (weights) can increase very fast as the size of the input increases. A convolutional neural network will reduce the number of parameters with the reduced number of connections, shared weights, and downsampling.

A ConvNet consists of many layers, including convolutional layers, max-pooling or average-pooling layers, and fully connected layers. Each of these layers has a 3-D arrangement of neurons that convert a 3-D input to a 3-D output. For instance, the first layer, or input layer, stores the images as three-dimensional inputs, with the image's height, width, and color channels representing its dimensions. The areas of these images are connected to the neurons in the first convolutional layer, which converts them into a 3-D output. Feature extraction is the process by which the hidden units (neurons) in each layer discover nonlinear combinations of the original inputs [18]. The inputs for the subsequent layers are the learned features, or activations, from the previous layer, and the learned features become the inputs to the classifier at the end of the network.

A ConvNet's architecture can change based on the kinds and quantity of layers it has. The specific data or application determines the kinds and quantity of layers that are included. For example, if you have categorical responses, you must have a classification function and a classification layer, whereas if your response is continuous, you must have a regression layer at the end of the network. A convolutional network consisting of merely one or two layers may be all that is needed to learn a little amount of grayscale visual input. Millions of colorful images with more complex data necessitated a more intricate network with several convolutional and fully linked layers. The CNN architecture is made up of four basic parts that are arranged in numerous stages or blocks: a convolution layer, a non-linearity activation function, a pooling or subsampling layer, and a filter bank known as kernels, sometimes referred to as activations, come from one layer and serve as the subsequent layer's inputs. Ultimately, the classifier at the network's conclusion uses the learned characteristics as inputs.



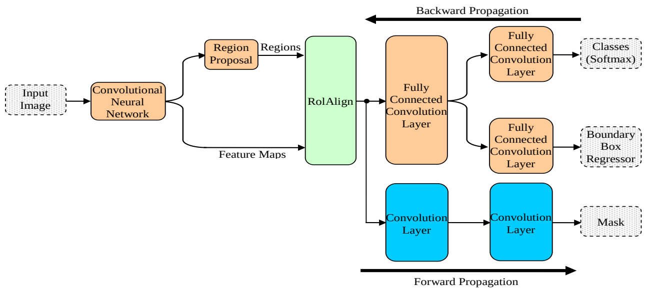
[Fig.1: Architecture of a Convolutional Neural Network] [18]

F. Region Based Convolutional Neural Network (RCNN)

The RCNN architecture is a widely embraced framework for conducting both semantic and instance segmentation tasks. Within this model, it performs dual tasks: predicting the bounding box locations for various objects in the image and generating masks for semantic segmentation. Figure 2 illustrates the fundamental structure of this architecture, and it can be readily extended to accommodate human pose estimation as well.

The core of this architecture initially involves the extraction of feature maps from an input image using a Convolutional Neural Network (CNN). These feature maps serve as input to a Region Proposal Network (RPN), responsible for proposing bounding box candidates to identify object presence. These bounding box candidates select regions from the CNN-derived feature map, potentially varying in size. To ensure uniformity, a layer called RoI Align is employed to resize the extracted features.

Subsequently, the extracted features are channeled into parallel branches of CNNs, where the final predictions for bounding boxes and segmentation masks are made. The objective of this detection algorithm is to train the model to precisely locate objects within the image.



[Fig.2: Block Diagram of RCNN] [3]

II. RELATED LITERATURE

Conducted a study that focused on developing a sticky bomb detection system [3]. They utilized a compass device and an Arduino board for this purpose, with the key approach involving the measurement of the magnetic field surrounding a targeted vehicle using the compass device. If a difference is detected with any of the coordinates, an alert message is sent to the car's owner for safety purposes [2]. investigated variables that can be used to identify terrorists, particularly in a crowded area. This was accomplished by creating a model for identifying suicide bombers [7]. used a metaheuristic approach for the development of suicide bomber detection. The goal of this author was to increase the rate of detecting suicide bombers attacks in order to reduce casualties. According to [3], the emphasis in the process of weapon detection should not be placed on where the features are located in the image but rather on how to detect them regardless of their position in the given images [14]. evaluated intelligent explosive detection using wireless sensor networks and the Internet of Things (IoT).

This work concentrated on the major threat to people posed by explosives placed in public areas such as parks, railway stations, and airports [13]. created a model that can increase the likelihood of identifying a suicide bomber at a checkpoint or marketplace with a sufficient standoff distance. Each sensor technology was used by the researcher, and it was analyzed using a simulation model that provided both the probability of detecting a bomber and the probability of a false detection [4]. introduced an innovative Automatic Hybrid Approach designed for the detection of concealed weapons through the application of deep learning techniques. In this approach, a conventional discrete wavelet transform was combined with a hybrid bag-of-words method to generate a fused image representation.

Convolutional Neural Network (CNN), along with a pre-trained CNN model. This CNN model utilized the features extracted from the fused image to train a multiclass Support Vector Machine (SVM) classifier. It's important to note that this approach demonstrated its effectiveness, particularly when applied to X-ray images. But X-ray is dangerous to the body system [19]. The study employed a Convolutional Neural Network (CNN) for the purpose of detecting humans in nighttime images captured by visible light camera sensors [20]. The primary objective was to identify humans in diverse environments, relying on the capabilities of a convolutional neural network [21].

This research explored a technique for detecting humans within individual nighttime images acquired through a visible light camera, employing a CNN as the underlying method [22]. The study further assessed and compared the performance and accuracy achieved when using both the original images and images enhanced as input data for the CNN [15]. worked on Efficient Convolutional Network for human pose estimation [23]. He designed an efficient network architecture for human pose estimation that exploits a current design choice for network architectures with a low memory footprint and trained it using best-practice ingredients for efficient learning [24]. His aim was to learn features in different layers at multiple scales [6]. Created a street object detection algorithm based on Convolution Neural Networks using a generic model detection algorithm (CNN). The process of fine-tuning pre-trained models involved utilizing transfer learning, which entails adapting a generic deep learning model to a specific one with distinct weights and output configurations. This adaptation was performed using COCO's image task datasets.

developed Hawk-Eye surveillance systems that can detect people who pose a potential security threat to the public in real time [1]. From the reviewed literature, many researchers have worked on weapon detection, but there are still some gaps that need to be filled since the use of weapons to cause harm has not ceased in our communities, and none of the researchers cited worked on weapon detection using IoT sensor-based Convolutional Neural Networks; hence this study.

III. SYSTEM DESIGN

The researchers choose a bottom-up grouping because it is a well-liked segmentation method for the selective search. This method allows for continuous grouping until the entire image becomes a single region, naturally generating locations at all scales. Region-based characteristics were utilized because they can produce more detailed information than pixels. We employed the quick technique of [10], which proved to be well suited for this purpose. The iteration began with the creation of the initial regions, which were then grouped together using a greedy algorithm:

The system considered four different measures (color, texture, size, and fitness). The system will verify whether the object fulfills the color condition. The system will examine the texture of the object; if it matches, it will merge objects of the same size, recognize them as a single object, and also evaluate the object's fitness. When all these conditions are satisfied, the system binds the objects for classification. At the first stage, an initial iteration was performed on the input image when the initial value was 227 x 227 x 3 using equation (1).

$$T_n = \frac{n-f}{s} + 1 * \frac{n-f}{s} + 1 \quad \dots \quad (1)$$

Where n stands for Image size, f denotes Filter and s stands for Stride.

The input of the CNN is an ImageT.

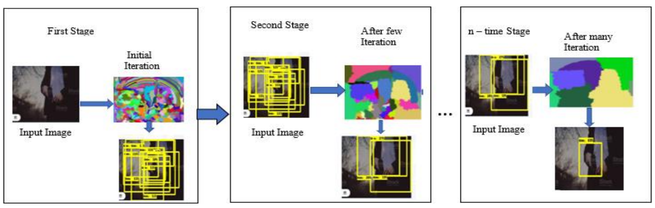
The filter is represented by equation (2)

$$T_j^l = A.F\left(\sum T^{l-1} * W_j^l + b_j^l\right) \quad \dots \quad (2)$$

The bounding boxes generated were numerous, which led to the second stage of the iteration. At the second iteration, the output from the first iteration becomes the values for the second iteration, and this was achieved using equation 3.

$$T_{n-1} = \frac{n+2p-f}{s} + 1 * \frac{n+2p-f}{s} + 1 \quad \dots \quad (3)$$

In this case, we have reduced the image size from (227 x 227) to (55 x 55); p represents padding, f represents filter, and s represents stride. The output from here will be an input to the next iteration. This process continues till the output becomes flattened to a one-dimensional metric in the fully connected layers that determine the presence of the object in the image. This is shown in Figure 3.



[Fig.3: Region of Interest Generation]

A. Materials and Method

There was no standard dataset for weapon detection on the internet for this study. Using this approach, a total

Retrieval Number:100.1/ijcns.B143004021124
DOI: 10.54105/ijcns.B1430.04021124
Journal Website: www.ijcns.latticescipub.com

Published By:
Lattice Science Publication (LSP)

of 500 weapon images were gathered by sourcing them from the internet. A selection of these samples is displayed in Figure 4. Subsequently, these images were resized to ensure optimal shapes and angles, a crucial step aimed at enhancing the accuracy of the model under development. Once individual images were prepared for each weapon class, they were then compiled into a dataset. These dataset images were transformed into a grayscale format with dimensions of 224 × 224 x 3 pixels, leveraging the Python programming language for this conversion process. The aim of the study is to propose a model that can provide highest accuracy, sensitivity, and specificity rates using Convolutional Neural Network.

To evaluate and contrast the classification performance of the models, metrics derived from the confusion matrix were employed. This matrix provides insights into sensitivity, specificity, precision, F1 score, and accuracy. Essentially, a confusion matrix is a tabular representation that records the count of both accurate and inaccurate predictions made by a classification model across a specified dataset. The case here is that either the model predicts the object correctly or incorrectly. Therefore, the classification problem can be classified as either positive or negative. True positives (TP) denote the instances where the model accurately predicted weapons correctly. Conversely, true negatives (TN) refer to the cases where the model correctly identified non-weapons or nuisances. False Positives (FP) is the number of cases that are incorrectly predicted weapon instances are referred to as true positives (TP). False negatives (FN) represent cases that were incorrectly identified as non-weapons or nuisances. To assess the performance of each algorithm, we summarize the results using a 2x2 confusion matrix that displays TP, TN, FP, and FN values. Each row of this matrix corresponds to an actual class, while each column relates to the model's predictions.

Sensitivity, a crucial measure, is the ratio of true positives to the sum of all positive assessments and is defined mathematically as:

$$Sensitivity = TP/(TP + FN) \quad \ldots \quad (4)$$

Specificity, another essential metric, represents the ratio of true negatives to the total number of negative assessments and is expressed as:

$$Specificity = TN/(TN + FP) \quad \ldots \quad (5)$$

The false positive rate (FPR) quantifies the proportion of false positives among all negative assessments, indicating the percentage of incorrectly labeled cases:

$$FPR = FP/(FP + TN) \quad \ldots \quad (6)$$

Accuracy, a measure of overall classification performance, is computed as the ratio of the total number of correct assessments to the total number of assessments, represented by:

$$Accuracy = (TP + TN)/(TP + TN + FP + FN \quad \ldots \quad (7)$$

Precision, also known as positive predictive value (PPV), calculates the proportion of true positives among positive predictions and is defined as:

$$Precision = TP/(TP + FP) \quad \ldots \quad (8)$$

The F1 score, or F measure, is an informative metric that takes into account both precision and recall values. It is a weighted average of these two metrics and can be defined as:

$$F1\ score = 2 * Precision * Recall Precision + Recall = TP/(TP + (FP + FN)/2) \quad \ldots \quad (9)$$

IV. RESULTS AND DISCUSSION

In this scenario, we employed the "Image Block" as the feature data (denoted as 'x') and the "Category Block" as the labels. To obtain the file paths of the images for 'x,' we utilized the "get_image_files" function from the fastai library. For labeling, we made use of the "parent_label" method to extract folder names. Figure 4 is the sample of the image downloaded for the study.

[Fig.4: Samples of the Downloaded Images]

To split the dataset into training and validation sets, the Random Splitter method was employed, and the images were resized to dimensions of 224x224x3 using "Random Resized Crop" with data augmentation techniques: the "aug_transforms()" function. Three existing models—ResNet-50, VGG-16, and AlexNet—were used to train the datasets in order to know which one will perform better. The results obtained for the models are shown in tables 1-3.

Table 1: Results Obtained for ResNet50 Model

Training	Train_loss	Accuracy	Roc_auc_score	f1_Score	Precision	Recall
Epoch 1	1.667144	0.721674	0.989986	0.10552	0.761953	0.721674
Epoch 2	0.827101	0.858704	0.996842	0.855396	0.874127	0.858704
Epoch 3	0.687501	0.865369	0.997437	0.862483	0.883647	0.865369
Epoch 4	0.294303	0.909624	0.998765	0.90745	0.916939	0.909624

Table 2: Results Obtained for VGG16 Model

Training	Train_loss	Accuracy	Roc_auc_score	f1	Precision	Recall
Epoch 1	1.456702	0.808851	0.993367	0.793508	0.83082	0.808851
Epoch 2	1.110005	0.822981	0.99409	0.806643	0.840556	0.822987
Epoch 3	0.866093	0.878699	0.996459	0.874678	0.88993	0.878699

Table 3: Results Obtained when Trained with Alexnet Model

Training	Train_loss	Accuracy	Roc_auc_score	f1	Precision	Recall
Epoch 1	1.655381	0.744335	0.986647	0.730747	0.75275	0.744335
Epoch 2	1.273647	0.773927	0.989283	0.766566	0.791419	0.773927
Epoch 3	1.105416	0.804319	0.992056	0.796196	0.812431	0.804319

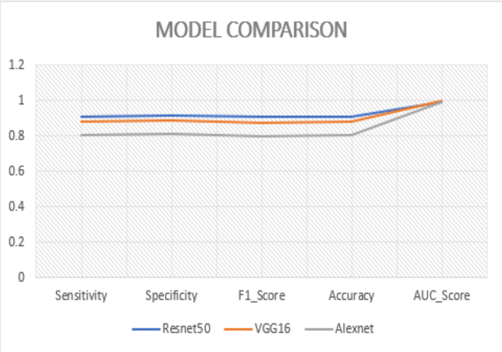
Retrieval Number:100.1/ijcns.B143004021124
DOI: 10.54105/ijcns.B1430.04021124
Journal Website: www.ijcns.latticescipub.com

Published By:
Lattice Science Publication (LSP)

Table 4 provides a comparison of the models based on the average values of sensitivity, specificity, F1 score, accuracy, and the area under the receiver operating characteristic curve (AUC). The experimental results reveal that the ResNet50 model outperformed other models in terms of sensitivity, specificity, F1 score, accuracy, and AUC values. Further details and a visual representation of these findings are illustrated in Figure 5.

Table 4: Comparison for the three Models

Models	Sensitivity	Specificity	F1_Score	Accuracy	AUC_Score
Resnet50	0.909624	0.916939	0.90745	0.909624	0.992056
VGG16	0.878693	0.88993	0.874678	0.878699	0.996459
Alexnet	0.804319	0.812431	0.796196	0.804319	0.992056



[Fig.5: The Models Comparison]

V. CONCLUSION

In this study we explored transfer learning because of the limited datasets we have and also to save the training time. Three feature extractors were used for the training; it was observed that ResNet50 performed better in terms of accuracy, sensitivity, and specificity than the VGG16 and AlexNet models. Therefore, ResNet50 can be recommended for use in detecting weapons when harmonized with other sensors to curb insecurity in our society; it works well in respect to the datasets available for the training.

ACKNOWLEDGEMENT

We show our hearts of gratitude to everyone that has contributed to the success of this research, most especially to the authors cited.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been sponsored or funded by any organization or agency. The independence of this research is a crucial factor in affirming its impartiality, as it has been conducted without any external sway.
- **Ethical Approval and Consent to Participate:** The data provided in this article is exempt from the requirement for ethical approval or participant consent.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Authors Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. Abdelmoamen, A., Member, A., & Echi, M. (2021). Hawk-Eye : An AI-Powered Threat Detector for Intelligent Surveillance Cameras. 1–12. DOI: https://doi.org/10.1109/ACCESS.2021.3074319
2. Adewumi, M. G., Adewale, O. S., Akinwumi, A. O., & Ajisola, K. T. (2022). Security Intelligence Framework for Suicide Bombers Identification in a Crowd. International Journal of Academic Research in Business and Social Sciences, 12(4), 697–706. DOI: https://doi.org/10.6007/ijarbss/v12-i4/13124
3. Albawi, S., & Mohammed, T. A. (2017). Understanding of a Convolutional Neural Network. April 2018. DOI: https://doi.org/10.1109/ICEngTechnol.2017.8308186
4. Al-shoukry, S. (2017). An Automatic Hybrid Approach to Detect Concealed objects. 12(16); 4736–4741. DOI: http://www.arpnjournals.org/jeas/research_papers/rp_2017/jeas_0817_6268.pdf
5. Bengio, Y., Lamblin, P., Popovici, D., and Larochelle, H., (2007). Greedy layer-wise training of deep Networks. In Neural Information Processing Systems. https://ieeexplore.ieee.org/document/6287632
6. Cai, W., Li, J., Xie, Z., Zhao, T., & Lu, K. (2018). Street object detection based on faster R-CNN. Chinese Control Conference, CCC, 2018-July (July 2018), 9500–9503. DOI: https://doi.org/10.23919/ChiCC.2018.8482613
7. Cotta, C. (2019). Metaheuristic approaches to the placement of suicide bomber detectors Metaheuristic Approaches to the Placement of Suicide Bomber Detectors. May 2018. DOI: https://doi.org/10.1007/s10732-017-9335-z
8. Dores, C., Reis, L., & Lopes, N. (2014). Internet of things and cloud computing. Information Systems and…, 6(2), 1–8. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6877071
9. Ezeah, E. C. I. and PC. (2015). Boko Haram Insurgency in Nigeria: A Public Perception Approach. Mgbakoigba, Journal of African Studies. 5(1); 1-16. https://www.researchgate.net/publication/337146610.
10. Felzenszwalb, P. F., and Huttenlocher, D. P. (2004). Efficient Graph-Based Image Segmentation. International Journal of Computer Vision, 59(2); 167–181. DOI: https://doi.org/10.1023/B:VISI.0000022288.19776.77
11. Ifeanyichukwu, F. (2019). Cultural Negligence as Key Cause of Terrorism in Nigeria: A Study. 9, 1–12. https://internationalpolicybrief.org/wp-content/uploads/2023/10/ARTICLE1-95.pdf
12. Meng, Z., Zhang, M. and Wang, H., (2020). CNN with pose segmentation for suspicious object detection in MMW security images. Sensor, 20, 4974, pp. 1 – 15. https://www.mdpi.com/1424-8220/20/17/4974
13. Minukas, J. B. M. (2010). Developing an Operational and Tactical Technologies to Produce the Highest Probability Methodology for Incorporating Existing of Detecting an Individual wearing an IED. https://core.ac.uk/download/pdf/36699007.pdf
14. Nalajala, P., Kumar, D. H, Harshavardhan, V. and Madhavi, G. (2016). Intelligent Detection of explosives using Wireless Sensor Network and Internet of Things (IOT), vol. 9, no. 42, pp. 391–397. https://serialsjournals.com/abstract/20865_cha-43.pdf
15. Rafi, U. (2016). An Efficient Convolutional Network for Human Pose Estimation. IEEE Journal of Computer Society, 10(6); 1002-1034.

https://www.vision.rwth-aachen.de/media/papers/rafibmvc16.pdf

16. Saghiri, M. A., Lotfi, M., & Aghili, H. (2014). United States Patent U S. Patent. United States Patent US, 2(12), 0–10. http://www.google.ch/patents/US8 68770
17. Silas, A. (2013). The Effects of Boko Haram Insurgency and the School System ; A Case Study of Selected States in Northern Nigeria. DOI: https://doi.org/10.7237/sjsa/137
18. Srivastava, N., G. Hinton, A. Krizhevsky, I. Sutskever, R. Salakhutdinov.(2014). Dropout: A Simple Way to Prevent Neural Networks from Over fitting. Journal of Machine Learning Research. Vol. 15, pp. 1929-1958. https://jmlr.org/papers/volume15/srivastava14a/srivastava14a.pdf
19. Yang, J., and Yang, G. (2018). Modified convolutional neural network based on dropout and the stochastic gradient descent optimizer. Algorithms, 11(3); 1–15. DOI: https://doi.org/10.3390/a11030028
20. Das, S., S, S., M, A., & Jayaram, S. (2021). Deep Learning Convolutional Neural Network for Defect Identification and Classification in Woven Fabric. In Indian Journal of Artificial Intelligence and Neural Networking (Vol. 1, Issue 2, pp. 9–13). DOI: DOI: https://doi.org/10.54105/ijainn.b1011.041221
21. Jasmine, R. R., & Thyagharajan, K. K. (2019). Hand-Held Object with Action Recognition Based On Convolutional Neural Network in Spatio Temporal Domain. In International Journal of Engineering and Advanced Technology (Vol. 9, Issue 2, pp. 4968–4975). DOI: https://doi.org/10.35940/ijeat.a1901.129219
22. Cibi, Ms. A., & Rose, Dr. R. J. (2020). Convolutional Neural Network for Automated Analyzing of Medical Images. In International Journal of Innovative Technology and Exploring Engineering (Vol. 9, Issue 7, pp. 687–691). DOI: https://doi.org/10.35940/ijitee.g5629.059720
23. Morsy, H. A. M. (2023). Optimization Methods for Convolutional Neural Networks – The LeNet-5 Algorithm. In International Journal of Recent Technology and Engineering (IJRTE) (Vol. 11, Issue 5, pp. 1–4). DOI: https://doi.org/10.35940/ijrte.e7355.0111523
24. Raj, H., Duggal., A., M., A. K. S., Uppara, S., & S., S. M. (2020). Hand Motion Analysis using CNN. In International Journal of Soft Computing and Engineering (Vol. 9, Issue 6, pp. 26–30). DOI: https://doi.org/10.35940/ijsce.f3409.059620

AUTHORS PROFILE

Moradeke Grace Adewumi, holds a PhD in Computer Science. Her areas of interest are Computer Vision and Information Security. She's thorough, intelligent, trustworthy, and dependable. She has published several articles both locally and internationally. She has a passion for research. She is a member of the Nigerian Computer Society (NCS) and a member of Organization of Women in Science for the Developed World (MOWSD).

Mughele, Ese Sophia, is the Pioneer Ag. Head of Department Cyber Security, Faculty of Computing, University of Delta, Agbor, Delta State, Nigeria. She had PhD degree in Computer Science, majoring in Machine Learning and Soft Computing. She is a member of the Computer Professionals Registration Council of Nigeria (CPN), the Nigerian Computer Society (NCS), and Nigeria Women in Information Technology (NIWIIT). Mughele has over 50 peer-reviewed, referenced publications, both national and international, to her credit.

Akinribido Comfort Tomiye, is currently in the department of Computer Science. She is resourceful, effficient and effective. She has also attended several conferences. Her research interest is in Cryptography, Steganography, Biometrics, Artificial Intelligent, Information Systems and Information Storage and Retrieval.

Rowland Ogunrinde is a passionate researcher who holds a bachelor's degree in business information systems from the University of East London (UEL), graduating top of his class in 2012 with a first-class degree with honors. He obtained a doctorate degree in Information Systems from the Universiti Putra Malaysia (UPM) in 2019. He lectured both in public and private Nigerian universities. He has published several articles both locally and internationally. His research interests include cloud computing, enterprise applications, and small and medium enterprises (SMEs).

Olumide Sunday Adewale is a Professor of Computer Science with a specialization in Computer Networking and Computer Security. He had held several positions, such as head of a department, dean of faculty, and director in different capacities at the Federal University of Technology, Akure, Nigeria. He is a public figure with a reputation. He has several publications, both nationally and internationally, to his credit.

Stella Chinye Chiemeke is Professor of Computer Science. She's currently the Vice Chancellor of the University of Delta, Delta State, Nigeria. She bagged her PhD in Computer Science from the Federal University of Technology, Akure in 2004. In the year 1986, she began a career as a programmer and rose to the rank of Professor in 2009 to become the second female Professor of Computer Science in Nigeria. She belongs to various professional bodies both in Nigeria and abroad. Stella specializes in Software Engineering, Digital Forensics, ICT Management, Information Systems Security, Computer Security and Reliability.